Diskrete Strukturen, SS 1996

Adalbert Kerber

2. Dezember 1996

Inhaltsverzeichnis

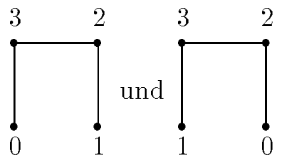
Vorwort

Dieses Manuskript ist als Einführung in die *konstruktive Theorie endlicher Diskreter Strukturen* und deren Anwendungen gedacht. Es gibt ziemlich genau eine vierstündige Vorlesung „Diskrete Strukturen" — mit zweistündigen Übungen — wieder, die ich im Sommersemester 1996 in Bayreuth gehalten habe.
Für weitere Einzelheiten sei auf die angegebene Literatur verwiesen, insbesondere auf [5].

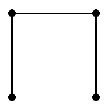
Bayreuth, den 2. Dezember 1996 — A. Kerber

Einleitung

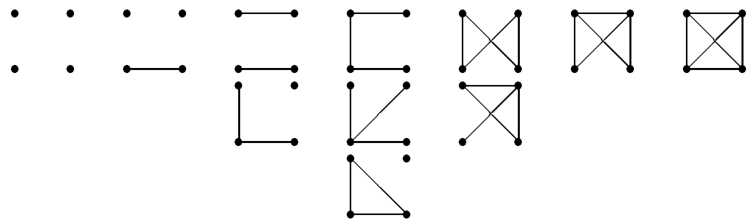
Bekannte Beispiele Diskreter Strukturen sind Graphen, Lineare Codes, molekulare Graphen, Designs usw. Allgemeiner verstehen wir unter einer endlichen Diskreten Struktur eine endliche Menge zusammen mit inneren und äußeren Verknüpfungen und Relationen.
Zu deren Beschreibung und Untersuchung gehen wir entsprechend schrittweise vor. Zunächst betrachten wir gewisse Diskrete Strukturen, die aus Mengen mit einer einzigen Relation bestehen. Bekannte Beispiele sind die bereits erwähnten Graphen, die aus Punkten und Kanten bestehen, wobei die Relation durch Umnumerieren der Punkte definiert ist: Graphen (genauer: *numerierte* Graphen), die auseinander durch Umnumerieren der Punkte entstehen, werden als im wesentlichen gleich angesehen, hier sind zwei Beispiele:



Jede dieser Äquivalenzklassen numerierter Graphen definiert einen *unnumerierten* Graphen. Hier ist eine Skizze des unnumerierten Graphen, der auf diese Weise als Äquivalenzklasse der beiden oben skizzierten numerierten Graphen definiert ist:

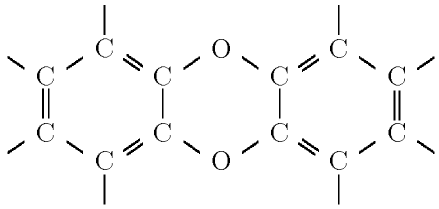


Solche unnumerierten Graphen sind besonders wichtig, denn man ist an Graphen als *Wechselwirkungsmodellen* interessiert, Graphen sind nämlich Inzidenzstrukturen, bei denen die Nummern der Punkte keine wesentliche Rolle spielen. Nachstehend sind als ein Beispiel die sämtlichen unnumerierten Graphen mit vier Punkten skizziert:



Wir werden einige effiziente Verfahren diskutieren, endliche Diskrete Strukturen zu konstruieren. Es gibt nämlich viele Anwendungen, wo man endliche Diskrete Strukturen wirklich *vor sich sehen muß (auf dem Bildschirm oder auf Papier).* Ein prominentes Beispiel ist die *Molekulare Strukturerkennung.* Dort geht es um die Zuordnung eines Moleküls — genauer: eines mathematischen Modells eines Moleküls — zu einem vorgegebenen Satz von Daten. In der Regel ist das Modell ein sogenannter molekularer Graph, beispielsweise der Benzolring. (Ein molekularer Graph ist ein sogenannter zusammenhängender Multigraph ("Multi-" wegen der eventuell auftretenden Mehrfachkanten, beispielsweise der Doppelkanten im Benzolring), dessen Punkt zusätzlich noch mit Atomnamen versehen sind. Solche Diskreten Strukturen sind also schon erheblich komplizierter als die oben erwähnten sogenannten schlichten Graphen.

Die Aufgabe der Mathematik innerhalb der Molekularen Strukturerkennung besteht dabei in der schnellen und redundanzfreien Bereitstellung aller molekularen Graphen, die zu dem vorgegebenen Datensatz passen. Besteht der Datensatz zum Beispiel nur aus der Summenformel C_6H_6 des Benzols, dann sind hierzu insgesamt 217 molekulare Graphen zu konstruieren, bei $C_8H_{16}O_2$ sind dies schon 13 190 Graphen, das Konstruktionsproblem wird also sehr schnell sehr umfangreich. Die Lösungsgesamtheit kann aber durch Nebenbedingungen klein gehalten werden, es geht insgesamt also um ein *Konstruktionsproblem mit Nebenbedingungen.* Ein bekanntes Beispiel bilden die Isomere des Dioxins, das sind die Moleküle mit der chemischen Formel $C_{12}O_2H_4Cl_4$, die die folgende Substruktur besitzen:



Wir werden zeigen, daß und auch warum es genau 22 solcher Isomere gibt, der Ausdruck des Ergebnisses eines entsprechenden Computerprogramms namens MOLGEN ist weiter unten abgebildet.
Zum Zweck der Entwicklung allgemeinerer Konstruktionsmethoden für solche Diskreten Strukturen werden wir geeignete algebraisch–kombinatorische Methoden bereitstellen, denen die Verwendung von Operationen endlicher Gruppen auf endlichen Mengen zugrundeliegt. Standardbeispiele für Anwendungen sind die schon erwähnten Graphen und die molekularen Graphen, aber auch Schaltfunktionen, Lineare Codes und physikalische Zustände. Danach machen wir zusätzliche Annahmen wie etwa die, daß die Menge auch noch angeordnet sei. Bei anderen wichtigen Anwendungsbeispielen sind die Mengen, auf denen Gruppen operieren, Vektorräume über endlichen Körpern. Sie spielen — als fehlerkorrigierende Lineare Codes — eine bedeutende Rolle. Auch hier sind diese Strukturen mit Hilfe einer Relation zu klassifizieren, nämlich nach der Güte ihrer Codierungs- und Decodierungseigenschaften, die mit Hilfe einer Metrik, der Hamming–Metrik, definiert werden. Hier braucht man aber nicht alle Codes, sondern nur die besten. Es handelt sich also auch hier um eine Konstruktion mit Nebenbedingungen.
Diesen *konstruktiven Aspekt* berücksichtigt man zweckmäßigerweise bereits beim *Definieren* der jeweiligen Diskreten Struktur, und wegen der meist sehr hohen Komplexität bzw. Vielfalt der auftretenden Strukturen geht man in mehreren Schritten vor: Zwischen Definition und Konstruktion, d.h. Angabe einer vollständigen Liste der Strukturen mit vorgegebenen Parametern (wie z.B. Graphen mit vorgegebener Anzahl von Punkten), lassen sich oft *Anzahlen* angeben (z.B. gibt es, wie oben bereits gesehen, genau 11 Graphen mit 4 Punkten), und diese lassen sich meist noch verfeinern zu erzeugenden Funktionen (z.B. ist $1+x+2x^2+3x^3+2x^4+x^5+x^6$ die erzeugende Funktion

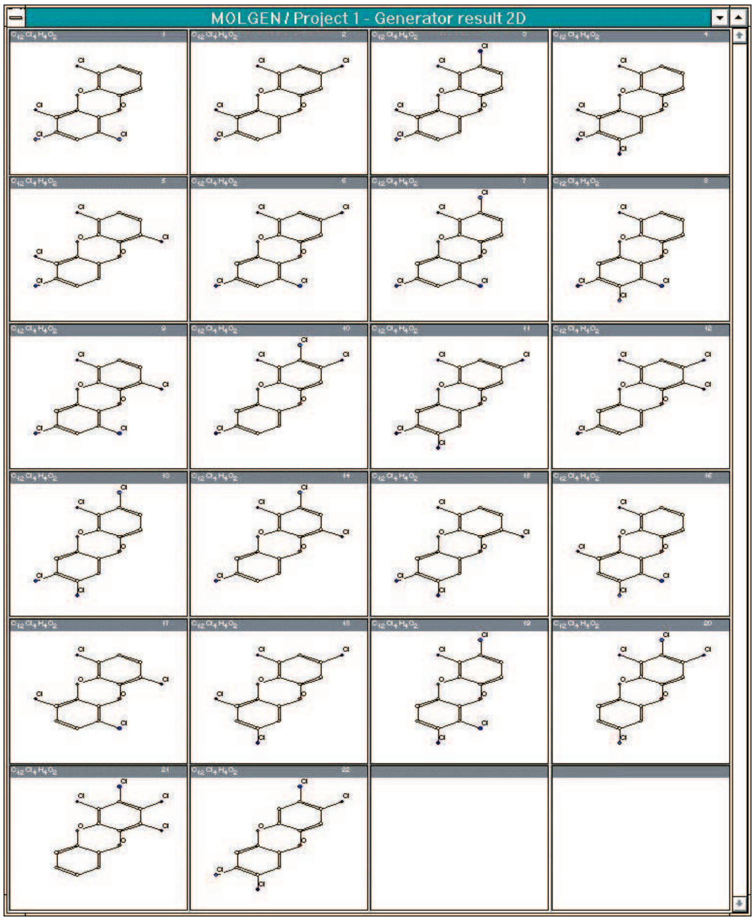


Abbildung 0.1: Die 22 Isomere des Dioxin

für die Anzahl von Graphen mit 4 Punkten nach Kantenzahl, d.h. es gibt beispielsweise genau 3 Graphen mit 4 Punkten und 3 Kanten). Man kann auch die Anzahl der Graphen mit p Punkten ermitteln, die eine vorgegebene Symmmetriegruppe haben. Unter anderem werden wir zeigen können, daß es keinen Graphen mit p Punkten gibt, der die alternierende Gruppe auf den Punkten als Symmetriegruppe hat. Diese Anzahlen sind natürlich schon an und für sich interessant, sie dienen aber auch wichtigen "höheren Zwecken", beispielsweise als *Abbruchregeln* bei der Konstruktion, oder auch bei der Ermittlung gewisser *Wahrscheinlichkeiten* bei der gleichverteilten Zufallserzeugung der betreffenden Strukturen. In vielen Fällen ist nämlich die Gesamtanzahl so übermäßig groß, daß man selbst mit sehr leistungsfähigen Rechnern keine vollständige Liste erzeugen kann. Will man dennoch Aussagen machen, beispielsweise Hypothesen überprüfen, dann bleibt hier nur stichprobenweises Vorgehen übrig, also die gleichverteilte Zufallserzeugung. Auch diese werden wir diskutieren, und es wird sich zeigen, daß auch hierfür der Ansatz zweckmäßig ist, endliche Diskrete Strukturen als Bahnen endlicher Gruppen auf endlichen Mengen zu definieren, wo immer dies möglich ist.

Die entsprechenden Anzahlangaben erhält man mit Hilfe des Lemmas von Cauchy–Frobenius und seinen Verfeinerungen (gewichtete Form, Lemma von Burnside etc.). Je weiter man diese Methoden verfeinert, um so schwieriger wird ihre Anwendung. Beispielsweise braucht man für die Abzählung nach Automorphismengruppe die sogenannte Markentafel der betreffenden Gruppe, d.h. man muß sehr viel über deren Untergruppenverband wissen. Glücklicherweise existieren mittlerweile sehr effiziente Computeralgebrasysteme, wie z.B. MOLGEN, SYMMETRICA oder DISCRETA, die hier in Bayreuth entwickelt wurden und ständig weiter ausgebaut werden, mit deren Hilfe man viele nichttriviale Fälle beherrschen kann.

Kapitel 1

Spezies von Strukturen

In diesem ersten Kapitel werden Spezies von Strukturen eingeführt. Hierbei handelt es sich um endliche Mengen $\mathcal{S}[M]$ die aus einer vorgegebenen Menge M dadurch entstehen, daß man alle Strukturen einer vorgegebenen Art, also z.B. aller Graphen bildet, die M als Punktemenge haben. Die Einführung dieses Begriffs erweist sich als sehr nützlich, sobald Verknüpfungen solcher Spezies eingeführt sind, z.B. eine Addition, eine Multiplikation, eine Substitution, eine Punktierung, eine Ableitung usw. Es zeigt sich nämlich dann, daß viele Strukturen durch Verknüpfung aus anderen Strukturen zusammengesetzt werden können, z.B. lassen sich Graphen aus zusammenhängenden Graphen zusammensetzen, Permutationen aus zyklischen Permutationen etc. Diesen Verknüpfungen zwischen Strukturen werden wir deshalb besondere Aufmerksamkeit widmen und zeigen, wie man die Zusammensetzung von Strukturen verwenden kann, um Strukturen abzuzählen und zu erzeugen.
Solche Spezies von Strukturen sind aber noch nicht genau das, was wir eigentlich wollen, denn es handelt sich hierbei zunächst um sog. numerierte Strukturen. Um zu unnumerierten Strukturen zu kommen, werden wir deshalb später den Begriff des Typs einer Struktur einführen.

1.1 Spezies von Strukturen

Unter einer $\mathcal{S}$-*Struktur* wollen wir ein Paar (σ, M) verstehen, wobei M eine Menge und σ eine durch die Struktur $\mathcal{S}$ vorbestimmte Konstruktion auf M ist, zum Beispiel die Konstruktion eines Graphen mit M als Punktemenge. M nennen wir dabei die *Grundmenge* der betreffenden Struktur, und die Menge aller (σ, M), die auf diese Weise entstehen, bezeichnen wir, wenn wir die Konstruktion nicht näher spezifizieren wollen, mit

$$\mathcal{S}[M].$$

Oft werden wir einfachheitshalber σ anstelle von (σ, M) schreiben, und wir werden σ eine $\mathcal{S}$–Struktur *auf* M nennen. Spezielle Strukturen erhalten suggestivere Bezeichnungen, so werden wir beispielsweise die folgenden Namen verwenden:

1.1.1 Spezielle Strukturen und ihre Bezeichnungen:

- $\mathcal{G}[M]$:= *die Graphen auf* M *(genauer: schlichte Graphen, d.h. es sind weder Doppelkanten noch Schleifen zugelassen),*
- $\mathcal{G}^z[M]$:= *die zusammenhängenden Graphen,*
- $\mathcal{G}^o[M]$:= *die orientierten Graphen (jede Kante ist gerichtet, aber parallele Kanten sind nicht zugelassen, ebensowenig Schleifen),*
- $\mathcal{B}[M]$:= *die Bäume, also die zyklenfreien Graphen,*
- $\mathcal{W}[M]$:= *die Wurzelbäume, das sind die Bäume, bei denen ein Punkt hervorgehoben ist,*
- $\mathcal{P}[M]$:= *die Potenzmenge von* M*,*
- $\mathcal{P}^{[k]}[M]$:= *die Menge aller Teilmengen der Ordnung* k *von* M*,*
- $Par[M]$:= *die Mengenpartitionen von* M*,*
- $Per[M]$:= *die Permutationen auf* M*,*
- $\mathcal{C}[M]$:= *die gerichteten Zyklen auf* M*,*
- $\mathcal{L}[M]$:= *die linearen Ordnungen auf* M*,*
- $End[M]$:= *die Endofunktionen auf* M*.*

$\diamond$

Man kann diese Mengen von Strukturen natürlich auch rein mengentheoretisch beschreiben, z.B. ist

$$End[M] = M^M := \{f \mid f\colon M \to M\}.$$

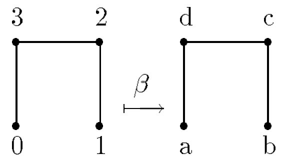
Weil ein Graph aus Punkten und Kanten besteht, und die Kanten als Zweiermengen der Punktemenge aufgefaßt werden können, erhalten wir mit Hilfe von

$$\mathcal{P}^{[2]}[M] = \{M' \subseteq M \mid |M'| = 2\}$$

die ausführlichere Version

$$\mathcal{G}[M] = \{(\gamma, M) \mid \gamma \subseteq \mathcal{P}^{[2]}[M]\}.$$

Ein Beispiel für eine solche Struktur ist also ein Graph $(\gamma, M) \in \mathcal{G}[M]$ mit M als Menge seiner Punkte. In der Einleitung sind zwei Graphen mit der Grundmenge $M = 4 := \{0, 1, 2, 3\}$ abgebildet. Solche mengentheoretischen Beschreibungen sind natürlich im allgemeinen nicht eindeutig, man kann beispielsweise Graphen auch als Abbildungen beschreiben (Übungsaufgabe 1.1.2).
Ein wesentliches Element der Speziestheorie ist der sogenannte *Transport* von Struktur mittels Bijektionen $\beta\colon M \to N$. Er bedeutet einfach ein *Umnumerieren* der Elemente der Grundmenge, gemäß der in Frage stehenden Struktur. Aus (σ, M) wird durch diesen Transport die Struktur $(\beta(\sigma), \beta(M)) =: (\tau, N)$. Hier ist ein Beispiel anhand von Graphen. Die Graphenstruktur wird von $M = \{0, 1, 2, 3\}$ auf $N := \{a, b, c, d\}$ mit Hilfe der Bijektion $\beta : 0 \mapsto a, 1 \mapsto b, 2 \mapsto c, 3 \mapsto d$ transportiert:



Der Transport der Graphenstruktur von der einen Menge auf die andere erfolgt offensichtlich durch einfaches Umnumerieren der Punkte mit Hilfe von β. Der Graph $(\gamma, M) \in \mathcal{G}[M]$ ergibt durch Anwendung von β den Graphen $(\beta(\gamma), N)$, wobei

$$\beta(\gamma) = \{\{\beta(m), \beta(m')\} \mid \{m, m'\} \in \gamma\}.$$

Etwas anders, aber ebenso leicht verständlich, funktioniert der Transport von Endofunktionen (ϵ, M) mit Hilfe von $\beta: M \to N$: Wir betrachten einfach den Funktionsgraphen $\{(m, \epsilon(m)) \mid m \in M\}$ von ϵ und wenden auf ihn den Transport längs β an:

$$\beta(\{(m, \epsilon(m)) \mid m \in M\}) = \{(\beta(m), \beta(\epsilon(m))) \mid m \in M\}$$

$$\{(\beta(m), \beta\epsilon\beta^{-1}(\beta(m))) \mid m \in M\} = \{(n, \beta\epsilon\beta^{-1}(n)) \mid n \in N\}.$$

Der Endofunktion ϵ von M ist demnach die Endofunktion $\beta(\epsilon) := \beta\epsilon\beta^{-1}$ zuzuordnen:

$$\beta(\epsilon) = \beta\epsilon\beta^{-1}.$$

Eine solche, von der jeweiligen Struktur abhängende, Vorschrift zum Umnumerieren bedarf also einer eigenen Bezeichnung, bei der der Name der jeweiligen Struktur (also die Konstruktionsvorschrift) ersichtlich wird. Wir wählen einfachheitshalber dieselbe Bezeichnung wie für die Struktur, nämlich

$$\mathcal{S}[\beta]: \mathcal{S}[M] \to \mathcal{S}[N], (\sigma, m) \mapsto (\mathcal{S}[\beta](\sigma), N).$$

Diese Abbildung $\mathcal{S}[\beta]$ heißt *Transport der $\mathcal{S}$–Struktur längs β*. Die Bildung der Strukturen und die Transportfähigkeit der Struktur von einer Menge M auf eine dazu bijektive Menge N fassen wir zusammen im Begriff *Spezies:*

1.1.2 Definition *Unter einer* Spezies *verstehen wir eine Regel $\mathcal{S}$, die*

- *jeder endlichen Menge M eine endliche Menge $\mathcal{S}[M]$, sowie*
- *jeder Bijektion $\beta: M \to N$ zwischen endlichen Mengen M und N eine Funktion $\mathcal{S}[\beta]: \mathcal{S}[M] \to \mathcal{S}[N]$ zuordnet, für welche gilt*

  $$\mathcal{S}[\alpha \circ \beta] = \mathcal{S}[\alpha] \circ \mathcal{S}[\beta], \ \mathcal{S}[\mathrm{id}_M] = \mathrm{id}_{\mathcal{S}[M]}.$$

  (Die Funktion $\mathcal{S}[\beta]$ ist natürlich eine Bijektion von $\mathcal{S}[M]$ auf $\mathcal{S}[N]$, vgl. Übungsaufgabe 1.1.1.)

$\diamond$

In der Sprache der Kategorien kann man das auch so formulieren: *Spezies sind covariante Funktoren von der Kategorie endlicher Mengen mit Bijektionen in die Kategorie der endlichen Mengen mit Funktionen.*

Wir wollen jetzt noch einige weitere Beispiele von Spezies einführen. Sie dienen unter anderem auch der Vorbereitung auf die Einführung von Verknüpfungen von Spezies und der Zerlegung von Spezies in einfachere (wie beispielsweise der Graphen in zusammenhängende Graphen und der Permutationen in Zyklen etc.).

1.1.3 Weitere Beispiele von Spezies

- $\mathcal{M}[M] := \{M\}$, *die Spezies* Menge, *sie ordnet M die einelementige Menge $\{M\}$ zu,*
- $\in[M] := M$, *die Spezies* Elemente, *sie ordnet M die Menge ihrer Elemente zu,*
- *Die Spezies* Singleton *sei:*

$$\mathcal{X}[M] := \begin{cases} \{M\} & \textit{falls } |M| = 1, \\ \emptyset & \textit{sonst.} \end{cases}$$

- *Die* Leere Spezies *ist definiert durch* $0[M] := \emptyset$.
- *Dagegen wird die Spezies* Leere Menge *so eingeführt:*

$$1[M] := \begin{cases} \{M\} & \textit{falls } M = \emptyset, \\ \emptyset & \textit{sonst.} \end{cases}$$

- *Schließlich heißt*

$$\mathcal{M}_k[M] := \begin{cases} \{M\} & \textit{falls } |M| = k, \\ \emptyset & \textit{sonst,} \end{cases}$$

  Spezies k-Menge.

(Die Bezeichnungen 0 für die leere Spezies und 1 für die Spezies Leere Menge werden klar, wenn wir die Addition und die Multiplikation von Spezies eingeführt haben, denn sie bilden diesbezüglich neutrale Elemente.)

◇

Da jede Bijektion $\beta: M \rightarrow N$ eine Bijektion $\mathcal{S}[\beta]$ von $\mathcal{S}[M]$ auf $\mathcal{S}[N]$ induziert, kommt es nicht auf die "Natur" der Elemente von M, sondern nur auf die Kardinalzahl dieser Menge an. Insbesondere hängt $|\mathcal{S}[M]|$ nur von $|M|$ ab. Wir nehmen uns deshalb, zu jeder natürlichen Zahl n, eine Standardmenge dieser Ordnung her, etwa $\underline{n} := \{1, \ldots, n\}$, und setzen

$$s_n := |\mathcal{S}[n]|.$$

1.1.4 Definition *Die erzeugende Funktion der s_n, also die formale Potenzreihe*

$$\mathcal{S}(x) := \sum_{n\geq 0} s_n \frac{x^n}{n!} \in \mathbb{Q}[x],$$

heißt auch die Kardinalitätenreihe *von $\mathcal{S}$.*

$\diamond$

Hier sind zunächst ein paar offensichtliche Spezialfälle:

1.1.5 Beispiele

- $\mathcal{L}(x) = 1 + x + x^2 + x^3 + \ldots = \frac{1}{1-x} = Per(x)$,
- $\mathcal{M}(x) = \sum \frac{x^n}{n!} = e^x$,
- $\in(x) = \sum n \cdot \frac{x^n}{n!} = x \cdot e^x$,
- $\mathcal{P}(x) = \sum 2^n \cdot \frac{x^n}{n!} = e^{2x}$,
- $\mathcal{X}(x) = x$,
- $1(x) = 1$,
- $0(x) = 0$.
- $\mathcal{G}(x) = \sum_{n>0} 2^{\binom{n}{2}} \cdot \frac{x^n}{n!}$,
- $End(x) = \sum n^{n\geq 0} \cdot \frac{x^n}{n!}$.

$\diamond$

Hierzu sollte noch angemerkt werden, daß wir, gemäß diesen erzeugenden Funktionen, die folgenden Mengen von Strukturen auf $\emptyset$ nicht leer sind:

$$\mathcal{L}[\emptyset] = \mathcal{M}[\emptyset] = \mathcal{P}[\emptyset] = 1[\emptyset] = End[\emptyset] = \{\emptyset\},$$

während

$$\in[\emptyset] = \mathcal{X}[\emptyset] = [\emptyset] = \mathcal{G}[\emptyset] = \emptyset.$$

Gelegentlich werden wir lange Erklärungen über die Anzahl der betreffenden Strukturen auf der Grundmenge $\emptyset$ umgehen wollen, was wir durch folgende Bezeichnung erleichtern können:

$$\mathcal{S}_+[M] := \begin{cases} \mathcal{S}[M], & \text{falls } M \neq \emptyset, \\ \emptyset, & \text{sonst.} \end{cases}$$

Zwei Spezies mit derselben Kardinalitätenreihen heißen *äquipotent.* Wir schreiben dafür — also für $\mathcal{S}(x) = \mathcal{T}(x)$:

$$\mathcal{S} \equiv \mathcal{T}.$$

Ein Beispiel ist offensichtlich

1.1.6 $$Per \equiv \mathcal{L}.$$

Eine strengere Bedingung an Spezies ist die *Isomorphie*, kurz

$$\mathcal{S} \simeq \mathcal{T},$$

bei der die Existenz kanonischer Bijektionen $\Theta_M \colon \mathcal{S}[M] \to \mathcal{T}[M]$ verlangt wird, so daß die folgenden Diagramme kommutativ sind, für alle endlichen Mengen M, N und alle Bijektionen $\beta \colon M \to N$:

$$\begin{tikzcd}
\mathcal{S}[M] \arrow[r, "\Theta_M"] \arrow[d, "\mathcal{S}[\beta]"'] & \mathcal{T}[M] \arrow[d, "\mathcal{T}[\beta]"] \\
\mathcal{S}[M] \arrow[r, "\Theta_N"] & \mathcal{T}[N]
\end{tikzcd}$$

Äquipotenz impliziert natürlich keineswegs Isomorphie, ein Standardbeispiel hierfür ist

1.1.7 Beispiel Wir wissen bereits von der Äquipotenz $Per \equiv \mathcal{L}$, und wir wollen jetzt zeigen, daß diese beiden Spezies, wie nicht anders zu erwarten, keineswegs isomorph sind. Isomorphie $Per \simeq \mathcal{L}$ ergäbe die Existenz von Bijektionen $\Theta_M \colon Per[M] \to \mathcal{L}[M]$ (wir haben $N := M$ gewählt!) mit

$$\mathcal{L}[\beta] \circ \Theta_M = \Theta_M \circ Per[\beta],$$

für jede Bijektion $\beta \colon M \to M$. Nehmen wir hierzu ein M mit $|M| > 1$, eine Bijektion $\beta \neq \mathrm{id}_M$ und $\pi := 1 \in Per[M]$. Weiter sei

$$(m_0 < \ldots < m_{|M|-1}) := \Theta_M(\pi).$$

Die Anwendung der linken Seite obiger Identität auf π ergibt

$$(\mathcal{L}[\beta] \circ \Theta_M)(\pi) = \mathcal{L}[\beta](m_0 < \ldots < m_{|M|-1})$$

$$= (\beta(m_0) < \ldots < \beta(m_{|M|-1})),$$

eine Anwendung der rechten Seite der Identität dagegen

$$(\Theta_M \circ Per[\beta])(\pi) = \Theta_M(\beta \circ \pi \circ \beta^{-1}) = \Theta_M(1)$$

$$= (m_0 < \ldots < m_{|M|-1}) \neq (\beta(m_0) < \ldots < \beta(m_{|M|-1})).$$

$\diamond$

Äquipotenz impliziert also keineswegs Isomorphie:

1.1.8 $$\mathcal{S} \equiv \mathcal{T} \not\Rightarrow \mathcal{S} \simeq \mathcal{T}.$$

Anstelle von $\mathcal{S} \simeq \mathcal{T}$ werden wir oft auch einfachheitshalber

$$\mathcal{S} = \mathcal{T}$$

schreiben!

Übungsaufgaben

Ü 1.1.1 Zeigen Sie, daß $\mathcal{S}[\beta]$ tatsächlich eine Bijektion ist.

Ü 1.1.2 Beschreiben Sie die Menge $\mathcal{G}[M]$ der Graphen auf M als Menge von Abbildungen.

1.2 Summe und Produkt von Spezies

Die einfachste der diversen Verknüpfungen von Spezies ist wohl die Bildung der Summe $\mathcal{S}+\mathcal{T}$ zweier Spezies $\mathcal{S}$ und $\mathcal{T}$, dabei wird auf einer endlichen Menge M sowohl die Strukturenmenge $\mathcal{S}[M]$ als auch die Strukturenmenge $\mathcal{T}[M]$ gebildet, und beide Mengen werden disjunkt vereinigt, d.h. es wird die Menge

$$\mathcal{S}[M]+\mathcal{T}[M]:=\mathcal{S}[M]\ \cup\ \mathcal{T}[M]=\mathcal{S}[M]\,\dot\cup\,\mathcal{T}[M]$$

gebildet, falls $\mathcal{S}[M]\cap\mathcal{T}[M]=\emptyset$, andernfalls macht man sie sozusagen mit Gewalt disjunkt, etwa indem man die folgende Menge erzeugt:

$$\begin{aligned}\mathcal{S}[M]+\mathcal{T}[M]&:=(\mathcal{S}[M]\times\{1\})\ \cup\ (\mathcal{T}[M]\times\{2\})\\&=(\mathcal{S}[M]\times\{1\})\,\dot\cup\,(\mathcal{T}[M]\times\{2\}).\end{aligned}$$

Wir definieren demgemäß:

1.2.1 Definition *Die* Addition *zweier Spezies, etwa von $\mathcal{S}$ und $\mathcal{T}$, erzeugt auf einer Menge M die disjunkte Vereinigung von $\mathcal{S}[M]$ und $\mathcal{T}[M]$:*

$$(\mathcal{S}+\mathcal{T})[M]:=\mathcal{S}[M]+\mathcal{T}[M]:=\mathcal{S}[M]\,\dot\cup\,\mathcal{T}[M].$$

Der Transport dieser Strukturensumme wird dementsprechend so eingeführt:

$$(\mathcal{S}+\mathcal{T})[\beta](\sigma):=\begin{cases}\mathcal{S}[\beta](\sigma) & \textit{falls } \sigma\in\mathcal{S}[M],\\ \mathcal{T}[\beta](\sigma) & \textit{falls } \sigma\in\mathcal{T}[M].\end{cases}$$

◇

Offensichtlich gilt für die Kardinalitätenreihen

1.2.2 $$(\mathcal{S}+\mathcal{T})(x)=\mathcal{S}(x)+\mathcal{T}(x).$$

Triviale Beispiele bilden Strukturen, für die es den Begriff des Zusammenhangs gibt, beispielsweise besteht die Menge aller Graphen auf M aus den zusammenhängenden und den nicht zusammenhängenden:

$$\mathcal{G}=\mathcal{G}^{z}+\mathcal{G}^{nz}.$$

Man kann die Summenbildung auch auf Familien ausdehnen:

1.2.3 Definition *Eine Familie* $(\mathcal{S}_i)_{i\in I}$ *von Spezies heißt* summierbar, *wenn für jede endliche Menge* M *nur endlich viele* $\mathcal{S}_i[M]$ *nicht leer sind. Für eine solche summierbare Familie definieren wir ihre Summe als*

$$\left(\sum_{i\in I}\mathcal{S}_i\right)[M] := \sum_{i\in I}\mathcal{S}_i[M] := \bigcup_{i\in I}\mathcal{S}_i[M]\times\{i\}.$$

◇

Dies ist kompatibel mit dem folgenden Zerlegungsbegriff:

1.2.4 Definition *Als* kanonische Zerlegung *von* $\mathcal{S}$ *bezeichnen wir die summierbare Familie* $(\mathcal{S}_n)_{n\geq 0}$ *mit*

$$\mathcal{S}_n[M] := \begin{cases} \mathcal{S}[M], & \textit{falls } |M| = n, \\ \emptyset, & \textit{sonst.} \end{cases}$$

Hierfür schreiben wir auch kurz

$$\mathcal{S} = \mathcal{S}_0 + \mathcal{S}_1, +\mathcal{S}_2 + \ldots .$$

Falls $\mathcal{S}_n = \emptyset$, *für* $n \neq k$, *dann sagt man auch,* $\mathcal{S}$ konzentriere *sich auf* k. ◇

Ein triviales Beispiel ist die Zerlegung von $\mathcal{M}$ in k-Mengen:

$$\mathcal{M} = \sum_k \mathcal{M}_k,\ \mathcal{M}_k := \begin{cases} \{M\}, & \text{falls } |M| = k, \\ \emptyset, & \text{sonst.} \end{cases}$$

auch die Zerlegung von Permutationen in Permutationen mit vorgegebener Anzahl von Zyklen und die Zerlegung von Mengenpartitionen in Partitionen vorgegebener Anzahl von Blöcken ergibt Zerlegungen, diese sind aber nicht kanonisch:

$$Per = \sum Per^{[k]},\ Par = \sum Par^{[k]}.$$

Die *Multiplikation* von Spezies benutzt das cartesische Produkt, ist aber nicht mit diesem gleichzusetzen, vielmehr werden wir später auch ein cartesisches Produkt von Spezies definieren.

