

Diskrete Strukturen

Grundlagen und Anwendungen

Henning Fernau

1. März 2016

Inhaltsverzeichnis

1 Einführung	XI
2 Zur elementaren Logik	1
3 Mathematische Grundlagen	3
3.1 Mengenlehre	3
3.1.1 Wie kann man Mengen angeben?	3
3.1.2 Vergleiche zwischen Mengen	5
3.1.3 Mathematische Induktion: ein Exkurs	8
3.1.4 Mengenoperationen	11
3.1.5 Mengenkonstruktionen	14
3.2 Relationen und gerichtete Graphen	15
3.2.1 Operationen auf Relationen	16
3.2.2 Mengensysteme	18
3.2.3 Relationen und Graphen	18
3.2.4 Eigenschaften von Relationen	20
3.3 Funktionen	25
3.3.1 Eigenschaften von Abbildungen	26
3.3.2 Folgen	28
3.4 Zur Größe von Mengen	31
3.4.1 Zum Begriff der Mächtigkeit	31
3.4.2 Endliche und unendliche Mengen	33
3.4.3 Kombinatorik	36
3.5 Quasiordnungen	41
3.5.1 Äquivalenzrelationen	42
3.5.2 Halbordnungen	44
3.6 Ungerichtete Graphen	47
3.7 Verknüpfungen	57
3.7.1 Gruppoide	57
3.7.2 Unterstrukturen und strukturerhaltende Abbildungen	59
3.7.3 Eigenschaften von Verknüpfungen	62
3.7.4 Kongruenzrelationen	67
3.8 Hüllen	68
4 Mathematische Anmerkungen	77
4.1 Mengenlehre	77
4.1.1 Cantor, Dedekind und Russel: Zur Geschichte der Mengenlehre	77

4.1.2	Mengenangaben	78
4.1.3	Zum Aufbau der Zahlen	79
4.1.4	Beweistechniken	80
4.1.5	Zu den Rechengesetzen	81
4.1.6	Sprachliche Anmerkungen	83
4.2	Relationen und gerichtete Graphen	84
4.2.1	Mehrstellige Relationen	84
4.2.2	Relationenalgebra	85
4.2.3	Bezeichnungen	86
4.3	Funktionen	87
4.3.1	Mengenfunktionen	87
4.3.2	Der Satz von Schröder und Bernstein	87
4.3.3	Endliche Folgen und das Mengenprodukt	89
4.4	Zur Größe von Mengen	89
4.4.1	Geschichtliches zum Begriff der Mächtigkeit von Mengen	89
4.4.2	Pascalsches Dreieck	90
4.4.3	Zählen von Färbungen	91
4.4.4	Etwas fortgeschrittene Kombinatorik: Das Sonnenblumenlemma von Erdős und Rado	92
4.4.5	Etwas fortgeschrittene Kombinatorik: Ramsey-Theorie	94
4.4.6	Zum Messen von Mengen	95
4.4.7	Diskrete Stochastik	96
4.5	Quasiordnungen	99
4.5.1	Zum Auswahlaxiom der Mengenlehre	99
4.6	Ungerichtete Graphen	101
4.6.1	Vom Doppelten Abzählen: Ein kombinatorischer Nachtrag	101
4.6.2	Geschichtliche, informative und sprachliche Anmerkungen zu Graphen	102
4.6.3	Eulersche Graphen	103
4.6.4	Matroide	105
4.7	Verknüpfungen	108
4.7.1	Anmerkungen zur Algebra	108
4.8	Hüllen	109
4.8.1	Topologische Gedanken	109
5	Beispiele und Anwendungen	111
5.1	Mengenlehre	111
5.1.1	Computer und Mengen	111
5.1.2	Soziale Netzwerke	112
5.1.3	Mengen und Datentypen	112
5.1.4	Bezeichnungen und Bezeichnetes	113
5.1.5	Venn-Diagramme	114
5.1.6	CSG: Constructive Solid Geometry	114
5.1.7	Punktmengen und Geometrie	115
5.1.8	Mengenalgebra: Wichtige Aussagen (Zusammenfassung)	119
5.2	Relationen und gerichtete Graphen	119
5.2.1	Relationale Datenbanken	119
5.2.2	Konkrete Beispiele	120
5.2.3	Das Königsberger Brückenproblem	121
5.2.4	Graphen als Modellierungswerkzeug	122

5.2.5	Graphenzeichnungen und Intuition	125
5.3	Funktionen	125
5.3.1	Input – Output: Funktionen für Informatiker	125
5.3.2	Der Graph einer Funktion	127
5.3.3	Endliche Folgen und Wörter	127
5.3.4	Induktiv definierte Folgen	128
5.3.5	Eine Zahlenfolge aus dem Finanzwesen	130
5.3.6	Zum Multiplizieren langer Zahlen	130
5.3.7	Nacheindeutigkeit und Vortotalität für Informatiker	132
5.3.8	Modellieren mit Mengen, Relationen und Funktionen	133
5.4	Zur Größe von Mengen	136
5.4.1	Indikatorfunktion und Bitvektor	136
5.4.2	Ein ausführlicheres Beispiel zur Summen- und Produktregel .	137
5.4.3	Sudoku	138
5.4.4	Wahrscheinlichkeitsrechnung bei Gleichverteilungen	139
5.5	Quasiordnungen	141
5.5.1	Ablaufplanung (Scheduling)	141
5.5.2	Wie kann man Transitivität algorithmisch testen?	142
5.5.3	Sortieren	143
5.6	Ungerichtete Graphen	146
5.6.1	Algorithmen in Beweisen	146
5.6.2	Modellieren mit Graphen	147
5.7	Verknüpfungen	151
5.7.1	Eine weitere ungewöhnlichere Mengenoperation	151
5.7.2	Relationen aus Verknüpfungen	151
5.7.3	Zum Zählen von Klammern: Die Zahlen von Catalan	153
5.7.4	Das Relationenprodukt als Halbgruppe	154
5.7.5	Anknüpfungen zu den Formalen Sprachen	154
5.7.6	Ein erstes Restklassenbeispiel	155
5.8	Hüllen	155
5.8.1	Der Algorithmus von Floyd/Warshall	155
6	Übungen	157
6.1	Mengenlehre	157
6.1.1	Mengenangaben	157
6.1.2	Zermelo-Zahlen	158
6.1.3	Mengengleichheit	158
6.1.4	Wie Mengen sich zueinander verhalten	158
6.1.5	Ein Induktionsbeweis für Ketten gleicher Mengen	159
6.1.6	Induktionsbeweis einer bekannten geschlossenen Form für eine Reihe	159
6.1.7	Monotoniegesetze	159
6.1.8	Assoziativgesetze	159
6.1.9	Distributivgesetze	159
6.1.10	Allgemeine Distributivitat	159
6.1.11	Disjunkttheit von Mengen	160
6.1.12	Rechnen mit der Mengendifferenz	160
6.1.13	Zur binomischen Formel	161
6.1.14	Zum Mengenprodukt	161
6.2	Relationen und gerichtete Graphen	161

6.2.1	Zum Verstehen von Relationenausdrücken	161
6.2.2	Zum Rechnen mit Relationenausdrücken	161
6.2.3	Kompakte Kennzeichnungen von Relationen mit dem Relationenprodukt	162
6.2.4	Monotoniegesetz	162
6.2.5	Zerlegungen	162
6.2.6	Mengensystemgraph	162
6.2.7	Nacheindeutigkeit und Vortotalität 1	162
6.2.8	Nacheindeutigkeit und Vortotalität 2	162
6.2.9	Abgeschlossenheit der Eigenschaften unter dem Relationenprodukt	163
6.2.10	Eigenschaften von Relationen	163
6.2.11	Eine Eigenschaft von Quasiordnungen	163
6.3	Funktionen	163
6.3.1	Urbilder einer Funktion	163
6.3.2	Der Kern einer Abbildung	163
6.3.3	Urbilder einer Abbildung	164
6.3.4	Eine Kennzeichnung von Injektionen	164
6.3.5	Zum Tauschoperator	164
6.3.6	Endliche und unendliche Folgen	164
6.3.7	Die geometrische Reihe	164
6.3.8	Die Fakultätsfunktion	164
6.3.9	Das Cantorsche Abzählungsschema	164
6.3.10	Indikatorfunktion	165
6.4	Zur Größe von Mengen	165
6.4.1	Äquivalenzsatz von Cantor	165
6.4.2	Surjektiv, injektiv, bijektiv	166
6.4.3	Gleichmächtig oder nicht?	166
6.4.4	Das Löschen eines Elements	166
6.4.5	Eigenschaften von Funktionen auf einer endlichen Menge	166
6.4.6	Dirichletsches Schubfachprinzip	166
6.4.7	Zählen von Relationen	167
6.4.8	Binomialkoeffizienten	167
6.4.9	Binomischer Lehrsatz	167
6.4.10	Zählen beim Schach	167
6.4.11	Betrunkene Seemänner	167
6.4.12	Zählen von Zerlegungen	168
6.4.13	Inklusions-Exklusionsprinzip	168
6.4.14	Zur Anwendung des Inklusions-Exklusionsprinzips	168
6.4.15	Zum Satz von Ramsey	168
6.5	Quasiordnungen	168
6.5.1	Quasiordnungen aus Quasiordnungen	168
6.5.2	Äquivalenzrelationen und das Relationenprodukt	169
6.5.3	Wie viele Äquivalenzrelationen gibt es?	169
6.5.4	Restklassen	169
6.5.5	Eine Eigenschaft von Äquivalenzklassen	169
6.5.6	Äquivalenzrelationen und Zerlegungen	169
6.5.7	Quasiordnungen auf den komplexen Zahlen	169
6.5.8	Zur Existenz von größten Elementen und Suprema	169
6.5.9	Quasiordnungen und Inverse	170