1.2.5 Definition *Das Produkt* $\mathcal{S}\cdot\mathcal{T}$ *zweier Spezies* $\mathcal{S}$ *und* $\mathcal{T}$ *definieren wir in folgender Weise:*

$$(\mathcal{S}\cdot\mathcal{T})[M] := \sum_{(M_0,M_1):M=M_0\dot\cup M_1}\mathcal{S}[M_0]\times\mathcal{T}[M_1],$$

wobei also über alle Paare von Teilmengen summiert wird, die M direkt zerlegen. Demgemäß wird der Transport dieser Produktstruktur so zu definieren sein:

$$(\mathcal{S} \cdot \mathcal{T})\,[\beta]((\sigma,\tau)) := (\mathcal{S}[\beta \downarrow M_0](\sigma), \mathcal{T}[\beta \downarrow M_1](\tau)),$$

für $(\sigma,\tau) \in \mathcal{S}[M_0] \times \mathcal{T}[M_1]$; $\downarrow$ bezeichnet dabei die Einschränkung der voraufgegangenen Abbildung auf die nachstehende Menge. ◇

1.2.6 Beispiele

- Ein Beispiel ist die Aufteilung von Permutationen in eine Menge von Fixpunkten zuzüglich eine fixpunktfreie Permutation, ein sogenanntes *Derangement:*

$$Per = \mathcal{M} \cdot Der.$$

- Ein weiteres Beispiel ist die Darstellung der Potenzmenge als Menge von Paaren, bestehend aus einer Teilmenge und deren Komplement:

$$\mathcal{P} = \mathcal{M} \cdot \mathcal{M},$$

- oder auch der Menge der k-Teilmengen als Menge von Paaren:

$$\mathcal{P}^{[k]} = \mathcal{M}_k \cdot \mathcal{M}.$$

- Schließlich kann man die Produktbildung von Spezies auch iterieren, d.h. man kann Potenzen von Spezies bilden:

$$Par^{[k]} = (\mathcal{M}_+)^k\,.$$

Hieraus ergeben sich einige nicht triviale Anwendungen, wenn wir noch folgendes bemerken (Übungsaufgabe 1.2.1):

1.2.7 Hilfssatz *Für die Kardinalitätenreihen von Spezies gilt*

$$(\mathcal{S} \cdot \mathcal{T})\,(x) = \mathcal{S}(x) \cdot \mathcal{T}(x).$$

◇

Wenden wir dies auf die oben aufgeführte Gleichung $Per = \mathcal{M} \cdot \mathcal{M}$ an, so ergibt sich die folgende Gleichung für die Kardinalitätenreihe von Der :

$$\frac{1}{1-x} = e^x \cdot Der(x),$$

aus der sich die folgende Gleichung für die Kardinalitätenreihe der Spezies Derangements ergibt (vgl. Übung 1.2.2):

$$Der(x) = \frac{e^{-x}}{1-x} = e^{-x} \cdot (1 + x + x^2 + x^3 + \ldots).$$

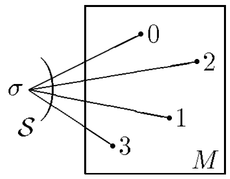
Hieraus wiederum erhalten wir einen expliziten Ausdruck für die Anzahl der Derangements einer Menge der Ordnung n :

$$der_n = n! \cdot \sum_{o}^{n} \frac{(-1)^k}{k!}.$$

Hier sind die ersten Werte einer Tabelle für diese Zahlen:

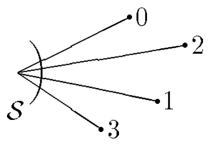
n	0	1	2	3	4	5	6	$\ldots$
der_n	1	0	1	2	9	44	265	$\ldots$

Bei der Veranschaulichung von Spezies, und insbesondere bei der Illustierung von Verknüpfungen, helfen Skizzen der folgenden Form: Eine Struktur σ skizzieren die Entwickler der Speziestheorie (die Gruppe um A. Joyal, F. Bergeron, G. Labelle und P. Leroux in Montreal) gerne etwa so:

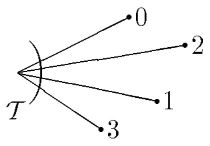


beschreibt $\sigma \in \mathcal{S}[M]$, wobei $M := 4$.

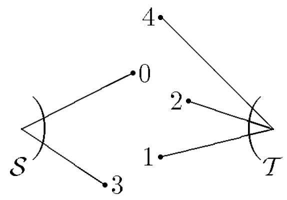
Die Umrahmung der Menge M sowie die Indizierung der Struktur mit dem Namen σ lassen wir oft einfachheitshalber weg. Ein Element von $(\mathcal{S} + \mathcal{T})[4]$ kann dann so visualisiert werden:



oder



Eine Struktur des Produkts dieser beiden Spezies wäre dann



Übungen

Ü 1.2.1 Beweisen Sie 1.2.7.

Ü 1.2.2 Zeigen Sie, daß eine formale Potenzreihe über einem kommutativen Ring mit Einselement genau dann invertierbar ist, wenn dies (im Ring) auch für das konstante Glied der Reihe gilt.

Ü 1.2.3 Leiten Sie eine Rekursionsformel für die Anzahlen von Derangements her.

1.3 Die Partitionelle Komposition

Eine weitere, allerdings etwas komplizierte, jedoch sehr wichtige Verknüpfung von Spezies ist die sogenannte *Partitionelle Komposition* zweier Spezies. Sie kann u.a. durch den Wunsch motiviert werden, zu Spezies $\mathcal{S}$ und $\mathcal{T}$ eine Spezies $\mathcal{S}(\mathcal{T})$ zu definieren, deren Kardinalitätenreihe durch Einsetzung der einen Reihe in die andere entsteht, d.h. für die gilt $\mathcal{S}(\mathcal{T})(x) = \mathcal{S}(\mathcal{T}(x))$.
Eine solche zusammengesetzte Spezies werden wir nun definieren, typische Beispiele für deren Anwendung sind die Zusammensetzung von Permutationen aus orientierten Zyklen oder auch die Zusammensetzung von Graphen aus zusammenhängenden Graphen. Auch die Endofunktionen lassen sich auf diese Weise aus Wurzelbäumen durch Einsetzen in Permutationen gewinnen.

1.3.1 Definition *Seien $\mathcal{S}$ und $\mathcal{T}$ zwei Spezies, wobei $\mathcal{T}[\emptyset] = \emptyset$ vorausgesetzt wird. Die* Partitionelle Komposition *von $\mathcal{S}$ mit $\mathcal{T}$ definieren wir durch*

$$\mathcal{S}(\mathcal{T})[M] := \bigcup_{p=\{p_0,\ldots,p_{r-1}\}\in Par[M]} \mathcal{S}[p] \times (\times_i \mathcal{T}[p_i])\,.$$

Dies bedeutet: Um $\mathcal{S}(\mathcal{T})[M]$ zu erhalten bildet man zunächst alle Mengenpartitionen $p \in Par[M]$. Besteht eine solche Partition p aus den (nicht leeren!) Blöcken $p_i, i = 0, \ldots, r-1$, dann bildet man auf jedem dieser Blöcke p_i die Menge aller $\mathcal{T}$-Strukturen, also die Mengen $\mathcal{T}[p_i]$, und dann das cartesische Produkt (über $i = 0, \ldots, r-1$) dieser Mengen von $\mathcal{T}$–Strukturen, welches man noch cartesisch mit $\mathcal{S}[p]$ (das ist die Menge der $\mathcal{S}$-Strukturen auf der Menge *p) multipliziert. Die gesuchte Menge von Strukturen $\mathcal{S}(\mathcal{T})[M]$ ist dann die Vereinigung all dieser cartesischen Produkte über alle Mengenpartitionen p von M. Elemente von $\mathcal{S}(\mathcal{T})[M]$ sind also Paare der Form*

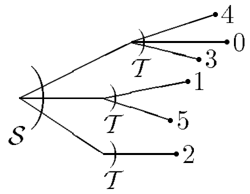
$$\rho = (\sigma; \tau_0, \ldots, \tau_{r-1}) := (\rho, M) = ((\sigma, p); (\tau_0, p_0), \ldots, (\tau_{r-1}, p_{r-1})).$$

Der Transport verläuft deshalb wie folgt:

$$\mathcal{S}(\mathcal{T})[\beta](\rho) := (\mathcal{S}[\beta](\sigma); \mathcal{T}[\beta](\tau_0), \ldots, \mathcal{T}[\beta](\tau_{r-1})).$$

Dabei meint $\mathcal{S}[\beta](\sigma)$ natürlich die Anwendung der von $\mathcal{S}[\beta]$ (das ja auf M und zunächst nicht auf p definiert ist) auf p induzierten Abbildung, deren Bild ja die p entsprechende Mengenpartition von N ist. Analoges gilt für $\mathcal{T}[\beta]$. ◇

Hier ist eine Skizze einer Struktur $\sigma \in (\mathcal{S} \circ \mathcal{T})[6]$:



Betrachten wir eine konkrete Anwendung:

1.3.2 Beispiel Sei $M := 3 = \{0,1,2\}$. Hier sind zunächst die Elemente der Menge $Par[3]$ aller Partitionen von M aufgelistet:

$$\{\{0,1,2\}\}, \{\{0,1\},\{2\}\}, \{\{0,2\},\{1\}\}, \{\{1,2\},\{0\}\}, \{\{0\},\{1\},\{2\}\}.$$

Wir wollen einmal $\mathcal{M}(\mathcal{C})[3]$ berechnen. Die erste Mengenpartition trägt hierzu folgendes bei:

$$\begin{aligned}\mathcal{M}[\{\{0,1,2\}\}] \times \mathcal{C}[\{0,1,2\}] &= \{\{\{0,1,2\}\}\} \times \{(012),(021)\} \\ &= \{(\{0,1,2\};(012)), (\{0,1,2\};(021))\}.\end{aligned}$$

(Der rechte Faktor im mittleren Ausdruck ist eine zweielementige Menge, bestehend aus den beiden Zyklen (012) und (021), der linke Faktor ist die einelementige Menge, bestehend aus der einelementigen Partition $\{\{0,1,2\}\}$.) Der nächste Summand der gesuchten Menge gehört zur zweiten Partition, er ist gleich

$$\{\{\{0,1\},\{2\}\}\} \times \{((01),(2))\}.$$

Dabei ist zu beachten, daß hier der zweite Faktor als das cartesische Produkt $\{(01)\} \times \{(2)\}$ zu lesen ist. Der dritte Summand entsteht hieraus durch Vertauschen von 1 und 2, das ergibt

$$\{\{\{0,2\},\{1\}\}\} \times \{((02),(1))\}.$$

Der vierte Summand ist entsprechend gleich

$$\{\{\{1,2\},\{0\}\}\} \times \{((12),(0))\}.$$

Schließlich ist noch der Summand zur Partition $\{\{0\},\{1\},\{2\}\}$ zu ermitteln, es ist

$$\{\{\{0\},\{1\},\{2\}\}\} \times \{((0),(1),(2))\}.$$

Vereinigen wir diese fünf Mengen, so entsteht eine Menge der Ordnung 6, und es ist offensichtlich, daß diese mit der symmetrischen Gruppe S_3 identifiziert werden kann: Die linken Faktoren $\mathcal{M}[p]$ in den Summanden sind redundant, und die Vereinigung der rechten Faktoren, also die Menge

$$\bigcup_p (\times_i \mathcal{C}[p_i])$$

besteht genau aus den verschiedenen Permutationen der symmetrischen Gruppe, diese können nämlich mit den Elementen von

$$\times_i \mathcal{C}[p_i]$$

identifiziert werden. Allgemeiner gilt demnach ganz offensichtlich die Isomorphie $\mathcal{M}(\mathcal{C}) \simeq Per$. Wie verabredet schreiben wir das einfachheitshalber als Identität und können demnach festhalten, daß

1.3.3 $$Per = \mathcal{M}(\mathcal{C}).$$

◇

Nach diesem Beispiel verwundert es wohl nicht, daß die Kardinalitätenreihe der Einsetzung die Einsetzung der Kardinalitätenreihen ist (Übungsaufgabe 1.3.1):

1.3.4 $$\mathcal{S}(\mathcal{T})(x) = \mathcal{S}(\mathcal{T}(x)).$$

Beispielsweise gilt also nach dem gerade besprochenen Beispiel:

$$\frac{1}{1-x} = Per(x) = \mathcal{M}(\mathcal{C}(x)) = e^{\mathcal{C}(x)},$$

woraus wir die Kardinalitätenreihe der Zyklen bekommen:

1.3.5 $$\mathcal{C}(x) = \log(1-x)^{-1} = \sum_{n>0} \frac{x^n}{n}.$$

Die Anzahl der Zyklen auf einer Menge der Ordnung n ist also:

$$c_n = (n-1)!,$$

was natürlich auch ganz anders hergeleitet werden kann (zum Beispiel aus der bekannten Ordnung der Konjugiertenklasse von Elementen eines bestimmten Zykeltyps).

Ganz analog ergeben sich die folgenden Formulierungen von Spezies als Einsetzungen:

$$\mathcal{G} = \mathcal{M}(\mathcal{G}^z), \;\; Par = \mathcal{M}(\mathcal{M}_+).$$

Daraus ergibt sich beispielsweise

$$\mathcal{G}^z(x) = \log(\mathcal{G}(x)), \;\; Par(x) = e^{e^x - 1}.$$

Übungsaufgaben

Ü 1.3.1 Zeigen Sie die Gültigkeit von

$$\mathcal{S}(\mathcal{T})(x) = \mathcal{S}(\mathcal{T}(x)).$$

Ü 1.3.2 Beweisen Sie, daß

$$End = Per(\mathcal{W}).$$

1.4 Ableitung, Punktierung, Funktorielle Komposition

Der Ableitung der Kardinalitätenreihe einer Spezies entspricht die Bildung der Ableitung der betrachteten Spezies:

1.4.1 Definition *Die Ableitung einer Spezies $\mathcal{S}$ definieren wir durch*

$$\mathcal{S}'[M] := \mathcal{S}[M^+],$$

wobei M^+ eine Menge sei, die aus M durch Erweiterung um ein weiteres Element entstanden ist. Im allgemeinen wird die Grundmenge M kein Element mit dem Namen $*$ enthalten, wir definieren deshalb — unter der Annahme, daß M dieses Element tatsächlich nicht umfaßt —

$$M^+ := M \cup \{*\}.$$

Für den Transport dieser abgeleiteten Struktur verwenden wir die kanonische Erweiterung der jeweiligen Bijektion auf die um das Element $*$ erweiterten Mengen:

$$\mathcal{S}'[\beta](\sigma) := \mathcal{S}[\beta^+](\sigma),$$

wobei

$$\beta^+ \colon M^+ \to N^+ \colon m \mapsto \begin{cases} \beta(m), & \textit{falls } m \in M, \\ *, & \textit{falls } m = *. \end{cases}$$

◇

Offenbar wird aus einem Zyklus $\zeta \in \mathcal{C}'[M]$, der ja einen Punkt $*$ enthält, durch Herausnehmen von $*$ eine lineare Ordnung auf M, es gilt also beispielsweise:

1.4.2 $$\mathcal{C}' = \mathcal{L}.$$

Für die Kardinalitätenreihen von Spezies und Ableitung gilt offensichtlich

1.4.3 $$\mathcal{S}'(x) = \frac{d}{dx}\mathcal{S}(x),$$

eine Anwendung auf 1.4.2 ergibt

1.4.4 $$\mathcal{C}(x) = \int_0^x \frac{dx}{1-x} = \log\frac{1}{1-x} = \sum_{n>0} \frac{x^n}{n},$$

eine Bestätigung des Ergebnisses $c_n = (n-1)!$ des voraufgehenden Paragraphen. Multiplizieren wir die Kardinalitätenreihe mit x, so entsteht die Kardinalitätenreihe der folgenden Konstruktion:

1.4.5 Definition *Die* Punktierung $\mathcal{S}^\bullet$ *von* $\mathcal{S}$ *entsteht, indem man bei jeder Struktur einen Punkt auszeichnet:*

$$\mathcal{S}^\bullet[M] := \mathcal{S}[M] \times M.$$

Der Transport wird ganz entsprechend geregelt:

$$\mathcal{S}^\bullet[\beta]((\sigma, m)) := (\mathcal{S}[\beta](\sigma), \beta(m)).$$

◇

Für die Kardinalitäten gilt

1.4.6 $$\mathcal{S}^\bullet(x) = x \cdot \mathcal{S}(x).$$

Es ist klar, daß auf diese Weise aus Bäumen Wurzelbäume werden, daß also beispielsweise gilt:

1.4.7 $$\mathcal{B}^\bullet = \mathcal{W}.$$

Eine besonders elegante Anwendung ist A. Joyals nachstehender Beweis eines berühmten kombinatorischen Resultats von Cayley. Er benutzt dazu die Kardinalitäten der Spezies $End_+, Per_+, \mathcal{L}_+$, die in naheliegender Weise gleich $End, Per, \mathcal{L}$ auf nicht leeren Mengen sein sollen und gleich der leeren Menge auf $\emptyset$, also ganz analog wie bei der Definition von $\mathcal{M}_+$.

1.4.8 Satz (Cayley) *Für die Anzahl der Bäume mit n Punkten gilt*

$$b_n = n^{n-2}.$$

Beweis: Aus

$$End_+ = Per_+(\mathcal{W}) \equiv \mathcal{L}_+(\mathcal{W}) = \mathcal{B}^{\bullet\bullet}.$$

ergibt sich durch Koeffizientenvergleich die Behauptung:

$$n^n = n^2 \cdot b_n.$$

□

Neben der Produktbildung von Spezies gibt es natürlich auch deren *cartesisches Produkt:*

1.4.9 Definition *Das* cartesische Produkt $\mathcal{S} \times \mathcal{T}$ *zweier Spezies* $\mathcal{S}$ *und* $\mathcal{T}$ *hat als Strukturenmengen die cartesischen Produkte der Strukturenmengen der Faktoren:*

$$(\mathcal{S} \times \mathcal{T})[M] := \mathcal{S}[M] \times \mathcal{T}[M].$$

Für den Transport gilt entsprechend

$$(\mathcal{S} \times \mathcal{T})[\beta]((\sigma, \tau)) := (\mathcal{S}[\beta](\sigma), \mathcal{T}[\beta](\tau)).$$

◇

Die Kardinalitätenreihe des cartesischen Produkts zweier Spezies ist das sogenannte *Hadamardprodukt* der Reihen der beiden Faktoren:

1.4.10 $$(\mathcal{S} \times \mathcal{T})(x) = \sum_n s_n t_n \frac{x^n}{n!}.$$

Bildet man die Menge der $\mathcal{S}$-Strukturen auf einer Menge von $\mathcal{T}$-Strukturen, so ergibt sich folgendes

1.4.11 Definition *Die* Komposition *einer Spezies* $\mathcal{S}$ *mit einer Spezies* $\mathcal{T}$ *ergibt, auf einer Grundmenge* M, *die folgende Menge von Strukturen:*

$$(\mathcal{S} \circ \mathcal{T})[M] := \mathcal{S}(\mathcal{T}[M]).$$

Der Transport geschieht wie folgt:

$$(\mathcal{S} \circ \mathcal{T})[\beta] := \mathcal{S}[\mathcal{T}[\beta]].$$

◇

Ein einleuchtendes Beispiel wird von den Graphen gebildet: Ein Graph mit n Punkten ist eine Teilmenge der Menge der Zweiermengen von Punkten, er kann nämlich offenbar mit derjenigen Teilmenge der Zweiermengen (= Punktepaare) identifiziert werden, die durch Kanten verbunden sind. Es folgt

1.4.12 $$\mathcal{G} = \mathcal{P} \circ \mathcal{P}^{[2]}.$$

Mit Hilfe der Produktbildung können wir das übrigens leicht noch weiter zerlegen:

$$\mathcal{G} = (\mathcal{M} \cdot \mathcal{M}) \circ (\mathcal{M} \cdot \mathcal{M}_2).$$

Unmittelbar aus der Definition dieser Komposition folgt die Form der Kardinalitätenreihe:

1.4.13 $$(\mathcal{S} \circ \mathcal{T})(x) = \sum_n (s \circ t)_n \frac{x^n}{n!} = \sum_n s_{t_n} \frac{x^n}{n!}.$$

Übungen

Ü 1.4.1 Beschreiben Sie die Ableitung $\mathcal{L}'$.

Ü 1.4.2 Beschreiben Sie die Punktierung von $\mathcal{W}$. (Man nennt die Elemente dieser Spezies auch *Wirbeltiere*.)

1.5 Typen von Strukturen

Bereits bei der Definition der Kardinalitätenreihe ist erwähnt worden, daß es nicht auf die "Natur" (was auch immer das sei) der Elemente von M ankommt, denn der Transport von Struktur ermöglicht ja, per Bijektion $\beta\colon M \to N$ von der Menge $\mathcal{S}[M]$ zur Menge $\mathcal{S}[N]$ überzugehen.Es genügt deshalb völlig, zu jedem $n \in \mathbb{N}$ die Menge von Strukturen $\mathcal{S}[n]$ zu betrachten.
Nun gibt es aber auch noch den Transport der Struktur *innerhalb der Grundmenge,* d.h. mit Hilfe von Bijektionen β von $\underline{n}$,

$$S_n \times \mathcal{S}[n] \to \mathcal{S}[n]\colon (\beta, \sigma) \mapsto \mathcal{S}[\beta](\sigma).$$

Diese Abbildungen fassen die $\mathcal{S}$–Strukturen auf $\underline{n}$ zu Äquivalenzklassen zusammen, den sogenannten Typen von Strukturen, denn die gerade beschriebene Abbildung von $S_n \times \mathcal{S}[n]$ nach $\mathcal{S}[n]$ beschreibt eine Operation der symmetrischen Gruppe, die Typen sind gerade deren Bahnen.
Weil wir dies sehr intensiv nutzen werden — oft kommt es viel mehr auf die Typen (=unnumerierte Strukturen) als auf die Strukturen selbst an — wird jetzt dieser Begriff in einiger Allgemeinheit definiert, bevor wir zu den Anwendungen auf die Spezies kommen.

Sei G eine multiplikativ geschriebene Gruppe und X eine nicht leere Menge. Eine *Operation* von G auf X von links wird durch eine Abbildung der folgenden Form beschrieben:

$$G \times X \to X\colon (g, x) \mapsto gx, \text{ mit } g(g'x) = (gg')x, \text{ und } 1x = x.$$

Wir kürzen dies verbal dadurch ab, daß wir sagen G *operiert* auf X, oder indem wir einfach X eine G*–Menge* nennen, oder auch indem wir schreiben

$${}_GX,$$

denn G operiert von links auf X. (Es ist klar, daß man ganz analog Operationen von Gruppen auf Mengen *von rechts* definieren kann. Tatsächlich werden wir solche Operationen von rechts von Zeit zu Zeit benutzen, manchmal sogar in Verbindung mit Operationen von links.)
Ein erstes und hier natürlich besonders wichtiges Beispiel ist obige Abbildung, die eine Operation der symmetrischen Gruppe beschreibt, denn es gilt ja wegen der Definition von Spezies sowohl

$$\mathcal{S}[\alpha](\mathcal{S}[\beta](\sigma)) = \mathcal{S}[\alpha] \circ \mathcal{S}[\beta](\sigma) = \mathcal{S}[\alpha \circ \beta](\sigma),$$

als auch

$$\mathcal{S}[\mathrm{id}_{\underline{n}}](\sigma) = \mathrm{id}_{\mathcal{S}}[n](\sigma) = \sigma.$$

1.5.1 Folgerung *Die Abbildung*

$$S_n \times \mathcal{S}[n] \to \mathcal{S}[n] \colon (\beta, \sigma) \mapsto \mathcal{S}[\beta](\sigma)$$

definiert eine Operation der symmetrischen Gruppe S_n auf der Menge $\mathcal{S}[n]$ der $\mathcal{S}$–Strukturen auf $\underline{n}$. □

Bevor wir weitere Beispiele betrachten, soll noch eine zweite äquivalente Formulierung erwähnt werden. Ein Homomorphismus δ von G in die *symmetrische Gruppe*

$$S_X := \{\pi \mid \pi \colon X \to X, \text{ bijektiv}\}$$

auf X heißt eine *Permutationsdarstellung von G auf X*. Es ist leicht nachzuprüfen (Übung 1.5.1), daß die Definition einer Operation, wie sie oben eingeführt wurde, äquivalent ist zu

$$\delta \colon g \mapsto \bar{g}, \text{ wobei } \bar{g} \colon x \mapsto gx, \text{ ist eine Permutationsdarstellung.}$$

Der *Kern* von δ wird mit G_X bezeichnet, es gilt also, mit $\bar{G} := \delta[G]$, die Isomorphie.

1.5.2 $$\bar{G} \simeq G/G_X.$$

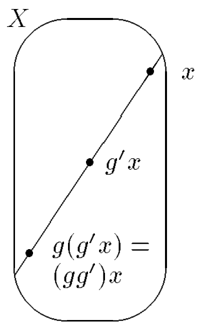
Im Falle daß $G_X = \{1\}$, nennt man die Operation *treu*. Ein sehr triviales Beispiel hierfür ist die *natürliche Operation* von S_X auf X bei der die entsprechende Permutationsdarstellung $\delta \colon \pi \mapsto \bar{\pi}$ einfach die identische Abbildung ist. Eine Anzahl weniger trivialer Beispiele wird gleich folgen.

Eine Operation von G auf X hat vor allem die folgende Eigenschaft, die unmittelbar aus den beiden Bedingungen folgt, die oben in der Definition angegeben wurden:

1.5.3 $$gx = x' \iff x = g^{-1}x'.$$

Dies ist der Grund für die Tatsache, daß eine Operation ${}_GX$ mehrere Strukturen auf X und G induziert. Der enge arithmetische und algebraische Zusammenhang zwischen diesen Strukturen macht das Konzept der Gruppenoperation so effizient. Zunächst definiert die Operation ${}_GX$ die folgende Äquivalenzrelation auf X (Übung 1.5.2):

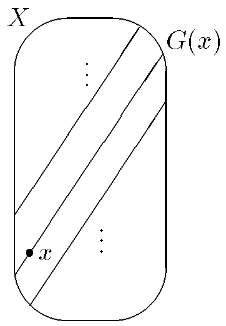
$$x \sim_G x' \ :\iff \exists\, g \in G \colon\ x' = gx.$$



Die Äquivalenzklassen

$$G(x) := \{gx \mid g \in G\}$$

heißen *Bahnen.* Nebenstehend ist die Bahn von $x \in X$ skizziert. Bitte beachten Sie, daß *jedes ihrer Elemente von jedem anderen Element dieser Bahn erreicht werden kann, diese Bahn ist also tatsächlich die Bahn von jedem ihrer Elemente unter der Operation von G!*
Da $\sim_G$ eine Äquivalenzrelation auf X ist, liefert eine *Transversale* T der Bahnen eine *Mengenpartition* von X, also eine vollständige Zerlegung von X in paarweise disjunkte und nicht leere Teilmengen $G(t), t \in T$:



1.5.4 $$X = \dot{\bigcup}_{t \in T} G(t).$$

Dies kann man wie angedeutet bildlich darstellen.

Die *Menge* aller Bahnen sei wie folgt bezeichnet

$$G\backslash\!\backslash X := \{G(t) \mid t \in T\} = \{G(x) \mid x \in X\}$$

und die Menge *aller* Transversalen dieser Bahnenmenge bezeichnen wir mit

$$\mathcal{T}(G\backslash\!\backslash X) := \{T \mid T \text{ Transversale von } G\backslash\!\backslash X\}.$$

Im Falle, daß sowohl G als auch X endlich sind, nennen wir die Operation eine *endliche Operation* . Wir notieren, daß wir, entsprechend 1.5.2, für jede endliche G–Menge X ohne Einschränkung der Allgemeinheit annehmen können, daß G endlich ist. Besitzt G genau eine Bahn auf X — das ist genau dann der Fall, wenn $G\backslash\!\backslash X = \{X\}$ — dann sagen wir die Operation sei *transitiv* bzw. *G operiere transitiv* auf X.
Gemäß 1.5.4 liefert eine Operation von G auf X eine Partition auf X. Das gilt also insbesondere für die oben angegebene Operation der symmetrischen Gruppe S_n auf $\mathcal{S}[n]$. Strukturen, die dann in demselben Block der Partition liegen, sind, wie wir sagen werden, vom selben *Typ.* Dies gilt also beispielsweise für Graphen, die durch Umnumerieren auseinander hevorgehen, für Endofunktionen ϵ und δ einer Menge

M, für die es eine Bijektion $\beta \in S_M$ gibt mit $\delta = \beta\epsilon\beta^{-1}$, usw. Wir ziehen daraus die

1.5.5 Folgerung *Die oben angegebene Operation von S_n auf der Menge $\mathcal{S}[n]$ der $\mathcal{S}$–Strukturen auf n zerlegt die Menge $\mathcal{S}[n]$ in Bahnen, die sogenannten* Typen *von Strukturen. (Analoges gilt natürlich für die Operation von S_M auf der Menge $\mathcal{S}[M]$.) Die Menge der Typen von $\mathcal{S}$–Strukturen auf M ist also gleich*

$$S_M \backslash\backslash \mathcal{S}[M].$$

□

Es ist trivial aber sehr wichtig zu bemerken, daß auch umgekehrt jede Mengenpartition von X (insbesondere also auch Äquivalenzrelation auf X), durch eine Operation einer Gruppe G auf X beschrieben werden kann: Seien, für eine Indexmenge I, X_i, $i \in I$, die Blöcke der Mengenpartition (die Klassen der Äquivalenzrelation), d.h. die X_i sind nicht leere paarweise disjunkte Teilmengen, deren Vereinigung gleich X ist. Dann operiert die folgende Untergruppe der symmetrischen Gruppe S_X auf X und hat die X_i als Bahnen:

1.5.6 $$\bigoplus_i S_{X_i} := \{\pi \in S_X \mid \forall\ i \in I\colon\ \pi X_i = X_i\}.$$

Fassen wir unsere Überlegungen in zwei Sätze, dann haben wir gerade folgendes erhalten:

1.5.7 Folgerung *Eine Operation von G auf X ist äquivalent zu einer Permutationsdarstellung von G auf X und liefert eine Partition von X in Bahnen. Umgekehrt entspricht jede Mengenpartition von (Äquivalenzrelation auf) X in natürlicher Weise einer Operation einer Untergruppe der symmetrischen Gruppe S_X, welche die Blöcke der Partition (die Klassen der Äquivalenzrelation) als Bahnen hat.*
□

Dies läßt sich insbesondere auf Diskrete Strukturen anwenden, denn sehr viele von ihnen (eigentlich alle, die hier diskutiert werden) können als Äquivalenzklassen auf Mengen und somit als Bahnen von Gruppen definiert werden, indem man die Definition der Äquivalenzrelation durch eine geeignete Gruppenoperation ersetzt. Im Vorgriff auf die nachfolgenden Untersuchungen von Gruppenoperationen und die anschließende erfolgreiche Anwendung der dabei erzielten Resultate (beispielsweise zur Abzählung von Bahnen oder zur Konstruktion von Bahnenrepräsentanten) wollen wir dies als wichtige Taktik apostrophieren:

1.5.8 Strategie I: Verwende Gruppenoperationen!
Bei der Untersuchung von Diskreten Strukturen, die als Äquivalenzklassen definiert werden können, ist es zweckmäßig, die Definition der Äquivalenzrelation durch eine geeignete Gruppenoperation zu ersetzen. □

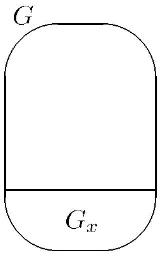
Übungen

Ü 1.5.1 Sei X eine vorgegebene G–Menge. Weisen Sie sorgfältig nach, daß $g \mapsto \bar{g}$ tatsächlich eine Permutationsdarstellung ist, d.h. daß $\bar{g} \in S_X$ und $\overline{g_1 \cdot g_2} = \overline{g_1} \cdot \overline{g_2}$.

Ü 1.5.2 Zeigen Sie, daß $\sim_G$ wirklich eine Äquivalenzrelation ist.

1.6 Die Typenreihe

Wir wollen uns im folgenden auf Typen von $\mathcal{S}$–Strukturen konzentrieren, beispielsweise auf *unnumerierte* Graphen. Gemäß Strategie I sind diese als Bahnen von symmetrischen Gruppen definiert, und es gilt jetzt, die Berechnung von deren Anzahl (zu vorgegebenem Parameter n) zu ermöglichen, oder sogar eine Transversale der Typen zu ermitteln. Zu diesem Zweck treiben wir die Theorie der Operationen von Gruppen auf Mengen weiter voran:



Den Bahnen $G(x)$, die *Teilmengen* von X sind, entsprechen gewisse *Untergruppen* von G. Für jedes $x \in X$ definieren wir seinen *Stabilisator*:

$$G_x := \{g \mid gx = x\},$$

eine Untergruppe (Übung 1.6.1) von G. Sie besteht aus den Elementen, die den *Punkt* x stabilisieren.

Für *Teilmengen* $\Delta \subseteq X$ von Punkten gibt es einmal die Untergruppe von Elementen von G, die Δ *punktweise* stabilisieren:

$$G_\Delta := \{g \mid \forall\ x \in \Delta : gx = x\},$$

sie heißt entsprechend der *punktweise Stabilisator* oder auch der *Zentralisator* von Δ, und sie ist von dem *mengenweisen Stabilisator* oder *Normalisator* von Δ zu unterscheiden:

$$G_{\{\Delta\}} := \{g \mid \{gx \mid x \in \Delta\} = \Delta\}.$$

Wir bemerken dazu, daß $G_{\{x\}} = G_x$, das $G_\Delta \subseteq G_{\{\Delta\}}$ und daß diese Notation mit der Bezeichnung G_X für den Kern der Permutationsdarstellung δ kompatibel ist, die der Operation ${}_GX$ entspricht.
Das letzte der fundamentalen Konzepte, die durch eine Operation von G auf X definiert werden, sind die *Fixpunkte*. Ein Punkt $x \in X$ heißt genau dann *Fixpunkt* von $g \in G$, wenn $gx = x$. Die Menge *aller* Fixpunkte von g wird wie folgt bezeichnet:

$$X_g := \{x \mid gx = x\}.$$

Allgemeiner setzen wir für jede Teilmenge $S \subseteq G$

$$X_S := \{x \mid \forall g \in S\colon\ gx = x\}.$$

Der Spezialfall X_G heißt auch die Menge der *Invarianten.*

Der erste Satz von Beispielen, der diese Konzepte illustriert, zeigt schon, daß viele wichtige gruppentheoretische Strukturen als Bahnen oder Stabilisatoren definiert werden können. Wir werden diese Strukturen im folgenden verwenden, und die Erkenntnis, daß sie als Bahnen bzw. als Stabilisatoren auftreten, wird uns dabei hilfreich sein:

1.6.1 Beispiele Wenn G eine Gruppe bezeichnet, dann gilt

- G operiert auf sich selbst per *Linksmultiplikation*:

  $$G \times G \to G : (g, x) \mapsto g \cdot x.$$

  Diese Operation heißt die *(linke) reguläre Darstellung* von G, sie ist offensichtlich transitiv, und alle auftretenden Stabilisatoren sind die $\{1\}$-Untergruppe.

- Wenn wir auf eine Untergruppe U, einschränken, dann erhalten wir auf diese Weise die Operation $U \times G \to G : (u, x) \mapsto u \cdot x$ von U auf G. Die Bahnen sind jetzt die *Rechtsnebenklassen*

  $$U(g) = Ug$$

  der Untergruppe U. Die Stabilisatoren sind wiederum trivial:

  $$U_g = \{1\}.$$

  Entsprechend ergeben sich die *Linksnebenklassen* gU als Bahnen, wenn wir die *Rechtsmultiplikation* betrachten.

Dies zeigt, daß verschiedene Rechtsnebenklasen wie auch verschiedene Linksnebenklassen von Untergruppen in Gruppen disjunkt sind.

- G operiert auf sich selbst per *Konjugation*:

  $$G \times G \to G : (g, x) \mapsto g \cdot x \cdot g^{-1}.$$

  Die Bahnen dieser Operationen sind die *Konjugiertenklassen* von Elementen,

  $$G(x) = C^G(x) := \{gxg^{-1} \mid g \in G\},$$

  und die Stabilisatoren sind die *Zentralisatoren* der Elemente:

  $$G_x = C_G(x) := \{g \mid gxg^{-1} = x\}.$$

Eine unmittelbare Konsequenz ist, daß verschiedene Konjugiertenklassen von Elementen disjunkt sind, denn sie sind ja Bahnen, und daß die Zentralisatoren von Elementen Untergruppen sind, denn sie sind ja Stabilisatoren.

- Bezeichnet wiederum U eine Untergruppe von G, $U \leq G$, dann operiert G auf der Menge $G/U := \{xU \mid x \in G\}$ der *Linksnebenklassen* von U wie folgt:

$$G \times G/U \to G/U \colon (g, xU) \mapsto gxU.$$

  Diese Operation ist transitiv, und der Stabilisator von xU ist die Untergruppe xUx^{-1} die konjugiert ist zu U.

Also ist xUx^{-1} ebenfalls eine Untergruppe.

- G operiert auf der Menge $L(G) := \{U \mid U \leq G\}$ aller Untergruppen per *Konjugation*:

$$G \times L(G) \to L(G) \colon (g, U) \mapsto gUg^{-1}.$$

  Die Bahnen dieser Operation sind die *Konjugugiertenklassen von Untergruppen,* und die Stabilisatoren sind die *Normalisatoren:*

$$G(U) = \widetilde{U} := \{\, gUg^{-1} \mid g \in G\},$$

  und

$$G_U = N_G(U) := \{g \mid gU = Ug\}.$$

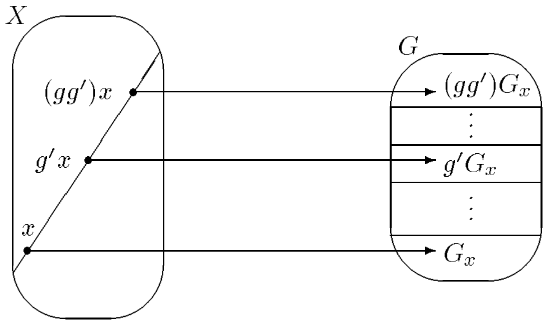
Also sind verschiedene Konjugiertenklassen von Untergruppen disjunkt, und Normalisatoren von Untergruppen sind ebenfalls Untergruppen. ◇

Kommen wir jetzt zu dem allgemeinen Fall zurück. Wir wollen zunächst die wichtigste, wenn auch offensichtliche Eigenschaft der Stabilisatoren von Elementen angeben: *Zu Punkten derselben Bahn gehören konjugierte Stabilisatoren, und die Stabilisatoren der Elemente einer Bahn bilden eine volle Konjugiertenklassen von Untergruppen:*

1.6.2 $G_{gx} = gG_xg^{-1}, \widetilde{G_x} = \{gG_xg^{-1} \mid g \in G\} = \{G_{x'} \mid x' \in G(x)\}.$

Ein weiterer entscheidender Punkt ist die folgende natürliche Bijektion zwischen der Bahn von x und der Menge der Linksnebenklassen des Stabilisators:

1.6.3 Hilfssatz *Die Abbildung $G(x) \to G/G_x \colon gx \mapsto gG_x$*



ist eine Bijektion zwischen der Bahn $G(x)$ und der Menge von Linksnebenklassen G/G_x.

Beweis: Nach 1.5.3 ist klar, daß für $x \in X$ die folgende Kette von Äquivalenzen gültig ist:

$$gx = g'x \iff g^{-1}g' \in G_x \iff g'G_x = gG_x.$$

Lesen wir dies von links nach rechts, dann sehen wir, daß $gx \mapsto gG_x$ eine Abbildung definiert, lesen wir dies von rechts nach links, so erkennen wir, daß diese Abbildung injektiv ist. Darüber hinaus ist diese Abbildung natürlich ganz offensichtlich auch noch surjektiv.

□

Dieses Resultat zeigt insbesondere, daß *die Länge einer Bahn gleich dem Index des Stabilisators irgendeines Elements ist,* wir erhalten also folgendes:

1.6.4 Folgerung *Ist G eine Gruppe die auf der Menge X operiert, dann haben wir für jedes $x \in X$:*

$$|G(x)| = |G/G_x|.$$

Ist insbesondere $|G|$ endlich, dann gilt für die Formel

$$|G(x)| = |G|/|G_x|,$$

die Länge jeder Bahn ist in diesem Fall ein Teiler der Gruppenordnung.

□

Eine Anwendung auf die obigen Beispiele ergibt:

1.6.5 Folgerung *Wenn G endlich ist, $g \in G$, und $U \leq G$, dann gelten für die Ordnungen der Konjugiertenklassen von Elementen und von Untergruppen die folgenden Gleichungen:*

$$|C^G(g)| = |G|/|C_G(g)| \ , \ \textit{und} \ \ |\widetilde{U}| = |G|/|N_G(U)|.$$

□

Das Resultat von 1.6.4 ist sehr wichtig für den Beweis des folgenden grundlegenden Lemmas zur Abzählung von Bahnen. Zusammen mit Verfeinerungen, die wir später noch sehen werden, ist es *das Grundhilfsmittel der Theorie der Abzählung von Bahnen endlicher Gruppenoperationen.*

1.6.6 Das Lemma von Cauchy-Frobenius *Die Anzahl der Bahnen einer endlichen Gruppe G die auf einer endlichen Menge X operiert, ist die mittlere Fixpunktzahl:*

$$|G\backslash\backslash X| = \frac{1}{|G|}\sum_{g\in G}|X_g|.$$

Beweis:

$$\sum_{g\in G}|X_g| = \sum_g \sum_{x\in X_g} 1 = \sum_x \sum_{g\in G_x} 1 = \sum_x |G_x|$$

$$=_{1.6.4} |G|\sum_x |G(x)|^{-1} = |G|\cdot|G\backslash\backslash X|.$$

□

Damit haben wir ein Mittel an der Hand, die Koeffizienten der erzeugenden Funktionen für die Typenanzahlen zu berechnen, die jetzt eingeführt werden soll:

1.6.7 Definition *Ist $\mathcal{S}$ eine Spezies, dann bezeichnen wir mit $\widetilde{\mathcal{S}}(x)$ die formale Potenzreihe:*

$$\widetilde{\mathcal{S}}(x) := \sum_n \widetilde{s}_n x^n,$$

wobei, mit dem Lemma von Cauchy-Frobenius,

$$\widetilde{s}_n := |S_n\backslash\backslash\mathcal{S}[n]| = \frac{1}{n!}\sum_{\beta\in S_n}|\mathcal{S}[n]_\beta|.$$

Sie ist also die erzeugende Funktion der Typenanzahlen und heißt dementsprechend die Typenreihe *von $\mathcal{S}$.*

◇

Hier sind einige einfache Fälle von Typenreihen aufgelistet, für deren Berechnung die explizite Anwendung des Cauchy-Frobenius noch nicht benötigt wird:

1.6.8 Beispiele

- $\widetilde{\mathcal{L}}(x) = \widetilde{\mathcal{M}}(x) = \frac{1}{1-x} = 1 + x + x^2 + x^3 + \ldots,$
- $\widetilde{\mathcal{C}}(x) = \widetilde{\in}(x) = \frac{x}{1-x} = x + x^2 + x^3 + \ldots,$
- $\widetilde{\mathcal{P}}(x) = \left(\frac{1}{1-x}\right)^2 = 1 + x + 2 \cdot x^2 + 3 \cdot x^3 + \ldots,$
- $\widetilde{\mathcal{X}}(x) = x, \widetilde{1}(x) = 1, \widetilde{0}(x) = 0.$

$\diamond$

Wir bemerken noch, daß offensichtlich für die Typenreihen von Summe und Produkt gilt

1.6.9 $\quad \widetilde{(\mathcal{S}+\mathcal{T})}(x) = \widetilde{\mathcal{S}}(x) + \widetilde{\mathcal{T}}(x), \ \widetilde{(\mathcal{S}\cdot\mathcal{T})}(x) = \widetilde{\mathcal{S}}(x) \cdot \widetilde{\mathcal{T}}(x).$

Schließlich sei noch vermerkt, daß Äquipotenz keineswegs die Gleichheit der Typenreihen impliziert:

1.6.10 $$\mathcal{S} \equiv \mathcal{T} \not\Rightarrow \widetilde{\mathcal{S}}(x) = \widetilde{\mathcal{T}}(x).$$

Die nächste Bemerkung hilft, die notwendigen Rechnungen bei der Anwendung des Lemmas von Cauchy-Frobenius erheblich abzukürzen. Sie zeigt nämlich, daß wir die Summation über alle Elemente $g \in G$ durch eine Summation über eine *Transversale der Konjugiertenklassen* ersetzen können, denn die Anzahl der Fixpunkte erweist sich als konstant auf jeder dieser Klassen:

1.6.11 Hilfssatz *Die Abbildung*

$$X_{g'} \to X_{gg'g^{-1}} : x \mapsto gx$$

ist eine Bijektion, die Funktion

$$\chi : G \to \mathbb{N} : g \mapsto |X_g|$$

also eine Klassenfunktion, d.h. sie ist konstant auf den Konjugiertenklassen der Elemente von G. Wir haben also für alle $g, g' \in G$, die Gleichung $|X_{g'}| = |X_{gg'g^{-1}}|$.

Beweis: Daß $x \mapsto gx$ eine Bijektion zwischen den beiden Mengen $X_{g'}$ und $X_{gg'g^{-1}}$ bildet, ergibt sich aus der nachfolgenden Äquivalenz:

$$g'x = x \iff gg'g^{-1}(gx) = gx.$$

□

Die Abbildung $\chi\colon g \mapsto |X_g|$ heißt der *Charakter* der Operation von G auf X, bzw. von ${}_GX$.

1.6.12 Folgerung *Sei ${}_GX$ eine endliche Operation und $\mathfrak{C}$ eine Transversale der Konjugiertenklassen von G, dann gilt:*

$$|G\backslash\!\backslash X| = \frac{1}{|G|}\sum_{g\in\mathfrak{C}} |C^G(g)||X_g| = \sum_{g\in\mathfrak{C}} \frac{|X_g|}{|C_G(g)|}.$$

Eine andere Formulierung des Lemmas von Cauchy-Frobenius benutzt die von der Operation definierte Permutationsdarstellung $g \mapsto \bar{g}$. Die Permutationsgruppe $\bar{G}$, das Bild von G unter dieser Darstellung, ergibt die Operation ${}_{\bar{G}}X$ von $\bar{G}$ auf X, die dieselben Bahnen hat. Es gilt also auch folgendes:

1.6.13 Folgerung *Wenn X eine endliche G–Menge definiert, dann gelten die folgenden Identitäten:*

$$|G\backslash\!\backslash X| = \frac{1}{|\bar{G}|}\sum_{\bar{g}\in\bar{G}} |X_{\bar{g}}| = \frac{1}{|\bar{G}|}\sum_{\bar{g}\in\bar{\mathfrak{C}}} |C^{\bar{G}}(\bar{g})||X_{\bar{g}}| = \sum_{\bar{g}\in\bar{\mathfrak{C}}} \frac{|X_{\bar{g}}|}{|C_{\bar{G}}(\bar{g})|},$$

wobei $\bar{\mathfrak{C}}$ eine Transversale der Konjugiertenklassen von $\bar{G}$ bedeutet.

Übungen

Ü 1.6.1 Zeigen Sie, daß G_x wirklich eine Untergruppe von G ist.

Ü 1.6.2 Sei ${}_GX$ eine endliche und transitive Operation, $x \in X$. Beweisen Sie

$$|G_x\backslash\!\backslash X| = \frac{1}{|G|}\sum_{g\in G} |X_g|^2.$$

1.7 Symmetrietypen von Abbildungen

Wir wollen jetzt einen recht allgemeinen Ansatz betrachten, der viele Beispiele diskreter Strukturen abdeckt, unter anderen umfaßt er die Endofunktionen, Graphen, Multigraphen, gerichtete Graphen, lineare Codes und vieles andere mehr. Hierzu werden wir Operationen einführen, die sich aus vorgegebenen Operationen ${}_GX$ und ${}_HY$ auf der Menge

$$Y^X := \{f \mid f : X \to Y\}$$

aller Abbildungen von X nach Y auf natürliche Weise ergeben:

1.7.1 Beispiel Operiert G auf X und H auf Y, dann operieren G, H und $H \times G$ kanonisch auf Y^X :

- $G \times Y^X \to Y^X : (g, f) \mapsto f \circ \bar{g}^{-1}$, d.h. (g, f) wird abgebildet auf $\tilde{f}$, *mit*
$$\tilde{f}(x) := \left(f \circ \bar{g}^{-1}\right)(x) = f(g^{-1}x).$$
- $H \times Y^X \to Y^X : (h, f) \mapsto \bar{h} \circ f$, *d.h.* (h, f) *wird abgebildet auf* $\tilde{f}$, *wobei*
$$\tilde{f}(x) := \left(\bar{h} \circ f\right)(x) = hf(x).$$
- $(H \times G) \times Y^X \to Y^X : ((h, g), f) \mapsto \bar{h} \circ f \circ \bar{g}^{-1}$, *d.h.* $((h, g), f)$ *wird abgebildet auf* $\tilde{f}$, *definiert durch*
$$\tilde{f}(x) := \left(\bar{h} \circ f \circ \bar{g}^{-1}\right)(x) = hf(g^{-1}x).$$

Es gibt eine vierte Operation, die die vorstehenden drei Operationen verallgemeinert. Um sie zu beschreiben, brauchen wir das *Kranzprodukt* $H \wr_X G$: Seine Grundmenge ist

$$H \wr_X G := H^X \times G = \{(\psi, g) \mid \psi : X \to H, g \in G\},$$

und die Multiplikation ist definiert durch

$$(\psi, g)(\psi', g') := (\psi\psi'_g, gg'),\ \ \psi\psi'_g(x) := \psi(x)\psi'_g(x) := \psi(x)\psi'(g^{-1}x).$$

$H \wr_X G$ operiert in folgender Weise kanonisch auf Y^X:

1.7.2 $$H \wr_X G \times Y^X \to Y^X : ((\psi, g), f) \mapsto \tilde{f},$$

wobei $\tilde{f}$ definiert wird durch $\tilde{f}(x) := \psi(x)f(g^{-1}x)$.

◇

Die Bahnen von $G, H, H \times G$ und $H \wr_X G$ auf Y^X nennen wir *Symmetrietypen von Abbildungen.* Die Operation von G, H, und $H \times G$ auf Y^X die oben eingeführt wurden, sind also tatsächlich Einschränkungen der Operation von $H \wr_X G$ auf Y^X.

1.7.3 Beispiele Wir hatten uns bereits überlegt, daß numerierte Graphen mit der Menge M als Punktemenge auch als Abbildungen von der Menge $\binom{M}{2}$ aller Punktepaare in die Menge $\{0,1\}$ aufgefaßt werden können. Wir können die Menge *aller numerierten Graphen auf M* demnach mit der Menge von Abbildungen

$$Y^X := 2^{\binom{M}{2}} = \mathcal{G}[M]$$

identifizieren, und die Menge *aller unnumerierten Graphen auf einer Punktmenge der Ordnung $|M|$* demnach mit der Menge von Symmetrietypen

$$S_M \backslash\!\backslash 2^{\binom{M}{2}}.$$

Ganz entsprechend können die numerierten k-Multigraphen, das sind die Multigraphen mit maximaler Kantenvielfachheit k, mit der Menge

$$(k+1)^{\binom{M}{2}}$$

der Abbildungen in die Menge $k+1 = \{0,1,\ldots,k\}$ der möglichen Vielfachheiten identifiziert werden. Die entsprechenden unnumerierten k-Multigraphen bilden dann die Bahnenmenge

$$S_M \backslash\!\backslash (k+1)^{\binom{M}{2}}.$$

Um die gerichteten Graphen zu definieren, also die Graphen mit gerichteten Kanten, aber ohne Schleifen und ohne Parallelkanten, ersetzen wir die Menge $\binom{M}{2}$ der ungeordneten Paare durch die Menge $M^2 - M$ der Paare aus verschiedenen Elementen. Die Menge dieser unnumerierten gerichteten Graphen, oder auch *Digraphen,* ist dann die Bahnenmenge

$$S_M \backslash\!\backslash 2^{M^2-M}.$$

Interessant sind auch die sogenannten *Halsketten,* das sind die Färbungen der Ecken eines regelmäßigen n-Ecks, mit der darauf operierenden zyklischen Gruppe C_n oder der Diedergruppe D_n, also die Menge der Bahnen einer dieser Gruppen auf der Menge F^n der Abbildungen von $n = \{0, \ldots, n-1\}$ in die Menge F der betrachteten Farben. Die Typen von Halsketten bzgl. C_n bilden also die Bahnenmenge

$$C_n \backslash\!\backslash F^n.$$

Eine weitere wichtige Klasse diskreter Strukturen bilden die sogenannten Schaltfunktionen, das sind die Abbildungen von der Menge 2^n aller 0-1-Folgen der Länge n in die Menge $\{0, 1\}$, es handelt sich hierbei also um

$$Y^X := 2^{(2^n)}.$$

Hier stellt sich die Frage, wieviele wesentlich verschiedene Schaltfunktionen es gibt, wenn man noch berücksichtigt, daß die n-Tupel vor der Eingabe noch permutiert und/oder deren Einträge lokal komplementiert werden können. Diese Operationen werden durch ein Kranzprodukt $S_2 \wr_n S_n$ beschrieben, das auf dem Definitionsbereich 2^n operiert. Die Äquivalenzklassen dieser Schaltfunktionen bilden also die Bahnenmenge

$$S_2 \wr_n S_n \backslash\!\backslash 2^{(2^n)}.$$

Ein weites Feld von Anwendungen besitzen die 0-1-Matrizen und geeignete Operationen auf diesen, können solche Matrizen doch als *Inzidenzstrukturen* angesehen werden, die Zeilen etwa als Punkte, die Spalten als Geraden. Spielen die Numerierungen von Punkten und Geraden, wie meist, keine Rolle, dann geht es dabei also um die Bahnenmenge

$$S_m \times S_n \backslash\!\backslash 2^{m \times n}.$$

Man kann aber auch das Kranzprodukt $S_m \wr_n S_n$ hierauf operieren lassen. Dazu gehen wir von der folgenden Operation von $S_m \wr_n S_n$ auf $m \times n$ aus:

$$S_m \wr_n S_n \times (m \times n) \to (m \times n) \colon ((\psi, \beta), (i, j)) \mapsto (\psi(\beta j) i, \beta j).$$

Diese Operation induziert auf der Menge von Abbildungen $2^{m \times n}$ die Operation (vgl.1.7.1):

1.7.4 $S_m \wr_n S_n \times 2^{m \times n} \to 2^{m \times n} \colon ((\psi, \beta), (a_{ik})) \mapsto (a_{\psi(j)^{-1} i, \beta^{-1} j}).$

Wegen $(\psi, \beta) = (\psi, 1)(\iota, \beta)$, können wir diese Operation auch in zwei Schritten vollziehen:

$$(a_{ij}) \longmapsto (a_{i, \beta^{-1} j}) \longmapsto (a_{\psi^{-1}(j) i, \beta^{-1} j}).$$

D.h. wir können zunächst die Spalten von (a_{ij}) derart permutieren, daß die Anzahlen der Einsen in denen Spalten der resultierenden Matrix von links nach rechts nicht anwächst: $\sum_i a_{i,\beta^{-1}1} \geq \sum_i a_{i,\beta^{-1}2} \geq \ldots$ Nachdem wir dies ausgeführt haben mit Hilfe einer geeigneten Permutation β, können wir noch ein ψ finden, das die Einsen jeder Spalte bündig nach oben verschiebt. Dies beweist, daß die Bahn von (a_{ij}) unter $S_m \wr_n S_n$ durch ein Element der folgenden Form charakterisiert wird:

$$\begin{pmatrix} 1 & \ldots & \ldots & \ldots & 1 & & \\ \vdots & & & \iddots & & & \\ 1 & \ldots & 1 & & & & \\ & & & & & & 0 \end{pmatrix} \in 2^{m \times n},$$

also durch eine Partition der Anzahl der Einsen in der Matrix (a_{ik}). $\diamond$

Wir wollen jetzt die oben angeführten Symmetrietypen von Abbildungen abzählen. Dazu werden wir zunächst die Anzahlen der Bahnen von $H \wr_X G$ auf Y^X bestimmen und das Ergebnis dann auf die zu $G, H, H \times G$ isomorphen Untergruppen einschränken. Und um nun die Bahnen des Kranzprodukts auf ökonomische Weise abzuzählen, benutzen wir die Tatsache, daß die Anzahl der Bahnen konstant auf den Konjugiertenklassen von Elementen ist. Wir werden deshalb zunächst einen Spezialfall eines Kranzprodukts betrachten, dessen Konjugiertenklassen wohlbekannt sind.

Uns ist schon das Kranzprodukt $H \wr_X G$ begegnet, wobei G eine Gruppe ist, die auf X operiert, während H auf Y wirkt. Betrachten wir jetzt den Spezialfall, bei dem G eine Permutationsgruppe ist, etwa $G \leq S_n$, und wo wir für ${}_G X$ die natürliche Operation von G auf $\underline{n}$ nehmen. In diesem Fall kürzen wir die Bezeichnungsweise wie folgt ab:

$$H \wr G := H \wr_n G.$$

Ein Spezialfall hiervon ist die $H \wr S_n$, die *volle monomiale Gruppe* vom Grad n über H. Viele wichtige Gruppen sind von dieser Form, und für diese Gruppen können wir leicht die Konjugiertenklassen bestimmen. Betrachten wir ein Element $(\psi, \beta) \in H \wr S_n$ und nehmen wir an, daß $C^1, C^2, \ldots$ die Konjugiertenklassen von H sind. Ist jetzt

$$\beta = \prod_\nu (j_\nu \ldots \beta^{l_\nu - 1} j_\nu),$$

die Standardzyklenschreibweise (d.h. $j_\nu \leq \beta^k j_\nu$, für alle k und $j_\nu < j_{\nu+1} < \ldots$), dann können wir deren ν-tem zyklischem Faktor $(j_\nu \ldots \beta^{l_\nu -1} j_\nu)$ das Element

1.7.5 $h_\nu(\psi, \beta) := \psi(j_\nu)\psi(\beta^{-1} j_\nu) \cdots \psi(\beta^{-l_\nu+1} j_\nu) = \psi \cdots \psi_{\beta^{l_\nu -1}}(j_\nu)$

von H zuordnen. Es heißt das *ν-te Zykelprodukt* zu (ψ, β).
Um jetzt die gewünschten Anzahlen von Symmetrietypen von Abbildungen herzuleiten, charakterisieren wir die Fixpunkte jedes (ψ, g) in $H \wr_X G$ auf Y^X und dann benutzen wir die folgenden natürlichen Einbettungen von G, H und $H \times G$ in $H \wr_X G$:

$$G \hookrightarrow H \wr_X G \colon g \mapsto (\iota, g),$$

wobei $\iota \colon X \to H \colon x \mapsto 1_H$,

$$H \hookrightarrow H \wr_X G \colon h \mapsto (\psi, 1_G),$$

wobei ψ die konstante Funktion mit dem Wert h sei.

$$H \times G \hookrightarrow H \wr_X G \colon (h, g) \mapsto (\psi, g),$$

wobei wieder ψ die konstante Funktion mit dem Wert h ist.
Der folgende Hilfssatz ist für die nachfolgenden Anwendungen des Lemmas von Cauchy-Frobenius von entscheidender Bedeutung:

1.7.6 Hilfssatz *Wir betrachten ein $f \in Y^X$, ein Element (ψ, g) von $H \wr_X G$ und nehmen an, daß*

$$\bar{g} = \prod_{\nu=1}^{c(\bar{g})} (x_\nu \, g x_\nu \ldots g^{l_\nu -1} x_\nu)$$

die Zerlegung von $\bar{g}$ in disjunkte Zyklen sei. Dann ist f ein Fixpunkt von (ψ, g) genau dann, wenn die folgenden beiden Bedingungen gelten:

- *Jedes $f(x_\nu)$ ist ein Fixpunkt des Zykelprodukts $h_\nu(\psi, g)$:*

$$f(x_\nu) \in Y_{h_\nu(\psi, g)}.$$

- *Die anderen Werte von f entstehen aus den Werten $f(x_\nu)$ entsprechend den folgenden Gleichungen:*

$$f(x_\nu) = \psi(x_\nu) f(g^{-1} x_\nu) = \psi(x_\nu)\psi(g^{-1} x_\nu) f(g^{-2} x_\nu) = \ldots \; .$$

Beweis: 1.7.2 besagt, daß f genau dann unter (ψ, g) fest bleibt, wenn seine Werte $f(x)$ den folgenden Gleichungen genügen.

$$f(x) = \psi(x)f(g^{-1}x) = \psi(x)\psi(g^{-1}x)f(g^{-2}x)\ldots$$

$$\ldots = \psi(x)\psi(g^{-1}x)\ldots\psi(g^{-l+1}x)f(x).$$

Dabei bedeutet l die Länge des zyklischen Faktors von $\bar{g}$, der den Punkt $x \in X$ enthält. Also muß insbesondere folgendes gelten:

$$f(x_\nu) = h_\nu(\psi, g)f(x_\nu),$$

d.h. $f(x_\nu)$ muß ein Fixpunkt von $h_\nu(\psi, g)$ sein, wie behauptet. Also hat jedes feste $f \in Y^X$, die behaupteten Eigenschaften, und umgekehrt.

□

Dies liefert, zusammen mit dem Lemma von Cauchy-Frobenius, die Anzahl der $H \wr_X G$–Bahnen auf Y^X, und die Einschränkungen auf die Einbettungen von G, H und $H \times G$ geben die Anzahlen von G–, H– und $H \times G$–Bahnen von Y^X:

1.7.7 Satz *Sind sowohl $_GX$ als auch $_HY$ endliche Operationen, dann erhalten wir den folgenden Ausdruck für die Gesamtzahl der Bahnen der entsprechenden Operation vom $H \wr_X G$ auf Y^X:*

$$|H \wr_X G \backslash\backslash Y^X| = \frac{1}{|H|^{|X|}|G|} \sum_{(\psi,g)\in H\wr_X G} \prod_{\nu=1}^{c(\bar{g})} |Y_{h_\nu(\psi,g)}|.$$

Die Einschränkung auf die Einbettungen von G, H und $H \times G$ ergibt:

$$|G \backslash\backslash Y^X| = \frac{1}{|G|} \sum_{g\in G} |Y|^{c(\bar{g})}, \ \ |H \backslash\backslash Y^X| = \frac{1}{|H|} \sum_{h\in H} |Y_h|^{|X|},$$

und

$$|(H \times G) \backslash\backslash Y^X| = \frac{1}{|H||G|} \sum_{(h,g)\in H\times G} \prod_i |Y_{h^i}|^{a_i(\bar{g})}.$$

Hiermit können wir auch Typenreihen berechnen, betrachten wir als Beispiel die Spezies Endofunktionen. Die symmetrische Gruppe S_M operiert auf $End[M]$, wie wir wissen, in folgender Weise:

$$S_M \times End[M] \to End[M]: (\beta, \epsilon) \mapsto \beta\epsilon\beta^{-1}.$$

Die Typen von Endofunktionen auf M sind also die Bahnen der Diagonale $\Delta(H \times G) := \Delta(S_M \times S_M)$, auf der Menge $Y^X := M^M$ der Endofunktionen auf M. Die gesuchten Koeffizienten der Monome der Typenfunktion sind demnach — wir benutzen die Einschränkung der letzten Formel aus Satz 1.7.7 auf die Diagonale — die Ordnungen von Bahnenmengen

$$|\Delta(S_M \times S_M)\backslash\backslash M^M| = \frac{1}{|M|!}\sum_{\beta \in S_M}\prod_i |M_{\beta^i}|^{a_i(\beta)} = \sum_a \prod_i \frac{|M_{\beta^i}|^{a_i(\beta)}}{i^{a_i} a_i!}.$$

(Die letzte Identität folgt mit der bekannten Charakterisierung der Konjugiertenklassen symmetrischer Gruppen und der Formel für deren Ordnungen.) Die rechte Seite dieser Gleichung ergibt, wenn wir über die Zykeltypen von $|M|$ summieren, den Koeffizienten von $x^{|M|}$ in der gesuchten Typenreihe $\widetilde{End}(x)$.

Übungen

Ü 1.7.1 Beweisen Sie durch Betrachtung geeigneter Operationen die folgenden Tatsachen:

- $\forall\ n \in \mathbb{N}^* : \ \sum_{d|n} \phi(d) = n.$
- $\forall$ Primzahl $p: \ (p-1)! \equiv -1\ (p)$ (Wilson).
- $\forall z \in \mathbf{Z}, p$ Primzahl, $n \in \mathbb{N}^* : \ z^{(p^n)} \equiv z^{(p^{n-1})}\ (p^n).$
- $\forall z \in \mathbf{Z}, n \in \mathbb{N}^*$ so daß $\mathrm{ggT}(z,n) = 1 : \ z^{\phi(n)} \equiv 1\ (n)$ (Euler).

1.8 Beispiele: Graphen, lineare Codes

Um diese Resultate über die Anzahlen von Symmetrietypen von Abbildungen jetzt auf Spezialfälle anzuwenden, bleibt jeweils $c(\bar{g})$, $|Y_h|$, $|Y_{h^i}|$ oder $|Y_{h_\nu}(\psi, g)|$ zu berechnen, was ziemlich mühsam sein kann, wie das folgende Beispiel zeigt.

1.8.1 Beispiele Wir würden gerne aus 1.7.7 eine Formel für die Anzahl der Graphen auf v Punkten herleiten. Dazu müssen wir die Anzahlen der zyklischen Faktoren von $\bar{\beta}$, derjenigen Permutation also, die von $\beta \in S_v$ auf der Menge aller Paare von Punkten induziert wird, aus dem Zykeltyp von β berechnen.

1.8.2 Hilfssatz *Ist $\beta \in S_v$, dann gilt:*

- *Jeder i-Zyklus von β, i ungerade, trägt zu $\bar{\beta}$ genau $(i-1)/2$ zyklische Faktoren bei, jeder von diesen ist ein i-Zyklus.*
- *Jeder i-Zyklus von β, i gerade, trägt zu $\bar{\beta}$ genau einen Zyklus der Länge $i/2$ bei, sowie $(i/2)-1$ weitere Zyklen, von denen jeder die Länge i hat.*
- *Jedes Paar zyklischer Faktoren von β, etwa ein i-Zyklus und ein j-Zyklus, trägt zu $\bar{\beta}$ genau $ggT(i, j)$ zyklische Faktoren bei. Jeder von diesen hat die Länge $kgV(i, j)$.*
- *Alle zyklischen Faktoren von $\bar{\beta}$ entstehen auf diese Weise.*

Beweis:
i) Sei i ungerade. Ohne Einschränkung der Allgemeinheit können wir annehmen, daß der betrachtete i-Zyklus gleich $(0, \ldots, i-1)$ ist. Wir betrachten ein $k < (i-1)/2$ und die Wirkung von $(0 \ldots i-1)$ auf das Punktepaar $\{0, k\}$. Es zeigt sich dabei, daß $\bar{\beta}$ die folgende zyklische Permutation von 2-Mengen enthält:

$$(\{0, k\}, \{1, k+1\}, \ldots, \{i-k-1, i-1\}, \{1-1, i-k\}, \ldots, \{k-1, i-1\}).$$

Dieser Zyklus hat die Länge i, und die Zyklen dieser Form, die aus verschiedenen $k < (i-1)/2$ entstehen, sind paarweise disjunkt. Hinzukommt, daß dies sämtliche zyklische Faktoren sind, die aus $(0, \ldots, i-1)$ entstehen, denn wir haben für jedes solche k, weil i ungerade ist:

$$(\{0, k\}, \{1, k+1\}, \ldots) = (\{0, i-k\}, \{1, i-k+1\}, \ldots).$$

ii) Ist i gerade, etwa $i = 2j$, dann können wir annehmen, daß der zyklische Faktor von β gleich $(0 \dots 2j-1)$ ist. Er liefert, für $1 \leq k \leq j-1$, die $(i/2)-1$ verschiedenen i-Zyklen

$$(\{0,k-1\},\{1,k\},\dots,\{i-k,i-1\},\{0,i-k+1\},\dots,\{k-2,i-1\}),$$

sowie den $(i/2)$-Zyklus

$$(\{0,j\},\dots,\{j-1,2j-1\}).$$

iii) Ein Paar zyklischer Faktoren von β, etwa $(0...i-1)(i...i+j-1)$ trägt zu $\bar{\beta}$ das folgende Produkt disjunkter Zyklen bei:

$$(\{0,i+k-1\},\{1,i+k\},\dots)(\{0,i+k\},\{1,i+k+1\},\dots)\dots$$

Die Länge dieser zyklischen Faktoren ist $\mathrm{kgV}(i,j)$, und die Anzahl ist deshalb gleich $\mathrm{ggT}(i,j)$.
iv) ist klar.

□

Dieser Hilfssatz ergibt die Zykelstruktur von $\bar{\beta}$ und infolgedessen auch die gesuchte Anzahl $c(\bar{\beta})$ zyklischer Faktoren, die wir für eine Berechnung der Anzahl der Graphen mit v Punkten gemäß dem Lemma von Cauchy-Frobenius benötigen:

1.8.3 Folgerung *Für jedes $\bar{\beta}$ auf der Menge der Punktepaare haben wir:*

- *Ist i ungerade, dann gilt*

$$a_i(\bar{\beta}) = \frac{a_i(\beta)}{2}(ia_i(\beta)-1)+a_{2i}(\beta)+\sum_{\substack{r<s\\ kgV(r,s)=i}} a_r(\beta)a_s(\beta)ggT(r,s).$$

- *Ist i gerade, dann haben wir*

$$a_i(\bar{\beta}) = \frac{a_i(\beta)}{2}(ia_i(\beta)-2)+a_{2i}(\beta)+\sum_{\substack{r<s\\ kgV(r,s)=i}} a_r(\beta)a_s(\beta)ggT(r,s).$$

- *Die Gesamtanzahl zyklischer Faktoren von Permutationen $\bar{\beta}$, die von Permutationen β vom Typ a auf der Menge der Punktepaare induziert werden, ist demnach*

$$c(\bar{a}) = \frac{1}{2}\sum_i i\cdot a_i(\beta)^2 - \frac{1}{2}\sum_{i\ odd} a_i(\beta) + \sum_{r<s} a_r(\beta)a_s(\beta)ggT(r,s).$$

Also erhalten wir, mit einer Anwendung des Lemmas von Cauchy-Frobenius:

1.8.4 Folgerung *Die Anzahl der k-Graphen auf v Punkten ist*

$$\frac{1}{v!}\sum_{\beta\in S_v}(k+1)^{c(\bar{\beta})},$$

wobei $c(\bar{\beta})$ wie oben definiert ist. Ausführlicher formuliert, mit Hilfe der Zykeltypen von v ergibt sich diese Anzahl zu

$$\sum_{a\vdash v}\frac{(k+1)^{c_a}}{\prod_i i^{a_i}a_i!},\quad wobei\ c_{\bar{a}} := \frac{1}{2}\sum_i i\cdot a_i^2 - \frac{1}{2}\sum_{i\ odd} a_i + \sum_{r<s} a_r a_s ggT(r,s),$$

die Anzahl der zyklischen Faktoren von $\bar{\beta}$, β von Typ a. Die Typenreihe der Spezies Graphen ist demnach

$$\widetilde{\mathcal{G}}(x) = \sum_{v>0}\left(\sum_{a\vdash v}\frac{(k+1)^{c_a}}{\prod_i i^{a_i}a_i!}\right)\cdot x^v.$$

Eine Tabelle mit den ersten dieser Anzahlen ist:

$v\backslash k$	0	1	2	3	4
1	1	1	1	1	1
2	1	2	3	4	5
3	1	4	10	20	35
4	1	11	66	276	900
5	1	34	792	10688	90005
6	1	156	25506	1601952	43571400

◇

Ein typisches Beispiel einer *Kranzproduktoperation* zeigt sich in der Theorie fehlerkorrigierender *linearer Codes*. Ein linearer Code ist ein Unterraum eines endlichen Vektorraums, etwa des n-dimensionalen Vektorraums über dem Galoisfeld $GF(q)$, der mit der folgenden Menge von Abbildungen identifiziert werden kann:

$$Y^X := GF(q)^n.$$

Die Gesamtheit aller (n,k)-*Codes über* $GF(q)$ ist die Menge $\mathcal{U}(n,k,q)$ der Unterräume der Dimension k. Solche linearen Codes sind sehr nützlich, vor allem dienen sie als *fehlerkorrigierende Codes*. Da die Fehler, um die es hierbei geht, *Übertragungsfehler* sind, also Fehler, die einzelne Komponenten übertragener Codevektoren verfälschen, führen wir eine adäquate Metrik ein: Für Vektoren v und w auf $GF(q)^n$ setzen wir

$$d(v,w) := |\{i \mid v_i \neq w_i\}|,$$

und nennen diese Anzahl verschiedener Koordinaten die *Hamming-distanz* von v und w. Ein wichtiger Indikator für die Qualität eines fehlerkorrigierenden Codes C ist seine *Minimaldistanz*

$$d := \min\{d(c,0) \mid c \in C - \{0\}\}.$$

Ein (n,k)-Code über $GF(q)$ mit dieser Minimaldistanz heißt dann kurz auch *(n,k,d)-Code.* Der entscheidende Punkt in der Theorie linearer Codes ist die Tatsache, daß ein (n,k,d)-Code C *in der Lage ist, bis zu $\lfloor (d-1)/2 \rfloor$ Übertragungsfehler auf folgende Weise zu korrigieren.* Nehmen wir an, das Codewort $c \in C$ sei übertragen worden, eventuell fehlerhaft, der empfangene Vektor sei $v \in GF(q)^n$. Dann können wir diesen empfangenen Vektor in einen der (bzgl. Hamming-Distanz) nächstliegenden Codevektor decodieren. Sind bei der Übertragung tatsächlich nicht mehr als $\lfloor (d-1)/2 \rfloor$ Koordinaten verfälscht worden, dann gibt es genau einen nächstliegenden Codevektor, und dieser ist gerade c. Diese sogenannte *Maximum-likelihood-Decodierung* führt also zum Original zurück, die aufgetretenen Fehler sind richtig korrigiert worden.