6.5.10	Vergleichbarkeit	170
6.5.11	Sortieren	170
6.6	Ungerichtete Graphen	170
6.6.1	Zwillinge	170
6.6.2	Isomorphie: Ein Beweis	170
6.6.3	Isomorphie: Beispiele	171
6.6.4	Vom Nutzen der Isomorphie	171
6.6.5	Eine Kennzeichnung von Pfaden	171
6.6.6	Knoten- und Kantenanzahlen in Bäumen	171
6.6.7	Eine weitere Baumkennzeichnung	171
6.6.8	Ein Spannbaumalgorismus	171
6.6.9	Cayley-Formel	171
6.7	Verknüpfungen	171
6.7.1	Absorbierende Elemente	171
6.7.2	Komplexprodukt	172
6.7.3	Produktgruppoide	172
6.7.4	Komplementbildung als Homomorphismus	172
6.7.5	Isomorphie als Äquivalenzrelation	172
6.7.6	Äquivalenzrelationen liefern Homomorphismen	172
6.7.7	Quasiordnungen aus Homomorphismen	172
6.7.8	Assoziativität	173
6.7.9	Konkatenation	173
6.7.10	Potenzen von Relationen	173
6.7.11	Kommutativität	173
6.7.12	Idempotente Elemente	173
6.7.13	Idempotente Untermonoide	173
6.7.14	Funktionengruppoide	174
6.7.15	Eigenschaften von Verknüpfungen und gewissen zugehörigen Relationen	174
6.7.16	Halbverbände aus Halbordnungen	174
6.8	Hüllen	174
6.8.1	Abgeschlossene Intervalle	174
6.8.2	Konvexe Mengen	175
6.8.3	Oberhalbmenge	175
6.8.4	Hüllen und abgeschlossene Systeme	175
6.8.5	Hüllen und Halbordnungen	175
6.8.6	Hüllen und Gruppoide	176
6.8.7	Zur Implementierung des Relationenprodukts	176
6.8.8	Äquivalenzhüllen: Charakterisierung	176
6.8.9	Äquivalenzhüllen	176
7	Ausgewählte Lösungen	177
7.1	Mengenlehre	177
7.1.1	Mengenangaben	177
7.1.2	Zermelo-Zahlen	177
7.1.3	Mengengleichheit	177
7.1.4	Wie Mengen sich zueinander verhalten	178
7.1.5	Ein Induktionsbeweis für Ketten gleicher Mengen	179
7.1.6	Induktionsbeweis einer bekannten geschlossenen Form für ei- ne Reihe	180

7.1.7	Monotoniegesetze	180
7.1.8	Assoziativgesetze	181
7.1.9	Distributivgesetze	181
7.1.10	Allgemeine Distributivität	181
7.1.11	Disjunkttheit von Mengen	182
7.1.12	Rechnen mit der Mengendifferenz	182
7.1.13	Zur binomischen Formel	182
7.1.14	Zum Mengenprodukt	183
7.2	Relationen und gerichtete Graphen	183
7.2.1	Zum Verstehen von Relationenausdrücken	183
7.2.2	Zum Rechnen mit Relationenausdrücken	184
7.2.3	Kompakte Kennzeichnungen von Relationen	184
7.2.4	Monotoniegesetz	184
7.2.5	Zerlegungen	184
7.2.6	Mengensystemgraph	185
7.2.7	Nacheindeutigkeit und Vortotalität 1	185
7.2.8	Nacheindeutigkeit und Vortotalität 2	185
7.2.9	Abgeschlossenheit der Eigenschaften unter dem Relationenprodukt	186
7.2.10	Eigenschaften von Relationen	186
7.2.11	Eine Eigenschaft von Quasiordnungen	186
7.3	Funktionen	186
7.3.1	Urbilder einer Funktion	186
7.3.2	Der Kern einer Abbildung	187
7.3.3	Urbilder einer Abbildung	187
7.3.4	Eine Kennzeichnung von Injektionen	187
7.3.5	Zum Tauschoperator	187
7.3.6	Endliche und unendliche Folgen	187
7.3.7	Die geometrische Reihe	188
7.3.8	Die Fakultätsfunktion	188
7.3.9	Das Cantorsche Abzählungsschema	188
7.3.10	Indikatorfunktion	188
7.4	Zur Größe von Mengen	188
7.4.1	Äquivalenzsatz von Cantor	188
7.4.2	Surjektiv, injektiv, bijektiv	189
7.4.3	Gleichmächtig oder nicht?	189
7.4.4	Das Löschen eines Elements	190
7.4.5	Eigenschaften von Funktionen auf einer endlichen Menge	190
7.4.6	Dirichletsches Schubfachprinzip	190
7.4.7	Zählen von Relationen	190
7.4.8	Binomialkoeffizienten	191
7.4.9	Binomischer Lehrsatz	192
7.4.10	Zählen beim Schach	192
7.4.11	Betrunkene Seemänner	192
7.4.12	Zählen von Zerlegungen	193
7.4.13	Inklusions-Exklusionsprinzip	193
7.4.14	Zur Anwendung des Inklusions-Exklusionsprinzips	194
7.4.15	Zum Satz von Ramsey	194
7.5	Quasiordnungen	194
7.5.1	Quasiordnungen aus Quasiordnungen	194

7.5.2	Äquivalenzrelationen und das Relationenprodukt	194
7.5.3	Wie viele Äquivalenzrelationen gibt es?	195
7.5.4	Restklassen	195
7.5.5	Eine Eigenschaft von Äquivalenzklassen	196
7.5.6	Äquivalenzrelationen und Zerlegungen	196
7.5.7	Quasiordnungen auf den komplexen Zahlen	196
7.5.8	Zur Existenz von größten Elementen und Suprema	196
7.5.9	Quasiordnungen und Inverse	196
7.5.10	Vergleichbarkeit	197
7.5.11	Sortieren	197
7.6	Ungerichtete Graphen	198
7.6.1	Zwillinge	198
7.6.2	Isomorphie: Ein Beweis	198
7.6.3	Isomorphie: Beispiele	199
7.6.4	Vom Nutzen der Isomorphie	199
7.6.5	Eine Kennzeichnung von Pfaden	199
7.6.6	Knoten- und Kantenanzahlen in Bäumen	199
7.6.7	Eine weitere Baumkennzeichnung	199
7.6.8	Ein Spannbaumalgorismus	200
7.6.9	Cayley-Formel	200
7.7	Verknüpfungen	200
7.7.1	Absorbierende Elemente	200
7.7.2	Komplexprodukt	200
7.7.3	Produktgruppoide	201
7.7.4	Komplementbildung als Homomorphismus	201
7.7.5	Isomorphie als Äquivalenzrelation	202
7.7.6	Äquivalenzrelationen liefern Homomorphismen	202
7.7.7	Quasiordnungen aus Homomorphismen	202
7.7.8	Assoziativität	202
7.7.9	Konkatenation	202
7.7.10	Potenzen von Relationen	202
7.7.11	Kommunitativität	203
7.7.12	Idempotente Elemente	203
7.7.13	Idempotente Untermonoide	203
7.7.14	Funktionengruppoide	203
7.7.15	Eigenschaften von Verknüpfungen und gewissen zugehörigen Relationen	204
7.7.16	Halbverbände aus Halbordnungen	204
7.8	Hüllen	204
7.8.1	Abgeschlossene Intervalle	204
7.8.2	Konvexe Mengen	204
7.8.3	Oberhalbmenge	205
7.8.4	Hüllen und abgeschlossene Systeme	205
7.8.5	Hüllen und Halbordnungen	205
7.8.6	Hüllen und Gruppoide	206
7.8.7	Zur Implementierung des Relationenprodukts	206
7.8.8	Äquivalenzhüllen: Charakterisierung	206
7.8.9	Äquivalenzhüllen	206

8	Ergänzende algebraische Gedanken	207
8.1	Boolesche Algebra	207
8.1.1	Definition und Beispiele	207
8.1.2	Rechengesetze in Booleschen Algebren	211
8.1.3	Halbordnungen auf Booleschen Algebren	214
9	Schrifttum	219

Kapitel 1

Einführung

Es gibt schon zahlreiche gute Bücher zum Thema “Diskrete Mathematik”.

Was ist also die Motivation, ein weiteres derartiges Skript zu schreiben?

Ein wesentlicher Grund ist die Beobachtung, dass die typische studentische Zuhörerschaft einer solchen Veranstaltung sehr heterogen ist. Das macht es schwierig, einen Kurs zu entwickeln, der allen Bedürfnissen und Erfordernissen entspricht.

Allen Lesern¹ möchten wir nahelegen, den Skriptabschnitt über “Mathematische Grundlagen” durchzuarbeiten.

- Es gibt die sehr an Mathematik interessierten Zuhörer, die genau wissen möchten, warum gewisse Sachverhalte so und nicht anders sind. Diesen möchten wir dadurch entgegenkommen, dass wir in einem mit “Mathematische Anmerkungen” versehenen Skriptabschnitt weitere Zusammenhänge und Querbezüge darlegen, Erweiterungen erklären usf., die für ein tieferes Verständnis der Materie wichtig erscheinen. Dort sind auch manche geschichtliche Abrisse enthalten, die unseres Erachtens hilfreich für ein besseres Verstehen des Inhalts sind, da derlei geschichtliche Einbettungen auch helfen, die Ergebnisse aus ihrer Zeit heraus zu sehen und Mathematik als historisch-sozialen Prozess zu begreifen. Es wird sich für diese Leserschaft empfehlen, jenen Abschnitt parallel zu den “Mathematischen Grundlagen” durchzugehen.
- Es gibt die vielleicht breite Masse der Zuhörer, die wohl die Wichtigkeit der Sachverhalte einsehen, aber ein nicht so starkes Interesse gegenüber den mathematischen Beweisführungen entgegenbringen. Diesen empfehlen wir, insbesondere die im Skriptabschnitt “Beispiele und Anwendungen” enthaltenen Dinge parallel zu den “Mathematischen Grundlagen” durchzuarbeiten.
- Ähnliches möchten wir den Lesern empfehlen, die zumindest zunächst diese Materie als reine Pflichtübung ansehen. Vielleicht hilft es diesen Teilnehmern, sogar gleich nach der Einführung gewisser Begriffe in den “Beispielen und Anwendungen” zu stöbern, um für sich genügend Motivation zu gewinnen, um dann die weiteren Ausführungen der “Mathematischen Grundlagen” zu lesen.
- Wer mit dem Gedanken spielt, sich in Richtung Theoretische Informatik zu vertiefen, sollte eigentlich alle Teile des Skriptes eingehender durcharbeiten. Für

¹Um den Lesefluss nicht zu stören, verzichten wir hier und an allen weiteren Stellen an die ausdrückliche Anführung weiblicher grammatischer Formen wie “Leserin”, “Hörerin” usf. Selbstverständlich mögen sich Leserinnen, Hörerinnen usf. in gleicher Weise angesprochen fühlen.

ihn sind sowohl die mathematischen als auch die informatischen Querbezüge wichtig zu wissen.

- Für alle Leserkreise haben wir zahlreiche Verweise sowohl auf die Literatur als auch auf Quellen im Internet eingebaut, damit insbesondere auch die elektronische Fassung gerne zum Stöbern genutzt wird.

Allen Lesern sei empfohlen, den Skriptabschnitt mit den “Übungen” durchzuarbeiten. Auch hier werden verschieden geprägte Leser unterschiedliche Interessen entwickeln. Zu ausgewählten Aufgaben gibt es im Abschnitt “Ausgewählte Lösungen” weitere Erläuterungen, wenn auch nicht notwendigerweise “Musterlösungen”.