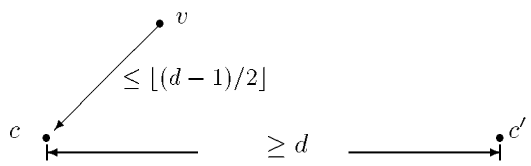


Abbildung 1.1: Die Maximum-Likelihood-Decodierung

Die Qualität eines (n,k)-Codes hängt deshalb vor allem von der Minimaldistanz d ab.
Um einen Überblick über die interessanten linearen Codes zu erhalten, die in $GF(q)^n$ liegen, führen wir jetzt eine geeignete Äquivalenzrelation auf der Gesamtheit aller Codes ein. Und da wir Codes anhand metrischer Eigenschaften unterscheiden, tun wir dies durch

Benutzung der Gruppe aller *Isometrien* von $GF(q)^n$. Diese besteht aus den Matrizen, die in jeder ihrer n Zeilen und Spalten genau einen von 0 verschiedenen Eintrag enthalten. Man kann nämlich leicht sehen, daß die einzigen Isometrien *simultane Permutationen der Koordinaten* der Vektoren sind, *zusammen mit simultanen Multiplikationen von Koordinaten mit von 0 verschiedenen Körperelementen.* Diese Gruppe ist gerade das Kranzprodukt

$$H \wr_X G := GF(q)^* \wr S_n$$

aus der multiplikativen Gruppe $GF(q)^*$ des Grundkörpers und der symmetrischen Gruppe. Wir wiederholen deshalb die Operation auf $GF(q)^n$ (vgl. 1.7.2), sie zeigt, daß die Wirkung von (ψ, π) tatsächlich aus einer Permutation der Koordinaten und Multiplikationen von Koordinaten mit von Null verschiedenen Elementen des Grundkörpers besteht:

$$(\psi, \pi)(a_0, \ldots, a_{n-1}) := (\psi(0)a_{\pi^{-1}0}, \ldots, \psi(n-1)a_{\pi^{-1}(n-1)}).$$

Zwei lineare Codes sind genau dann *metrisch äquivalent*, und damit codierungstheoretisch von derselben Qualität, wenn sie isometrisch sind. Die Menge der Äquivalenzklassen linearer Codes ist also gerade die Menge aller Bahnen der Isometriegruppe auf dem Verband aller Unterräume von $GF(q)^n$, die Grundmenge dieses Verbands ist die disjunkte Vereinigung der Mengen $\mathcal{U}(n,k,q)$ aus den Unterräumen der Dimensionen k ist, $0 \leq k \leq n$:.

$$\mathcal{L}(n,q) = \bigcup_k \mathcal{U}(n,k,q)$$

Da die Isometriegruppe die Dimension eines Unterraums erhält, kann nach der Dimension der Unterräume aufgegliedert werden:

1.8.5 $$GF(q)^* \wr S_n \backslash\!\backslash \mathcal{L}(n,q) = \bigcup_k GF(q)^* \wr S_n \backslash\!\backslash \mathcal{U}(n,k,q).$$

Wir haben damit folgendes bewiesen:

1.8.6 Die metrische Klassifizierung der linearen Codes *Die Isometrieklassen linearer (n,k)-Codes über $GF(q)$ sind die Bahnen*

$$GF(q)^* \wr S_n \backslash\!\backslash \mathcal{U}(n,k,q).$$

Es geht also um die Ermittlung von Transversalen dieser Bahnenmengen. Hier stoßen wir jedoch auf ein schwerwiegendes Problem, denn die Mengen $\mathcal{U}(n,k,q)$, auf denen die Isometriegruppe operiert, sind zu abstrakt um nach dem gegenwärtigen Stand der Programmiertechnik ohne weiteres auf einem Computer verarbeitet werden zu können. Wir müssen deshalb Basen einführen und die Vektorräume durch Generatormatrizen ersetzen, d.h. durch Matrizen, deren Zeilen eine Basis des in Frage stehenden Unterraums bilden. Leider ist diese Menge

$$GF(q)_k^{k\times n} := \{A \in GF(q)^{k\times n} \mid Rang(A) = k\} =: ((GF(q)^k)^n)_k$$

aller solchen Generatormatrizen (also aller $k \times n$-Matrizen vom Rang k) recht groß, und es kommt hinzu, daß wir auch die operierende Gruppe vergößern müssen, denn Vektorräume besitzen im allgemeinen mehrere Basen. Aus diesem Grund müssen wir die Isometriegruppe mit der vollen linearen Gruppe $GL_k(q)$ multiplizieren, diese wirkt nämlich transitiv auf der Menge $((GF(q)^k)^n)_k$. Insgesamt haben wir damit folgende Konkretisierung erreicht:

1.8.7 Folgerung *Ein Repräsentantensystem der Isometrieklassen von (n,k)-Codes über $GF(q)$ wird von jeder Transversale der Bahnenmenge*

$$GL_k(q) \times GF(q)^* \wr S_n \backslash\backslash ((GF(q)^k)^n)_k$$

erzeugt.

Dies eröffnet eine Möglichkeit, vollständige Listen von linearen Codes zu erzeugen. Dies ist natürlich nur für kleine n durchführbar. Wesentlich weiter kommt man, wenn man mit den Anzahlen solcher Codes zufrieden ist. Hierfür eignet sich die im folgenden beschriebene *rekursive Methode* (Slepian, Fripertinger). Sie vermeidet die Rangbedingung bei der betrachteten Menge von Matrizen, anstelle von $GF(q)_k^{k\times n}$ wird $GF(q)^{k\times n}$ benutzt, und man setzt

$$t_{n,k,q} := |GL_k(q) \times GF(q)^* \wr S_n \backslash\backslash (GF(q)^k)^n|.$$

Da man den Codes, die zu Bahnen auf Matrizen von kleinerem Rang gehören, schon bei den Exponenten $l < k$ begegnet ist, gilt

1.8.8 Folgerung *Die Anzahl der Isometrieklassen von (n,k)-Codes über $GF(q)$ ist*

$$c_{n,k,q} := t_{n,k,q} - t_{n,k-1,q},$$

mit der Anfangsbedingung $t_{n,1,q} = 1$.

Die Anwendung des Cauchy-Frobenius Lemmas auf diese Situation ist jedoch für $q \neq 2$ keineswegs einfach (vgl. H.Fripertinger [3]). Einige interessante Aussagen ergiben sich noch, wenn man folgende Lemmata verwendet:

1.8.9 Hilfssatz *Die Operation eines direkten Produkts $H \times G$ auf einer Menge M, ergibt eine natürliche Operation des Faktors H auf der Menge der Bahnen von G:*

$$H \times (G \backslash\backslash M) \to G \backslash\backslash M : (h, G(m)) \mapsto G(hm),$$

sowie eine natürliche Operation von G auf den Bahnen von H:

$$G \times (H \backslash\backslash M) \to H \backslash\backslash M : (g, H(m)) \mapsto H(gm).$$

Darüberhinaus besteht die Bahn von $G(m) \in G \backslash\backslash M$ unter H aus den Bahnen von G auf M, die $(H \times G)(m)$ bilden, während die Bahn von $H(m) \in H \backslash\backslash M$ unter G die Menge ist, die aus den Bahnen von H auf M bestehen, welche $(H \times G)(m)$ bilden. Es gilt demnach u.a. die folgende Identität:

$$|H \backslash\backslash (G \backslash\backslash M)| = |G \backslash\backslash (H \backslash\backslash M)| = |(H \times G) \backslash\backslash M|.$$

□

Insbesondere kann also jede Operation der Form ${}_{H \times G}Y^X$ als Operation von H auf $G \backslash\backslash Y^X$ betrachtet werden oder auch als Operation von G auf $H \backslash\backslash Y^X$. Für unser Problem der Abzählung von linearen Codes ergibt dies die Bijektivität von $GL_k(q) \times GF(q)^* \wr S_n \backslash\backslash (GF(q)^k)^n$ und

$$GL_k(q) \backslash\backslash GF(q)^* \wr S_n \backslash\backslash (GF(q)^k)^n.$$

Das entsprechende Resultat für Kranzprodukte stammt von W. Lehmann:

1.8.10 Hilfssatz *Die folgende Abbildung ist eine Bijektion:*

$$\Phi : H \wr_X G \backslash\backslash Y^X \to G \backslash\backslash (H \backslash\backslash Y)^X : H \wr_X G(f) \mapsto G(F),$$

wenn $F \in (H \backslash\backslash Y)^X$ definiert wird durch $F(x) := H(f(x))$. Insbesondere ist also

$$|H \wr_X G \backslash\backslash Y^X| = |G \backslash\backslash \left(H \backslash\backslash Y)^X\right)|.$$

Beweis: Es ist leicht einzusehen, daß Φ wohldefiniert ist. Zum Nachweis der Injektivität von Φ sei $G(F) = G(F')$, etwa $F' = F \circ \bar{g}^{-1}$. Dies impliziert

$$H(f'(x)) = F'(x) = F(g^{-1}x) = H(f(g^{-1}x)),$$

für jedes $x \in X$. Demnach muß, für jedes x, ein $\psi(x)$ existieren mit $f'(x) = \psi(x)f(g^{-1}x)$. Fassen wir zusammen, dann gilt es also $(\psi, g) \in H \wr_X G$ mit $f' = (\psi, g)f$, es gilt also $H \wr_X G(f) = H \wr_X G(f')$, und das war zu zeigen.
Um nachzuweisen, daß Φ surjektiv ist, nehmen wir an, daß $G(F) \in G\backslash\!\backslash(H\backslash\!\backslash Y)^X$, also $F \in (H\backslash\!\backslash Y)^X$. Dann ist also, für jedes $x \in X$, $F(x) \in H\backslash\!\backslash Y$. Wir wählen ein Element y_x aus dieser Bahn, so daß also hierfür gilt $F(x) = H(y_x)$, und wir tun dies für alle $x \in X$. Definieren wir jetzt mit Hilfe dieser Auswahl ein $f \in Y^X$ durch $f(x) := y_x$, dann gilt hierfür

$$H(f(x)) = H(y_x) = F(x),$$

dieses f ist also ein Urbild von F, und die Surjektivität von Φ ist damit bewiesen.

□

Dies erlaubt eine weitere Umformulierung unseres Abzählproblems: $GL_k(q) \times GF(q)^* \wr S_n\backslash\!\backslash(GF(q)^k)^n$ ist bijektiv zu

$$GL_k(q)\backslash\!\backslash S_n\backslash\!\backslash(GF(q)^*\backslash\!\backslash GF(q)^k)^n.$$

Offensichtlich können wir uns aus codierungstheoretischen Gründen auf Generatormatrizen beschränken, die keinerlei Spalte enthalten, die aus lauter Nullen besteht, denn Nullspalten der Generatormatrix bedeuten ja, daß es im Code Koordinaten gibt, die für alle Codevektoren gleich Null sind. Solche Koordinaten sind überflüssig, sie übertragen keine Information. Wir können uns deshalb auf die folgende Menge von Bahnen beschränken:

$$GL_k(q)\backslash\!\backslash S_n\backslash\!\backslash(GF(q)^*\backslash\!\backslash(GF(q)^k - \{0\}))^n.$$

Die innere Bahnenmenge der multiplikativen Gruppe kann (vergleiche 1.7.1 für die Operation) durch die Menge der Abbildungen in den projektiven Raum als $P_{k-1}(q)$ ersetzt werden, denn jede solche Bahn ist gerade ein eindimensionaler Unterraum. Wir erhalten also letztendlich die folgende Bahnenmenge:

1.8.11 $$GL_k(q)\backslash\!\backslash S_n\backslash\!\backslash P_{k-1}(q)^n.$$

Sie zeigt den engen Zusammenhang zwischen der Theorie der linearen Codes und der endlichen Geometrie. Die innere Bahnenmenge

$$S_n \backslash\!\backslash P_{k-1}(q)^n$$

kann genau angegeben werden: Zwei Funktionen $f, f' \in Y^X$ liegen genau dann in derselben Bahn von S_X, wenn sie dieselben Folgen von Vielfachheiten haben, mit denen sie die Werte y annehmen, also wenn

$$\forall\ y \in Y\colon |f^{-1}(y)| = |f'^{-1}(y)|.$$

Die Folge dieser Vielfachheiten werden wir später den Inhalt dieser Funktionen nennen. Interessante Spezialfälle solcher Inhalte sind die Funktionen vom Inhalt $1 = |f^{-1}(y)|$, für alle $y \in Y$. Solche Codes heißen *Simplex-Codes*. Es sind die zu den *Hamming-Codes* dualen Codes Aber darauf werden wir später zurückkommen.

1.9 Die Zyklenreihe

Wir wollen zunächst unsere Methoden differenzieren, um auch Bahnen mit vorgegebenen Eigenschaften abzählen zu können. Dazu führen wir eine Gewichtsfunktion auf $_GX$ ein, d.h. eine Abbildung von X in einen kommutativen Ring, die konstant ist auf den Bahnen von G auf X. Das Cauchy-Frobenius-Lemma wird dementsprechend zu einer Formel verfeinert, die die Anzahl von Bahnen mit vorgeschriebenen Gewicht angibt. Z.B. wird uns diese befähigen, Graphen mit vorgegebener Anzahl von Punkten auch nach Kantenzahl abzuzählen. Das Ergebnis ist eine erzeugende Funktion, die sich aus einem Polynom, dem sogenannten Zykelindex ergibt. Diesen Zykelindex werden wir dann verallgemeinern und schließlich werden wir als Summe verallgemeinerter Zykelindizes eine formale Potenzreihe erhalten, die sogenannte Zyklenreihe, sie verallgemeinert sowohl die Kardinalitätenals auch die Typenreihe.

In den vorangegangenen Paragraphen wurden Gruppenoperationen eingeführt, das Lemma von Cauchy-Frobenius wurde bewiesen und wir haben gewisse Operationen von Gruppen auf Mengen der Form Y^X im Detail untersucht. Wir sahen, daß verschiedene Strukturen wie unnumerierte Graphen und Isometrieklassen linearer Codes als Bahnen auf solchen Mengen von Abbildungen definiert werden können, so daß wir eine Methode an die Hand bekamen, die die *Gesamtanzahl* solcher Strukturen abzuzählen erlaubt. Jetzt entsteht die Frage, wie wir auch die *Anzahl von Bahnen mit gewissen vorgegebenen Eigenschaften* abzählen können, etwa die Anzahl der Graphen mit v Punkten und e Kanten. Die Antwort auf viele Fragen wird mit Hilfe eines *Gewichts* gegeben werden können, meist ist das eine Abbildung von der Menge, auf der die Gruppe operiert, in einen Polynomring über $\mathbb{Q}$. Das Endresultat wird dabei eine *erzeugende Funktion* für das gegebene Abzählproblem sein, d.h. wir werden ein multivariates Polynom erhalten, das die gewünschten Bahnenanzahlen als Koeffizienten seiner verschiedenen monomialen Summanden hat. Das grundlegende Hilfsmittel hierbei ist

1.9.1 Das Lemma von Cauchy-Frobenius, gewichtete Form
Sei $_GX$ eine endliche Operation und $w: X \to R$ eine Abbildung von X in einem kommutativen Ring, R der $\mathbb{Q}$ als Teilring enthält. Ist w konstant auf den Bahnen von G auf X, dann gilt, für jede Transver-

sale T der Bahnen,

$$\sum_{t\in T} w(t) = \frac{1}{|G|}\sum_{g\in G}\sum_{x\in X_g} w(x) = \frac{1}{|\bar{G}|}\sum_{\bar{g}\in\bar{G}}\sum_{x\in X_{\bar{g}}} w(x).$$

Beweis: Die folgenden Gleichungen sind offensichtlich richtig, die letzte von ihnen benutzt die Annahme, daßw konstant auf den Bahnen ist:

$$\sum_{g\in G}\sum_{x\in X_g} w(x) = \sum_{x}\sum_{g\in G_x} w(x)$$

$$= \sum_{x} |G_x| w(x) = |G| \sum_{x} |G(x)|^{-1} w(x) = |G| \sum_{t\in T} w(t).$$

Dies beweist die erste der behaupteten Gleichungen, die zweite folgt mit dem Homomorphiesatz.

□

Dieses Resultat impliziert 1.6.6 (man setze $w\colon x \mapsto 1$), das wir manchmal auch als *konstante Form* des Lemmas von Cauchy-Frobenius bezeichnen. Um 1.9.1 auf die Abzählung von Symmetrieklassen von Abbildungen f in Y^X anwenden zu können, führen wir zu gegebenem $W\colon Y \rightarrow R$, R ein kommutativer Ring mit $\mathbb{Q}$ als Teilring, das *multiplikative Gewicht* $w\colon Y^X \rightarrow R$ ein, das wie folgt definiert ist

1.9.2 $$w(f) := \prod_{x\in X} W(f(x)),$$

und wir bemerken, daß für endliche Operationen $_GX$ und $_HY$ das folgende richtig ist:

1.9.3 Folgerung *Ist W konstant auf den Bahnen von H auf Y, dann ist w konstant auf den Bahnen von $H \wr_X G$, $H \times G$, H und G auf Y^X. Darüber hinaus ist, für jedes W, die entsprechende multiplikative Gewichtsfunktion w konstant auf den Bahnen von G auf Y^X.*

Demnach können wir 1.9.1 anwenden, sobald wir die Summe der Gewichte all der f ermittelt haben, die fest bleiben unter $(\psi, g) \in H \wr_X G$. Diese Summe von Gewichten folgt direkt aus der Charakterisierung der Gesichtspunkte von (ψ, g) die in 1.7.6 gegeben wurde:

1.9.4 Folgerung *Mit derselben Bezeichnung wie in 1.7.6, und für ein (ψ, g) aus $H \wr_X G$, eine Funktion $W\colon Y \rightarrow R$ die konstant ist auf den*

Bahnen von H, und für die entsprechende multiplikative Gewichtsfunktion $w\colon Y^X \to R$, erhalten wir die Gleichung

$$\sum_{f\in Y^X_{(\psi,g)}} w(f) = \prod_\nu \sum_{y\in Y_{h_\nu(\psi,g)}} W(y)^{l_\nu}.$$

Eine Anwendung der gewichteten Form des Lemmas von Cauchy-Frobenius 1.9.1 auf 1.9.3 liefert jetzt die gewichtserzeugende Funktion für die Abzählung von Symmetrieklassen nach Gewicht:

1.9.5 Satz *Seien ${}_GX$ und ${}_HY$ endliche Operationen, $W\colon Y \to R$ eine Abbildung in einen kommutativen Ring, der $\mathbb{Q}$ als Teilring enthält, und w das entsprechende multiplikative Gewicht auf Y^X gemäß 1.9.2. Es gilt dann:*

- *Ist W konstant auf den Bahnen von H auf Y, dann ist w konstant auf den Bahnen von $H \wr_X G$ auf Y^X, und für jede Transversale $\mathcal{T}$ dieser Bahnen haben wir,*

  $$\sum_{t\in\mathcal{T}} w(t) = \frac{1}{|H|^{|X|}|G|} \sum_{(\psi,g)\in H\wr_X G} \prod_{\nu=1}^{c(\overline{g})} \sum_{y\in Y_{h_\nu(\psi,g)}} W(y)^{l_\nu}.$$

  Darüber hinaus ist w auch konstant auf den Bahnen von $H\times G$ und H, so daß wir per Einschränkungen die folgenden Ausdrücke für die Summen der Gewichte der Elemente einer Transversale erhalten

  $$\frac{1}{|H||G|} \sum_{(h,g)\in H\times G} \prod_{i=1}^{|X|} \left(\sum_{y\in Y_{h^i}} W(y)^i\right)^{a_i(\bar{g})},$$

  und

  $$\frac{1}{|H|} \sum_{h\in H} \left(\sum_{y\in Y_h} W(y)\right)^{|X|}.$$

- *Für jedes $W\colon Y \to R$ ist die multiplikative Gewichtsfunktion $w\colon Y^X \to R$ konstant auf den Bahnen von G auf Y^X, und die Summe der Gewichte über eine Transversale der Bahnen ist gleich*

  $$\frac{1}{|G|} \sum_{g\in G} \prod_{i=1}^{|X|} \left(\sum_{y\in Y} W(y)^i\right)^{a_i(\bar{g})}.$$

Die allgemeinste Gewichtsfunktion erhält man, wenn man für W eine Abbildung benutzt, die jedes $y \in Y$ auf eine eigene Unbestimmte eines Polynomrings abbildet. Um die Notation einfach zu halten, benutzen wir denselben Buchstaben $y \in Y$ für die Unbestimmte, setzen also $W: Y \to \mathbb{Q}[Y]: y \mapsto y$, wobei $\mathbb{Q}[Y]$ den Polynomring über $\mathbb{Q}$ bezeichnet mit der Menge Y als einer Menge von kommutierenden Unbestimmten. Das multiplikative Gewicht ist dann einfach

$$w(f) = \prod_x f(x) = \prod_y y^{|f^{-1}(y)|},$$

ein Monom in $\mathbb{Q}[Y]$. Wenn wir jetzt den *Inhalt* von $f \in Y^X$ so definieren

1.9.6 $$I(f): Y \to \mathbb{N}: y \mapsto |f^{-1}(y)|,$$

d.h. $I(f)(y)$ ist die Vielfachheit mit der f den Wert y annimmt, dann ergibt sich

1.9.7 Folgerung *Die Anzahl der $G-$Klassen auf Y^X, deren Elemente den Inhalt $I(f)$ haben, ist der Koffizient des Monoms*

$$\prod_y y^{I(f)(y)}$$

in dem Polynom

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} \left(\sum_{y \in Y} y^i \right)^{a_i(\overline{g})}.$$

□

Ein hübsches Beispiel hierfür ist die Lösung des folgenden sogenannten *Halskettenproblems*:

1.9.8 Beispiel Wir fragen nach der Anzahl verschiedener Halsketten mit n Perlen mit bis zu m verschiedenen Farben und mit vorgegebenem Inhalt und bezüglich der zyklischen Gruppe C_n als Symmetriegruppe. Eine Anwendung von 1.9.7 ergibt

1.9.9 Folgerung *Die Anzahl verschiedener Halsketten mit b_i Perlen in der i–ten Farbe, $i \in m$, ist der Koeffizient von $y_0^{b_0} \ldots y_{m-1}^{b_{m-1}}$ in dem Polynom*

$$\frac{1}{n} \sum_{d|n} \phi(d)(y_0^d + \ldots + y_{m-1}^d)^{n/d},$$

wobei ϕ die Euler-Funktion bezeichnet.

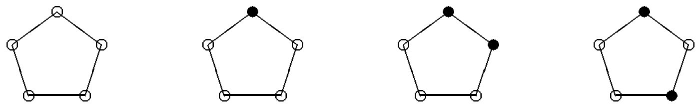


Abbildung 1.2: Vier der acht verschiedenen Halsketten

Als numerisches Beispiel nehmen wir $m := 2$ und $n := 5$ und erhalten die erzeugende Funktion

$$\frac{1}{5}((y_0 + y_1)^5 + 4(y_0^5 + y_1^5)) = y_0^5 + y_0^4 y_1 + 2y_0^3 y_1^2 + 2y_0^2 y_1^3 + y_0 y_1^4 + y_1^5.$$

Dabei bedeutet der Koeffizient des monomialen Summanden $2y_0^3y_1^2$, daß es genau zwei verschiedene Halsketten aus fünf Perlen gibt, von denen drei von der ersten Farbe und zwei von der zweiten Farbe sind. Die Abbildung 1.2 zeigt vier der acht verschiedenen Halsketten, die anderen vier erhält man durch einfaches Vertauschen der beiden Farben.

$\diamond$

Wir haben in 1.9.7 gesehen, daß die erzeugende Funktion für die Abzählung der G–Klassen auf Y^X nach Gewicht gleich

$$\frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} \left(\sum_{y \in Y} y^i \right)^{a_i(\bar{g})}.$$

ist. Dieses Polynom erhält man aus

$$Z(G,X) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} z_i^{a_i(\overline{g})} \in \mathbb{Q}[z_1, \ldots, z_{|X|}],$$

indem man einfach die Unbestimmte z_i durch das Polynom $\sum_y y^i$ ersetzt. Es kommt also vor allem auf die Kenntnis des Polynoms $Z(G,X)$ an. Wir nennen dieses Polynom den *Zykelindex* von ${}_GX$, denn es listet die Zykelstruktur der Elemente $\bar{g} \in \bar{G}$ auf. (Wir sollten aber erwähnen, daß $Z(G,X) = Z(H,X)$ *nicht* bedeutet, daß $\bar{G}$ und $\bar{H}$ isomorph sind, es gibt Gegenbeispiele.)

Wollen wir die Unbestimmten explizit angeben bzw. durch Zahlen $r_i \in \mathbb{Q}$ ersetzen, dann schreiben wir ausführlicher

$$Z(G, X; z_1, \ldots, z_{|X|}) \text{ bzw. } Z(G, X; r_1, \ldots, r_{|X|}).$$

Wir erhalten also beispielsweise (cf. 1.7.7):

1.9.10 Folgerung *Die Anzahl der G–Klassen auf Y^X ist*

$$Z(G, X; |Y|, \ldots, |Y|).$$

□

Um diesen Substitutionsprozeß zu verallgemeinern, der die erzeugende Funktion für die Abzählung der G-Bahnen nach Gewicht ergibt, setzen wir, für jedes Polynom p in $\mathbb{Q}[u_1, \ldots, u_m]$,

$$Z(G, X \mid p(u_1, \ldots, u_m)) := Z(G, X)|_{z_i := p(u_1^i, \ldots, u_m^i)}$$

$$= \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} p(u_1^i, \ldots, u_m^i)^{a_i(\bar{g})} \in \mathbb{Q}[u_1, \ldots, u_m],$$

und wir nennen diesen Prozeß *Pólya-Substitution.* Unter Benutzung dieser Bezeichnungsweise können wir die Folgerung 1.9.7 auch so formulieren:

1.9.11 Der Satz von Pólya *Die erzeugende Funktion für die Abzählung von G-Bahnen auf Y^X nach Inhalt kann aus dem Zykelindex von ${}_GX$ erhalten werden und zwar durch Pólya–Substitution von $\sum_{y \in Y} y$ im Zykelindex $Z(G, X)$. Diese erzeugende Funktion gleicht also*

$$Z(G, X \mid \sum_{y \in Y} y) = Z(G, X)|_{z_i := \Sigma y^i}.$$

□

Zur Anwendung in konkreten Fällen bleibt also schließlich die Berechnung des Zykelindex von ${}_GX$. Hierzu ein paar

1.9.12 Beispiele

- Der Zykelindex der 1-Untergruppe von S_n und deren natürlicher Darstellung auf n ist

$$Z(\{1\}, n) = z_1^n.$$

- Der Zykelindex der natürlichen Operation der zyklischen Gruppe C_n auf n ist (beachten Sie 1.9.9)

$$Z(C_n, n) = \frac{1}{n} \sum_{d|n} \phi(d) z_d^{n/d}.$$

- Der Zykelindex der natürlichen Operation der Diedergruppe D_n der Ordnung $2n$ auf der Menge n (die als Eckenmenge eines regulären n–ecks betrachtet werden kann, so daß D_n die Symmetriegruppe ist) erfüllt, falls $n \geq 3$,

$$Z(D_n, n) = \frac{1}{2} Z(C_n, n) + \begin{cases} \frac{1}{2} z_1 z_2^{(n-1)/2}, & n \text{ ungerade}, \\ \frac{1}{4}(z_2^{n/2} + z_1^2 z_2^{(n-2)/2}), & n \text{ gerade}. \end{cases}$$

  Dies ergibt sich aus der Tatsache, daß die Rotationen eine zyklische Untergruppe der Ordnung n bilden, während die restlichen Elemente Spiegelungen sind, die entweder genau einen Eckpunkt festlassen (bei ungeradem n) oder zwei Eckpunkte oder gar keinen fest lassen (falls n gerade ist), und daß sie die restlichen Punkte zu Punktepaaren zusammenfassen, die vertauscht werden.

- Weiterhin haben wir die folgenden Zykelindizes der natürlichen Operationen von S_n und A_n

$$Z(S_n, n) = \sum_{a \dashv n} \prod_k \frac{1}{a_k!} \left(\frac{z_k}{k}\right)^{a_k},$$

$$Z(A_n, n) = \sum_{a \dashv n} (1 + (-1)^{a_2 + a_4 + \cdots}) \prod_k \frac{1}{a_k!} \left(\frac{z_k}{k}\right)^{a_k}.$$

◇

Für die Graphen von 4 Punkten und deren Abzählung benutzen wir den Zykelindex

1.9.13
$$Z(S_4, \binom{4}{2}) = \frac{1}{24}(z_1^6 + 9 z_1^2 z_2^2 + 8 z_3^2 + 6 z_2 z_4),$$

der aus 1.8.3 erhalten werden kann. Er liefert die erzeugende Funktion

$$Z(S_4, \binom{4}{2} \mid y_0 + y_1) = y_0^6 + y_0^5 y_1 + 2 y_0^4 y_1^2 + 3 y_0^3 y_1^3 + 2 y_0^2 y_1^4 + y_0 y_1^5 + y_1^6,$$

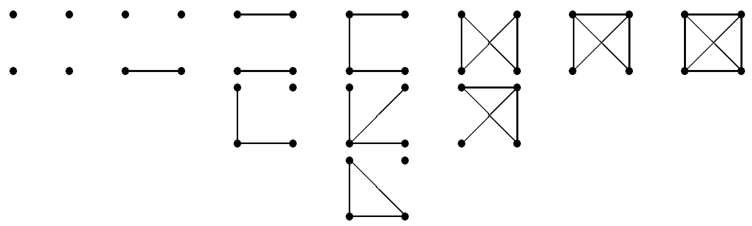


Abbildung 1.3: Die Graphen mit 4 Punkten

in Übereinstimmung mit Abbildung 1.3. Um uns das Leben zu erleichtern, können wir hierbei $y_0 + \ldots + y_{m-1}$ durch $1 + y_1 + \ldots + y_{m-1}$ ersetzen, im Fall daß $|Y| = 2$ gilt, können wir sogar $1+y$ anstelle von $y_0 + y_1$ oder $1 + y_1$ schreiben, so daß z.B. die erzeugende Funktion für die Graphen auf 4 Punkten nach Anzahl der Kanten die folgende Form bekommt:

$$Z(S_4, \binom{4}{2} \mid 1 + y) = 1 + y + 2y^2 + 3y^3 + 2y^4 + y^5 + y^6.$$

Hier ist der Koeffizient von y^k gleich der Anzahl der Graphen mit 4 Punkten, die genau k Kanten enthalten, so daß sich ganz analog folgendes allgemeine Resultat ergibt

1.9.14 Folgerung *Die Gesamtanzahl der Graphen mit v Punkten gleicht*

$$Z(S_v, \binom{v}{2}; 2, \ldots, 2),$$

□

Wir wollen jetzt eine formale Potenzreihe (in abzählbar vielen Unbestimmten $z_1, z_2, \ldots$) einführen, die sich aus verallgemeinerten Zykelindizes zusammensetzt und sowohl die Kardinalitäten- als auch die Typenreihe verallgemeinert.

Betrachten wir zunächst den Zykelindex noch etwas genauer: Es gilt

$$Z(G, X) := \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{|X|} z_i^{a_i(\bar{g})}$$

$$= \frac{1}{|\bar{G}|} \sum_{\bar{g} \in \bar{G}} \prod_{i=1}^{|X|} z_i^{a_i(\bar{g})} = \frac{1}{|\bar{G}|} \sum_{a \vdash |X|} |C^{\bar{a}} \cap \bar{G}| \prod_{i=1}^{|X|} z_i^{a_i}.$$

Wenn wir jetzt noch eine Klassenfunktion $\chi\colon G \to \mathbb{C}$ einschieben, entsteht der *verallgemeinerte Zykelindex*

$$Z(G,X,\chi) := \frac{1}{|G|}\sum_{g\in G}\chi(g)\prod_{i=1}^{|X|} z_i^{a_i(\bar g)} = \frac{1}{|\bar G|}\sum_{a\vdash|X|}\chi_a|C^a\cap\bar G|\prod_{i=1}^{|X|} z_i^{a_i},$$

und die Gleichung

$$Z(G,X) = \frac{1}{|X|!}\sum_{a\vdash|X|}\frac{|X|!|C^a\cap\bar G|}{|G||C^a|}|C^a|\prod_{i=1}^{|X|} z_i^{a_i}$$

zeigt uns, daß jeder Zykelindex $Z(G,X)$ ein verallgemeinerter Zykelindex der symmetrischen Gruppe ist:

$$Z(G,X) = Z(S_X,X,\chi), \text{wobei } \chi\colon S_X \to \mathbb{C}\colon \beta \mapsto \frac{|X|!|C^{S_n}(\beta)\cap\bar G|}{|G||C^{S_n}(\beta)|}.$$

Die bereits angekündigte gemeinsame Verallgemeinerung von Kardinalitäten- und Typenreihe ergibt sich durch Summation solcher verallgemeinerten Zykelindizes:

$$Z(S_n,n,\chi^{\mathcal{S}}) = \frac{1}{n!}\sum_{a\vdash n}\chi_a^{\mathcal{S}}|C^a|\prod_{i=1}^{n} z_i^{a_i},$$

wobei

$$\chi^{\mathcal{S}}\colon S_n \to \mathbb{C}\colon \beta \mapsto a_1(\mathcal{S}[\beta])$$

der Charakter der Operation von S_n auf der Menge von Strukturen $\mathcal{S}[n]$ ist. Der Wert dieses Charakters ist eine Klassenfunktion, $\chi_a^{\mathcal{S}}$ sei der Wert auf der Konjugiertenklasse der Elemente vom Zykeltyp a. Dabei ist zu beachten, daß die Exponenten $a_i(\beta)$ die Anzahlen von Zyklen von $\beta\in S_n$ sind und *nicht* etwa Anzahlen von Zyklen der von β auf $\mathcal{S}[n]$ induzierten Permutation $\mathcal{S}[\beta]$!

Wir wollen jetzt in diesen Zykelindizes Ersetzungen vornehmen, bei denen wir Summanden von Kardinalitätenreihen und von Typenreihen erhalten. Unter Benutzung der oben eingeführten expliziten Schreibweise erhalten wir zunächst, daß die Ersetzung $z_1 := x, z_2 = 0, z_3 = 0, \ldots$ gerade die Anzahl der $\mathcal{S}$-Strukturen auf n mal $x^n/n!$ ergibt,

1.9.15 $$Z(S_n,n,\chi^{\mathcal{S}};x,0,0,\ldots) = |\mathcal{S}[n]|\cdot\frac{x^n}{n!},$$

denn der einzig übrigbleibende Summand ist der zum Einselement. Aus dem Lemma von Cauchy-Frobenius ergibt sich, daß die die Erzetzung $z_1 := x, z_2 := x^2, z_3 := x^3, \ldots$ gerade die Typenanzahl mal x^n liefert:

1.9.16 $$Z(S_n, n, \chi^{\mathcal{S}}; x, x^2, x^3, \ldots) = |S_n \backslash\!\backslash \mathcal{S}[n]| \cdot x^n.$$

Insgesamt erhalten wir also, wenn wir die *Zyklenreihe* als Summe

$$Z_{\mathcal{S}} := Z_{\mathcal{S}}(z_1, z_2, \ldots) := \sum_{n \geq 0} Z(S_n, n, \chi^{\mathcal{S}}; z_1, z_2, \ldots)$$

definieren, die angekündigte Aussage, daß diese Reihe eine interessante Verallgemeinerung darstellt:

1.9.17 Folgerung *Die Zyklenreihe ergibt durch geeignete Ersetzungen sowohl die Kardinalitäten- als auch die Typenreihe:*

$$\mathcal{S}(x) = Z_{\mathcal{S}}(x, 0, \ldots),\ \widetilde{\mathcal{S}}(x) = Z_{\mathcal{S}}(x, x^2, \ldots).$$

Eine weitere interessante Eigenschaft der Zyklenreihe ergibt sich mit folgendem

1.9.18 Hilfssatz *Ist $_GX$ eine endliche Operation mit Bahen ω_i, Repräsentanten $x_i \in \omega_i$, Stabilisatoren $G_i := G_{x_i}$, sowie einer Klassenfunktion χ auf G und einer Funktion w auf X, die auf den Bahnen ω_i konstant ist und dort die Werte w_i hat, dann gilt:*

$$\sum_i w_i \frac{1}{|G_i|} \sum_{g \in G_i} \chi(g) = \frac{1}{|G|} \sum_{g \in G} \chi(g) \sum_{x \in X_g} w(x).$$

Beweis:
$$\sum_{g \in G} \chi(g) \sum_{x \in X_g} w(x) = \sum_{x \in X} w(x) \sum_{g \in G_x} \chi(g)$$

$$= \sum_i |\omega_i| w_i |G_i| \frac{1}{|G_i|} \sum_{g \in G_i} \chi(g) = \sum_i w_i |G| \frac{1}{|G_i|} \sum_{g \in G_i} \chi(g).$$

□

Wir wollen diesen Hilfssatz auf Spezies anwenden und setzen dazu

$$w\colon \sigma \mapsto 1,\ \chi\colon \beta \mapsto \prod_k z_k^{a_k(\beta)}.$$

Es ergibt sich, wie man leicht nachprüft, für die $\mathcal{S}$-Strukturen auf n, deren S_n-Bahnen ω_i, Repräsentanten $\sigma_i \in \omega_i$ und ihre Stabilisatoren $(S_n)_i$:

$$\frac{1}{n!} \sum_{\beta \in S_n} |\mathcal{S}[n]_\beta| \prod_k z_k^{a_k(\beta)} = \frac{1}{n!} \sum_{\beta \in S_n} a_1(\mathcal{S}[\beta]) \prod_k z_k^{a_k(\beta)}$$

$$= \sum_i \frac{1}{|(S_n)_i|} \sum_{\beta \in (S_n)_i} \prod_k z_k^{a_k(\beta)}.$$

Wir ersetzen jetzt in allen diesen Ausdrücken die Unbestimmte z_k durch x^k und erhalten

$$|S_n \backslash\backslash \mathcal{S}[n]| \cdot x^n = Z(S_n, n, \chi^{\mathcal{S}}; x, x^2, \ldots) = \sum_i Z((S_n)_i, n; x, x^2, \ldots).$$

Summation über alle n liefert hieraus insbesondere die Gleichung

1.9.19 $$\widetilde{\mathcal{S}}(x) = \sum_n \sum_i Z((S_n)_i, n; x, x^2, \ldots).$$

1.9.20 Beispiele Hier sind einige leicht nachzuvollziehende Beispiele:

- $Z_{\mathcal{X}} = z_1$,
- $Z_{\mathcal{L}} = \frac{1}{1-z_1}$,
- $Z_{Per} = \prod_{i \geq 1} \frac{1}{1-z_i}$.

$\diamond$

Der Vergleich der Zyklenreihen von Per und $\mathcal{L}$ zeigt, daß die Äquipotenz keineswegs die Gleichheit der Zyklenreihen impliziert:

1.9.21 $$\mathcal{S} \equiv \mathcal{T} \not\Rightarrow Z_{\mathcal{S}} = Z_{\mathcal{T}}.$$

Unter einer *Gewichtung w einer Spezies $\mathcal{S}$* verstehen wir natürlich eine Abbildung w in einen kommutativen Ring R, der $\mathbb{Q}$ als Teilring enthält, die auf allen $\mathcal{S}[M]$ definiert und mit dem Transport verträglich ist:

$$w(\mathcal{S}[\beta](\sigma)) = w(\sigma).$$

Hieraus folgt vor allem die Konstanz von w auf den Typen von $\mathcal{S}$-Strukturen. Das Paar $(\mathcal{S}, w)$, also die gewichtete Spezies, bezeichnen wir kurz mit $\mathcal{S}_w$. Als Kardinalitätenreihe von $\mathcal{S}_w$ definieren wir

$$\mathcal{S}_w(x) := \sum_n \left(\sum_{\sigma \in \mathcal{S}[n]} w(\sigma) \right) \frac{x^n}{n!},$$

als Typenreihe

$$\widetilde{\mathcal{S}_w}(x) := \sum_n \left(\sum_{t \in T_n} w(t) \right) x^n$$

(wobei T_n eine Transversale von $S_n \backslash\!\backslash \mathcal{S}[n]$ bezeichne), und als Zyklenreihe

$$Z_{\mathcal{S}_w}(z_1, z_2, \ldots) := \sum_n Z(S_n, n, \chi_w^{\mathcal{S}}; z_1, z_2, \ldots),$$

wobei

$$\chi_w^{\mathcal{S}} \colon \beta \mapsto \sum_{\sigma \in \mathcal{S}[n]_\beta} w(\sigma).$$

1.9.22 Beispiele

- Eine Gewichtung von Per ist offenbar die folgende Abbildung w in $\mathbb{Q}[y]$:

  $$w \colon \beta \mapsto y^{c(\beta)}, \;\; c(\beta) := \sum_i a_i(\beta).$$

  Die Kardinaltitätenreihe ist hier

  $$Per_w(x) = \sum_n \left(\sum_{a \vdash n} \frac{n!}{\prod_i i^{a_i} a_i!} \cdot y^{\Sigma_i a_i} \right) \cdot \frac{x^n}{n!},$$

  die Typenreihe ist

  $$\widetilde{Per_w}(x) = \sum_n \left(\sum_{a \vdash n} y^{\Sigma_i a_i} \right) \cdot x^n = \sum_n [y]^n x^n,$$

  wenn $[y]^n := y(y+1)\cdots(y+n-1)$ die Aufsteigende Faktorielle bedeutet (vgl. Übungsaufgabe 1.9.3).

- Eine zweite Gewichtung von Per, die die gerade angegebene verallgemeinert, ist

  $$v \colon \beta \mapsto y_1^{a_1(\beta)} y_2^{a_2(\beta)} \cdots \in \mathbb{Q}[y_1, y_2, \ldots].$$

Hier ergibt sich

$$Per_v(x) = \sum_n \left(\sum_{a \vdash n} \frac{n!}{\prod_i i^{a_i} a_i!} \cdot \prod_i y_i^{a_i} \right) \cdot \frac{x^n}{n!},$$

die Typenreihe ist

$$\widetilde{Per_w}(x) = \sum_n \left(\sum_{a \vdash n} \prod_i y_i^{a_i} \right) \cdot x^n = \sum_n \prod_i \frac{1}{1 - x^i y_i}.$$

Übungsaufgaben

Ü 1.9.1 Drücken Sie die Anzahl selbstkomplementärer Graphen mit gegebener Punktezahl mit Hilfe des Zykelindex aus.

Ü 1.9.2 Berechnen Sie die Zyklenreihe von $\mathcal{M}$.

Ü 1.9.3 Beweisen Sie, daß

$$\sum_{a \vdash n} y^{\Sigma_i a_i} = [y]^n := y(y+1)\cdots(y+n-1).$$

1.10 Abzählung nach Stabilisatorklasse

Erinnern wir uns zunächst daran, daß nach 1.6.2 die Elemente einer Bahn als Stabilisatoren eine volle Konjugiertenklasse $\widetilde{U}$ von Untergruppen von G haben. Wir sagen, daß $\widetilde{U}$ der *Typ* dieser Bahn sei. Die *Menge* aller Bahnen vom Typ $\widetilde{U}$, zu einer gegebenen Untergruppe U von G, heißt das $\widetilde{U}$*–Stratum* und wird wie folgt bezeichnet

$$G\backslash\!\!\backslash_{\widetilde{U}} X.$$

Betrachten wir jetzt den Verband $L(G)$ der Untergruppen von G. Wir nehmen an, die Gruppe G sei endlich, $L(G)$ also eine lokal endliche Halbordnung bezüglich der Inklusion $\leq$, so daß wir die Moebiusinversion verwenden können. Weiterhin nehmen wir an, daß die Untergruppen U^i von G so numeriert seien, daß gilt

1.10.1 $$U^i \leq U^k \implies i \leq k.$$

Unter dieser Annahme sind die *Zeta-Matrix* und die *Moebius-Matrix* von G,

$$\zeta(G) := \big(\zeta(U^i, U^k)\big), \text{ und } \mu(G) := \big(\mu(U^i, U^k)\big) = \zeta(G)^{-1}$$

obere Dreiecksmatrizen. Betrachten wir als Beispiel: $G := S_3$. Diese Gruppe hat den Untergruppenverband aus Abb. 1.4,

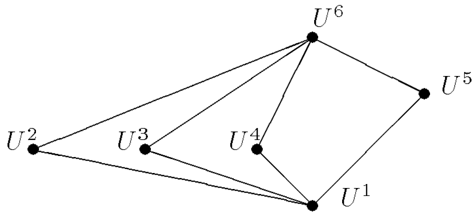


Abbildung 1.4: Der Untergruppenverband von S_3

wobei $U^1 = \langle 1\rangle$, $U^2 = \langle(12)\rangle$, $U^3 = \langle(13)\rangle$, $U^4 = \langle(23)\rangle$, $U^5 = \langle(123)\rangle$, und $U^6 = S_3$. Es gilt also

$$\zeta(S_3) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ & 1 & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 1 \\ & & & 1 & 0 & 1 \\ & & & & 1 & 1 \\ & & & & & 1 \end{pmatrix},$$

und demnach

$$\mu(S_3) = \begin{pmatrix} 1 & -1 & -1 & -1 & -1 & 3 \\ & 1 & 0 & 0 & 0 & -1 \\ & & 1 & 0 & 0 & -1 \\ & & & 1 & 0 & -1 \\ & & & & 1 & -1 \\ & & & & & 1 \end{pmatrix}.$$

Um $|G\backslash\!\backslash_{\widetilde{U}} X|$ zu berechnen betrachten wir jetzt zu einer endlichen Operation ${}_GX$ und einer ihrer Untergruppen U die Menge der gemeinsamen Fixpunkte der Elemente von U :

$$X_U := \{x \mid \forall g \in U\colon\ gx = x\}.$$

Burnside nannte die Ordnung $|X_U|$ dieser Menge die *Marke* von U auf X. Wir drücken sie mit Hilfe der Längen von Strata aus:

$$\begin{aligned} |X_U| &= \sum_{x:U\le G_x} 1 = \sum_{V:U\le V\le G}\ \sum_{x:V=G_x} 1 = \sum_{V:U\le V\le G} \frac{1}{|\widetilde{V}|} \sum_{x:G_x\in\widetilde{V}} 1 \\ &= \sum_{V:U\le V\le G} \frac{|G/V|}{|\widetilde{V}|} \sum_{t\in T:G_t\in\widetilde{V}} 1 = \sum_{V:U\le V\le G} \frac{|G/V|}{|\widetilde{V}|} |G\backslash\!\backslash_{\widetilde{V}} X|, \\ &= \sum_V \zeta(U,V)\frac{|G/V|}{|\widetilde{V}|}|G\backslash\!\backslash_{\widetilde{V}} X|, \end{aligned}$$

wobei T eine Transversale der Bahnen von G auf X bezeichnet. Gemäß der Moebiusinversion ist diese Gleichung äquivalent zu

1.10.2 $$|G\backslash\!\backslash_{\widetilde{U}} X| = \frac{|\widetilde{U}|}{|G/U|} \sum_V \mu(U,V)|X_V|.$$

Um diesen Ausdruck zu vereinfachen, betrachten wir die Menge $\widetilde{L}(G)$ der Konjugiertenklassen von Untergruppen von G:

$$\widetilde{L}(G) := \{\widetilde{U}_1, \ldots, \widetilde{U}_d\},\ \text{mit Repräsentanten } U_i \in \widetilde{U}_i.$$

(U^i darf nicht mit U_i verwechselt werden!) Setzen wir jetzt

1.10.3 $$b_{ik} := \frac{|\widetilde{U}_i|}{|G/U_i|} \sum_{V\in\widetilde{U}_k} \mu(U_i, V),\ \text{und } B(G) := (b_{ik}),$$

dann können wir 1.10.2 mit Hilfe der Matrix $B(G)$ umformulieren. Diese Matrix wollen wir die *Burnside-Matrix* von G nennen (tatsächlich hat Burnside die Inverse von $B(G)$ eingeführt und sie als Markentafel bezeichnet). Wir wollen deshalb das folgende Lemma (und *nicht* das Lemma von Cauchy-Frobenius, das oft irrtümlich Burnside zugeschrieben wird) mit Burnsides Namen belegen:

1.10.4 Burnsides Lemma *Ist $_GX$ eine endliche Operation, dann genügt der Vektor der Längen $|G\backslash\!\backslash_{\widetilde{U}_i} X|$ der Strata von G auf X der Gleichung*

$$\begin{pmatrix} \vdots \\ |G\backslash\!\backslash_{\widetilde{U}_i} X| \\ \vdots \end{pmatrix} = B(G) \cdot \begin{pmatrix} \vdots \\ |X_{U_i}| \\ \vdots \end{pmatrix}.$$

Um dies aus 1.10.2 herzuleiten, brauchen wir nur zu bemerken, daß $|X_U|$ konstant ist auf den Konjugiertenklassen von U, denn die folgende Abbildung ist eine Bijektion:

1.10.5 $$X_U \longrightarrow X_{gUg^{-1}} : x \mapsto gx.$$

Wir wollen dieses Lemma jetzt benutzen, um die G–Klassen von Y^X nach Typ abzuzählen. Da $f \in Y^X$ genau dann unter jedem $g \in U_i$ fest bleibt, wenn f konstant ist auf jeder Bahn von U_i auf X, erhalten wir:

1.10.6 Folgerung *Die Anzahl der Symmetrieklassen von G auf Y^X vom Typ $\widetilde{U}_i$ ist der i-te Eintrag der folgenden einspaltigen Matrix*

$$B(G) \cdot \begin{pmatrix} \vdots \\ |Y|^{|U_i\backslash\!\backslash X|} \\ \vdots \end{pmatrix}.$$

Also ist beispielsweise die Anzahl der k–Graphen mit v Punkten, die vom Typ $\widetilde{U}_j$ sind, U_j eine Untergruppe von S_v, das Element in der j-ten Zeile der Matrix

$$B(S_v) \cdot \begin{pmatrix} \vdots \\ (k+1)^{|U_i\backslash\!\backslash\binom{v}{2}|} \\ \vdots \end{pmatrix}.$$

Für $v := 4$ ergibt eine Anwendung der Burnsidematrix der symmetrischen Gruppe (die mit SYMMETRICA, GAP oder MAGMA berechnet werden kann)

$$\begin{pmatrix}
1/24 & -1/4 & -1/8 & -1/6 & 1/4 & . & 1/12 & 1/2 & . & 1/6 & -1/2 \\
 & 1/2 & . & . & -1/2 & . & . & -1 & . & . & 1 \\
 & & 1/4 & . & -1/4 & -1/4 & -1/4 & . & 1/2 & . & . \\
 & & & 1/2 & . & . & . & -1/2 & . & -1/2 & 1/2 \\
 & & & & 1/2 & . & . & . & -1/2 & . & . \\
 & & & & & 1/2 & . & . & -1/2 & . & . \\
 & & & & & & 1/6 & . & -1/2 & -1/6 & 1/2 \\
 & & & & & & & 1 & . & . & -1 \\
 & & & & & & & & 1 & . & -1 \\
 & & & & & & & & & 1/2 & -1/2 \\
 & & & & & & & & & & 1
\end{pmatrix}$$

die Tabelle 1.1. Die letzte Spalte dieser Tabelle zeigt u.a., daß es genau

$\widetilde{U}_i \backslash k$	0	1	2	3	4
$\widetilde{U}_1$	0	0	11	100	465
$\widetilde{U}_2$	0	2	21	84	230
$\widetilde{U}_3$	0	1	9	36	100
$\widetilde{U}_4$	0	0	0	0	0
$\widetilde{U}_5$	0	2	9	24	50
$\widetilde{U}_6$	0	0	0	0	0
$\widetilde{U}_7$	0	0	1	4	10
$\widetilde{U}_8$	0	2	6	12	20
$\widetilde{U}_9$	0	2	6	12	20
$\widetilde{U}_{10}$	0	0	0	0	0
$\widetilde{U}_{11}$	1	2	3	4	5
$\sum$	1	11	66	276	900

Tabelle 1.1: Multigraphen mit 4 Punkten, abgezählt nach Typ

900 4–Graphen mit 4 Punkten gibt, und daß von diesen genau 465 vom Typ $\widetilde{U}_1$ sind. Wir bemerken darüber hinaus, daß die vierte, die sechste und die zehnte Zeile dieser Tabelle aus lauter Nullen bestehen,

was die Frage aufwirft, ob ähnliches auch für größere k gilt. Diese Zeilen gehören zu $U_4 \simeq A_3, U_6 \simeq C_4$ und $U_{10} \simeq A_4$. Eine kürzere Formulierung dieser Frage liest sich wie folgt: Kommen A_3, C_4 oder A_4 als Automorphismengruppen von Multigraphen mit 4 Punkten vor? Oder noch allgemeiner: *Welche Untergruppen von G kommen als Stabilisatoren von Untergruppen $f \in Y^X$ vor*? Um diese Frage zu beantworten, verwenden wir die Tatsache, daß der Stabilisator von f in der symmetrischen Gruppe S_X die folgende Untergruppe ist:

$$(S_X)_f = \bigoplus_{y \in Y} S_{f^{-1}(y)}.$$

Dies impliziert

1.10.7 Folgerung *Die Stabilisatoren der $f \in Y^X$ sind Untergruppen $U \leq G$, deren zugehörigen Permutationsgruppen $\bar{U}$ der folgenden Gleichung genügen*

$$\bar{U} = S_\alpha \ \cap \ \bar{G},$$

wobei $\bar{G}$ der Gruppe G entspricht, und S_α die direkte Summe der folgenden symmetrischen Gruppen auf den Bahnen von U ist:

$$S_\alpha := \bigoplus_{\omega \in U \backslash\backslash X} S_\omega.$$

Jetzt können wir zumindest eine der oben gestellten Fragen über Automorphismengruppen von Graphen beantworten:

1.10.8 Folgerung *Die alternierende Gruppe A_v kommt nicht als Stabilisator von Multigraphen mit v Punkten vor, falls $v \geq 3$.*

Beweis: Die Annahme $\bar{A}_v = S_\alpha \cap \bar{S}_v$ ergibt nämlich, weil A_v transitiv auf $\binom{v}{2}$ operiert, daß S_α die volle symmetrische Gruppe auf $\binom{v}{2}$ ist, also $\bar{A}_v = \bar{S}_v$, ein Widerspruch sobald $v > 2$.

□

Ein ähnliches Resultat gilt für die zyklische Gruppe C_v (vgl. Übungsaufgabe 1.10.2) und für die alternierende Untergruppe A_{v-1} (Übung 1.10.3).

Eine weitere unmittelbare Konsequenz von 1.10.2 ist ein Ausdruck für die Anzahl der Bahnen vorgeschriebener Länge. Wenn wir nämlich für $U, V \leq G$ folgende Abkürzung benutzen:

1.10.9 $$\mu(U, \widetilde{V}) := \sum_{W \in \widetilde{V}} \mu(U, W),$$

ergibt sich aus 1.10.2

1.10.10 Folgerung *Ist $_GX$ eine endliche Operation, dann ist die Anzahl der Bahnen der Länge k von G auf X gleich*

$$\frac{1}{k}\sum_{i:|G/U_i|=k}|\widetilde{U}_i|\sum_j \mu(U_i,\widetilde{U}_j)|X_{U_j}|,$$

insbesondere ist die Anzahl der asymmetrischen Bahnen, *d.h. die Anzahl der Bahnen vom Typ $\widetilde{1}$ bzw. von maximaler Länge $|G|$, gleich*

$$\frac{1}{|G|}\sum_j \mu(1,\widetilde{U}_j)|X_{U_j}|.$$

Hier ist ein wohlbekanntes Beispiel aus der Galoistheorie.

1.10.11 Beispiel Betrachten wir den endlichen Körper $GF(q), q := p^m, p$ eine Primzahl, und dessen Erweiterungskörper $GF(q^n)$ vom Grad n. Der Galoistheorie entnehmen wir, daß die Galoisgruppe G dieser Erweiterung von dem *Frobenius-Isomorphismus*

$$\sigma\colon GF(q^n)\to GF(q^n)\colon x\mapsto x^q,$$

erzeugt wird, dieser ist von der Ordnung n:

$$G=\langle\sigma\rangle=\{1,\sigma,\ldots,\sigma^{n-1}\}\simeq C_n.$$

Darüber hinaus besitzt $GF(q^n)$ eine *Normalbasis*, d.h. es existieren Elemente $x\in GF(q^n)$ so daß $\{x,\sigma x,\ldots,\sigma^{n-1}x\}$ eine $GF(q)$–Basis von $GF(q^n)$ ist. Drücken wir jetzt die Elemente von $GF(q^n)$ als $GF(q)$–Linearkombinationen der Elemente dieser Basis aus:

$$\sum_{i=1}^n f(i)\sigma^i x,\ \ f(i)\in GF(q),$$

dann können wir sie mit Vektoren $f=(f(0),\ldots,f(n-1))\in q^n$ identifizieren, auf denen der Erzeuger σ der Galois-Gruppe als zyklische Verschiebung operiert. Also zeigt die Existenz einer Normalbasis, daß die Operation der Galois-Gruppe G auf $GF(q^n)$ der kanonischen Operation der zyklischen Gruppe C_n auf q^n entspricht Wir bezeichnen die Menge dieser Bahnen (maximaler) Länge mit

$$G\backslash\!\!\backslash_{|G|}X=G\backslash\!\!\backslash_{\widetilde{1}}X,$$

und wir berechnen die Anzahl

$$|G\backslash\!\backslash_{|G|}GF(q^n)| = |C_n\backslash\!\backslash_n q^n|$$

dieser Bahnen maximaler Länge n der Galois-Gruppe. Weil die zyklische Gruppe C_n einen Untergruppenverband hat, der isomorph ist zum Verband der Teiler d von n, ist die Moebiusfunktion μ auf $L(C_n)$ die zahlentheoretische Moebiusfunktion. Außerdem wird die eindeutig bestimmte Untergruppe der Ordnung d in C_n, von der Potenz $(0\dots n{-}1)^{n/d}$ des vollen Zyklus erzeugt und diese Potenz besteht aus genau n/d disjunkten Zyklen, von denen jeder die Länge d hat. Weiterhin ist $f \in q^n$ ein Fixpunkt dieser Untergruppe $\langle(0\dots n-1)^{n/d}\rangle$ genau dann, wenn f konstant ist auf den zyklischen Faktoren von $(0\dots n-1)^{n/d}$. Wir erhalten also aus 1.10.10 die Gleichung

1.10.12 $$|G\backslash\!\backslash_{|G|}GF(q^n)| = |C_n\backslash\!\backslash_n q^n| = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d},$$

wobei μ die zahlentheoretische Moebiusfunktion bedeutet. Wir bemerken, daß die Anzahl der asymmetrischen Bahnen gleich der Anzahl irreduzibler normierter Polynome mit Nullstellen in $GF(q^n)$ und Koeffizienten in $GF(q)$ ist, denn nach der Galoistheorie wird eine Wurzel eines Polynoms von jedem Element der Galoisgruppe auf eine Wurzel abgebildet.

◇

Wir können auch noch allgemeiner die Bahnen maximaler Länge von C_n auf m^n betrachten. Ihre Anzahlen

$$l_{mn} := |C_n\backslash\!\backslash_n m^n| = \frac{1}{n}\sum_{d|n}\mu(d)m^{n/d}$$

heißen *Dedekind-Zahlen.* Die folgenden Tabelle zeigt die obere linke Ecke der Matrix aller Dedekind-Zahlen:

$m\backslash n$	1	2	3	4	5	6	7
1	1	0	0	0	0	0	0
2	2	1	2	3	6	9	18
3	3	3	8	18	48	116	312
4	4	6	20	60	204	670	2340
5	5	10	40	150	624	2580	11160
6	6	15	70	315	1554	7735	39990
7	7	21	112	588	3360	19544	117648

.

Die $f \in m^n$ können wir als *Worte*

$$f = f(0) \ldots f(n-1)$$

der *Länge* n über dem *Alphabet* m betrachten. Die *lexikographisch kleinsten* Elemente in der Bahn (kurz: $f \leq C_n(f)$) der Länge n von C_n auf m^n bilden die *kanonische Transversale*

$$L_n(m) := \{f \in m^n \mid |C_n(f)| = n, f \leq C_n(f)\};$$

ihre Elemente nennt man die *Lyndon-Worte* der Länge n über dem Alphabet m. Die Vereinigung all dieser Mengen

$$L(m) := \bigcup_n L_n(m)$$

heißt die *Lyndon-Menge* über dem Alphabet von m.
Generell wollen wir die Vereinigung der asymmetrischen Bahnen von G auf X, also die Menge der $x \in X$ mit trivialem Stabilisator, wie folgt bezeichnen:

$$\overline{{}_G X} := \{x \in X \mid G_x = \{1\}\}.$$

Da diese Menge Vereinigung von lauter Bahnen der Länge $|G|$ ist, folgt aus 1.10.2 für die Ordnung dieser Teilmenge von X :

1.10.13 $$|\overline{{}_G X}| = |G| \cdot |G \backslash\backslash_{\widetilde{1}} X| = \sum_i \mu(1, \widetilde{U}_i)|X_{U_i}|.$$

Analog bezeichnen wir die Spezies *asymmetrische S-Strukturen* mit $\overline{\mathcal{S}}$, setzen also

$$\overline{\mathcal{S}}[n] := \{\sigma \in \mathcal{S}[n] \mid (S_n)_\sigma = \{1\}\}.$$

Für die Kardinalitätenreihe dieser Spezies gilt nach 1.10.13:

$$\overline{\mathcal{S}}(x) = \sum_n \sum_i \mu(1, \widetilde{U}_i)|\mathcal{S}[n]_{U_i}| \cdot \frac{x^n}{n!},$$

wobei innen über die Nummern i der Konjugiertenklassen $\widetilde{U}_i$ von Untergruppen der symmetrischen Gruppe S_n zu summieren ist. Für die Typenreihe haben wir

$$\widetilde{\overline{\mathcal{S}}}(x) = \sum_n \frac{1}{n!} \sum_i \mu(1, \widetilde{U}_i)|\mathcal{S}[n]_{U_i}| \cdot x^n = \overline{\mathcal{S}}(x).$$

Hier sind also Kardinalitäten- und Typenreihe gleich, was auf den ersten Blick verwundern mag, jedoch nicht verwunderlich ist, denn die eine ist ja in exponentieller Form geschrieben, die andere nicht, und es handelt sich um Operationen symmetrischer Gruppen.
Der Beweis der gewichteten Form 1.9.1 des Lemmas von Cauchy-Frobenius war ebenso leicht wie der Beweis der konstanten Form1.6.6; dasselbe gilt für die entsprechende gewichtete Form von Burnsides Lemma, die wir jetzt einführen wollen. Wir erinnern uns dazu daran, daß nach 1.10.2, für Repräsentanten t von Bahnen vom Typ $\widetilde{U}$ aus einer Transversalen T der Bahnen von G auf X gilt:

$$|G\backslash\backslash_{\widetilde{U}}X| = \sum_{t\in T: G_t\in\widetilde{U}} 1 = \frac{|\widetilde{U}|}{|G/U|}\sum_{V\leq G}\mu(U,V)\sum_{x\in X_V} 1.$$

Wenn wir jetzt die Einsen auf beiden Seiten der letzten Gleichung durch die Gewichte der entsprechenden Elemente ersetzen, erhalten wir die folgende Identität

$$\sum_{t\in T: G_t\in\widetilde{U}} w(t) = \frac{|\widetilde{U}|}{|G/U|}\sum_{V\leq G}\mu(U,V)\sum_{x\in X_V} w(x).$$

Mit Hilfe der Bijektion aus 1.10.5, die gewichtserhaltend ist, ergibt sich

1.10.14
$$\sum_{t\in T: G_t\in\widetilde{U}_i} w(t) = \frac{|\widetilde{U}_i|}{|G/U_i|}\sum_{k}\mu(U_i,\widetilde{U}_k)\sum_{x\in X_{U_k}} w(x).$$

Eine direkte Konsequenz ist das angestrebte Resultat über die Abzählung nach Gewicht und Stabilisatorklasse:

1.10.15 Das Lemma von Burnside, gewichtete Form *Sei $_GX$ eine endliche Operation und $w\colon X\to R$ eine Abbildung von X in einen kommutativen Ring R der $\mathbb{Q}$ als Teilring enthält. Ist w konstant auf den Bahnen von X, dann haben wir, für die Elemente t einer Transversalen T der Bahnen und für den Vektor der Summen der Gewichte von Transversalen der Strata $G\backslash\backslash_{\widetilde{U}_i}X$ von G auf X, die Gleichung*

$$\begin{pmatrix} \vdots \\ \sum_{t:G_t\in\widetilde{U}_i} w(t) \\ \vdots \end{pmatrix} = B(G)\cdot\begin{pmatrix} \vdots \\ \sum_{x:U_i\leq G_x} w(x) \\ \vdots \end{pmatrix}.$$

Diese gewichtete Form von Burnsides Lemma wurde erstmals in P. Stockmeyer's Dissertation behauptet und bewiesen. Er lieferte Anwendungen dieses Resultats auf die Abzählung von Graphen (bzw. von Symmetrieklassen von Abbildungen) nach Gewicht und Typ:

1.10.16 Folgerung *Die erzeugende Funktion für die Abzählung von G–Klassen auf Y^X vom Typ $\widetilde{U}_j$ nach Gewicht $w\colon f \mapsto \prod f(x) \in \mathbb{Q}[Y]$ ist die j-te Zeile der folgenden einspaltigen Matrix:*

$$B(G)\cdot\begin{pmatrix} \vdots \\ \prod_{\nu=1}^{|U_i\backslash\backslash X|}\sum_y y^{l_\nu(U_i)} \\ \vdots \end{pmatrix},$$

wobei $l_\nu(U_i)$ die Länge der ν-ten Bahnen von U_i auf X bedeutet.

Beispielsweise erhalten wir für Graphen mit $v = 4$ Punkten die folgende Spalte (bezogen auf dieselbe Numerierung der Konjugiertenklassen von Untergruppen, die wir oben bereits benutzt haben):

$$B(S_{\underline{4}})\cdot\begin{pmatrix} (y_0+y_1)^6 \\ (y_0+y_1)^2(y_0^2+y_1^2)^2 \\ (y_0+y_1)^2(y_0^2+y_1^2)^2 \\ (y_0^3+y_1^3)^2 \\ (y_0+y_1)^2(y_0^4+y_1^4) \\ (y_0^4+y_1^4)(y_0^2+y_1^2) \\ (y_0^2+y_1^2)^3 \\ (y_0^3+y_1^3)^2 \\ (y_0^4+y_1^4)(y_0^2+y_1^2) \\ y_0^6+y_1^6 \\ y_0^6+y_1^6 \end{pmatrix} = \begin{pmatrix} 0 \\ y_0^4y_1^2+y_0^2y_1^4 \\ y_0^3y_1^3 \\ 0 \\ y_0^5y_1+y_0y_1^5 \\ 0 \\ 0 \\ 2y_0^3y_1^3 \\ y_0^4y_1^2+y_0^2y_1^4 \\ 0 \\ y_0^6+y_1^6 \end{pmatrix}.$$

Kehren wir jetzt zu der gewichteten Form von Burnsides Lemma zurück. Wir wollen einen Spezialfall im Detail diskutieren. Von besonderem Interesse ist nämlich die Abzählung nach Gewicht und *asymmetrischen* Symmetrieklassen, d.h. der Bahnen mit trivialer Stabilisatorklasse $\widetilde{1}$. Die zugehörige erzeugende Funktion ergibt sich unmittelbar aus 1.10.14:

1.10.17 $$\sum_{t\in\mathfrak{T}:G_t=1} w(x) = \sum_k \frac{\mu(1,U_k)}{|N_G(U_k)|}\sum_{x:U_k\leq G_x} w(x).$$

Diese erzeugende Funktion heißt *asymmetrische Reihe.* Z.B. erhält man die asymmetrische Reihe der Operation ${}_G(Y^X)$ durch Pólya-Einsetzung von $\sum y$ in den *asymmetrischen Index*

1.10.18 $$A(G,X) := \sum_k \frac{\mu(1,U_k)}{|N_G(U_k)|} \prod_i z_i^{|U_k \backslash\!\backslash_i X|},$$

wobei $U_k \backslash\!\backslash_i X$ die Menge der Bahnen der Länge i von U_k auf X bedeutet.