Die Trennung in die nunmehr genannten Skriptabschnitte ist bewusst, da wir dadurch verhindern möchten, den allzu bequemen Weg des passiven Rezipierens zu gehen. Nur wenn Sie die Aufgaben selber lösen, können Sie Ihr Verständnis überprüfen. Blättern Sie also nicht allzu rasch zu den Lösungen. Sollten Sie keine Lösung in jenem Abschnitt vorfinden, so bedeutet dies, dass wir davon ausgehen, dass eine derartige Lösung einfach zu erhalten sein sollte, sobald man vorherige Aufgaben selber durchgearbeitet hat und deren Lösungen dann mit den im Skript enthaltenen verglichen hat.

Das Material dieses Skriptes wurde für eine entsprechende Veranstaltung für Informatiker und Wirtschaftsinformatiker an der Universität Trier ausgewählt. Die Veranstaltung wird regelmäßig als zweistündige Vorlesung im Wintersemester angeboten, umfasst also insgesamt etwa 30 Vorlesungsstunden. Dazu kommen etwa 15 Übungsstunden.

Ausdrücklich danken möchte ich meinen Assistenten Daniel Meister und Markus Schmid, ohne deren Hinweise sicherlich manche Darstellungen sehr viel schlechter gewesen wären und dieses Projekt wohl auch gar nicht zustande gekommen wäre. Gleichfalls möchte ich mich bei den Studenten für konstruktive Kritik bedanken.

Kapitel 2

Zur elementaren Logik

An der Universität Trier ist der Einstieg ins Informatik-Studium zum Sommer- wie Wintersemester möglich. Das wird insbesondere dadurch gewährleistet, dass als Einstieg in Grundlagen der Theoretischen Informatik zum Sommersemester eine Vorlesung über “Elementare Logik” und zum Wintersemester eine solche über Diskrete Strukturen angeboten wird. Beides behandelt Grundpfeiler der Mathematik. Aber genauso, wie in der Logik-Veranstaltung zumindest aus Bequemlichkeit auch Mengennotationen verwendet werden, so möchten wir auch in dieser Veranstaltung ab und an logische Symbole in Formeln verwenden.

Für ein erstes Grundverständnis ist es hinreichend, diese Symbole überhaupt lesen zu können. Das – und nur das – soll in diesem Kapitel kurz vorgestellt werden.

Eine *Aussage* ist (abstrakt) etwas, das entweder falsch oder wahr sein kann. “Wahr” und “falsch” nennt man auch *Wahrheitswerte*. In unserem Zusammenhang werden dies mathematische Aussagen sein. In der Aussagenlogik werden derlei Aussagen mit gewissen Operatoren verknüpft. Die wichtigsten hiervon sind:

\wedge	Das logische Und, auch <i>Konjunktion</i> genannt.
\vee	Das logische Oder, auch <i>Disjunktion</i> genannt.
\Rightarrow	Folgerung oder <i>Implikation</i> .
\iff	<i>Äquivalenz</i> .
\neg	Verneinung oder <i>Negation</i> .

Eine kurze formale Beschreibung finden Sie in Abschnitt 3.7.

Sind p und q Aussagen, so gilt:

- $p \wedge q$ ist genau dann wahr, wenn sowohl p als auch q wahr ist.
- $p \vee q$ ist genau dann falsch, wenn sowohl p als auch q falsch ist.
- $p \Rightarrow q$ ist genau dann falsch, wenn p wahr, aber q falsch ist.
- $p \iff q$ ist genau dann falsch, wenn p und q unterschiedliche Wahrheitswerte haben.
- $\neg p$ ist genau dann wahr, wenn p falsch ist.

Am uneinsichtigsten ist wohl die Festlegung der Implikation. Dies bedeutet nämlich, dass eine Implikation $p \implies q$ wahr ist, wenn die Voraussetzung (Prämissen) p falsch ist. Also ist die folgende Aussage (logisch) wahr:

Wenn der Mond aus grünem Käse besteht, so kreist die Sonne um die Erde.

Allgemeiner kann man auch *Aussageformen* (auch Prädikate genannt) betrachten; so hängt der Wahrheitswert von $p(x)$ mit der Bedeutung “ x ist Primzahl” ab von der “Eingabe” x . Mit Aussageformen kann man wiederum Aussagen mit der Hilfe von sogenannten Quantoren bilden. Diese sind:

$\forall x$	gelesen “für alle x gilt:”, der <i>Allquantor</i> ,
$\exists x$	gelesen “es gibt ein x mit:”, der <i>Existenzquantor</i> .

Die Quantoren \forall und \exists binden sozusagen die Eingabe und dienen dazu, aus Aussageformen wieder Aussagen zu machen.

Von besonderem Interesse in der Logik sind Aussagen, die immer wahr sind. Diese heißen auch *Tautologien*. Tautologien sind Grundlage der meisten elementaren Schlussweisen in mathematischen Beweisen, wie wir noch sehen werden.

Dieser kurze Abriss kann und soll selbstverständlich nicht eine genauere Behandlung mit der Thematik ersetzen. Wer neugierig geworden ist und mehr erfahren möchte, dem sei die Einführung von Uwe Schöning empfehlen [38].

Kapitel 3

Mathematische Grundlagen

3.1 Mengenlehre

Auf Georg Cantor geht die folgende grundlegende Definition zurück:

Definition 3.1.1 Eine Menge ist eine Zusammenfassung bestimmter, wohlunterschiedener Dinge unserer Anschauung oder unseres Denkens, welche Elemente der Menge genannt werden, zu einem Ganzen.

Um auszudrücken, dass x ein Element der Menge M ist, schreibt man $x \in M$.

Um auszudrücken, dass x kein Element der Menge M ist, schreibt man $x \notin M$.

Die leere Menge enthält gar keine Elemente, man notiert für sie kurz: \emptyset .

3.1.1 Wie kann man Mengen angeben?

Beispiele für Mengen und ihre üblichen Bezeichnungen

$\mathbb{N} = \{0, 1, 2, 3, 4, \dots\}$: die Menge der natürlichen Zahlen,

$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \dots\}$: die Menge der ganzen Zahlen,

\mathbb{Q} : die Menge der rationalen Zahlen,

\mathbb{R} : die Menge der reellen Zahlen.

Manche Mengen können wir durch vollzähliges Aufschreiben ihrer Elemente angeben, z.B. eine Schulklassie oder einen Kurs (als Menge der zugehörigen Schüler) durch Auflistung der Schüler(namen):

$$M = \{\text{Martin, Michael, Carla, ...}\}$$

Natürlich haben die “Punkte” in einer genauen Beschreibung nichts zu suchen. Im letzten Beispiel soll nur angedeutet werden, dass die Namensliste unvollständig ist. Jeder kann aber einige derartige Liste (vollständig) zum Beispiel für seinen ersten Leistungskurs (Stammkurs) aufstellen.

Die in der Definition aufgeworfene Frage der Wohlunterscheidbarkeit der zusammengefassten Gegenstände wird in Abschnitt 5.1 anhand eines Informatik-Beispiels besprochen. Auch an dem Beispiel der Schulklassie lässt sich das bereits verdeutlichen. Zum Beispiel könnte es sein, dass zwei Schüler denselben (Vor-)Namen tragen. Diese Schwierigkeit tritt umso eher auf, je größer die Gruppe der Personen ist. Deshalb bekommt zum Beispiel jede Studentin und jeder Student an einer Universität eine eindeutige Matrikelnummer bei der Einschreibung zugeordnet.

Übereinkunft: Bei Auflistungen wollen wir “Doppelungen” aus Bequemlichkeit zulassen. Diese “zählen” aber nur einfach. Durch diese Übereinkunft verletzen wir die in der Definition geforderte Wohlunterscheidbarkeit nicht.

Eine weitere Frage bei der Definition von Menge ist, was genau denn “Dinge unserer Anschauung oder unseres Denkens” sein mögen. Welche Objekte wollen wir hier zulassen? Am besten handelt es sich natürlich um solche Gegenstände, über die wir genau Bescheid wissen. Es ist genau genommen gar nicht so einfach, sich insbesondere mit Anderen darüber zu einigen, was als bekannt vorausgesetzt werden darf. Wenn wir, wie soeben vereinbart, “Doppelungen” bei der Angabe von Mengen zulassen wollen, müssen wir diese ja auch erkennen können. Mit anderen Worten, wir müssen einsehen, wann zwei “Dinge unserer Anschauung oder unseres Denkens” übereinstimmen. Wir werden also voraussetzen müssen, dass eine Übereinkunft darüber besteht, was denn die Gleichheit von diesen Dingen ausmacht. Machen wir es also einmal konkret: Welche “Dinge unserer Anschauung oder unseres Denkens” kennen wir alle zweifelsfrei? Streng genommen gibt es nur ein solches Ding, das wir bereits eingeführt haben, nämlich die leere Menge. Wir wissen, welche Elemente zu ihr gehören, und keine weiteren Absprachen sind darüber nötig, da ja insbesondere keine Dinge darin enthalten sind, die nur einigen der Leser vertraut sind. Hieraus können wir nun beispielsweise die Menge $M = \{\emptyset\}$ bilden. Man beachte, dass M nicht dasselbe wie \emptyset ist, denn M enthält ja selbst ein Element, nämlich \emptyset . Somit kennen wir jetzt schon zwei verschiedene Dinge, nämlich \emptyset und M . Daraus könnten wir wieder eine neue, noch größere Menge bilden, nämlich $\{\emptyset, M\}$. Auf diese Weise können wir immer größere Mengen bilden aus Dingen unseres Denkens, über die wir jedenfalls insofern Einigkeit haben, als dass wir wissen, ob sie untereinander gleich sind oder nicht. Diese Möglichkeit der Mengenbildung werden wir noch im Folgenden ausnutzen.

Eine weitere Lösung dieses Problems besteht darin, dass wir uns vorweg auf ein sogenanntes *Universum* von Gegenständen einigen, aus denen heraus wir dann Mengen bilden dürfen. Dann kann man Mengen auch durch Eigenschaften (oder formaler Aussageformen) P beschreiben:

$x \in M \iff P(x)$ notiert man oft auch: $M = \{x \mid P(x)\}$ oder $M = \{x : P(x)\}$.

Das Universum kann bei dieser Schreibweise mit angegeben werden, z.B.:

- $[a, b] := \{x \in \mathbb{R} \mid a \leq x \wedge x \leq b\}$: ein *abgeschlossenes Intervall*
 - $[n] := \{m \in \mathbb{N} \mid m < n\}$ die *Menge der kleinsten n natürlichen Zahlen*
 - $\{x \in \mathbb{R} \mid x^2 - 2x = -1\}$: die *Lösungsmenge einer Gleichung*.
- Frage: Welche Zahlen beinhaltet diese Menge?

Eine andere Möglichkeit besteht in der *induktiven Definition* einer Menge. Hierbei werden zunächst einfachste Elemente der Menge ausdrücklich benannt und dann beschrieben, wie man kompliziertere Elemente aus einfacheren aufbauen kann.

Betrachten wir dazu folgendes Beispiel. Wir wollen definieren, was eine Strichliste sein soll.