1.10.19 Folgerung *Die erzeugende Funktion für die Abzählung asymmetrischer G-Klassen auf Y^X nach multiplikativem Gewicht ist gleich*

$$A(G,X \mid \sum y).$$

Im Fall der zyklischen Gruppe ist der asymmetrische Index gleich:

1.10.20 $$A(C_n,n) = \frac{1}{n}\sum_{d|n} \mu(d) z_d^{n/d}.$$

Im Fall der symmetrischen Gruppe erhalten wir den folgenden asymmetrischen Index:

$$A(S_n,n) = \frac{1}{n!}\sum_{V \leq S_n} \mu(1,V) \prod_i z_i^{|V \backslash\!\backslash_i \underline{n}|}.$$

In diesem speziellen Beispiel können wir eine zweite Formulierung für diese Reihe angeben, denn die asymmetrischen Bahnen bestehen aus den injektiven Abbildungen. Diese liefert die folgende Gleichung:

$$A(S_n,n) = C(A_n,n) - C(S_n,n).$$

Vergleichen wir die Koeffizienten des Monoms z_n auf beiden Seiten dieser Gleichung, so erhalten wir per Moebiusfunktion auf dem Untergruppenverband der symmetrischen Gruppe das nachfolgende Resultat:

1.10.21 $$\sum_{V \ transitiv} \mu(1,V) = (-1)^{n-1}(n-1)!.$$

Diese Anwendung zeigt, daß explizite Ausdrücke für asymmetrische Reihen sehr hilfreich sind.

Übungsaufgaben

Ü 1.10.1 Beweisen Sie die folgende Identität für Elemente der Burnside Matrix:

$$b_{ik} = \mu(\widetilde{U}_i, U_k)\frac{|\widetilde{U}_k|}{|G/U_i|}, \text{ wobei } \mu(\widetilde{U}_i, U_k) := \sum_{V \in \widetilde{U}_i} \mu(V, U_k).$$

Ü 1.10.2 Zeigen Sie, daß die zyklische Gruppe C_v nicht als Automorphismengruppe von Multigraphen von v Punkten vorkommt, sobald $v \geq 2$.

Ü 1.10.3 Beweisen Sie, daß die Untergruppe A_{v-1} von A_v nicht als Automorphismengruppe eines Multigraphen auf v Punkten vorkommt, sobald $v \geq 3$.

1.11 Operationen auf Halbordnungen und Halbgruppen

Wir betrachten jetzt Operationen von endlichen Gruppen, die eine Halbordnung, eine Multiplikation, oder die beiden Operationen $\wedge$ und $\vee$ eines endlichen Verbandes respektieren. Mit anderen Worten, wir wollen jetzt *Operationen endlicher Gruppen als Gruppen von Automorphismen von Halbordnungen, Halbgruppen und Verbänden untersuchen*, in folgendem Sinn: Sei $(X, \leq)$ eine Halbordnung. Die Gruppe G operiert auf X genau dann als eine Gruppe von *Automorphismen,* wenn folgendes richtig ist:

1.11.1 $$\forall\, g \in G,\; x, x' \in X\colon\; x \leq x' \implies gx \leq gx'.$$

(Offenbar hätten wir $\implies$ auch durch $\iff$ ersetzen können, die angegebene Bedingung ist nur scheinbar schwächer!) Wir werden dies wie folgt abkürzen
$$_G(X, \leq),$$
und wir nennen dies eine *ordnungstreue Operation.*

1.11.2 Hilfssatz *Wenn $_G(X, \leq)$ eine ordnungstreue Operation bezeichnet, dann gilt folgendes:*

- *Je zwei Elemente in derselben Bahn sind unvergleichbar, d.h. die Bahnen einer solchen Operation sind Antiketten.*

- *Die Bahnen ω_i von G auf X können so numeriert werden, daß gilt:*
$$\omega_i \ni x \leq x' \in \omega_k \implies i \leq k.$$

- *Für jede Bahn ω und festes $x \in X$ hängen die Anzahlen*
$$|\{x' \in \omega \mid x \leq x'\}| \text{ und } |\{x' \in \omega \mid x \geq x'\}|$$
nur von der Bahn ab, die x enthält und nicht von dem gewählten Repräsentanten.

- *Für alle $x, x' \in X$ haben wir*
$$\frac{|\{x'' \in X \mid x \leq x'' \in G(x')\}|}{|\{x''' \in X \mid x' \geq x''' \in G(x)\}|} = \frac{|G(x')|}{|G(x)|}.$$

Beweis:
i) Wäre $x \in X$ vergleichbar mit $gx \neq x$, etwa (ohne Einschränkung der Allgemeinheit) $x < gx$, dann hätten wir

$$x < gx < g^2x < \ldots < g^{-1}x < x,$$

einen Widerspruch.
ii) Betrachten wir $x_1, x_2 \in \omega_i, x'_1, x'_2 \in \omega_k, i \neq k$. Wir nehmen an, daß $x_1 < x'_1$, und daß x_2 und x'_2 vergleichbar sind. Dann ergäbe $x_2 > x'_2$, für geeignete $g, g' \in G$: $gx_1 = x_2 > x'_2 = g'x'_1$, es würde also gelten $x_1 > g^{-1}g'x'_1$, was den Widerspruch $x'_1 > g^{-1}g'x'_1$ ergibt. Also kann die Teilordnung in eine totale Ordnung eingebettet werden, welche die Teilordnung respektiert:

$$\underbrace{x_1, x_2, \ldots, x_{|\omega_0|}}_{\in\ \omega_0}, \underbrace{x_{|\omega_0|+1}, \ldots, x_{|\omega_0|+|\omega_1|}}_{\in\ \omega_1}, \ldots, \text{wobei } x_i < x_k \Rightarrow i < k.$$

iii) ist klar wegen 1.11.1
iv) folgt mit Hilfe einer trivialen "doppelten Abzählung". Wir betrachten den bipartiten Graphen, der aus den beiden Bahnen $G(x)$ und $G(x')$ besteht, wobei vergleichbare Elemente durch eine Kante verbunden sind (vgl. Abbildung 1.5).

□

1.11.3 Beispiel Unser wichtigstes Beispiel für eine ordnungstreue Operation ist die Operation von G auf der per Inklusion halbgeordneten Menge $L(G)$ ihrer Untergruppen, also die Operation von G auf $(L(G), \subseteq)$ per Konjugation:

1.11.4 $$G \times L(G) \to L(G) \colon (g, U) \mapsto gUg^{-1}.$$

Diese Operation respektiert die Halbordnung $\subseteq$, die wir wie bei Gruppen meist üblich mit $\leq$ abkürzen:

1.11.5 $$U \leq U' \implies gUg^{-1} \leq gU'g^{-1}.$$

Jede Halbordnung, also auch die von $L(G)$, wird durch ihre Zetafunktion beschrieben, deren Inverse die Moebiusfunktion ist. Die Moebiusfunktion auf $L(G)$ haben wir bereits bei der Definition der Burnsidematrix

1.11.6 $$B(G) = (b_{ik}) = \begin{pmatrix} \ddots & & 0 \\ & \frac{|\widetilde{U}_i|}{|G/U_i|} & \\ 0 & & \ddots \end{pmatrix} \cdot (\mu(U_i, \widetilde{U}_k)).$$

von G verwendet. Die Bedeutung dieser Matrix für die Abzählung von Bahnen nach Stabilisatorklasse ist bei der Formulierung der konstanten und der gewichteten Version von Burnsides Lemma klar geworden. Ihre Inverse wurde von Burnside eingeführt (1911) und als *Markentafel* bezeichnet. Wir bezeichnen diese Matrix mit $M(G) := (m_{ik}) := B(G)^{-1}$ und bemerken, daß nach der oben angegebenen Faktorisierung von $B(G)$ gilt:

1.11.7 $$M(G) = (\mu(U_i, \widetilde{U}_k))^{-1} \cdot \begin{pmatrix} \ddots & & 0 \\ & \frac{|G/U_i|}{|\widetilde{U}_i|} & \\ 0 & & \ddots \end{pmatrix}.$$

Zur Berechnung der Einträge dieser Matrix brauchen wir also nur die Inverse von $(\mu(U_i, \widetilde{U}_k))$ zu ermitteln. Hierzu wenden wir den vierten Punkt von 1.11.2 an und bekommen

$$|\widetilde{U}_i|\zeta(U_i, \widetilde{U}_k) = |\widetilde{U}_k|\zeta(\widetilde{U}_i, U_k).$$

Diese Gleichung impliziert (nachrechnen!)

$$(\mu(U_i, \widetilde{U}_k))^{-1} = (\zeta(U_i, \widetilde{U}_k)) = (\frac{|\widetilde{U}_k|}{|\widetilde{U}_i|}\zeta(\widetilde{U}_i, U_k)),$$

woraus sich schließlich die gesuchte explizite Darstellung der Koeffizienten der Markentafel ergibt:

1.11.8 $$m_{ik} = \frac{|G/U_k|}{|\widetilde{U}_k|}\zeta(U_i, \widetilde{U}_k) = \frac{|G/U_k|}{|\widetilde{U}_i|}\zeta(\widetilde{U}_i, U_k) \ \in \mathbb{N}.$$

($m_{ik} \in \mathbb{N}$ schließen wir aus der ersten Identität, denn die Ordnung einer Konjugiertenklasse von Untergruppen gleicht dem Index des Normalisators.) ◇

Ein Verband $(L, \wedge, \vee)$, beispielsweise $L(G)$, definiert eine Halbordnung $(L, \leq)$ und außerdem liefert er zwei *Halbgruppen* $(L, \wedge)$ und $(L, \vee)$, denn diese beiden Verknüpfungen sind ja assoziativ nach der Definition eines Verbandes. Wir fragen deshalb, ob eine ordnungstreue Operation auch mit diesen Verknüpfungen kompatibel ist.

1.11.9 Hilfssatz *Sei $(L, \wedge, \vee)$ ein Verband auf dem eine endliche Gruppe G operiert. Die folgenden drei Bedingungen sind äquivalent:*

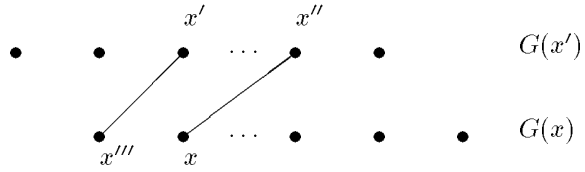


Abbildung 1.5: Zwei Bahnen auf der Halbordnung

- $\forall\ x, x', g:\ \ x < x' \Longrightarrow gx < gx'$,
- $\forall\ x, x', g:\ \ g(x \wedge x') = gx \wedge gx'$,
- $\forall\ x, x', g:\ \ g(x \vee x') = gx \vee gx'$.

Beweis:
i)$\Rightarrow$ ii): Da $x \wedge x'$ kleiner oder gleich sowohl x als auch x' ist, erhalten wir aus i), daß $g(x \wedge x')$ kleiner gleich gx und gx' ist. Dies ergibt

$$g(x \wedge x') \leq gx \wedge gx'. \qquad (\star)$$

Wäre $g(x \wedge x')$ echt kleiner als $gx \wedge gx'$, dann hätten wir, nach i):

$$g^2(x \wedge x') < g(gx \wedge gx') \leq g^2x \wedge g^2x',$$

wobei die letzte Ungleichung aus $(\star)$ folgt, es ergäbe sich, für jedes $n \in \mathbb{N}$,

$$g^n(x \wedge x') < g^n x \wedge g^n x',$$

was zu einem Widerspruch führt, wenn wir $n := |\langle g \rangle|$ setzen. Demnach muß $g(x \wedge x') = gx \wedge gx'$ gelten.

i)$\Rightarrow$ iii) folgt ganz analog.

ii)$\Rightarrow$ i): $x < x'$ liefert $x \wedge x' = x$, so daß $g(x \wedge x') = gx$, also, nach ii), $gx \leq gx'$. Dies impliziert $gx < gx'$, denn $x \neq x'$.

iii)$\Rightarrow$ i) folgt ganz entsprechend.

$\square$

Der Hilfssatz 1.11.9 bedeutet, daß es genügt nachzuprüfen, ob die Operation die Halbordnung respektiert, *oder* eine der beiden Verknüpfungen $\wedge$ oder $\vee$. In jedem dieser Fälle können wir die Bezeichnung ${}_G(L, \leq)$ verwenden, wir können diese Situation aber auch wie folgt bezeichnen

$${}_G(L, \wedge, \vee)$$

und eine solche Operation eine *verbandstreue Operation* nennen.

1.11.10 Beispiel G operiert auf $L(G)$ ordnungstreu per Konjugation. Diese Operation ist kompatibel mit Infimums- und Supremumsbildung, was direkt aus 1.11.9 folgt:

$$g(U \wedge U')g^{-1} = g(U \cap U')g^{-1} = gUg^{-1} \wedge gU'g^{-1},$$

$$g(U \vee U')g^{-1} = g\langle U \cup U'\rangle g^{-1} = gUg^{-1} \vee gU'g^{-1}.$$

$\diamond$

1.11.8 zeigt, daß die Einträge von $M(G)$ die Halbordnung

$$(\widetilde{L}(G), \preceq)$$

beschreiben, die aus den Konjugiertenklassen $\widetilde{U}_i$ von Untergruppen besteht, zusammen mit der Halbordnung

1.11.11 $$\widetilde{U}_i \preceq \widetilde{U}_k \;:\Longleftrightarrow\; \exists\, U \in \widetilde{U}_i, V \in \widetilde{U}_k : \; U \leq V.$$

1.11.8 impliziert nämlich

1.11.12 $$m_{ik} \neq 0 \iff \widetilde{U}_i \preceq \widetilde{U}_k.$$

Burnside nannte $M(G)$ aus folgendem Grund Markentafel:

1.11.13 Hilfssatz *Der Eintrag m_{ik} ist die Anzahl der Linksnebenklassen von U_k in G, die unter der Linksmultiplikation mit Elemten von U_i fest bleiben:*

$$m_{ik} = |(G/U_k)_{U_i}|.$$

Beweis:

$$|\{gU_k \mid \forall x \in U_i : xgU_k = gU_k\}| = \frac{1}{|U_k|}|\{g \in G \mid g^{-1}U_ig \leq U_k\}|$$

$$= \frac{|G|}{|U_k||\widetilde{U}_i|}|\{V \in \widetilde{U}_i \mid V \leq U_k\}| = \frac{|G/U_k|}{|\widetilde{U}_i|}\zeta(\widetilde{U}_i, U_k) = m_{ik}.$$

$\square$

Demnach ist m_{ik} sozusagen die *Marke,* die U_i hinterläßt, wenn U_i auf den Linksnebenklassen von U_k operiert.

$\diamond$

Eine unmittelbare Konsequenz von 1.11.2 ist

1.11.14 Folgerung *Bezeichnet* $_G(L,\wedge,\vee)$ *eine endliche verbandstreue Operation mit Bahnen, die gemäß 1.11.2 numeriert sind, dann bilden die Anzahlen*

$$a_{ik}^{\wedge} := |\{x' \in \omega_k \mid x \wedge x' = x\}| \;\; a_{ik}^{\vee} := |\{x' \in \omega_k \mid x \vee x' = x\}|, \; x \in \omega_i,$$

eine obere Dreiecksmatrix $A^{\wedge} := (a_{ik}^{\wedge})$ *bzw. eine untere Dreiecksmatrix* $A^{\vee} := (a_{ik}^{\vee})$. *In beiden Fällen besteht die Hauptdiagonale aus Einsen, beide Matrizen sind also invertierbar über* $\mathbb{Z}$. *Darüber hinaus hängen die Elemente dieser Matrizen über folgende Gleichung zusammen.*

$$|\omega_i| \cdot a_{ik}^{\wedge} = |\omega_k| \cdot a_{ki}^{\vee}.$$

Jetzt betrachten wir den allgemeineren Fall, bei dem eine Gruppe G als eine Gruppe von Automorphismen auf einer *Halbgruppe* $(X,\cdot)$ operiert, d.h. wir nehmen an, daß die Operation den folgenden Bedingungen genügt

$$\forall\, x, x', g: \;\; g(x \cdot x') = gx \cdot gx'.$$

Solche Operationen heißen *Halbgruppenoperationen* und wir bezeichnen sie wie folgt

$$_G(X,\cdot),$$

$\omega_0,\ldots,\omega_{d-1}$ seien die Bahnen von G auf X. Eine triviale, aber wichtige Bemerkung ist (Übungsaufgabe 1.11.3):

1.11.15 Hilfssatz *Für alle Bahnennummern* i,j,k *und* $z \in \omega_k$ *hängt die Anzahl*

$$|\{(x,x') \in \omega_i \times \omega_j \mid x \cdot x' = z\}|$$

der Lösungen (x,x') *von* $x \cdot x' = z$ *in* $\omega_i \times \omega_j$ nicht *von dem gewählten* z *sondern nur von dessen Bahn ab. Wir können diese Anzahl deshalb mit*

1.11.16 $$a_{ijk}^{\cdot} := |\{(x,x') \in \omega_i \times \omega_j \mid x \cdot x' = z\}|$$

bezeichnen. (Der aufmerksame Leser bemerkt den oberen Index "·" der die Multiplikation, die betrachtet wird hervorhebt, und der deshalb kein *Fliegenschmutz ist.)*

□

Jetzt führen wir den Ring ein, der diese Anzahlen als Strukturkonstanten hat. Dazu betrachten wir zunächst den *Halbgruppenring* von X über $\mathbb{Z}$, also die Menge

$$\mathbb{Z}^X = \{f \mid f\colon X \to \mathbb{Z}\},$$

zusammen mit punktweiser Addition und Faltung als Multiplikation:

$$(f+f')(x) := f(x)+f'(x),\ (f\star f')(x) := \sum_{x'\cdot x''=x} f(x')f'(x'').$$

Wir bezeichnen diesen *Ring* mit $\mathbb{Z}^{X,\cdot}$. Seine Elemente schreiben wir als "formale Summen"

$$f = \sum_{x\in X} f_x x,\ \text{wobei } f_x := f(x).$$

Haben wir jetzt zusätzlich eine Operation ${}_GX$ gegeben, dann nennen wir diejenigen f, die fest unter jedem $g \in G$ bleiben, also die $f \in \mathbb{Z}^X_G$, *G–invariant* oder die *G–Invarianten* (vgl. die Notation X_G die im ersten Paragraphen eingeführt worden ist). Diese Invarianten bilden einen wichtigen Teilring (Übungsaufgabe 1.11.4), dessen wichtigste Eigenschaften in dem folgenden Hilfssatz zusammengefaßt sind:

1.11.17 Hilfssatz

- *Die G–Invarianten $f \in \mathbb{Z}^X$ bilden den Unterring:*

  $$\mathbb{Z}_G^{X,\cdot} := \{f : X \to \mathbb{Z} \mid \forall g \in G\colon f = f \circ \bar{g}^{-1}\}.$$

  Er besteht aus denjenigen $f\colon X \to \mathbb{Z}$, die konstant auf den Bahnen sind.

- *Dieser Unterring hat als $\mathbb{Z}$–Basis die* Bahnensummen

  $$\underline{\omega_i} := \sum_{x\in\omega_i} x \ \in\ \mathbb{Z}_G^{X,\cdot},$$

  das sind die charakteristischen Funktionen der Bahnen von G auf X.

- *Die Strukturkonstanten von $\mathbb{Z}_G^{X,\cdot}$ sind die $a^{\cdot}_{ijk}$ die in 1.11.16 definiert wurden, d.h. für die Produkte der Basiselemente gilt*

  $$\underline{\omega_i}\cdot\underline{\omega_j} = \sum_k a^{\cdot}_{ijk}\ \underline{\omega_k}.$$

Auf diese Weise ergibt jede Operation einer endlichen Gruppe G auf einem endlichen Verband $(L,\wedge,\vee)$ als Gruppe von Verbandsautomorphismen die beiden Ringe $\mathbb{Z}^{L,\wedge}$ und $\mathbb{Z}^{L,\vee}$ zusammen mit ihren Teilringen

$$\mathbb{Z}_G^{L,\wedge} \text{ and } \mathbb{Z}_G^{L,\vee},$$

deren multiplikative Struktur durch die folgenden Strukturkonstanten gegeben ist,

$$a^{\wedge}_{ijk} := |\{(x, x') \in \omega_i \times \omega_j \mid x \wedge x' = z\}|,$$

$$a^{\vee}_{ijk} := |\{(x, x') \in \omega_i \times \omega_j \mid x \vee x' = z\}|,$$

zu festem $z \in \omega_k$. Ein paradigmatisches Beispiel hierfür bildet wieder der Untergruppenverband $L := L(G)$ und die Operation G auf diesem per Konjugation.
Wir können jetzt den wichtigsten Satz dieses Paragraphen (W. Plesken) beweisen:

1.11.18 Satz *Sei* ${}_G(L, \wedge, \vee)$ *eine endliche Verbandsoperation von* G *mit Bahnen* $\omega_0, \ldots, \omega_{d-1}$ *und deren Summen* $\underline{\omega_0}, \ldots, \underline{\omega_{d-1}}$, *numeriert gemäß 1.11.2, dann gilt:*

- *Die Abbildung*

  $$\underline{\omega_k} \mapsto \begin{pmatrix} a^{\wedge}_{1k} \\ \vdots \\ a^{\wedge}_{dk} \end{pmatrix}$$

  ist ein Ringisomorphismus zwischen $\mathbb{Z}^{L,\wedge}_G$ *und* $\mathbb{Z}^d$, *während*

- *die Abbildung*

  $$\underline{\omega_k} \mapsto \begin{pmatrix} a^{\vee}_{1k} \\ \vdots \\ a^{\vee}_{dk} \end{pmatrix}$$

  einen Ringisomorphismus zwischen $\mathbb{Z}^{L,\vee}_G$ *und* $\mathbb{Z}^d$ *ergibt,*

wenn $\mathbb{Z}^d$ *mit punktweiser Addition und Multiplikation versehen ist.*

Beweis: Um zunächst die Homomorphie zu beweisen, betrachten wir das Produkt $a^{\wedge}_i \cdot a^{\wedge}_j$ aus i–ter und j–ter Spalte von $A^{\wedge}$. Wir wollen verifizieren, daß es der Gleichung $a^{\wedge}_i \cdot a^{\wedge}_j = \sum_k a^{\wedge}_{ijk} a^{\wedge}_k$ genügt. Aus der Definition von $a^{\wedge}_{li}$ erhalten wir (für festes $x \in \omega_l$):

$$a^{\wedge}_{li} \cdot a^{\wedge}_{lj} = |\{y \in \omega_i \mid y \geq x\}| \cdot |\{z \in \omega_j \mid z \geq x\}|$$

$$= |\{(y, z) \in \omega_i \times \omega_j \mid x \leq (y \wedge z)\}| = \sum_k a^{\wedge}_{ijk} a^{\wedge}_{lk},$$

was die Homomorphie beweist. Um die Isomorphie nachzuprüfen, benutzen wir daß $A^\wedge := (a^\wedge_{ik})$ Dreiecksmatrizen ist nach 1.11.14 und lauter Einsen entlang der Hauptdiagonalen hat, also invertierbar ist über $\mathbb{Z}$. Dies zeigt, daß obige Abbildung sogar $\mathbb{Z}$–Isomorphismus ist, und es vervollständigt den Beweis der ersten Behauptung, die zweite folgt ganz analog.

□

Diese Resultate zeigen die fundamentale Bedeutung der *Spalten* von $A^\wedge$. Aber auch die *Zeilen* haben interessanten Eigenschaften (vgl. Übung 1.11.5).

Dekorative Verbände, auf denen endliche Gruppen als Gruppen von Automorphismen operieren, werden von den Flächen, Kanten und Ecken der regulären Polyeder gebildet: Das Tetradeder, der Würfel, das Oktaeder, das Dodekaeder und das Ikosaeder. Betrachten wir den einfachsten Fall, das *Tetraeder* (Abb. 1.6). Es hat 4 Flächen, 6

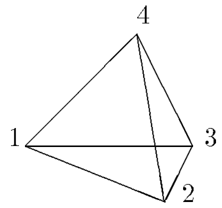


Abbildung 1.6: Das Tetraeder

Kanten, 4 Ecken, und zusammen mit dem Tetrader T und der leeren Menge $\emptyset$ bildet es einen Verband L der Ordnung 16, der mit Hilfe der Inklusion halbgeordnet ist. Es ist offensichtlich, daß die alternierende Gruppe A_4 auf L operiert und dabei die Inzidenz respektiert, also auf L als eine Gruppe von Automorphismen operiert. Die entsprechenden Matrizen $A^\wedge$ und $A^\vee$ sind die folgenden beiden:

$$A^\wedge = \begin{pmatrix} 1 & 4 & 6 & 4 & 1 \\ & 1 & 3 & 3 & 1 \\ & & 1 & 2 & 1 \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}, \quad A^\vee = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 3 & 1 & \\ 1 & 4 & 6 & 4 & 1 \end{pmatrix}.$$

Ein Beispiel eines Hadamardprodukts zweier Spalten von einer dieser

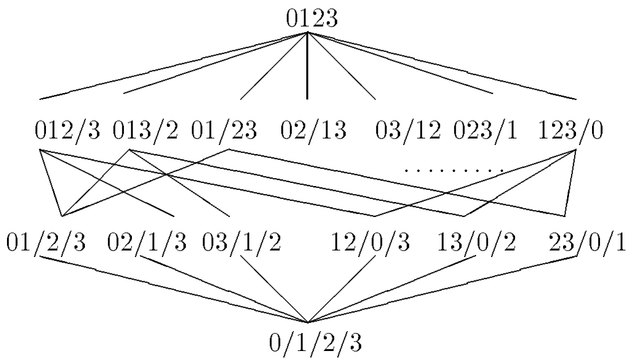


Abbildung 1.7: Der Verband $SP(4)$

Matrizen ist

$$a_3^\wedge \cdot a_4^\wedge = \begin{pmatrix} 24 \\ 9 \\ 2 \\ 0 \\ 0 \end{pmatrix} = 2a_3^\wedge + 3a_2^\wedge.$$

Diese Identität zeigt, daß $a_{343}^\wedge = 2$ und $a_{342}^\wedge = 3$, was bedeutet, daß jede Kante auf *genau zwei* Weisen als das Infimum einer Fläche und einer Kante gebildet werden kann, während eine Ecke auf *genau drei* Weisen als ein solches Infimum darstellbar ist.
Unser nächstes Beispiel ist der Verband $SP(n)$ aus der *Menge aller Mengenpartitionen* von $n = \{0, \ldots, n-1\}$, geordnet durch die *Verfeinerung*. Dieser Verband heißt der*Partitionenverband* von n, der Spezialfall $SP(4)$ ist in Abbildung 1.7 dargestellt, wobei die Aufteilung der 4 Elemente in Blöcke durch "/" indiziert wird.
Ordnen wir die Längen der Blöcke von $p \in SP(n)$ in einer nicht ansteigenden Sequenz α, so erhalten wir eine Zahlpartition

$$\alpha(p) = (\alpha_0, \alpha_1, \ldots) \vdash n,$$

die wir den *Typ* von p nennen. Die folgenden Tatsachen kann man leicht nachprüfen (Übungsaufgabe 1.11.6):

1.11.19 Hilfssatz *Für die natürliche Operation von S_n auf $SP(n)$ gilt:*

- *S_n operiert als eine Gruppe von Automorphismen auf $SP(n)$:*

$$p \leq p' \Longleftrightarrow \pi p \leq \pi p'.$$

- *Der Verband $(SP(n), \leq)$ ist isomorph zu dem Teilverband von $L(S_n)$ der aus den Stabilisatoren der Mengenpartition besteht.*

- *Die Bahnen von S_n auf $SP(n)$ sind die Teilmengen der Partitionen gleichen Typs:*

$$S_n(p) = S_n(p') \Longleftrightarrow \alpha(p) = \alpha(p').$$

Die Matrizen $A^\wedge$ und $A^\vee$ von $SP(4)$ sind

$$A^\wedge = \begin{pmatrix} 1 & 6 & 3 & 4 & 1 \\ & 1 & 1 & 2 & 1 \\ & & 1 & 0 & 1 \\ & & & 1 & 1 \\ & & & & 1 \end{pmatrix}, \quad A^\vee = \begin{pmatrix} 1 & & & & \\ 1 & 1 & & & \\ 1 & 2 & 1 & & \\ 1 & 3 & 0 & 1 & \\ 1 & 6 & 3 & 4 & 1 \end{pmatrix}.$$

Wiederum ergeben die Produkte von Spalten interessante Abzählresultate, beispielsweise zeigt

$$a_2^\vee \cdot a_3^\vee = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 0 \\ 18 \end{pmatrix} = 2a_3^\vee + 12a_5^\vee$$

daß es genau zwei Möglichkeiten gibt, eine Mengenpartition vom Typ (2^2) von 4 als Supremum $p \vee p'$ einer Partition p vom Typ $(2, 1^2)$ und einer Partition p' vom Typ (2^2) darzustellen. Die Gleichung zeigt darüber hinaus, daß die Mengenpartition 0123 vom Typ (4) auf genau 12 Weisen als Supremum $p \vee p'$ dargestellt werden kann, wobei $\alpha(p) = (2, 1^2)$ und $\alpha(p') = (2^2)$. Dies kann man leicht an der Abbildung 1.7 nachprüfen.

Weitere wichtige endliche Verbände sind die Verbände der Unterräume endlicher Vektorräume. Wir bezeichnen mit

$$\mathfrak{L}(d, q)$$

den Verband der Unterräume des d–dimensionalen Vektorraums $V := GF(q)^d$ über dem Galois-Feld $GF(q)$. Die volle lineare Gruppe $GL(V)$, also $GL_d(q)$, operiert als Gruppe von Automorphismen, und die Bahnen sind die Unterräume derselben Dimension. Aus technischen Gründen setzen wir $d = m + n$ und behaupten:

1.11.20 Hilfssatz *Für natürliche Zahlen m und n, wobei $0 < n$, ist die Anzahl der Unterräume $U \leq GF(q)^{m+n}$ der Dimension n gleich*

$$\begin{bmatrix} m+n \\ n \end{bmatrix}_q := \frac{(q^{m+n}-1)\cdot\ldots\cdot(q^{m+1}-1)}{(q^n-1)\cdot\ldots\cdot(q-1)}.$$

Beweis: Es ist leicht zu sehen, daß die Anzahl der n–Tupel aus linear unabhängigen Elementen von $GF(q)^{m+n}$ gleich ist

$$(q^{m+n}-1)(q^{m+n}-q)\cdot\ldots\cdot(q^{m+n}-q^{n-1}).$$

Dasselbe Argument zeigt, daß die Anzahl verschiedener Basen von $GF(q)^n$ gleich ist

$$(q^n-1)(q^n-q)\cdot\ldots\cdot(q^n-q^{n-1}).$$

Also ist die Anzahl der Unterräume der Dimension n gleich dem Quotienten dieser beiden Anzahlen, und man erhält die Behauptung durch Kürzen von Potenzen von q.

□

Die Einträge von $A^\vee$ und die Einträge von $A^\wedge$ erhält man durch eine Anwendung von 1.11.14:

1.11.21 Folgerung *Für den Verband $\mathfrak{L}(d,q)$ gilt*

$$A^\wedge = \left(\begin{bmatrix} d-i \\ k-i \end{bmatrix}_q\right)_{i,k\in d}, \quad A^\vee = \left(\begin{bmatrix} i \\ k \end{bmatrix}_q\right)_{i,k\in d}.$$

Wir können die Matrix $A^\vee$ für jede Primzahlpotenz q erhalten, indem wir einfach die folgende Matrix an der Stelle q berechnen:

$$\left(\begin{bmatrix} i \\ k \end{bmatrix}\right) = \begin{pmatrix} 1 & & & \\ 1 & 1 & & \\ 1 & 1+x & 1 & \\ 1 & 1+x+x^2 & 1+x+x^2 & 1 \\ 1 & 1+x+x^2+x^3 & 1+x+2x^2+x^3+x^4 & \ldots \\ \ldots & \ldots & \ldots & \ldots \end{pmatrix}.$$

Übungsaufgaben

Ü 1.11.1 Zeigen Sie, daß jedes Element in der Hauptdiagonale der Markentafel jedes Element in derselben Spalte der Markentafel teilt.

Ü 1.11.2 Ist $\widetilde{U}_i \preceq \widetilde{U}_j \preceq \widetilde{U}_k$, dann genügen die entsprechenden Elemente in der k-ten Spalte der Markentafel den Ungleichungen

$$m_{ik} \geq m_{jk} \geq m_{kk}.$$

Ü 1.11.3 Beweisen Sie 1.11.15.

Ü 1.11.4 Prüfen Sie die erste Behauptung von 1.11.17 nach.

Ü 1.11.5 Zeigen Sie, daß die Matizen $A_i^\wedge := (a_{ijk}^\wedge)$ die Zeilen von $A^\wedge$ als Eigenvektoren haben. Was sind ihre Eigenwerte?

Ü 1.11.6 Beweisen Sie 1.11.19.

Ü 1.11.7 Zeigen Sie, daß die Matrix $A^\vee$ des Verbandes $SP(n)$ rekursiv berechnet werden kann.

Ü 1.11.8 Berechnen Sie die Matrizen $A^\wedge$ und $A^\vee$ für Würfel und Ikosaeder, auf denen jeweils die Gruppen S_4 und A_5 operieren.

Ü 1.11.9 Berechnen Sie die Matrizen für die Operation von S_n auf dem Verband der Teilmengen von n.