- $|$ ist eine Strichliste.
- Ist s eine Strichliste, so ist auch $s|$ eine Strichliste.
- Nichts weiter sind Strichlisten.

Nunmehr können wir festlegen: Sei S die Menge aller Strichlisten. Mit der “Pünktchenschreibweise” können wir unsere Intuition stützen:

$$S = \{\|, \|, \|\|, \|\|\|, \|\|\|\|, \dots\}$$

Diese Schreibweise ist aber ungenau und daher unschön und überdies auch oft unklar.

3.1.2 Vergleiche zwischen Mengen

Im Folgenden werden wir zwei wichtige Vergleichsmöglichkeiten für Mengen (konkret Gleichheit und Einschluss) kennenlernen. Wir gehen hier wie auch sonst davon aus, dass ein Universum von Gegenständen (und sei es unausgesprochen) festgelegt wurde.

Definition 3.1.2 Zwei Mengen M_1 und M_2 heißen gleich, i.Z.: $M_1 = M_2$, genau dann, wenn sie dieselben Elemente enthalten.

An dieser Formulierung erkennen wir wiederum das vorher besprochene, scheinbar zirkuläre Problem: Mengengleichheit können wir nur definieren, wenn wir “Elementgleichheit” als Begriff zur Verfügung haben.

Wir können die vorige Definition auch leicht mit logischer Symbolik hinschreiben: M_1 und M_2 sind gleich genau dann, wenn für alle x gilt: $x \in M_1 \iff x \in M_2$.

Definition 3.1.3 Zwei Mengen M_1 und M_2 heißen ungleich, i.Z.: $M_1 \neq M_2$, genau dann, wenn sie nicht dieselben Elemente enthalten.

Zum Beispiel gilt: $\{1, 2, 2, 1\} = \{1, 2\} = \{2, 1\} \neq \{1\}$, Nach unserer Übereinkunft ist mehrfache Nennung von Elementen bei Mengen ebenso unerheblich wie die unterschiedliche Reihenfolge der Nennung bei der Auflistung der Elemente. Deshalb sind die ersten drei Mengen untereinander gleich. Hingegen sind diese Mengen alle von der zuletzt im Beispiel genannten verschieden, da das Element 2 in der letzteren Menge nicht enthalten ist.

Wie beweist man Mengengleichheit im Allgemeinen?

Nach der Definition von Mengengleichheit $M_1 = M_2$ muss man zeigen:

Genau dann, wenn x in M_1 liegt, dann liegt x auch in M_2 .

Diese Vorgehensweise nennt man auch *elementweises Argumentieren*.

Der Beweis von $M_1 = M_2$ erfolgt in der Regel in zwei Schritten (Richtungen):

(a) Wenn $x \in M_1$, so $x \in M_2$ sowie (b) Wenn $x \in M_2$, so $x \in M_1$.

Das genau bedeutet nämlich die Formulierung “Genau dann, wenn ..., dann ...”

Definition 3.1.4 Es seien M und N Mengen. N heißt Teilmenge von M (i.Z. $N \subseteq M$) gdw. M heißt Obermenge von N (i.Z. $M \supseteq N$) gdw. $\forall x(x \in N \Rightarrow x \in M)$; also: Für jedes x gilt: Wenn $x \in N$, so $x \in M$.

Gilt überdies $N \neq M$, so sprechen wir von einer echten Teilmenge bzw. einer echten Obermenge und notieren $N \subset M$ bzw. $M \supset N$. Die Beziehung $N \subseteq M$ wird auch als Inklusion oder Einschluss (von N in M) angesprochen.

Beispiel 3.1.1 $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Was wird hier genau behauptet? Wie zeigt man das?

Lemma 3.1.2 Es sei A einen Menge. Dann gilt: $\emptyset \subseteq A$.

Beweis: Für die elementweise Argumentation muss man einsehen, dass

$$x \in \emptyset \implies x \in A$$

stets wahr ist, weil nämlich die Voraussetzung, dass x ein Element der leeren Menge ist, stets falsch ist. \square

Satz 3.1.3 Es seien N und M Mengen. Dann gilt: $N = M$ gdw. $(N \subseteq M) \wedge (M \subseteq N)$.

Lesen Sie den folgenden sehr formelhaften jedoch auch einfachen Beweis laut vor. Das sollte helfen, ihn Schritt für Schritt nachzuvollziehen. Man vergleiche den Beweis auch mit den “logischen Anmerkungen” zur Mengengleichheit in Abschnitt 4.1.

Beweis: (elementweise Argumentation) $N = M$ gdw. $\forall x(x \in N \iff x \in M)$ gdw.

$$\forall x((x \in N \implies x \in M) \wedge (x \in M \implies x \in N)) \text{ gdw.}$$

$$\forall x(x \in N \implies x \in M) \wedge \forall x(x \in M \implies x \in N) \text{ gdw. } (N \subseteq M) \wedge (M \subseteq N). \quad \square$$

Aus Lemma 3.1.2 und Satz 3.1.3 folgt sofort, dass die Sprech- und Schreibweise für “leere Menge” sinnvoll sind:

Folgerung 3.1.4 Es gibt nur eine leere Menge.

Genaueres und Ergänzendes hierzu finden Sie in Abschnitt 4.1.2.

Venn-Diagramme

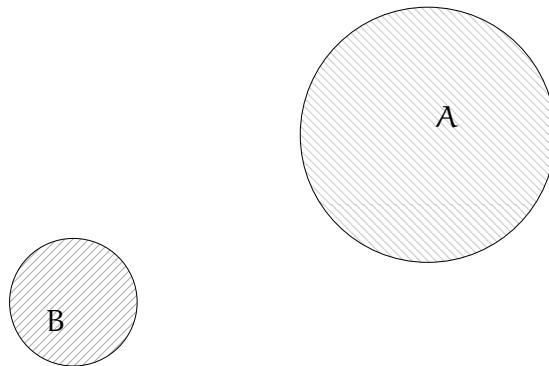


Abbildung 3.1: Zwei Mengen A und B, die so beschaffen sind, dass sie keine gemeinsamen Elemente besitzen.

Der Logiker John Venn erdachte sich – in Fortentwicklung entsprechender Verfahren von Leonhard Euler – graphische Methoden zur vereinfachten Argumentation innerhalb der Logik. Allgemein verbreitet haben sich die so genannten *Venn-Diagramme* allerdings zur Beschreibung der Verhältnisse zwischen Mengen. Insbesondere bei wenigen Mengen (sagen wir zwei oder drei) lassen sich die unterschiedlichen Lagen, in denen sich Elemente befinden können (oder eben auch nicht), so gut veranschaulichen. Dazu stellt man sich die fraglichen Mengen als zumeist kreisförmig abgegrenzte Bereiche in der Ebene vor. Selbst bei zwei Mengen A und B gibt es nun schon mehrere unterschiedliche Situationen.

- Bild 3.1 zeigt den Fall, das kein Element sowohl in A als auch in B liegt.

- In Bild 3.2 sieht man, dass es Punkte gibt, die sowohl in A als auch in B liegen, aber auch solche, die nur in A oder auch nur in B sich befinden.
- Bild 3.3 verdeutlicht die Situation, wenn A Obermenge von B ist.

Tatsächlich interpretiert man Venn-Diagramme meist etwas anders. Ein Bild wie 3.4 soll lediglich veranschaulichen, welche möglichen Lagen Elemente bezüglich der drei Mengen A, B und C einnehmen könnten, unabhängig von der Definition der Mengen selbst. So schön diese Art Veranschaulichung auf den ersten Blick sein mag, so ist bei ihrer Verwendung (selbst zur Stützung der Intuition) doch Vorsicht geboten.

- Ein Venn-Diagramm kann nahelegen, dass ein Fall betrachtet werden muss, der gar nicht eintreten kann, weil die entsprechende “Region” gar keine Elemente enthält. Die Darstellung der leeren Menge ist nicht möglich.
- Umgekehrt können ungeschickt gezeichnete Venn-Diagramme nahelegen, dass gewisse Fälle nicht eintreten können, obwohl sie möglicherweise entscheidend bei der Diskussion eines Sachverhaltes sind. Zum Beispiel mag die Diskussion der Fälle der möglichen Lagen von den Mengen A und B zueinander anhand der Bilder 3.1, 3.2 sowie 3.3 nahelegen, den wohl möglichen Fall $A = B$ völlig zu vernachlässigen. Die Venn-Diagramme waren insofern “ungeschickt” gewählt, als dass die unterschiedlichen Durchmesser der Kreise, die die Mengen A und B darstellen sollten, eben jenen Fall ausschließen.

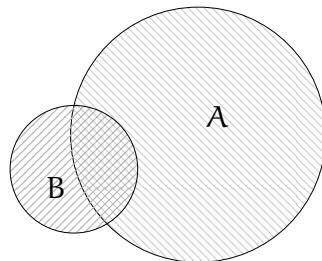


Abbildung 3.2: Zwei Mengen A und B, die so beschaffen sind, dass sie zwar gemeinsame Elemente besitzen, aber A besitzt auch “private” Elemente, die nicht in B liegen, und umgekehrt.

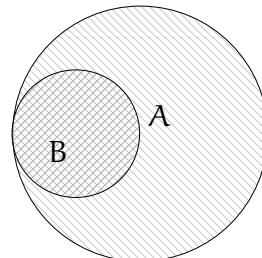


Abbildung 3.3: B ist hier Teilmenge von A.

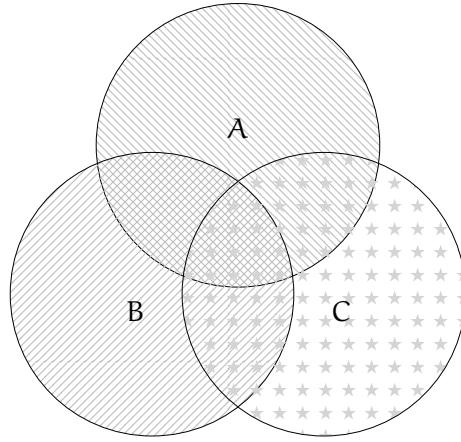


Abbildung 3.4: Veranschaulichung möglicher Beziehungen zwischen den drei Mengen A, B und C.

Einfache Aussagen über Einschluss und Gleichheit

Satz 3.1.5 Es seien A, B und C Mengen. Dann gilt:

1. $A \subseteq A$.
2. Aus $A \subseteq B$ und $B \subseteq C$ folgt $A \subseteq C$.
3. Aus $A \subseteq B$ und $B \subseteq A$ folgt $A = B$.

Beweis: Die erste Behauptung ist trivial, und die letzte ist Teil von Satz 3.1.3.

ad 2.: Es gelte $A \subseteq B$ und $B \subseteq C$. Betrachte ein beliebiges $x \in A$.

Wegen $A \subseteq B$ gilt dann $x \in B$, und wegen $B \subseteq C$ folgt $x \in C$. \square

Satz 3.1.6 Es seien A, B und C Mengen. Dann gilt:

1. $A = A$.
2. Aus $A = B$ und $B = C$ folgt $A = C$.
3. Aus $A = B$ folgt $B = A$.

Beweis: Die erste Behauptung folgt aus Satz 3.1.3 und Satz 3.1.5.1.

ad 2.: Es gelte $A = B$ und $B = C$,

also (i) $A \subseteq B$ und $B \subseteq C$ sowie (ii) $A \supseteq B$ und $B \supseteq C$ gemäß Satz 3.1.3.

Mit Satz 3.1.5.2 folgt aus (i) $A \subseteq C$ und aus (ii) $A \supseteq C$. Satz 3.1.3 liefert die Behauptung.

Die dritte Behauptung folgt unmittelbar aus der Definition der Mengengleichheit. \square

3.1.3 Mathematische Induktion: ein Exkurs

Zermelo-Zahlen: Ein Exkurs in den formalen Aufbau der Zahlen

Ähnlich wie Strichlisten hat Ernst Zermelo die natürlichen Zahlen eingeführt:

- \emptyset ist eine natürliche Zahl, genannt *Null*.

- Ist n_Z eine natürliche Zahl, so ist ihr *Nachfolger* n'_Z eine natürliche Zahl; n'_Z enthält alle Elemente von n_Z und zusätzlich die Menge n_Z als Element. Den hochgestellten Strich sprechen wir auch als *Nachfolgerstrich* an.
- Nichts weiteres sind natürliche Zahlen.

Dadurch wird die *Menge \mathbb{N}_Z der natürlichen Zahlen* (nach Zermelo) definiert.

In üblicherer Schreibweise – der Index Z soll auf Zermelo verweisen – :

$$0_Z := \emptyset \sim 0, 1_Z := \emptyset' = \{\emptyset\} \sim 1, 2_Z := \{\emptyset\}' = \{\{\emptyset\}, \emptyset\} \sim 2.$$

Diese Definition soll klarmachen, dass wir grundsätzlich auch die natürlichen Zahlen und Aussagen darüber auf die Mengenlehre zurückführen könnten. Das ist allerdings in voller Stringenz sehr mühevoll und unterbleibt im Folgenden zumeist.

Das Induktionsaxiom für die natürlichen Zahlen ist wohl das bekannteste der sogenannten Peano-Axiome, die eine mögliche Formalisierung der natürlichen Zahlen darstellen. Es lautet (in einer möglichen Fassung, mehr dazu im Abschnitt 4.1):

Ist X eine Menge natürlicher Zahlen, die die Null enthält und mit jeder Zahl n auch ihren Nachfolger $n + 1$, so gilt $X = \mathbb{N}$.

Um zu beweisen, dass $X = \mathbb{N}$ gilt für eine Menge natürlicher Zahlen X , genügt es daher zu zeigen:

- $0 \in X$.
- Für alle natürlichen Zahlen n gilt: Falls $n \in X$, so auch $n + 1 \in X$.

In der üblichen Interpretation der Zahlen sieht man leicht, dass die Zermelo-Zahlen dieses Induktionsaxiom erfüllen.

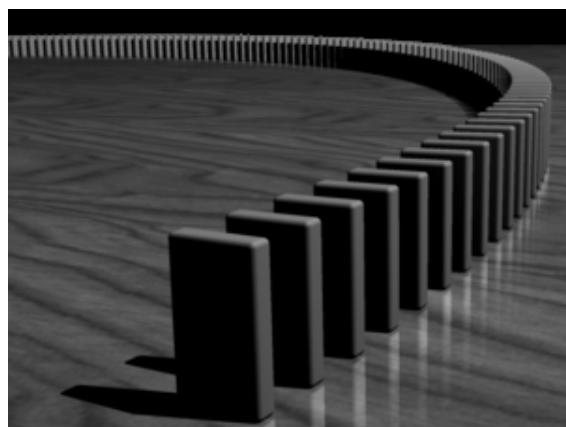


Abbildung 3.5: Der Dominoeffekt: Wenn der erste Stein fällt, fallen alle.

Induktion kann mit dem “Dominoeffekt” veranschaulicht werden, wie in Bild 3.5 zu sehen ist. Wir haben alle Dominosteine vollständig durchnummieriert: $D_0, D_1, D_2, \dots, D_3, \dots$. Die Aufstellung gewährleistet:
Wenn der k -te Dominostein D_k umfällt, so auch der $k + 1$ -te Stein D_{k+1} .
Jetzt fällt der Dominostein D_0 .

Folgerung: Schließlich werden alle Steine umgefallen sein.
Oder hätten Sie es lieber in Liedform ?

Grundgedanke der mathematischen Induktion

Es sei $p(n)$ eine Aussageform, die von $n \in \mathbb{N}$ abhängt.

Diese definiert die Menge $X_p = \{n \in \mathbb{N} \mid p(n)\}$.

Mathematische Induktion ist eine Beweistechnik, die auf dem Induktionsaxiom fußt und schematisch wie folgt arbeitet.

1. *Induktionsanfang* (IA) (auch *Anker* genannt): Zeige $p(0)$.

2. *Induktionsschritt* (IS) Es wird gezeigt, dass für alle $n \in \mathbb{N}$ gilt:

Aus $p(n)$ folgt $p(n + 1)$.

$p(n)$ heißt *Induktionshypothese* (IH) oder *Induktionsvoraussetzung* (IV).

$p(n + 1)$ ist die *Induktionsbehauptung* (IB)

Nach dem Prinzip der mathematischen Induktion folgt hieraus:

Für alle natürlichen Zahlen n gilt: $p(n)$, denn dann gilt: $X_p = \mathbb{N}$.

Ein erstes Beispiel für einen Induktionsbeweis finden Sie im Abschnitt 4.1, wo wir die Addition von Zermelo-Zahlen formal einführen. Induktive Beweise hängen eng mit induktiven Definitionen zusammen. Weitere Beispiele hierfür finden Sie durch das gesamte Skript hindurch.

Ketten von Inklusionen und Gleichheiten als Anwendung des Induktionsprinzips

Wir wollen im Folgenden “Rechenregeln” für Mengen und Mengenoperationen beweisen. Um diese sinnvoll anwenden zu können, müssen wir “Gleichungsketten” u.ä. aufschreiben dürfen in der aus der Schule bekannten Weise. Dieses Vorgehen wird durch die folgenden beiden Sätze gerechtfertigt.

Satz 3.1.7 *Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Es seien A_1, \dots, A_n Mengen.*

Gilt für alle i von $i = 1$ bis $n - 1$ der Einschluss $A_i \subseteq A_{i+1}$, so folgt $A_1 \subseteq A_n$.

Beweis: Wir führen einen Induktionsbeweis.

IA: Die Aussage gilt für die kleinste infrage kommende natürliche Zahl $n = 2$ in trivialer Weise.

Wir können ja $A_1 \subseteq A_2$ voraussetzen, woraus $A_1 \subseteq A_n$ wegen $n = 2$ sofort folgt.

IS: Wir müssen zeigen, dass aus der IV die IB folgt. Formulieren wir diese explizit.

IV: Die Aussage gilt für $n = N \geq 2$. Also: Sind A_1, \dots, A_N Mengen, sodass für alle $i \in \{1, \dots, N - 1\}$ die Inklusion $A_i \subseteq A_{i+1}$ gilt, so folgt $A_1 \subseteq A_N$.

IB: Die Aussage gilt für $n = N + 1$. Also ist zu zeigen: Sind A_1, \dots, A_{N+1} Mengen, sodass für alle $i \in \{1, \dots, N\}$ die Inklusion $A_i \subseteq A_{i+1}$ gilt, so folgt $A_1 \subseteq A_{N+1}$.

Zum Beweis der IB betrachten wir also $N + 1$ viele beliebige Mengen A_1, \dots, A_{N+1} , sodass für alle $i \in \{1, \dots, N\}$ die Inklusion $A_i \subseteq A_{i+1}$ gilt. Daraus folgt unmittelbar für die N vielen Mengen A_1, \dots, A_N , dass für alle $i \in \{1, \dots, N - 1\}$ die Inklusion $A_i \subseteq A_{i+1}$ gültig ist. Mit der IV können wir folgern: $A_1 \subseteq A_N$. Ferner gilt ja $A_N \subseteq A_{N+1}$. Mit Satz 3.1.5.2 folgt daraus $A_1 \subseteq A_{N+1}$, was zu zeigen war.

Nach dem Prinzip der mathematischen Induktion folgt die behauptete Aussage. \square

Satz 3.1.8 *Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Es seien A_1, \dots, A_n Mengen.*

Gilt für alle i von $i = 1$ bis $n - 1$ die Gleichheit $A_i = A_{i+1}$, so folgt $A_1 = A_n$.

Beweis: Mit Satz 3.1.3 folgt aus den Voraussetzungen:

- Für alle i von $i = 1$ bis $n - 1$ gilt der Einschluss $A_i \subseteq A_{i+1}$ sowie
- für alle i von $i = 1$ bis $n - 1$ gilt der Einschluss $A_{i+1} \subseteq A_i$.

Aus der ersten Aussage folgt mit Satz 3.1.7 sofort: $A_1 \subseteq A_n$ (\dagger).

Setzen wir $B_j = A_{n+1-j}$ für $j = 1$ bis $j = n$, so ergibt sich aus der zweiten Aussage (da aus $n+1-j = i+1$ folgt: $j = n-i$): Für alle i von $i = 1$ bis $n-1$ gilt der Einschluss $B_{n-i} \subseteq B_{n-i+1}$ und daraus wiederum: Für alle i von $i = 1$ bis $n-1$ gilt der Einschluss $B_i \subseteq B_{i+1}$. Somit ist auch hier Satz 3.1.7 anwendbar und ergibt: $B_1 \subseteq B_n$. Nach unserer Festlegung von B_j heißt dies: $A_n \subseteq A_1$. Mit Satz 3.1.3 folgt wegen (\dagger) nun die Behauptung $A_1 = A_n$. \square

Wir haben für Satz 3.1.8 bewusst einen Beweis angegeben, der auf Satz 3.1.7 zurückgreift. Genauso gut hätte man einen Induktionsbeweis führen können, der völlig analog zu dem von Satz 3.1.7 verlaufen wäre. Dieses wollen wir Ihnen zur Übung überlassen.

3.1.4 Mengenoperationen

Mengenalgebra: Vereinigung und Durchschnitt

Definition 3.1.5 Es seien A, B Mengen (mit Elementen desselben Universums).

Die Menge der Elemente, die zu A oder auch zu B gehören, wird als Vereinigung von A und B bezeichnet, i.Z. $A \cup B$.

Die Menge der Elemente, die sowohl zu A als auch zu B gehören, wird als Durchschnitt von A und B bezeichnet, i.Z. $A \cap B$.