1.12 Der Burnsidering

Wir sahen, wie Symmetrieklassen von Abbildungen nach Gewicht und Stabilisatorklasse abgezählt werden können, unter Benutzung der *Burnsidematrix,* der Inversen der Markentafel. Darüber hinaus haben wir Operationen von Gruppen auf Verbänden $(L, \wedge, \vee)$ kennengelernt, zusammen mit den Teilringen $\mathbb{Z}_G^{L,\wedge}$ und $\mathbb{Z}_G^{L,\vee}$ der Halbgruppenringe $\mathbb{Z}^{L,\wedge}$ und $\mathbb{Z}^{L,\vee}$, wobei die Matrizen $A^\wedge = (a_{ik}^\wedge)$ und $A^\vee = (a_{ik}^\vee)$ eine zentrale Rolle spielt. Wir wollen jetzt eine Brücke zwischen diesen beiden Problembereichen bauen, indem wir den Burnsidering $\Omega(G)$ von G einführen, den man in $\mathbb{Z}_G^{L(G),\wedge}$ einbetten kann. Die Matrix $A^\wedge$ dieses Rings steht in enger Beziehung zur Markentafel.
Um dies vorzubereiten führen wir eine Äquivalenzrelation auf den Operationen von G ein, indem wir $_GX$ und $_GX'$ als *ähnlich* bezeichnen, wenn es eine mit der Operation vertauschbare Bijektion $\theta\colon X \to X'$ gibt:

$$\forall\ x \in X, g \in G\colon\ \theta(gx) = g\theta(x).$$

In diesem Falle schreiben wir

$$_GX \approx {_GX'}.$$

Als nächstes bemerken wir, wie man eine vollständige Menge transitiver G–Mengen erhalten kann:

1.12.1 Hilfssatz *Sei G eine endliche Gruppe mit Konjugiertenklassen von Untergruppen $\widetilde{U}_1, \ldots, \widetilde{U}_d$ und Repräsentanten $U_i \in \widetilde{U}_i$. Dann gilt*

- *Die Mengen $G/U_i := \{gU_i \mid g \in G\}, 0 \leq i \leq d-1$, bestehend aus den Linksnebenklassen gU_i der Untergruppen U_i von G sind G–Mengen bezüglich der Operation $g : xU_i \mapsto gxU_i$.*
- *Diese G–Mengen sind transitiv und paarweise unähnlich.*
- *$\{G/U_0, \ldots, G/U_{d-1}\}$ ist ein vollständiges System transitiver und paarweise unähnlicher G–Mengen, sie bilden also eine Transversale der Ähnlichkeitsklassen transitiver G-Mengen.*

Die Ähnlichkeitsklassen transitiver Operationen von G bezeichnen wir so:

$$\overline{G/U_i} := \{_GX \mid {_GX} \ \approx\ {_G(G/U_i)}\},$$

Das *vollständige System* dieser Klassen ist also

$$\Omega := \{\overline{G/U_0}, \ldots, \overline{G/U_{d-1}}\}.$$

Betrachten wir die freie abelsche Gruppe

$$\mathbb{Z}^\Omega := \{\psi \mid \psi : \Omega \to \mathbb{Z}\}, \text{ mit } (\psi + \psi')(\overline{G/U_i}) := \psi(\overline{G/U_i}) + \psi'(\overline{G/U_i}).$$

Wir schreiben die $\psi \in \mathbb{Z}^\Omega$ wie üblich als "formale Summen"

$$\psi = \sum_{i=0}^{d-1} z_i \cdot \overline{G/U_i}, \text{ wobei } z_i := \psi(\overline{G/U_i}) \in \mathbb{Z}.$$

Die Addition der beiden formalen Summen

$$\overline{G/U_i} := 1_\mathbb{Z} \cdot \overline{G/U_i} \text{ und } \overline{G/U_k} := 1_\mathbb{Z} \cdot \overline{G/U_k}$$

in $\mathbb{Z}^\Omega$ kann man interpretieren als Bildung der disjunkten Vereinigung von G/U_i und G/U_k und nachträglichem Übergang zu der G–Ähnlichkeitsklasse $\overline{X}$ der resultierenden G–Menge X:

$$\overline{G/U_i} + \overline{G/U_k} = \overline{G/U_i \dot\cup G/U_k}.$$

Dies folgt natürlich aus der Tatsache, daß jede G–Menge eine eindeutige Zerlegung in Bahnen besitzt (es muß jedoch darauf hingewiesen werden, daß wir bei $i = k$ ebenfalls die *disjunkte* Vereinigung bilden müssen, d.h. $|G/U_i \dot\cup G/U_i| = 2|G/U_i|$). Also können wir *jede G–Menge X und ihre Ähnlichkeitsklasse $\overline{X}$ auf diese Weise mit einem eindeutig bestimmten Element der Teilmenge $\mathbb{N}^\Omega \subseteq \mathbb{Z}^\Omega$ identifizieren:*

1.12.2 $$\overline{X} = \sum_{i=0}^{d-1} |G\backslash\!\backslash_{\widetilde{U}_i} X| \cdot \overline{G/U_i}.$$

Darüber hinaus können wir auf $\mathbb{Z}^\Omega$ eine Multiplikation einführen, als lineare Fortsetzung von

$$\overline{G/U_i} \cdot \overline{G/U_j} := \sum_k b_{ijk} \overline{G/U_k}, \quad \text{falls} \quad \overline{G/U_i \times G/U_j} = \sum_k b_{ijk} \overline{G/U_k}.$$

Wir werden gleich sehen, daß dies tatsächlich eine wohldefinierte Multiplikation ist. Die entsprechenden Strukturkonstanten b_{ijk} sind die Anzahlen der Bahnen von G auf $G/U_i \times G/U_j$ (bezüglich der natürlichen Operation $g(x,y) := (gx, gy)$) die zu der Klasse $\overline{G/U_k}$ gehören.

Beispielsweise werden die Konjugiertenklassen von Untergruppen in $G := S_3$ durch die folgenden Untergruppen repräsentiert

$$U_0 := \{1\},\ U_1 := S_2,\ U_2 := A_3,\ U_3 := S_3,$$

wir erhalten also die folgende Transversale von Ähnlichkeitsklassen transitiver S_3–Mengen:

$$G/U_0 = S_3/\{1\},\ G/U_1 = S_3/S_2,\ G/U_2 = S_3/A_3,\ G/U_3 = S_3/S_3,$$

sie haben die Ordnungen 6,3,2,1. Es ist leicht nachzuprüfen, daß S_3 transitiv auf $G/U_1 \times G/U_2$ operiert, daß wir (beispielsweise mit Hilfe einer Überprüfung der Kardinalitäten) erhalten

$$\overline{G/U_1} \cdot \overline{G/U_2} = \overline{G/U_1 \times G/U_2} = \overline{G/U_0}.$$

1.12.3 Satz *Die folgende Abbildung definiert eine Einbettung des Rings* $(\mathbb{Z}^\Omega, +, \cdot)$ *in den Ring* $\mathbb{Z}_G^{L(G),\wedge}$*:*

$$\mathbb{Z}^\Omega \hookrightarrow \mathbb{Z}_G^{L(G),\wedge} : \overline{G/U_i} \mapsto |N_G(U_i) : U_i| \underline{\widetilde{U}_i},$$

wobei

$$\underline{\widetilde{U}_i} := \sum_{U \in \widetilde{U}_i} U \in \mathbb{Z}_G^{L(G),\wedge}.$$

Beweis: Die potentiellen Strukturkonstanten von $\mathbb{Z}^\Omega$ haben wir mit b_{ijk} bezeichnet, während die Strukturkonstanten von $\mathbb{Z}_G^{L(G),\wedge}$ die $a_{ijk}^\wedge$ sind , die in 1.11.17 eingeführt wurden. Es bleibt deshalb die folgende Gleichung nachzuprüfen:

$$b_{ijk} = \frac{|N_G(U_i)/U_i||N_G(U_j)/U_j|}{|N_G(U_k)/U_k|} a_{ijk}^\wedge.$$

Wegen $|\widetilde{U}_k| = |G/N_G(U_k)|$ haben wir

$$b_{ijk} = \frac{1}{|G/U_k|} |\{(x,y) \in G/U_i \times G/U_j \mid G_{(x,y)} \in \widetilde{U}_k\}|$$

$$= \frac{|\widetilde{U}_k|}{|G/U_k|} |\{(x,y) \in G/U_i \times G/U_j \mid G_{(x,y)} = G_x \cap G_y = U_k\}|$$

$$= \frac{|U_k|}{|N_G(U_k)|} |\{(U,V) \in \widetilde{U}_i \times \widetilde{U}_j \mid U \cap V = U_k\}| \frac{|N_G(U_i)||N_G(U_j)|}{|U_i||U_j|}$$

$$= \frac{|N_G(U_i)/U_i||N_G(U_j)/U_j|}{|N_G(U_k)/U_k|} a^{\wedge}_{ijk}.$$

□

Dies zeigt insbesondere, daß

$$\Omega(G) := (\mathbb{Z}^{\Omega}, +, \cdot)$$

ein Ring ist, wir nennen ihn den *Burnsidering* von G. Die Markentafel $M(G)$ von G steht in enger Beziehung zu der Matrix $A^{\wedge} = (a^{\wedge}_{ik})$ von $\mathbb{Z}_G^{L(G),\wedge}$:

1.12.4 Satz *Die Matrix $A^{\wedge}$ von $\mathbb{Z}_G^{L(G),\wedge}$ und die Markentafel $M(G)$ von G genügen der Gleichung*

$$M(G) = A^{\wedge} \cdot \begin{pmatrix} \ddots & & 0 \\ & |N_G(U_k)/U_k| & \\ 0 & & \ddots \end{pmatrix}.$$

Beweis: Unter Benutzung von 1.11.8 und 1.11.14 erhalten wir:

$$m_{ik} = \frac{|G/U_k|}{|\widetilde{U}_k|} |\{V \in \widetilde{U}_k \mid U_i \leq V\}| = |N_G(U_k)/U_k| a^{\wedge}_{ik}.$$

□

Wir haben gerade gesehen, wie der Burnsidering $\Omega(G)$ in den Ring $\mathbb{Z}_G^{L(G),\wedge}$, eingebettet werden kann, und wir wissen bereits aus 1.11.18 daß $\mathbb{Z}_G^{L(G),\wedge}$ isomorph ist zu $\mathbb{Z}^d$ via $\underline{\widetilde{U}_i} \mapsto a_i^{\wedge}$ so daß wir schließlich folgendes erhalten

1.12.5 Folgerung *Die folgende Abbildung ergibt durch lineare Erweiterung die Ringeinbettung:*

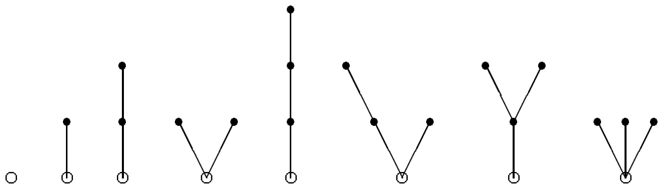
$$\varepsilon : \Omega(G) \hookrightarrow \mathbb{Z}^d : \overline{G/U_k} \mapsto \mu_k := \begin{pmatrix} m_{0,k} \\ \vdots \\ m_{d-1,k} \end{pmatrix}.$$

Wir nennen diese Spalten μ_k von $M(G)$ die *Marken* von G.
Auf diese Weise *können wir die endlichen G–Mengen mit den $\mathbb{N}$–Linearkombinationen der Marken von G identifizieren.* Da 1.12.5 eine Ringeinbettung beschreibt, entspricht dem Produkt in $\Omega(G)$ das Hadamardprodukt in $\mathbb{Z}^d$:

1.12.6 $$\varepsilon(\overline{G/U_i} \cdot \overline{G/U_j}) = \mu_i \cdot \mu_j.$$

Insbesondere kann $\mathcal{S}[n]$, die Menge der $\mathcal{S}$-Strukturen auf n, mit einem Element des Burnsiderings $\Omega(S_n)$ der symmetrischen Gruppe S_n identifiziert werden.

1.12.7 Beispiel Hier sind die kleinsten unnumerierten Wurzelbäume, also die Typen von numerierten Wurzelbäumen auf den Mengen $n = 1, 2, 3, 4$:



Mit Hilfe einer Bestimmung der jeweiligen Symmetriegruppen der zugehörigen numerierten Wurzelbäume erhalten wir die den Mengen $\mathcal{W}[n]$ entsprechenden Elemente aus den jeweiligen Burnsideringen:

n=1: Die Symmetriegruppe (=Stabilisator) des einzigen Wurzelbaums mit einem einzigen Punkt ist trivialerweise S_1, der unnumerierte Wurzelbaum ist also vom Typ $\widetilde{S_1}$, das entsprechende Element des Burnsideringes ist demnach

$$\overline{S_1/S_1}.$$

n=2: Der einzige Wurzelbaum mit zwei Punkten (genauer: jeder diesem entsprechende numerierte Wurzelbaum) hat als Symmetriegruppe die Untergruppe $S_1 \leq S_2$, das $\mathcal{W}[2]$ entsprechende Element des Burnsiderings ist also

$$\overline{S_2/S_1}.$$

n=3: Die beiden unnumerierten Wurzelbäume mit drei Punkten sind von verschiedenem Typ, der erste in der Abbildung ist vom Typ $\widetilde{S_1}$, der zweite ist vom Typ $\widetilde{S_2}$. Das $\mathcal{W}[3]$ entsprechende Element des Burnsiderings von S_3 ist demnach

$$\overline{S_3/S_1} + \overline{S_3/S_2}.$$

n=4: Hier sind die ersten beiden Wurzelbäume vom Typ $\widetilde{S_1}$, der dritte ist vom Typ $\widetilde{S_2}$, der vierte ist vom Type $\widetilde{S_3}$. $\mathcal{W}[4]$ entspricht also dem Element

$$2 \cdot \overline{S_4/S_1} + \overline{S_4/S_2} + \overline{S_4/S_3}.$$

Man kann die Ähnlichkeitsklassen $\overline{S_n/S_i}$ natürlich auch durch die Namen S_n-isomorpher Strukturen ersetzen. Hierbei benutzt man am besten Strukturen, die möglichst wenig spezifisch sind, also in unserem Beispiel nicht notwendig Wurzelbäume. Betrachten wir einmal die asymmetrischen Typen, also die unnumerierten Wurzelbäume mit trivialer Symmetriegruppe; sie sind S_n-isomorph zu S_n/S_1, gehören also zur Ähnlichkeitsklasse $\overline{S_n/S_1}$. Wir wollen diese Klasse nicht durch einen Wurzelbaum beschreiben, sondern durch eine Struktur, deren Abhängigkeit vom Parameter n in ihrer Bezeichnung klar zu Tage tritt. Eine solche Struktur ist u.a. die Struktur $\mathcal{X}^n$, denn die Menge der $\mathcal{X}^n$-Strukturen auf m ist leer, es sei denn, $m = n$, in welchem Fall diese Menge aus genau den n-Tupeln aus verschiedenen Elementen von n besteht:

$$\mathcal{X}^n[m] = \begin{cases} \{(i_0, \ldots, i_{n-1}) \mid i_j \neq i_k\} & n = m, \\ \emptyset & \text{sonst.} \end{cases}$$

Jedes solche injektive n-Tupel hat trivialen Stabilisator, $\mathcal{X}^n[n]$ ist also wirklich vom Typ $\widetilde{S_1}$:

$$\mathcal{X}^n[n] \subseteq \overline{S_n/S_1} = \overline{S_n/S_1 \oplus \ldots \oplus S_1}.$$

Ein weiterer leicht zu beschreibender Typ ist $\overline{S_n/S_{n-1}}$: Beispielsweise ist ganz offenbar

$$\mathcal{X} \cdot \mathcal{M}_{n-1}[n] \subseteq \overline{S_n/S_{n-1}} = \overline{S_n/S_1 \oplus S_{n-1}}.$$

Allgemeiner gilt:

$$\mathcal{X}^k \cdot \mathcal{M}_{n-k}[n] \subseteq \overline{S_n/S_1 \oplus \ldots \oplus S_1 \oplus S_{n-k}}.$$

Mit Hilfe dieser Strukturen können wir die oben angegebenen Elemente der Burnsideringe symmetrischer Gruppen, die den Wurzelbäumen mit $n = 1, 2, 3, 4$ Punkten entsprechen, ja sogar die Mengen der Wurzelbäume auf diesen Punktezahlen neu formulieren:

$$\mathcal{W} = \mathcal{X} + \mathcal{X}^2 + (\mathcal{X}^3 + \mathcal{X} \cdot \mathcal{M}_2) + (2\mathcal{X}^4 + \mathcal{X}^2 \cdot \mathcal{M}_2 + \mathcal{X} \cdot \mathcal{M}_3) + \ldots.$$

Man nennt dies auch die *molekulare Zerlegung,* es ist die Zerlegung in Bahnen, samt Bestimmung des jeweiligen Typs. Als *molekular* bezeichnet man jede Spezies $\mathcal{S}$, die nur trivial direkt in Spezies zerlegt werden kann, d.h. für die gilt

$$\mathcal{S} = \mathcal{T} + \mathcal{U} \Longrightarrow \mathcal{T} = 0 \text{ oder } \mathcal{U} = 0.$$

Die Zerlegung in Typen ergibt eine Zerlegung von $\mathcal{S}$ in molekulare Spezies, die die kanonische Zerlegung $\mathcal{S} = \sum_n \mathcal{S}_n$ verfeinert:

$$\mathcal{S} = \sum_n \mathcal{S}_n = \sum_n \sum_{\mathcal{T} \subseteq \mathcal{S}_n, \mathcal{T} \text{ mol.}} \mathcal{T}.$$

Die Menge $\mathfrak{M}$ *aller* molekularen Spezies ist die Menge der Spezies, deren Typen S_n-isomorph sind zu den Linksnebenklassenmengen S_n/U_i, mit $n \in \mathbb{N}$, wobei, zu festem n, U_i eine Transversale der Konjugiertenklassen der Untergruppen von S_n durchläuft. Hier sind die kleinsten molekularen Spezies aufgeführt:

$$\mathfrak{M} = \{1, \mathcal{X}, \mathcal{X}^2, \mathcal{M}_2, \mathcal{X}^3, \mathcal{X} \cdot \mathcal{M}_2, \mathcal{C}_3, \mathcal{M}_3, \ldots\}.$$

Eine weitere Verfeinerung erhält man durch die Einführung *atomarer* Spezies, das sind die molekularen Spezies $\neq 1$, die *bezüglich Multiplikation* nur trivial zerlegbar sind:

$$\mathcal{S} = \mathcal{T} \cdot \mathcal{U} \Longrightarrow \mathcal{T} = 1 \text{ oder } \mathcal{U} = 1.$$

Hier sind die kleinsten atomaren Spezies:

$$\mathfrak{A} = \{\mathcal{X}, \mathcal{M}_2, \mathcal{C}_3, \mathcal{M}_3, \ldots\}.$$

Jede Spezies kann als formale Potenzreihe über den atomaren Spezies aufgefaßt werden, also als Element von $\mathbb{N}[\mathcal{X}, \mathcal{M}_2, \mathcal{C}_3, \mathcal{M}_3, \ldots]$. Den Ring

$$\mathbb{Z}[\mathcal{X}, \mathcal{M}_2, \mathcal{C}_3, \mathcal{M}_3, \ldots],$$

in dem alle diese Elemente, also alle Spezies, liegen, nennt man den Ring der *virtuellen Spezies.* $\diamond$

Übungsaufgaben

Ü 1.12.1 Geben Sie das den schlichten Graphen mit 4 Punkten entsprechende Element des Burnsiderings $\Omega(S_4)$ an.

1.13 Bahnenberechnung

Wir wollen eine endliche Operation ${}_GX$ mit dem Ziel untersuchen, die Menge *aller* Bahnen, *spezielle* von diesen, eine *Transversale* der Bahnen oder auch die *Stabilisatoren* der Punkte zu berechnen. Natürlich ist die Bahnenberechnung hierfür grundlegend, wir diskutieren diese deshalb zuerst.
Im Falle daß $|X|$ und $|G|$ oder $|\bar{G}|$ sehr klein sind und G oder $\bar{G}$ als *Menge* zusammen mit der Operation jedes ihrer Elemente gegeben sind, können wir einfach die jeweilige Menge von Gruppenelementen auf x anwenden und erhalten die gewünschte Bahn $G(x)$. Es ist jedoch oft so, daß G durch eine Menge von Erzeugenden gegeben ist: $G = \langle g_0, \ldots, g_{r-1}\rangle$, zusammen mit den Operationen der g_i auf X. Dann setzen wir, für $x \in X$,

$$\Omega_0 := \{x\}, \text{ und } \Omega_i := \bigcup_{j=1}^{r} g_j\Omega_{i-1}, i \in \mathbb{N}^*.$$

Es ist klar, daß das kleinste i mit $\Omega_i = \Omega_{i-1}$ der folgenden Gleichung genügt

1.13.1 $$G(x) = \Omega_{i-1}.$$

Für eine konkrete Implementierung dieser Methode der Berechnung von $G(x)$ kann man sich noch folgendes zur Beschleunigung überlegen:

$$\Omega_i = \Omega_{i-2} \bigcup \left(\cup_j g_j(\Omega_{i-1} \backslash \Omega_{i-2})\right).$$

Eine Implementierung kann natürlich sehr stark von der jeweiligen Kenntnis von X, G und von der Operation ${}_GX$ abhängen. Beispielsweise ist, bei $|X| = 1$, natürlich $G(x) = \Omega_0$, während $G(x) = X$ gilt, falls $|G\backslash\!\backslash X| = 1$. Wir können also das Lemma von Cauchy-Frobenius als *Abbruchregel* benutzen. Die Kenntnis von $|G\backslash\!\backslash X|$ ist besonders dann hilfreich, wenn wir die gesamte Bahnenmenge $G\backslash\!\backslash X$ haben wollen, in welchem Fall wir mit der restlichen Menge $X\backslash G(x)$ entsprechend verfahren. Wie dies zu implementieren ist, ist klar.
Eine der vielen Fragen, die sich jetzt stellen, ist die nach einer Gewinnung von Erzeugendensystemen. Hier hilft das folgende Resultat:

1.13.2 Hilfssatz (Schreier) *Ist U eine endliche Untergruppe von $G = \langle g_0, \ldots, g_{r-1}\rangle$, die wie folgt in Linksnebenklassen von U zerfällt:*

$$G = \bigcup_{i=0}^{s-1} h_iU, \text{ wobei } h_0 = 1,$$

und ist die Abbildung ϕ definiert durch

$$\phi\colon G \longrightarrow \{h_0, \ldots, h_{s-1}\}\colon g \mapsto h_i, \ \textit{falls } g \in h_i U,$$

dann wird U von den Elementen $\phi(g_i h_k)^{-1} g_i h_k$ erzeugt:

$$U = \langle \phi(g_i h_k)^{-1} g_i h_k \mid i \in r, k \in s \rangle.$$

Beweis: Nehmen wir an, daß $u_0 = a_0 \ldots a_{t-1} \in U$, wobei die a_i Elemente der Menge der Erzeugenden $\{g_0, \ldots, g_{r-1}\}$ sind. Wir setzen

$$u_i := a_i \ldots a_{t-1}, \text{ und } x_i := \phi(u_i),$$

so daß insbesondere $x_0 = \phi(u_0) = 1$. Setzen wir jetzt $x_t := 1$, dann können wir u_0 in der folgenden Form schreiben

$$u_0 = (x_0^{-1} a_0 x_1)(x_1^{-1} a_1 x_2) \ldots (x_{t-1}^{-1} a_{t-1} x_t).$$

Es gilt $x_i = \phi(u_i) = \phi(a_i u_{i+1}) = \phi(a_i x_{i+1})$, denn $x_{i+1} = \phi(u_{i+1})$ bedeutet daß $u_{i+1} = x_{i+1} u'$, für geeignetes $u' \in U$, so daß $a_i u_{i+1} = a_i x_{i+1} u'$. Es gilt demnach

$$u = \phi(a_0 x_1)^{-1} a_0 x_1 \phi(a_1 x_2)^{-1} a_1 x_2 \ldots,$$

was den Beweis vervollständigt.

□

1.13.3 Beispiel Wir wollen diese Möglichkeit, Erzeugende von Untergruppen zu gewinnen, einmal auf die Ermittlung von Erzeugenden alternierender Gruppen anwenden. Dazu gehen wir von dem bekannten Erzeugendensystem der symmetrischen Gruppen aus:

$$S_n = \langle (12), (12 \ldots n) \rangle, n \geq 2,$$

und benutzen die folgende Zerlegung in Linksenbenklassen:

$$S_n = A_n \cup (12) A_n,$$

d.h. wir nehmen

$$g_0 = (12), g_1 = (1 \ldots n), h_0 = 1, h_1 = (12).$$

In der folgenden Tabelle listen wir die zu berechnenden Ausdrücke auf:

$g_i h_k$	$\Phi(g_i h_k)$	$\Phi(g_i h_k)^{-1}$	$\Phi(g_i h_k)^{-1} g_i h_k$
(12)	(12)	(12)	1
1	1	1	1
$(1 \ldots n)$	$\begin{cases} 1 & 2 \nmid n \\ (12) & 2 \mid n \end{cases}$	$\begin{cases} 1 & 2 \nmid n \\ (12) & 2 \mid n \end{cases}$	$\begin{cases} (1 \ldots n) & 2 \nmid n \\ (2 \ldots n) & 2 \mid n \end{cases}$
$(13 \ldots n)$	$\begin{cases} (12) & 2 \nmid n \\ 1 & 2 \mid n \end{cases}$	$\begin{cases} (12) & 2 \nmid n \\ 1 & 2 \mid n \end{cases}$	$\begin{cases} (13 \ldots n2) & 2 \nmid n \\ (13 \ldots n) & 2 \mid n \end{cases}$

Dies ergibt Erzeugendensysteme aus zwei Elementen für die alternierenden Gruppen:

$$A_n = \begin{cases} \langle (1 \ldots n), (13 \ldots n2) \rangle, & \text{falls } n \text{ ungerade,} \\ \langle (2 \ldots n), (13 \ldots n) \rangle, & \text{falls } n \text{ gerade ist.} \end{cases}$$

$\diamond$

Es gibt aber auch andere Methoden, die Anwendung von Gruppen zur Bahnenberechnung zweckmäßig zu organisieren. Die wichtigste, weil problemorientierte Methode ist die Verwendung sogenannter Simsketten, die jetzt eingeführt werden sollen. Simsketten sind Untergruppenketten, die aus Stabilisatoren bestehen. Wir numerieren deshalb die Elemente der Menge X, auf der die in Frage stehende Gruppe G operiert, oder, noch einfacher, wir setzen voraus, X sei die Menge n. Anstelle der Gruppe G betrachten wir ihr Bild in S_n, also die Permutationsgruppe $\bar{G}$ auf dieser Menge. Die *punktweisen* Stabilisatoren von Teilmengen $k \subseteq n$, also die Untergruppen der Form

$$\bar{G}_k := \{\pi \in \bar{G} \mid \forall i \in k \colon \pi i = i\},$$

bilden die folgende Untergruppenkette

$$\bar{G} = \bar{G}_0 \geq \bar{G}_1 \geq \ldots \geq \bar{G}_{n-1} \geq \bar{G}_n = \{1\}.$$

Es gibt demnach ein kleinstes b mit

1.13.4 $$\bar{G} = \bar{G}_0 \geq \ldots \geq \bar{G}_b = \{1\}$$

Wir nennen die *Menge* b die *Basis* der Operation von G auf n, ihre Kardinalzahl b deren *Länge*, und 1.13.4 die *Simskette* dieser Operation. Jetzt betrachten wir Zerlegungen in Linksnebenklassen

1.13.5 $$\bar{G}_{i-1} = \bigcup_{j=0}^{r(i)-1} \pi_j^{(i)} \bar{G}_i, \pi_0^{(i)} = 1,$$

und wir bemerken, daß jedes $\pi \in \bar{G}$ auf eindeutige Weise in diesen Nebenklassenrepräsentanten ausgedrückt werden kann:

1.13.6 $$\pi = \pi_{j_1}^{(1)} \cdots \pi_{j_b}^{(b)}.$$

Es gilt also insbesondere:

1.13.7 $$|\bar{G}| = \prod_{i=1}^{b} r(i).$$

Dies zeigt, daß die Speicherung der $\pi_j^{(i)}, i \in b, j \in r(i)$, einen ökonomischen Umgang mit den Elementen von $\bar{G}$ erlaubt, wir brauchen nämlich nur die Elemente des nachfolgenden Baumes zu durchlaufen. Das Ziel der folgenden Überlegungen wird sein, diesen Baum so weit als möglich zu beschneiden. Eine erste diesbezügliche Markierung zeigt, daß wir diesen Baum unterhalb einer gewissen Ebene beschneiden können, die von dem gegebenen Punkt der Bahn abhängt, die berechnet werden soll:

1.13.8 $$\begin{array}{ccccccc} & \pi_0^{(1)} & & \cdots \quad \cdots \quad \cdots & & \pi_{r(1)-1}^{(1)} & \\ & \swarrow \cdots \searrow & & \cdots & & \swarrow \cdots \searrow & \\ \pi_0^{(1)}\pi_1^{(2)} & \cdots & \pi_0^{(1)}\pi_{r(2)-1}^{(2)} & \cdots & \pi_{r(1)-1}^{(1)}\pi_1^{(2)} & \cdots & \pi_{r(1)-1}^{(1)}\pi_{r(2)-1}^{(2)} \\ \swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow & \cdots & \swarrow \cdots \searrow \end{array}$$

Das Ziel der folgenden Überlegungen wird sein, diesen Baum so weit als möglich zu beschneiden. Eine erste diesbezügliche Markierung zeigt, daß wir diesen Baum unterhalb einer gewissen Ebene beschneiden können, die von dem gegebenen Punkt der Bahn abhängt, die berechnet werden soll: Wegen $\pi_j^{(i)} k = k$, für $i > k$, gilt folgendes für die Bahn von $k \in n$ unter G:

1.13.9 $$G(k) = \{\pi_{j_1}^{(1)} \ldots \pi_{j_k}^{(k)} k \mid j_1 \in r(1), \ldots, j_k \in r(k)\}.$$

Demnach reduziert die Kenntnis der Simskette die Anzahl notwendiger nachzuprüfender Operationen erheblich. Die Berechnung der Basis ist deshalb sehr wichtig.

1.13.10 Beispiel Betrachten wir beispielsweise die Operationen von S_p auf der Menge der 2–elementigen Teilmengen von p. Um die Basis von $\bar{G} = \bar{S_p}$ zu berechnen, betten wir zunächst die Menge aller 2–elementigen Teilmengen von p in n ein, $n := \binom{p}{2}$, indem wir die Paare lexikographisch anordnen:

$$\{1,2\} < \{1,3\} < \ldots < \{1,p\} < \{2,3\} < \ldots < \{2,p\} < \ldots < \{p-1,p\},$$

und die Parre dementsprechend durch die natürlichen Zahlen $1, \ldots, \binom{p}{2}$ ersetzen. Eine leichte Rechnung zeigt, daß, gemäß dieser Numerierung, die folgende Kette von Young-Untergruppen

$$S_p \geq S_{(2,p-2)} \geq S_{(1,1,1,p-3)} \geq \ldots \geq S_{(1,\ldots,1,2)} \geq \{1\}$$

per Einbettung die folgende Simskette ergibt

$$\bar{G} = \bar{S}_p \geq \bar{S}_{(2,p-2)} \geq \bar{S}_{(1,1,1,p-3)} \geq \ldots \geq \bar{S}_{(1,\ldots,1,2)} \geq \{1\}.$$

Also ist $p-2$ die Basis für die kanonische Operation von $\bar{S}_p$ auf der Menge der 2–elementigen Teilmenge,bezogen auf deren lexikographische Anordnung. Für den Spezialfall $p := 5$ erhalten wir demnach die Simskette (bezogen auf die obige Numerierung der Punktepaare)

$$\bar{S}_5 \geq \bar{S}_{(2,3)} \geq \bar{S}_{(1,1,1,2)} \geq \{1\}.$$

$\diamond$

Eine weitere hilfreiche Eigenschaft der Basis kann wie folgt beschrieben werden

1.13.11 Hilfssatz *Die Elemente $\pi \in \bar{G}$ sind durch ihre Operation auf der Basis b vollständig bestimmt.*

Beweis: Ist nämlich $\pi i = \rho i$, für jedes $i \in b$, dann gilt $\pi^{-1}\rho \in \bar{G}_b = \{1\}$, so daß $\pi = \rho$.

$\square$

1.14 Transversalenberechnung

Die zentrale — zumindest die schwierigste — Aufgabe der *konstruktiven Theorie diskreter Strukturen* ist natürlich die Berechnung von Katalogen solcher Strukturen, etwa die Berechnung der Menge aller schlichten Graphen mit vorgegebener Punkte- und Kantenzahl, die Konstruktion aller wesentlich verschiedenen linearen Codes mit gegebenen Parametern n, k, d, die Konstruktion aller molekularen Graphen zu gegebener chemischer Formel usw. Wie in der Einleitung bereits erwähnt wurde, gibt es tatsächlich viele Situationen in den Anwendungen, wo solche Kataloge erforderlich sind, etwa in der Molekularen Strukturerkennung. Generell stehen wir also jetzt vor der Aufgabe, Transversalen von Bahnen zu berechnen.
Als einen Ansatz, der sich schon bestens bewährt hat, verwenden wir den grundlegenden Hilfssatz 1.6.3, der zeigt, daß Bahnen ähnlich Linksnebenklassenmengen sind:

$$_H(H(x)) \approx {}_H(H/H_x),$$

woraus unmittelbar folgt, daß die auf eine Untergruppe G von H eingeschränkte Operation auf $H(x)$ ähnlich der Operation von G auf H/H_x ist:

1.14.1 $$_G(H(x)) \approx {}_G(H/H_x).$$

Dies eröffnet eine weitere Strategie, diskrete Strukturen zu berechnen:

1.14.2 Strategie II: Verwende geeignete Obergruppen!
Sind die vorgegebenen diskreten Strukturen als Bahnen einer Gruppe G auf einer Menge X definiert, dann kann man in folgender Weise Repräsentanten dieser Bahnen und damit die diskreten Strukturen auf X ermitteln:

- *Man wählt eine geeignete Obergruppe H von G, die ebenfalls auf X operiert, bzw. eine Obergruppe $\bar{H} \leq S_X$ von $\bar{G}$, und schränkt die Betrachtung auf jeweils eine von deren Bahnen $H(x)$ ein (schon dies ist sehr oft ein erheblicher Gewinn, weil dadurch die zu verarbeitenden Mengen in der Regel deutlich kleiner sind: $H(x)$ anstelle von X).*
- *Man ermittelt den Stabilisator H_x und eine Transversale der Menge H/H_x seiner Linksnebenklassen.*
- *Schließlich bleibt festzustellen, welche Elemente der Transversalen von H/H_x zu derselben Bahn von G gehören.*

Insgesamt ergibt sich dann die gesuchte Transversale als Vereinigung der Transversalen der G-Bahnen auf den H-Bahnen:

$$\bigcup_{H(x)\in H\backslash\backslash X} T_x,\ T_x \textit{ eine Transversale von } G\backslash\backslash H(x).$$

1.14.3 Beispiel Wir wollen die Anwendung dieser Strategie auf die Konstruktion einer Transversalen der G–Klassen auf $Y^X := m^n$ beschreiben. Dazu werden wir die Betrachtung auf G–Klassen festen Inhalts $\lambda = (\lambda_0, \ldots, \lambda_{m-1})$ einschränken, $\lambda_i := |f^{-1}(i)|$, denn wir wissen, daß die symmetrische Gruppe S_n auf dieser Menge transitiv ist, so daß die angegebene Strategie angewandt werden kann.
Gehen wir von der *kanonischen Abbildung* f mit diesem Inhalt aus:

$$f_\lambda := (f_\lambda(0), \ldots, f_\lambda(n-1)) := (\underbrace{0, \ldots, 0}_{\lambda_0}, \ldots, \underbrace{m-1, \ldots, m-1}_{\lambda_{m-1}}).$$

Die Menge aller Abbildungen von diesem Inhalt werden wir wie folgt bezeichnen:

$$m^n_\lambda := \{\pi f_\lambda = f_\lambda \circ \pi^{-1} \mid \pi \in S_n\} = S_n(f_\lambda).$$

Wir wollen eine Transversale von m^n_λ konstruieren, und zwar aus einer Transversalen von

$$S_n/(S_n)_{f_\lambda}.$$

Es gilt also, zunächst einmal eine Transversale dieser Menge von Linksnebenklassen zu bestimmen. Anstelle der Elemente dieser Transversalen, also anstelle von Gruppenelementen, können wir natürlich auch die diesen entsprechenden $f \in m^n_\lambda$ nehmen, das ist anschaulicher.
Eine Abbildung $f \in m^n_\lambda$ kann durch ihr λ–*Tabloid*

$$\begin{array}{l} \hline i_0 \ldots i_{\lambda_0-1} \\ \hline j_0 \ldots j_{\lambda_1-1} \\ \hline \ldots \end{array}\ ,$$

beschrieben werden, das die Elemente des Urbilds $f^{-1}(k)$ von $k \in m$ in seiner k-ten Zeile enthält, etwa in aufsteigender Reihenfolge, also z.B.

$$f(i_0) = \ldots = f(i_{\lambda_0-1}) = 1, \text{ und } i_0 < \ldots < i_{\lambda_0-1}.$$

Betrachten wir als ein Beispiel die Graphen mit 4 Punkten und 2 Kanten, also $n = \binom{4}{2} = 6$, $m = 2$, und $\lambda = (4,2)$. Bevor wir aber die 15 $(4,2)$–Tabloide in allen Einzelheiten hinschreiben, ist es zweckmäßig zu bemerken, daß in jedem Tabloid die nullte Zeile (wir numerieren von Null an!) durch die restlichen Zeilen eindeutig bestimmt wird, die das *verkürzte* Tabloid bilden. In unserem Beispiel brauchen wir also nur jeweils die zweite Zeile anzugeben, hier sind diese zweiten Zeilen:

$$\overline{\underline{12}},\ \overline{\underline{13}},\ \overline{\underline{14}},\ \overline{\underline{15}},\ \overline{\underline{16}},\ \overline{\underline{23}},\ \overline{\underline{24}},\ \overline{\underline{25}},\ \overline{\underline{26}},\ \overline{\underline{34}},\ \overline{\underline{35}},\ \overline{\underline{36}},\ \overline{\underline{45}},\ \overline{\underline{46}},\ \overline{\underline{56}}.$$

Entsprechend obigem Argument müssen wir die Bahnen von $\bar{S_4}$ auf dieser Menge bestimmen. Wiederholen wir, daß die Elemente $1, \ldots, 6 \in 6$ auf denen S_6 operiert, für die Paare $\{1,2\}, \ldots, \{3,4\}$ von Punkten stehen. Die Untergruppe

$$\bar{S_4} \hookrightarrow S_6$$

die von $S_4 = \langle (12), (1234) \rangle$ auf dieser Menge von Punktepaaren induziert wird ist

$$\bar{S_4} = \langle (24)(35), (1463)(25) \rangle,$$

und deshalb ist eine der beiden Bahnen von $\bar{S_4}$ auf der Menge der $(4,2)$–Tabloide gleich

$$\omega_2 := \{\overline{\underline{16}}, \overline{\underline{25}}, \overline{\underline{34}}\},$$

während die andere Bahn ω_1 aus den restlichen 12 verkürzten Tabloiden besteht. (Es sei noch bemerkt, daß wir in einer Vorberechnung anhand der oben beschriebenen Abzählungstheorie ermitteln können, daß die Anzahl der Graphen mit 4 Punkten und 2 Kanten gleich *zwei*, ist, ein Resultat, das als *Abbruchregel* sehr hilfreich ist, wie schon das gegenwärtige Beispiel zeigt!)
Die lexikographisch kleinsten Elemente dieser Bahnen ω_1, ω_2 sind die Tabloide die $\overline{\underline{56}} \in \omega_1$ und $\overline{\underline{34}} \in \omega_2$ entsprechen. Diese Tabloide sind

$$\begin{array}{c}\overline{\underline{1234}}\\ \underline{56}\end{array} \quad \text{und} \quad \begin{array}{c}\overline{\underline{1256}}\\ \underline{34}\end{array}.$$

Die entsprechenden dAbbildungen $f, f' \in 2^6$ sind

$$f = (1,1,1,1,2,2),\ \text{und}\ f' = (1,1,2,2,1,1).$$

Also bilden die beiden Graphen aus Abbildung 1.8 eine vollständige Menge von Graphen mit 4 Punkten und 2 Kanten! Die gerade

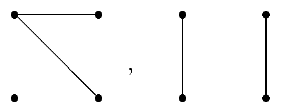


Abbildung 1.8: Die Graphen mit 4 Punkten und 2 Kanten

beschriebene Methode ihrer Bestimmung ist natürlich mühsam, sie kann aber für Kataloge von Graphen mit ≤ 7 Punkten benutzt werden. Weitere Verfeinerungen ermöglichen die Berechnung von Katalogen bis hin zu $v = 12$.