A und B heißen disjunkt gdw. $A \cap B = \emptyset$.

Im Venn-Diagramm von Bild 3.2 ist also der gesamte schraffierte Bereich (unabhängig von der Richtung der Schraffur) zur Vereinigung von A und B gehörig. Der Durchschnitt der Mengen ist in dem Bild der doppelt schraffierte Bereich.

Mengenoperationen versus Mengengleichheit und Einschluss

Zwischen der vorher besprochenen Teilmengenbeziehung und diesen beiden Operationen gibt es enge und wichtige Zusammenhänge. Diese werden wir nun studieren.

Satz 3.1.9 Es seien A und B Mengen. Dann gilt:

1. $A \cap B \subseteq A \subseteq A \cup B$;
2. $A \cap B \subseteq B \subseteq A \cup B$.

Machen Sie sich die Behauptungen zunächst anhand von Bild 3.2 klar. Venn-Diagramme sind aber keine Beweise. Diese werden bei Mengen in der Regel elementweise geführt.

Beweis: Wir lösen die Satzformulierung in einzelne Behauptungen auf.

(a) Behauptung: $A \cap B \subseteq A$ und $A \cap B \subseteq B$.

Es sei $x \in A \cap B$. Dann gilt $x \in A$ und $x \in B$ nach Def. des Durchschnitts.

(b) Behauptung: $A \subseteq A \cup B$.

Es sei $x \in A$. Dann gilt natürlich, dass $x \in A$ oder $x \in B$ wahr ist, also $x \in A \cup B$.

(c) Behauptung: $B \subseteq A \cup B$.

$x \in B \implies x \in A \cup B$ sieht man entsprechend zu (b). \square

Lemma 3.1.10 Es sei A eine Menge.

- $A \cup \emptyset = \emptyset \cup A = A$;
- $A \cap \emptyset = \emptyset \cap A = \emptyset$.

Dies bedeutet, dass die leere Menge ähnlichen Rechenregeln gehorcht (bezüglich Vereinigung und Durchschnitt) wie die Null bei den natürlichen Zahlen (bezüglich Addition und Multiplikation). Genauer gesagt ist die leere Menge bezüglich der Vereinigung ein neutrales Element und bezüglich des Durchschnitts ein absorbierendes Element. Auf diese Begriffe werden wir später in allgemeinerem Zusammenhang eingehen.

Beweis: Satz 3.1.9 liefert sofort: $A \subseteq A \cup \emptyset$. Wir zeigen nun die umgekehrte Inklusion durch elementweise Argumentation. Es sei nun $x \in A \cup \emptyset$. Nach Definition der Vereinigung gilt somit $x \in A$ oder aber $x \in \emptyset$. Da \emptyset aber gar keine Elemente enthält, muss $x \in A$ notwendigerweise gelten. Mit Satz 3.1.3 folgt $A = A \cup \emptyset$.

In gleicher Weise kann man begründen, dass $A = \emptyset \cup A$ gilt. Mit Satz 3.1.8 folgt, dass alle drei angegebenen Mengen gleich sind.

Die zweite Gleichungskette zeigt man noch einfacher: Satz 3.1.9 liefert $A \cap \emptyset \subseteq \emptyset$. Lemma 3.1.2 liefert die umgekehrte Inklusion, d.h. mit Satz 3.1.3 folgt $A \cap \emptyset = \emptyset$. \square

Völlig analog zeigt man:

Lemma 3.1.11 *Es sei A einen Teilmenge des Universums \mathcal{U} .*

- $A \cup \mathcal{U} = \mathcal{U} \cup A = \mathcal{U}$;
- $A \cap \mathcal{U} = \mathcal{U} \cap A = A$.

Der folgende Satz gestattet sogar zwei *Charakterisierungen der Inklusion*. Machen Sie sich diesen mit der Hilfe von Venn-Diagrammen klar.

Satz 3.1.12 *Es seien A und B Mengen. Dann gilt:*

$$(A \cup B = B) \iff A \subseteq B \iff (A \cap B = A).$$

Wenn wir die Äquivalenz dreier Aussagen p, q, r beweisen wollen, so könnten wir natürlich alle hierbei behaupteten Implikationen beweisen. Dies bedeutet immerhin sechs Teilebeweise. Günstiger (da weniger aufwendig) ist jedoch der *Ringschluss*. Wir zeigen nur die drei Implikationen $p \implies q$, $q \implies r$ und $r \implies p$. Die Gesetze der Logik liefern die scheinbar fehlenden drei Implikationen. Mehr zu dieser Beweistechnik finden Sie im Abschnitt 4.1

Beweis: (a) Behauptung: Aus $A \cup B = B$ folgt $A \subseteq B$.

Nehmen wir also an, $A \cup B = B$ und betrachte irgendein $x \in A$. Nach Def. der Vereinigung gilt: $x \in A \cup B$. Aus der Annahme folgt: $x \in B$. Da x beliebig, folgt die behauptete Inklusion.

(b) Behauptung: Aus $A \subseteq B$ folgt $A \cap B = A$.

Wegen Satz 3.1.3 und Satz 3.1.9 bleibt zu zeigen: Aus $A \subseteq B$ folgt, dass $A \subseteq A \cap B$. Sei also $x \in A$ beliebig. Da $A \subseteq B$, gilt $x \in B$. Also liegt x sowohl in A als auch in B , und somit in $A \cap B$.

(c) Behauptung: Aus $A \cap B = A$ folgt $A \cup B = B$.

Mit Satz 3.1.9 bleibt zu zeigen: Gilt $A \cap B = A$ und ist $x \in A \cup B$ beliebig, so folgt $x \in B$. Mit $x \in A \cup B$ gilt (i) $x \in A$ oder (ii) $x \in B$. Da für Fall (ii) die Beh. trivial folgt, sei nun $x \in A$. Wegen $A \cap B = A$ gilt dann aber auch $x \in B$ und somit die Beh. \square

Satz 3.1.13 *Es seien A, B und C Mengen. Dann gelten folgende Monotoniegesetze:*

$$(A \subseteq B) \implies ((A \cup C \subseteq B \cup C) \wedge (A \cap C) \subseteq (B \cap C)).$$

Der Beweis sei Ihnen zur Übung überlassen.

Rechenregeln für Vereinigung und Durchschnitt

Für Mengenoperationen gelten ähnliche Rechenregeln, wie sie aus dem Rechnen mit Zahlen bekannt sind. Beginnen wir unsere Untersuchungen aber mit einem Gesetz, das eben keinen Widerpart im Ihnen geläufigen Zahlreich hat, nämlich dem sogenannten *Idempotenzgesetz*.

Satz 3.1.14 Für jede Menge A gilt: $A \cup A = A$ und $A \cap A = A$. (Idempotenzgesetz)

Beweis: Satz 3.1.12 zeigt, dass sowohl $A \cup A = A$ als auch $A \cap A = A$ gleichwertig sind mit $A \subseteq A$. $A \subseteq A$ gilt stets (Satz 3.1.5.1). \square

Kommen wir jetzt zu bekannten Eigenschaften von Operationen, nämlich der Kommutativität und der Assoziativität.

Satz 3.1.15 Für alle Mengen A, B gilt: $A \cup B = B \cup A$; $A \cap B = B \cap A$. (Kommutativgesetz)

Beweis: Wir beschränken uns auf den Beweis von $(A \cup B) \subseteq (B \cup A)$.

Die anderen drei zu beweisenden Inklusionen (siehe Satz 3.1.3) zeigt man ähnlich. Sei also $x \in (A \cup B)$ beliebig. Nach der Def. der Vereinigung ergeben sich zwei mögliche Fälle:

Fall 1.: $x \in A$. Dann gilt $x \in B \cup A$ wegen Satz 3.1.9.

Fall 2.: $x \in B$. Dann gilt $x \in B \cup A$ ebenso wegen Satz 3.1.9. \square

Satz 3.1.16 Für alle Mengen A, B, C gilt: (Assoziativgesetz)
 $(A \cup B) \cup C = A \cup (B \cup C)$; $(A \cap B) \cap C = A \cap (B \cap C)$.

Der Beweis sei Ihnen zur Übung überlassen.

Satz 3.1.17 Für alle Mengen A, B, C gilt: (Distributivgesetze)

$(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$; $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Beweis: Wir beschränken uns auf den Beweis von $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.

Die anderen drei zu beweisenden Inklusionen (siehe Satz 3.1.3) zeigt man ähnlich.

Sei also $x \in (A \cup B) \cap C$ beliebig. Nach der Def. des Durchschnitts gilt sowohl $x \in A \cup B$ als auch $x \in C$. Nach der Def. der Vereinigung ergeben sich zwei mögliche Fälle:

Fall 1.: $x \in A$ und $x \in C$. Dann gilt $x \in A \cap C$ und $x \in (A \cap C) \cup (B \cap C)$ wegen Satz 3.1.9.

Fall 2.: $x \in B$ und $x \in C$. Dann gilt $x \in B \cap C$ und $x \in (A \cap C) \cup (B \cap C)$ wegen Satz 3.1.9. \square

Beispiel: Aus der Schule sind Distributivgesetze wie $(a + b) \cdot c = a \cdot c + b \cdot c$ für Zahlen a, b, c bekannt. Allerdings gilt $(a \cdot b) + c = (a + c) \cdot (b + c)$ meist nicht, obwohl das manche Schüler sicher gerne sähen. Insofern sind die Distributivgesetze für Vereinigung und Durchschnitt auf der einen Seite zwar bekannt, auf der anderen Seite aber mit ihrem dualen Charakter doch überraschend.

Mengenalgebra: Differenz und Komplement

Definition 3.1.6 Es seien A, B Mengen (mit Elementen desselben Universums \mathcal{U}).

Die Menge der Elemente, die zwar zu A aber nicht zu B gehören, wird als Differenz von A und B bezeichnet; Schreibweise: $A \setminus B$.

Speziell ist $\overline{A} := \mathcal{U} \setminus A$ das Komplement von A .

Machen Sie sich diese beiden Operationen mit der Hilfe von Venn-Diagrammen klar. Auf der Ebene der Logik (d.h., über Eigenschaften) können wir aussprechen:

- $A \setminus B = \{x \mid (x \in A) \wedge \neg(x \in B)\} = \{x \mid (x \in A) \wedge (x \notin B)\};$
- $\overline{A} = \{x \mid x \notin A\}.$

Wir haben das Komplement mit der Hilfe der Differenz eingeführt. Man hätte aber auch genau andersherum vorgehen können, wie die folgende Aussage lehrt, deren elementaren Beweis wir hier auslassen. Daher genügt es, sich mit einer der beiden Operationen näher zu beschäftigen. Wir werden dies mit dem Komplement machen.