$\diamond$

Kehren wir jetzt wieder zur Gleichung 1.14.1 zurück. Die Bahnen von G auf H/H_x sind gerade die Doppelnebenklassen

$$G(hH_x) := \bigcup_{g \in G} ghH_x = GhH_x,$$

so daß wir eine natürliche Bijektion zwischen der Bahnenmenge von G auf $H(x)$ und der Menge $G\backslash H/H_x$ dieser Doppelnebenklassen bekommen:

$$G\backslash\!\backslash H(x) \to G\backslash H/H_x : G(hx) \mapsto GhH_x.$$

Was für Bahnen gilt, ist für transitive Operationen richtig, es folgt also

1.14.4 Folgerung *Ist ${}_HX$ transitiv und G eine Untergruppe von H, dann haben wir für jedes $x \in X$ eine natürliche Bijektion*

$$\varphi : G\backslash\!\backslash X \to G\backslash H/H_x : G(hx) \mapsto GhH_x.$$

Ist D eine Transversale der Menge von Doppelnebenklassen $G\backslash H/H_x$ dann erhalten wir aus dieser die folgende Transversale der Bahnen von G :

$$T := \{hx \mid h \in D\}.$$

$\square$

Diese Tatsache soll deshalb hervorgehoben werden, man kann sie tatsächlich als Grundlage einer *Strategie* nehmen.

1.14.5 Strategie III: Verwende Doppelnebenklassen! *Wann immer diskrete Strukturen als Äquivalenzklassen auf einer Menge X definiert werden können, ist es im Prinzip möglich, die folgende Strategie zur Konstruktion des vollständigen Katalogs dieser Strukturen auf X zu verwenden:*

- *Zunächst definiert man — gemäß Strategie I (vgl. 1.5.8) — die Strukturen auf X als Bahnen einer endlichen Gruppe G auf X, indem man die Äquivalenzrelation durch eine Gruppenoperation ${}_GX$ ersetzt. (vergleiche 1.5.7).*

- *Danach sucht man — gemäß Strategie II (vgl. 1.14.2) — eine geeignete Obergruppe H von G und schränkt die Betrachtung auf eine einzelne von deren Bahnen $H(x)$ ein. Falls man eine auf ganz X transitiv operierende Gruppe nimmt, ist das keine Einschränkung des Blickwinkels, andernfalls hat man den nachfolgend beschriebenen Vorgang für jede einzelne von diesen Bahnen durchzuziehen.*

- *Hat man ein solches H gewählt, dann ergibt sich für jedes $x \in X$ eine Bijektion zwischen der Menge der Bahnen $G\backslash\backslash H(x)$ und der Menge $G\backslash H/H_x$ von Doppelnebenklassen:*

$$G\backslash\backslash H(x) \to G\backslash H/H_x : G(hx) \mapsto GhH_x.$$

- *Man berechnet deshalb im nächsten Schritt zu jeder Bahn $H(x)$ eine Transversale D_x der Doppelnebenklassenmengen $G\backslash H/H_x$, vereinigt diese Transversalen zu einer Menge $D = \cup D_x$ und bekommt aus dieser Vereinigung von Transversalen D schließlich eine Transversale T der Bahnen von G auf X :*

$$T := \{hx \mid h \in D\}.$$

Die Elemente dieser Transversalen T bilden einen vollständigen Katalog der gegebenen diskreten Strukturen auf X!

□

Eine interessante Anwendung von Doppelnebenklassen ist die Berechnung von *Designs.* Hier geht es in vielen Fällen zunächst einmal um den Nachweis der *Existenz* von Designs mit vorgegebenen Parametern. Beispielsweise hat man viele Jahre lang nach sogenannten 7-Designs mit kleinen Paramtern (s.u.) gesucht, nachdem erste

6-Designs konstruiert worden waren. Hat man diese Frage nach der Existenz positiv beantworten können, dann will man natürlich auch wissen, wie grøß der Katalog aller Designs mit den vorgegebenen Parametern ist. Wir wollen hier zunächst aber nur das Existenzproblem diskutieren. Es soll gezeigt werden, wie Doppelnebenklassen zur Konstruktion erster 7-Designs verhalfen (vgl. [2]), indem die Verwendung von obiger Doppelnebenklassenstrategie eine ganz enorme *Datenreduktion* ergab, die das gegebene Existenzproblem erst in die Reichweite einer Computerlösung brachte.
Ein $t-(v,k,\lambda)$-*Design* ist ein Paar $(V,\mathcal{B})$, bestehend aus einer Menge V von Punkten (vertices) und einer Menge $\mathcal{B}$ von Blöcken, mit

$$|V| = v, \mathcal{B} \subseteq \binom{V}{k}, \forall\, T \in \binom{V}{t} : |\{B \in \mathcal{B} \mid T \subseteq B\}| = \lambda.$$

Designs mit $\lambda = 1$ heißen *Steinersysteme.* Man kann diese Designs mit Hilfe einer Matrix $M^v_{t,k}$ beschreiben: Ihre Zeilen gehören zu den $T \in \binom{V}{t}$, ihre Spalten zu den $B \in \binom{V}{k}$, und die Elemente m^v_{TB} von $M^v_{t,k}$ sind so definiert:

$$m^v_{TB} := \begin{cases} 1, & \text{falls } T \subseteq B, \\ 0, & \text{sonst.} \end{cases}$$

Ein $t-(v,k,\lambda)$-Design $(V,\mathcal{B})$ ist demnach eine Teilmatrix von $M^v_{t,k}$, die gerade aus den Spalten besteht, die zu den Blöcken des Designs gehören. Dies wiederum kann man leicht in der Sprache der linearen Gleichungssysteme formulieren:

1.14.6 Folgerung *Numeriert man die Elemente von V bzw. von $\binom{V}{k}$, dann ergeben sich die $t-(v,k,\lambda)$-Designs mit Punktemenge V (bijektiv) aus den die 0-1-Lösungen x des linearen Gleichungssystems*

$$M^v_{t,k} \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}.$$

Die Blöcke des Designs zu x sind die k-Teilmengen von V, die durch die von Null verschiedenen Koordinaten von x bestimmt werden.

Bei der Suche nach 7-Designs hatte man schon seit vielen Jahren die Hoffnung, es könne $7-(33,8,\lambda)$-Designs geben, λ war aber unbekannt, auch das wohl ein Grund dafür, daß dieses Problem so lange offen blieb. Bei diesen Parametern erhält man eine Matrix $M^{33}_{7,8}$ mit etwa $6 \cdot 10^{13}$ Elementen, und es ist klar, daß die Suche nach 0-1-Lösungen einer Gleichung mit einer derart großen Koeffizientenmatrix hoffnungslos ist. Die Strategie, die hier dennoch zu einer Lösung führte ist hier die folgende:

1.14.7 Strategie IV: Vorgeben einer Symmetriegruppe!
Man schränke die Betrachtung bei zu umfangreichen Problemen auf Strukturen mit vorgegebener Stabilisatorklasse ein.

Dieses Verfahren ist natürlich ziemlich riskant, wenn es um die Lösung von Existenzproblemen geht, denn es kann natürlich sehr leicht sein, daß es zu vorgegebener Konjugiertenklasse von Untergruppen *keine* Struktur von diesem Typ gibt. Aber es gibt auch andere Fälle, zu denen glücklicherweise gewisse 7-Designs gehören:

1.14.8 Beispiel Ein Element π der symmetrischen Gruppe S_V heißt genau dann ein *Automorphismus* des Designs $(V, \mathcal{B})$, wenn gilt

$$\pi\mathcal{B} := \{\pi B := \{\pi b \mid b \in B\} \mid B \in \mathcal{B}\} = \mathcal{B}.$$

Eine Gruppe aus solchen Automorphismen heißt *eine Gruppe von Automorphismen* des Designs, und die maximale Gruppe dieser Art, also

$$Aut(V, \mathcal{B}) := \{\pi \in S_V \mid \pi\mathcal{B} = \mathcal{B}\},$$

heißt *die (volle) Automorphismengruppe* von $(V, \mathcal{B})$. Die Aufgabe ist, alle Designs mit vorgegebenen Parametern und vorgegebener Gruppe $A \leq Aut(V, \mathcal{B})$ zu ermitteln. (Das naheliegende weiterführende Problem der Bestimmung aller Designs mit $A = Aut(V, \mathcal{B})$ wollen wir hier nicht diskutieren, es ist aber sehr interessant!)
Um dieses Problem in die Reichweite moderner Computertechnik zu bringen, betrachtet man anstelle von $M^v_{t,k}$ die folgende wesentlich kleinere Matrix. Zu vorgegebener Untergruppe $A \leq S_V$ bildet man eine sogenannte *Inzidenzmatrix*

$$M^A_{t,k} := (m^A_{T,K}).$$

(Diese Matrix ist übrigens eine Teilmatrix der Matrix $A^\wedge$ zum Verband der Teilmengen von V!) T durchläuft dabei eine Transversale von $A \backslash\!\backslash \binom{V}{t}$ und K eine Transversale von $A \backslash\!\backslash \binom{V}{k}$. Die Einträge dieser Matrix werden wie folgt definiert:

$$m^A_{T,K} := |\{K' \in A(K) \mid T \subseteq K'\}|.$$

Das fundamentale Resultat ist

1.14.9 Der Satz von Kramer und Mesner *Die Menge aller $t-(v,k,\lambda)$-Designs mit A als einer Gruppe von Automorphismen ergibt sich aus der Menge aller 0-1-Lösungen x des linearen Gleichungssystems*

$$M_{t,k}^A \cdot x = \begin{pmatrix} \lambda \\ \vdots \\ \lambda \end{pmatrix}.$$

Betrachten wir zunächst ein ganz kleines Beispiel: Die Parameter seien $t := \lambda := 1$, $v := 4$ und $k := 2$. Als gewünschte Automorphismengruppe wählen wir

$$A := \langle (1234), (24) \rangle,$$

das ist eine Untergruppe der Ordnung 8 in S_4. Die Menge der Punkte ist also $V := \{1,2,3,4\}$, so daß wir die Bahnen von A auf folgenden Mengen berechnen müssen:

$$\binom{V}{k} = \{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\},$$

und

$$\binom{V}{t} = \{\{1\},\{2\},\{3\},\{4\}\}.$$

Diese Bahnenmengen sind offensichtlich

$$A \backslash\backslash \binom{V}{k} = \{\{\{1,2\},\{1,4\},\{2,3\},\{3,4\}\},\{\{1,3\},\{2,4\}\}\},$$

und

$$A \backslash\backslash \binom{V}{t} = \{\{1,2,3,4\}\}.$$

Diese Bahnen parametrisieren die Zeilen und Spalten der gesuchten Inzidenzmatrix, die nach der Definition ihrer Einträge die folgende Form hat:

$$M_{t,k}^A = \begin{pmatrix} 2 & 1 \end{pmatrix}.$$

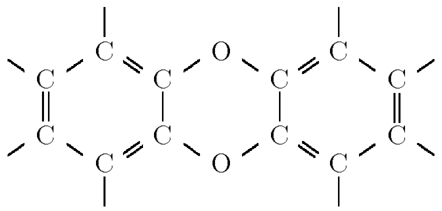
Da die rechte Seite gleich $(\lambda) = (1)$ ist, gibt es genau eine 0-1-Lösung des entsprechenden Gleichungssystems, nämlich

$$x = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Es gibt demnach genau ein $1-(4,2,1)$-Design mit A als einer Gruppe von Automorphismen. $\diamond$

Wir können jetzt auch das in der Einleitung erwähnte Problem der Bestimmung aller Dioxinisomere lösen:

1.14.10 Beispiel Die Isomere des Dioxin werden durch die molekularen Graphen mit der chemischen Formel $C_{12}O_2H_4Cl_4$ beschrieben, die die folgende Substruktur besitzen:



Das heißt, diese molekularen Graphen entsprechen den *wesentlich verschiedenen* Verteilungen von genau 4 Wasserstoff- und 4 Chloratomen auf die 8 freien Valenzen dieser Substruktur. "Wesentlich verschieden" bezieht sich dabei auf die Symmetriegruppe dieses Skeletts, genauer: dessen Plazierung im Raum, die als planar und regelmäßig angenommen wird. Die Symmetriegruppe ist also die Kleinsche Vierergruppe V_4.
Diese Plazierungen der Wasserstoff- und Chloratome können wir also als Abbildungen

$$f \in Y^X = \{H, Cl\}^8$$

auffassen, die vom Inhalt $(4,4)$ sind. Zu bestimmen ist also die Ordnung von, noch besser natürlich eine Transversale von

$$V_4 \backslash\!\backslash \{H, Cl\}^8_{(4,4)},$$

einer Menge, die — wie wir seit kurzem wissen — bijektiv ist zur Menge von Doppelnebenklassen

$$V_4 \backslash S_8 / S_4 \oplus S_4.$$

Ermitteln wir deshalb noch eine Formel zur Berechnung der Kardinalität von Doppelnebenklassenmengen.

1.14.11 Hilfssatz *Sind A und B Untergruppen von G, dann gilt für die Menge der (A,B)-Doppelnebenklassen in G :*

$$A \backslash G / B := \{AgB \mid g \in G\} = (A \times B) \backslash\!\backslash G,$$

sowie

$$|A\backslash G/B| = \frac{|G|}{|A||B|}\sum_{g\in C}\frac{|C^G(g)\cap A||C^G(g)\cap B|}{|C^G(g)|}.$$

Beweis: Das Cauchy-Frobenius Lemma liefert die gesuchte Anzahl von Doppelnebenklassen. Zu seiner Anwendung benötigen wir die Anzahl $|G_{(a,b)}|$ von Fixpunkten von $(a,b)\in G$. Diese ist:

$$|\{g \mid a = gbg^{-1}\}| = \begin{cases} |C_G(a)| = |C_G(b)| & \text{falls } a,b \text{ konjugiert,}\\ 0 & \text{sonst.}\end{cases}$$

Daraus ergibt sich

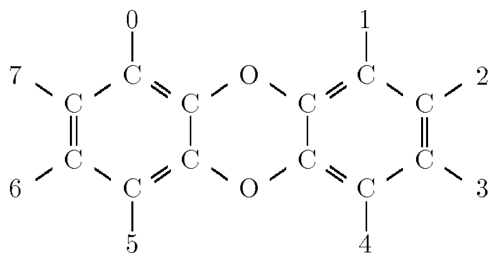
$$|A\backslash G/B| = \frac{1}{|A||B|}\sum_{a\in A}|C^G(a)\cap B||C_G(a)|$$

$$= \frac{1}{|A||B|}\sum_{g\in\mathfrak{C}}|C^G(g)\cap A||C^G(g)\cap B||C_G(g)|,$$

wobei $\mathfrak{C}$ eine Transversale der Konjugiertenklassen in G bezeichnet. Hieraus folgt die Behauptung.

□

Wenden wir dies auf die Dioxinisomere an. Da die Kleinsche Vierergruppe operiert, müssen wir deren Erzeugende oder alle Elemente angeben. Dazu numerieren wir die freien Valenzen der Substruktur:



Die Kleinsche Vierergruppe $\bar{V}_4$, die Symmetriegruppe dieses (jetzt numerierten) Skeletts, wird von den beiden Spiegelungen an der horizontalen und vertikalen Achse erzeugt, also gilt

$$\bar{V}_4 = \langle (05)(14)(23)(67), (01)(27)(36)(45)\rangle,$$

Diese Gruppe besteht aus der Identität und 3 Permutationen, die aus je vier 2-Zyklen bestehen. Da in S_8 genau 105 Permutationen von diesem Typ, und in S_4 genau 3 Permutationen liegen, die aus genau zwei 2-Zyklen bestehen, ergibt sich aus obiger Formel für die Anzahl der Doppelnebenklassen

$$|\bar{V_4}\backslash S_8/S_4 \oplus S_4| = \frac{8!}{4 \cdot 4! \cdot 4!}\left(1 + \frac{3 \cdot 3 \cdot 3}{105}\right) = 22.$$

Die entsprechenden molekularen Graphen sind in der Einleitung bereits abgebildet worden.

◇

1.15 Gleichverteilte Zufallserzeugung

Die Berechnung einer Bahnentransversalen ist nur beschränkt durchführbar, da es sich meist um sehr große Mengen von Bahnen handelt, z. B. gibt es ca. 10^9 Graphen mit 11 Punkten. Dennoch will man unter Umständen Hypothesen für Graphen, Codes, Designs oder andere diskrete Strukturen mit weit mehr Punkten testen. Hier bleibt nur die Stichprobe übrig, d. h. man sucht nach einer Methode, Graphen mit gegebener Punktezahl *gleichverteilt zufallszuerzeugen.* Hierzu bietet sich das folgende Resultat an:

1.15.1 Der Algorithmus von Dixon und Wilf *Für eine endliche Gruppenoperation $_GX$ kann man wie folgt Bahnenrepräsentanten gleichverteilt zufallserzeugen:*

- *Man wählt zunächst eine Konjugiertenklasse C von G mit Wahrscheinlichkeit*

$$p(C) := \frac{|C||X_g|}{|G||G\backslash\!\!\backslash X|},\ \textit{für } g \in C.$$

- *Dann nimmt man ein $g \in C$ und erzeugt zu diesem zufällig und gleichverteilt einen Fixpunkt $x \in X_g$.*

Dieses x ist dann über die Bahnen gleichverteilt:

$$p(x \in \omega) = \frac{1}{|G\backslash\!\!\backslash X|}.$$

Beweis: Seien Let $C_1, \ldots, C_r$ die Konjugiertenklassen der Elemente von G, mit Repräsentanten $g_i \in C_i$. Mit dem Lemma von Cauchy-Frobenius erhalten wir

$$\sum_{i=1}^{r} p(C_i) = \frac{\sum_i |C_i||X_{g_i}|}{\sum_g |X_g|} = 1,$$

$p(-)$ definiert also tatsächlich eine Wahrscheinlichkeitsverteilung. Ist jetzt $\omega \in G\backslash\!\!\backslash X$, dann gilt

$$p(x \in \omega) = \sum_i p(C_i) p(x \in X_{g_i} \cap \omega)$$

$$= \sum_i p(C_i) \frac{|X_{g_i} \cap \omega|}{|X_{g_i}|} = \sum_i \frac{|C_i||X_{g_i}|}{|G||G\backslash\!\!\backslash X|} \frac{|X_{g_i} \cap \omega|}{|X_{g_i}|}$$

$$= \frac{1}{|G||G\backslash\!\!\backslash X|}\sum_i |C_i||X_{g_i}\cap\omega| = \frac{1}{\sum_g |X_g|}\sum_g |X_g\cap\omega|.$$

Nun ist aber

$$\sum_g |X_g\cap\omega| = \sum_{g\in G}\sum_{x\in X_g\cap\omega} 1 = \sum_{x\in\omega}\sum_{g\in G_x} 1 = \sum_{x\in\omega}|G_x|,$$

was gleich ist $|G_y||\omega| = |G|$, für jedes $y\in\omega$, und wir sind fertig.

□

Der Algorithmus läßt sich gut auf Symmetrieklassen anwenden, betrachten wir wieder unser Standardbeispiel:

1.15.2 Beispiel Wir wollen Graphen mit 4 Punkten gleichverteilt zufallserzeugen. Die Konjugiertenklassen von S_4 sind durch die eigentlichen Partitionen von 4 parametrisiert, dies sind die Partitionen $(4),(3,1),(2^2),(2,1^2)$ und (1^4) von 4. Die Ordnungen der entsprechenden Konjugiertenklassen sind 6,8,3,6 und 1. Die von Repräsentanten dieser Konjugiertenklassen auf der Menge der Punktepaare induzierten Permutationen haben die folgenden Anzahlen zyklischer Faktoren: 2,2,4,4 und 6, so daß die Anzahlen von Fixpunkten die folgenden sind: 4,4,16,16 und 64. Dies ergibt für die jeweiligen Wahrscheinlichkeiten die Werte

$$3/33, 4/33, 6/33, 12/33, 8/33.$$

Wir können diese Werte noch mit 33 multiplizieren, um ganze Zahlen zu erhalten, es ergeben sich die Zahlen 3,4,6,12,8. Diese akkumulieren wir noch und erhalten

$$3, 7, 13, 25, 33.$$

Ein Generator, der Zufallszahlen zwischen 1 und 33 erzeugt, wählt dann entsprechend die Konjugiertenklasse. Wählt er beispielsweise eine der Zahlen 1,2 oder 3, dann bedeutet dies die Wahl der ersten Konjugiertenklasse, also der Konjugiertenklasse zur Partition (4), die aus den Viererzyklen besteht, während die Erzeugung von 4,5,6 oder 7 die Wahl der Konjugiertenklasse aus den Dreierzyklen bedeutet.

Nehmen wir an, der Zufallsgenerator erzeuge die Zahl 12. Diese bedeutet die Wahl der Konjugiertenklasse zur Partition (2^2), also der Klasse der Doppeltranspositionen. In dieser Klasse liegt (12)(34). Die hiervon auf den 6 Punktepaaren (die von den Punkten mit den Nummern 0,1,2,3 gebildet werden) induzierte Permutation ist

$$\overline{(12)(34)} = (\{0,1\})(\{0,2\},\{1,3\})(\{0,3\},\{1,2\})(\{2,3\}).$$

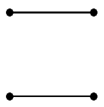


Abbildung 1.9: Der zufallserzeugte numerierte Graph

Fixpunkte hiervon können wir nun dadurch gleichverteilt zufallserzeugen, indem wir den zyklischen Faktoren gleichverteilt und zufällig den Wert 0 oder 1 zuordnen. Liefert uns ein entsprechender Zufallsgenerator die Sequenz 1,0,0,1, dann ist die entsprechende Abbildung $f \in 2^{\binom{4}{2}}$ ein numerierte Graph, der den Graphen aus Abbildung 1.9 repräsentiert.

$\diamond$

Diese Methode kann leicht zu einem Verfahren verfeinert werden, das ausschließlich Graphen mit gegebener Punkte- und Kantenzahl gleichverteilt zufallserzeugt bzw. noch allgemeiner Repräsentanten mit vorgegebenem Gewicht liefert. Ist nämlich wieder ${}_GX$ eine endliche Operation, $w\colon X \to R$ eine Gewichtsfunktion, dann operiert ja G auch auf der Menge der Bahnen mit vorgegebenem Gewicht $r \in R$, d. h. G operiert auf dem Urbild $w^{-1}[\{r\}]$ von $r \in R$,, und wir brauchen in 1.15.1 nur die Faktoren im Zähler und Nenner entsprechend zu ersetzen, so dß sich folgendes ergibt:

1.15.3 Folgerung *Wenn wir die Konjugiertenklasse $C \subseteq G$ mit der Wahrscheinlichkeit*

$$p(C) := \frac{|C||w^{-1}[\{r\}]_g|}{|G||G\backslash\backslash w^{-1}[\{r\}]|},$$

wählen und dann ein $g \in C$ herausnehmen und dazu einen Fixpunkt $x \in X_g$ vom Gewicht r gleichverteilt zufallserzeugen, dann ist x gleichverteilt auf die Bahnen von diesem Gewicht.

Ist die operierende Gruppe die symmetrische, dann läuft eine Anwendung des Algorithmus von Dixon und Wilf auf die Auswahl einer eigentlichen Partition hinaus. Wir sollten deshalb nicht vergessen, daß die Anzahl eigentlicher Partitionen von $n \in \mathbb{N}$ sehr rasch anwächst.

Hier sind einige von diesen Anzahlen:

n	Anzahl eig. Partitionen
10	42
20	627
40	37338
60	$\approx 10^6$
100	$\approx 2 \cdot 10^8$

Diese Tabelle zeigt, daß man sehr bald schon die Speicherung all der entsprechenden Wahrscheinlichkeiten besser vermeidet, ebenso natürlich deren Vorberechnung. Für praktische Zwecke startet man in solchen Fällen die Generierung dann direkt und rechnet die $p(C_i)$ nur so weit aus wie nötig, d.h. nur dann, wenn die vom Zufallsgenerator erzeugte Zahl den Wert $\sum_{j=1}^{i-1} p(C_j)$ überschreitet. Die Effizienz dieser Methode hängt natürlich auch stark von der gewählten Reihenfolge der Konjugiertenklassen ab. Man sollte diese Numerierung so wählen, daß die entsprechenden Wahrscheinlichkeiten nicht ansteigen, d.h. man sollte $p(C_i) \geq p(C_{i+1})$ haben. Asymptotische Betrachtungen (vgl. Oberschelp, Dixon/Wilf) zeigen, daß daß man im Fall der Graphengenerierung gut die lexikographische Reihenfolge der eigentlichen Partitionen wählen kann. (Asymptotisch geht ja der Stabilisator gegen die triviale Untergruppe, so daß man bald auch mit der gleichverteilten Zufallsauswahl *numerierter* Graphen nicht schlecht fährt.)

Man kann diese Methode auch für gleichverteilte Zufallserzeugung von Repräsentanten aus Bahnen vorgegebenen Typs $\widetilde{U}$ benutzen. Eine Alternative hierzu ist die folgende Vorgehensweise. Da jede Bahne $\omega \in G\backslash\!\backslash X$ von diesem Typ Elemente x enthält, die U als Stabilisator besitzen, können wir von X_U jedes Element wegnehmen, das einen größeren Stabilisator hat. Dazu genügt natürlich die Wegnahme der Elemente aus den Mengen X_V, für die U maximal ist in V. Den Rest bezeichen wir so:

$$\hat{X}_U := X_U \backslash \bigcup_{U max. V} X_V.$$

Der Schnitt von $\omega \in G\backslash\!\backslash_{\widetilde{U}} X$ mit $\hat{X}_U$ ist die Bahn eines $x \in \omega$ mit $G_x = U$, und zwar die Bahn unter dem *Normalisator* $N_G(U)$, wie man leicht einsieht. Da $G_x = U$ können wir stattdessen sogar die *Faktorgruppe* $N_G(U)/U$ nehmen und erhalten:

1.15.4 Hilfssatz *Jede Transversale von* $(N_G(U)/U)\backslash\!\backslash \hat{X}_U$ *ist auch Transversale der Bahnen vom Typ* $\widetilde{U}$ *von* G *auf* X.

Wollen wir dabei probabilistische Methoden verwenden, dann ist noch die Bemerkung hilfreich, daß die Bahnen von $N_G(U)/U$ auf $\hat{X}_U$ sämtlich von derselben Ordnung $|N_G(U)/U|$ sind. Wir erhalten also insgesamt:

1.15.5 Satz (Laue) *Nimmt man gleichverteilt Elemente aus $\hat{X}_U$, so sind diese über die Bahnen vom Typ $\widetilde{U}$ von G auf X gleichverteilt.*

Ist beispielsweise $U := \{1\}$, dann ist $\hat{X}_U = \hat{X}_1$ gleich X minus Vereinigung der Fixpunktmengen X_V, genommen über alle minimalen Untergruppen $V \leq G$. Ist insbesondere $G := C_n$, dann sind die minimalen Untergruppen gerade die zyklischen Gruppen $C_p \leq C_n$, p eine Primzahl. Dasselbe gilt für $G := S_n$, aber in diesem Fall können natürlich mehrere solche Untergruppe C_p, zu einem festen p, vorhanden sein. Wegen $N_G(1) = G$ können wir gemäß 1.15.5 leicht Repräsentanten der Bahnen maximaler Länge $|\bar{G}|$ gleichverteilt zufallserzeugen.

1.15.6 Beispiel Ein interessantes Beispiel bilden die normierten Polynome gegebenen Grades, die über $GF(q)$ irreduzibel sind. Dazu erinnern wir uns an die Galoistheorie: Die Galoisgruppe führt Wurzeln in Wurzeln über, die normierten irreduziblen Polynome vom Grad n über $GF(q)$ entsprechen also gerade den Bahnen der Länge n der Galoisgruppe G von $GF(q^n)$ über $GF(q)$. Nun wird diese Galoisgruppe G bekanntlich von der Abbildung

$$\sigma \colon GF(q^n) \rightarrow GF(q)$$

erzeugt und ist demnach zyklisch von der Ordnung n :

$$G = \{1, \sigma, \ldots, \sigma^{n-1}\} \simeq C_n.$$

Die Existenz einer Normalbasis von $GF(q^n)$ über $GF(q)$ besagt, daß es $x \in GF(q^n)$ gibt, so daß $\{x, \sigma x, \ldots, \sigma^{n-1}x\}$ eine $GF(q)$-Basis ist. Schreiben wir die Elemente als Linearkombinationen in einer solchen Basis, dann sind sie von der Form

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

also mit den Abbildungen $f \in GF(q)^n$ identifizierbar. Letztere wiederum sind n-Tupel $(f(0), \ldots, f(n-1))$, auf denen das erzeugende

Element der Galoisgruppe als zyklische Vertauschung wirkt. Die gesuchten Polynome, bzw. deren Wurzelmengen, entsprechen also gerade den Bahnen der maximalen Länge n der zyklischen Gruppe C_n auf der Menge von Abbildungen q^n, und ihre Anzahl ist demnach gerade gleich

$$\frac{1}{n} \sum_{t|n} \mu(t) q^{n/t}.$$

Betrachten wir als konkreten Fall $q := 2, n := 6$. Die Menge $\hat{X}_1$ gleicht hier $GF(q)^n$ minus Fixpunktemengen $GF(q)_{C_p}$, für die Primteiler p von n. Diese Mengen, die abzuziehen sind, kann man hier leicht ausrechnen: $GF(2)^6_{C_2}$ ist

$$\{000000, 100100, 010010, 001001, 110110, 101101, 011011, 111111\},$$

während

$$GF(2)^6_{C_3} = \{000000, 101010, 010101, 111111\}.$$

Ziehen wir diese beiden Mengen von $GF(2)^6$ ab, dann verbleibt

$$100000, 110000, 101000, 100010, 111000, 110100, 110010, 111100, 111110.$$

Daraus ergeben sich mit Hilfe einer Normalbasis die bekannten 9 irreduziblen normierten Polynome vom Grad 6 über $GF(2)$.

$\diamond$

Literaturverzeichnis

[1] F. Bergeron, G. Labelle, P. Leroux. Théorie des espèces et combinatoire des structures arborescentes. *Publication du LACIM*, vol. 19, 1994.

[2] A. Betten, A. Kerber, A. Kohnert, R. Laue, A. Wassermann. Es gibt 7-Designs mit kleinen Paramtern! *Bayreuther Math. Schriften,* 49:213, 1995.

[3] H. Fripertinger. Enumeration of isometry-classes of linear (n, k)-codes over $GF(q)$ in SYMMETRICA. *Bayreuther Math. Schriften*, 49:215-223, 1995.

[4] H. Fripertinger. Cycle indices of linear, affine and projective groups. To be published.

[5] A. Kerber. *Algebraic Combinatorics via Finite Group Actions*. B. I. Wissenschaftsverlag, Mannheim, Wien, Zürich, 1991. ISBN 3-411-14521-8.

[6] G. Pólya. Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen. *Acta Mathematica*, 68:145 – 254, 1937.

[7] D. Slepian. Some Further Theory of Group Codes. *The Bell System Technical Journal*, 39:1219 – 1252, 1960.

Index