Lemma 3.1.18 $A \setminus B = A \cap \overline{B}.$

Ebenso ohne Beweis notieren wir zwei erste Komplement-Rechenregeln:

Lemma 3.1.19 Für das Universum \mathcal{U} gilt: $\overline{\mathcal{U}} = \emptyset, \overline{\emptyset} = \mathcal{U}.$

Eine weitere einfache Eigenschaft ist:

Lemma 3.1.20 Wir betrachten eine beliebige Menge A mit Elementen aus dem Universum \mathcal{U} . Dann gilt: $A \cap \overline{A} = \emptyset$ und $A \cup \overline{A} = \mathcal{U}$. (Komplementgesetz)

M und \overline{M} heißen auch *komplementär* zueinander. Diese (symmetrische) Begrifflichkeit ist motiviert durch:

Lemma 3.1.21 $\overline{\overline{M}} = M$ (Doppeltes Komplement)

Der folgende Beweis sollte “vorgelesen” für Jedermann Sinn ergeben. Diejenigen, die schon etwas “Logik” mitbekommen haben, werden aber erkennen, dass hier das Doppelnegationsgesetz benutzt wird.

Beweis: $\overline{\overline{M}} = \{x \mid x \notin \overline{M}\} = \{x \mid \neg(\neg x \in M)\} = \{x \mid x \in M\} = M.$ □

Diejenigen unter Ihnen, die sich schon mit Logik beschäftigt haben, werden nicht nur die Ähnlichkeit der Rechenregeln für Komplement und Negation, sondern auch die für Vereinigung und Disjunktion sowie für Durchschnitt und Konjunktion bemerkt haben. Ein daher bekanntes Gesetz fehlt noch, um diese Listen zu vervollständigen: das von de Morgan.

Satz 3.1.22 Für beliebige Teilmengen A, B eines Universums \mathcal{U} gilt:
 $\overline{A \cup B} = \overline{A} \cap \overline{B}$ sowie $\overline{A \cap B} = \overline{A} \cup \overline{B}.$

Beweis: Wieder zeigen wir nur eine von vier Inklusionen. Es sei $x \in \overline{A \cup B}$ beliebig. x liegt also weder in A noch in B . Das heißt: $x \notin A$ und $x \notin B$. Nach Definition des Komplements und des Durchschnitts gilt daher: $x \in \overline{A} \cap \overline{B}.$ □

Man veranschauliche sich den Sachverhalt mit Venn-Diagrammen.

3.1.5 Mengenkonstruktionen

Es gibt zwei einfache aber wichtige Möglichkeiten, aus gegebenen Mengen weitere aufzubauen.

Definition 3.1.7 Zu jeder Menge M gibt es eine weitere Menge, die Potenzmenge von M , geschrieben 2^M , die genau die Teilmengen von M als Elemente enthält.

Beispiel: $2^{\{1,2,3\}} = \{\{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1\}, \{2\}, \{3\}, \emptyset\}.$

Lemma 3.1.23 Die Potenzmenge 2^M enthält in Sonderheit die Elemente \emptyset und M .

Beweis: Es bleibt zu zeigen: $\emptyset \in 2^M$, also: $\emptyset \subseteq M$.

Die Implikation $(x \in \emptyset \implies x \in M)$ ist stets wahr, da die Prämisse falsch ist. \square

Definition 3.1.8 Die Produktmenge der Mengen M und N ist die Menge, deren Elemente die geordneten Paare (x, y) sind mit $x \in M$ und $y \in N$.

Formaler: $M \times N := \{(x, y) \mid x \in M \wedge y \in N\}$.

Kennzeichnend ist: $(x, y) = (x', y')$ genau dann, wenn $x = x'$ und $y = y'$ gilt.

Die Operation \times heißt auch Mengenprodukt.

Der Gleichheitsbegriff für geordnete Paare zeigt, dass diese von sogenannten ungeordneten Paaren, also zweielementigen Mengen, wohl zu unterscheiden sind. Im Abschnitt 6.1 wird das in einer Aufgabe genauer untersucht. Dort sieht man auch, dass der Begriff des geordneten Paares grundsätzlich auf bekannte Begriffe zurückgeführt werden könnte. Wir haben darauf verzichtet, da durch die Verwendung von Koordinaten in der Schule das Konzept eigentlich schon bekannt ist.

Für das Mengenprodukt lassen sich wieder einige schöne Rechenregeln formulieren. Die entsprechenden elementweisen Beweise seien Ihnen als Übungsaufgaben überlassen. Veranschaulichen Sie sich die Situation anhand von Punktmengen in der Ebene.

Satz 3.1.24 Es gelten die folgenden Distributivgesetze für beliebige Mengen M, N, P :

- $M \times (N \cup P) = (M \times N) \cup (M \times P)$;
- $M \times (N \cap P) = (M \times N) \cap (M \times P)$.

Außerdem gilt für die leere Menge folgende Regel:

Lemma 3.1.25 $M \times \emptyset = \emptyset \times M = \emptyset$.

3.2 Relationen und gerichtete Graphen

Vieles aus dem vorigen Abschnitt wird Ihnen doch schon bekannt gewesen sein, nur möglicherweise nicht in der dargebrachten Abstraktion. Das wird auf den jetzt folgenden Abschnitt nicht zutreffen. Dieser ist jedoch unumgänglich für das Verständnis der folgenden Abschnitte.

Definition 3.2.1 Es seien M_1 und M_2 Mengen. Gilt $R \subseteq M_1 \times M_2$, so ist R eine (zweistellige) Relation zwischen M_1 und M_2 . Gilt $M = M_1 = M_2$, sprechen wir auch von einer zweistelligen Relation auf oder über M .

Da R selbst eine (spezielle) Menge ist, kann man Elemente (x, y) von R selbstverständlich durch $(x, y) \in R$ ausweisen. Üblich ist aber auch die Infixnotation xRy .

Beispiele:

$M = \{g \mid g \text{ ist Gerade in der Ebene}\}$. Parallelitätsrelation \parallel auf M :

$$g \parallel h \iff g \text{ und } h \text{ liegen parallel.}$$

$M = \mathbb{Z}$ Teilerrelation | auf M : $a | b \iff \exists k : b = a \cdot k$.

$M = \mathbb{R}$: Kleinerrelation $<$ auf M .

$M = \mathbb{Z}$; Paritätsrelation P auf M : $(x, y) \in P \iff 2 \mid (x + y)$.

$M = \mathbb{R}$: $[0, 1] \times [0, 1]$ ist das (ausgefüllte) Einheitsquadrat

$M = 2^U$ für ein Universum U : $\{(A, B) \mid A \subseteq B\}$ ist die Inklusionsrelation

Spezielle Relationen über Menge M :

Nullrelation: $R = \emptyset$.

Allrelation: $R = M \times M$

Diagonale: $\Delta_M = \{(x, x) \mid x \in M\}$.

Hinweis: Nullrelation und Allrelation auch für Relationen zwischen Mengen gebräuchlich.

3.2.1 Operationen auf Relationen

Da Relationen Mengen sind, können wir die bekannten Mengenoperationen “übernehmen”. Wir erhalten also durch Vereinigung, Durchschnitt, Mengendifferenz und Komplementbildung neue Relationen zwischen M_1 und M_2 , sofern die Ausgangsrelationen solche zwischen M_1 und M_2 sind. Ebenso sind Teilmengen von Relationen zwischen M_1 und M_2 wieder solche zwischen M_1 und M_2 , die auch *Teilrelationen* heißen.

Beispiel: Δ_M ist die *Ungleichheitsrelation*.

Beispiel: Betrachte $< \subset \mathbb{R} \times \mathbb{R}$ und $\Delta_{\mathbb{R}}$; definiere $\leq := < \cup \Delta_{\mathbb{R}}$.

Beispiel: Betrachte $| \subset \mathbb{Z} \times \mathbb{Z}$. $| \cap \Delta_{\mathbb{Z}}$ beschreibt ... ???

Eigentliche Relationenoperationen

Definition 3.2.2 Es sei $R \subseteq M_1 \times M_2$. Die Inverse von oder Transposition zu R ist gegeben durch: $R^- := \{(y, x) \mid (x, y) \in R\}$.

Beispiel: $P^- = P$ für die Paritätsrelation P , aber was “bedeutet” $|^-$?

Satz 3.2.1 Es seien M_1 und M_2 Mengen sowie $R, S \subseteq M_1 \times M_2$. Dann gilt:

1. $(R^-)^- = R$.
2. $(R \cup S)^- = R^- \cup S^-$.
3. $(R \cap S)^- = R^- \cap S^-$.

Beweis: ad 1.: $(x, y) \in (R^-)^-$ gdw. $(y, x) \in R^-$ gdw. $(x, y) \in R$.

ad 2.: Es sei $(y, x) \in (R \cup S)^-$. Damit gilt $(x, y) \in R \cup S$.

1. Fall: Gilt $(x, y) \in R$, so $(y, x) \in R^-$. 2. Fall: Gilt $(x, y) \in S$, so $(y, x) \in S^-$.

In jedem Fall ist also $(y, x) \in R^- \cup S^-$. Die umgekehrte Richtung sieht man ähnlich.

ad 3.: Analog zu 2. □

Definition 3.2.3 Es seien M_1, M_2, M_3 Mengen. Es sei $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$. Das Relationenprodukt $R \circ S \subseteq M_1 \times M_3$ ist wie folgt definiert:

$$\forall x \in M_1 \forall z \in M_3 (x, z) \in (R \circ S) \iff \exists y \in M_2 ((x, y) \in R \wedge (y, z) \in S).$$

Hinweis: Das Relationenprodukt kann man sich gut mit Graphen veranschaulichen. Formal behandeln wir dies erst weiter unten, aber ein Blick auf Bild 3.6 mag bereits jetzt zum Verständnis dieses Begriffs helfen.

Hinweis: Man kann das Relationenprodukt auch zum “Herausfiltern” gewisser Eigenschaften von Elementen nutzen. Derlei Elemente können wir ja in einer Teilmenge A der Gesamtmenge

M sammeln. Die Diagonale Δ_A können wir jetzt zum Filtern benutzen. Ist beispielsweise $R \subseteq M \times M$, so ist

$$R \circ \Delta_A = \{(x, y) \in M \times M \mid (x, y) \in R \wedge y \in A\}.$$

Beispiel: Wir können so die Teilbarkeitsrelation und die Paritätsrelation verknüpfen:

Nach Def.: $(x, z) \in (| \circ P) \iff \exists y (x | y \wedge (2 | (y + z)))$.

Also: $| \circ P = \{(x, z) \in \mathbb{Z} \times \mathbb{Z} : (2 | x \implies 2 | z)\}$.

Satz 3.2.2 (Assoziativgesetz) Es seien M_1, M_2, M_3, M_4 Mengen. Es seien $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$ sowie $T \subseteq M_3 \times M_4$. Dann gilt: $(R \circ S) \circ T = R \circ (S \circ T)$.

Beweis: Es sei $(w, z) \in (R \circ S) \circ T$ beliebig.

Nach Definition gibt es ein $y \in M_3$ mit $(w, y) \in (R \circ S)$ und $(y, z) \in T$.

Nach Definition gibt es ferner ein $x \in M_2$ mit $(w, x) \in R$ und $(x, y) \in S$.

Somit gilt aber $(x, z) \in S \circ T$ und mithin $(w, z) \in R \circ (S \circ T)$.

Die umgekehrte Richtung sieht man entsprechend. \square

Satz 3.2.3 (Monotoniegesetz) Es seien M_1, M_2, M_3 Mengen. Es seien $P, Q \subseteq M_1 \times M_2$ und $R, S \subseteq M_2 \times M_3$. Dann gilt: $(P \subseteq Q \wedge R \subseteq S) \implies (P \circ R) \subseteq (Q \circ S)$.

Satz 3.2.4 (Existenz eines neutralen Elements) Ist R eine Relation über der Menge M , so ist: $R = R \circ \Delta_M = \Delta_M \circ R$.

Satz 3.2.5 (Existenz eines absorbierenden Elements) Ist R eine Relation zwischen den Mengen M_1 und M_2 , so ist: $\emptyset = R \circ \emptyset = \emptyset \circ R$.

Die Beweise dieser letzten beiden Sätze sind eine leichte Übungsaufgabe.

Satz 3.2.6 Es seien M_1, M_2, M_3 Mengen sowie $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$. Dann gilt: $(R \circ S)^- = S^- \circ R^-$.

Beachte die umgedrehte Reihenfolge der Relationen!

Beweis: Es sei $(x, z) \in (R \circ S)^-$, also $(z, x) \in R \circ S$.

Also gibt es ein $y \in M_2$ mit $(z, y) \in R$ und $(y, x) \in S$.

Nach Definition der Inversen heißt das: $(y, z) \in R^-$ und $(x, y) \in S^-$.

Daher gilt: $(x, z) \in S^- \circ R^-$ wie behauptet. Die Umkehrung sieht man ähnlich. \square

Satz 3.2.7 ((Sub-)Distributivgesetze) Auf die genaue Angabe der Bereiche der Relationen wird verzichtet, da die Ergebnisse mnemotechnisch möglichst günstig notiert wurden.

1. $(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$;
2. $T \circ (R \cup S) = (T \circ R) \cup (T \circ S)$;
3. $(R \cap S) \circ T \subseteq (R \circ T) \cap (S \circ T)$;
4. $T \circ (R \cap S) \subseteq (T \circ R) \cap (T \circ S)$.

Beweis: Wir zeigen nur 4. Es sei $(x, z) \in T \circ (R \cap S)$. Also gibt es ein y mit: (a) $(x, y) \in T$ und (b) $(y, z) \in R \cap S$. Da mit (b) (1) $(y, z) \in R$ und (2) $(y, z) \in S$, folgt aus (a) und (1) $(x, z) \in (T \circ R)$ und aus (a) und (2) $(x, z) \in (T \circ S)$, woraus zusammen die Beh. folgt. \square

Frage: Warum nicht Gleichheit in den letzten beiden Beziehungen?

$M = \{1, 2\}$, $T = M \times M$, $R = \{1\} \times M$, $S = \overline{R} = \{2\} \times M$ bei 4.

3.2.2 Mengensysteme

Definition 3.2.4 Ist M eine Grundmenge, so heißt eine Teilmenge \mathfrak{M} von 2^M auch ein Mengensystem (über M). Ist $\emptyset \notin \mathfrak{M}$, sind alle Elemente von \mathfrak{M} paarweise disjunkt, aber gibt es zu jedem Element $a \in M$ eine a enthaltene Menge in \mathfrak{M} , so heißt \mathfrak{M} eine Zerlegung von M . Die Elemente von \mathfrak{M} heißen auch Klassen der Zerlegung \mathfrak{M} .

Beispiel: Ist $M = \{a, b, c\}$, so ist $\{\emptyset, \{a, b, c\}\}$ ein Mengensystem, das keine Zerlegung von M ist, da \emptyset darin als Element enthalten ist. $\{\{a\}, \{a, b, c\}\}$ ist ebenfalls ein Mengensystem, das keine Zerlegung von M ist, da die Disjunktheitsforderung nicht erfüllt ist. Dahingegen ist $\{\{a\}, \{b, c\}\}$ eine Zerlegung. Schließlich ist $\{\{a\}, \{b\}\}$ keine Zerlegung von M , da es ein Element von M gibt, nämlich c , das in keinem Element aus dem Mengensystem als Element vorkommt.

So wie Relationen Teilmengen von Produktmengen sind, sind Mengensysteme Teilmengen von Potenzmengen. Sie entsprechen also den zuvor eingeführten Mengenkonstruktionen.

3.2.3 Relationen und Graphen

Wir werden hier Graphen zunächst “nur” zur Veranschaulichung von Begriffen aus dem Bereich der Relationen verwenden. Später werden wir ihnen eine eigene (kombinatorische) Bedeutung zugestehen. Um diese Veranschaulichung auch bildlich darstellen zu können, werden wir uns ausdrücklich auf endliche Grundmengen beschränken, obwohl auch “unendliche Graphen” betrachtet werden. Der Begriff der Endlichkeit ist sicherlich intuitiv klar. Wir werden ihn in Def. 3.2.7 formal einführen und danach genauer untersuchen.

Definition 3.2.5 Ein Paar $G = (V, E)$ bezeichnet einen gerichteten Graphen, wenn

- V eine endliche Menge ist, die Knotenmenge von G und
- $E \subseteq V \times V$ die Kantenmenge von G ist.

Für eine Kante $e = (x, y)$ nennen wir x auch Anfangsknoten und y Endknoten. Eine Kante heißt Schlinge, wenn ihr Anfangsknoten mit ihrem Endknoten übereinstimmt.

- Ein gerichteter Graph, der mit jeder Kante (x, y) auch die “andere Richtung” (y, x) enthält, und der keine Schlingen besitzt, heißt ungerichteter Graph.
- Ein gerichteter Graph G heißt paar, wenn sich V zerlegen lässt in V_1, V_2 mit $V = V_1 \cup V_2$ und $V_1 \cap V_2 = \emptyset$, sodass $E \subseteq V_1 \times V_2$.
- Ein ungerichteter Graph G heißt paar, wenn sich V zerlegen lässt in V_1, V_2 mit $V = V_1 \cup V_2$ und $V_1 \cap V_2 = \emptyset$, sodass $E \subseteq (V_1 \times V_2) \cup (V_2 \times V_1)$.

Gerichtete Graphen kann man sich dadurch veranschaulichen, dass man die Knoten $x \in V$ als Punkte in die Ebene zeichnet und eine Kante $(x, y) \in E$ durch eine Linie zwischen den Punkten x und y (in der Ebene) zeichnet, wobei dann bei y noch ein kleiner Pfeil eingetragen wird, um die Richtung der Kante anzudeuten. Ist G ungerichtet, so lässt man die Pfeilspitzen einfach weg und zeichnet auch nur eine Kante zwischen x und y , sofern $\{(x, y), (y, x)\} \subseteq E$.

Relationen hängen wie folgt mit gerichteten Graphen zusammen:

- Ist R eine Relation zwischen M_1 und M_2 und sind M_1 und M_2 endlich, so lässt sich R als paarer gerichteter Graph G deuten, indem wir zunächst $V_1 := \{1\} \times M_1$ und $V_2 := \{2\} \times M_2$ setzen und dann $V = V_1 \cup V_2$ sowie

$$((a, x), (b, y)) \in E \iff (a = 1 \wedge b = 2 \wedge (x, y) \in R)$$

Falls $M_1 \cap M_2 = \emptyset$, können wir auch $V_1 = M_1$ und $V_2 = M_2$ sowie $E = R$ setzen. Die erste Komponente 1 bzw. 2 in der allgemeinen Konstruktion dient lediglich dazu, die Disjunkttheit der Mengen V_1 und V_2 zu erzwingen. Wir nennen G den *paaren Relationengraph* von R .

- Ist R eine Relation auf M und ist M endlich, so lässt sich R (außerdem) als gerichteter Graph $G = (M, R)$ deuten.
- Ist $G = (V, E)$ ein gerichteter Graph, dann ist E eine Relation auf V , die sogenannte *Adjazenzrelation*.
- Ist $G = (V, E)$ ein ungerichteter Graph, so kann man auch noch die *Inzidenzrelation*

$$I_G = \{(v, e) \in V \times E \mid \exists u \in V : (u, v) = e\}$$

zwischen V und E betrachten.

Daher kann man Graphen auch zur Veranschaulichung von Operationen und Eigenschaften von Relationen verwenden.

- Ist R eine Relation zwischen M_1 und M_2 und sind M_1 und M_2 endlich und disjunkt sowie $G = (M_1 \cup M_2, R)$ der zugehörige paare gerichtete Graph, so entsteht $G^- = (M_1 \cup M_2, R^-)$ aus G , bildlich betrachtet, durch konsequentes Umdrehen aller Pfeilrichtungen.
- Sind M_1, M_2, M_3 endliche, nicht leere und (o.E.) paarweise disjunkte Mengen und $R \subseteq M_1 \times M_2$ sowie $S \subseteq M_2 \times M_3$ zwei Relationen, so kann man sich $B = R \times S$ wie folgt veranschaulichen: Man zeichnet die paaren gerichteten Graphen $G = (M_1 \cup M_2, R)$ und $H = (M_2 \cup M_3, S)$, indem die Ecken aus M_1, M_2 bzw. M_3 auf drei zueinander parallele vertikale Linien eingetragen werden und dann die (gerichteten) Kanten von G und H . Es werden also die Graphen G und H dargestellt, aber so, dass sich G und H die Knotenmenge M_2 teilen. Es entsteht so der Eindruck, G und H zusammen stellten einen einzigen Graphen GH dar. Es gilt nun, $(x, y) \in B$ herauszufinden, indem man in GH schaut, ob man von x nach y gelangen kann, und zwar mit einem "Zwischenschritt". So gelangt man von der Ausgangslage auf der linken Seite von Bild 3.6 zu der Darstellung von B auf der rechten Seite des Bildes.
- Sind R und S zwei Relationen über einer endlichen Menge M , so können wir uns beide in ein Diagramm eingetragen vorstellen, beispielsweise R als rote Kanten und S als schwarze Kanten. Wir zeichnen also zwei Graphen mit derselben Knotenmenge M , und die Kantenmengen unterscheiden wir farblich. Die Relation $B = R \circ S$ können wir uns als Menge blauer Kanten wie folgt erhalten:

Wann immer wir eine rote Kante von x nach y und eine schwarze Kante von y nach z im Diagramm erkennen, so zeichnen wir eine blaue Kante von x nach z , und wir werden auch keine anderen blauen Kanten einzeichnen.

Dann ist der "blaue Graph" gerade eine Darstellung der Relation B .

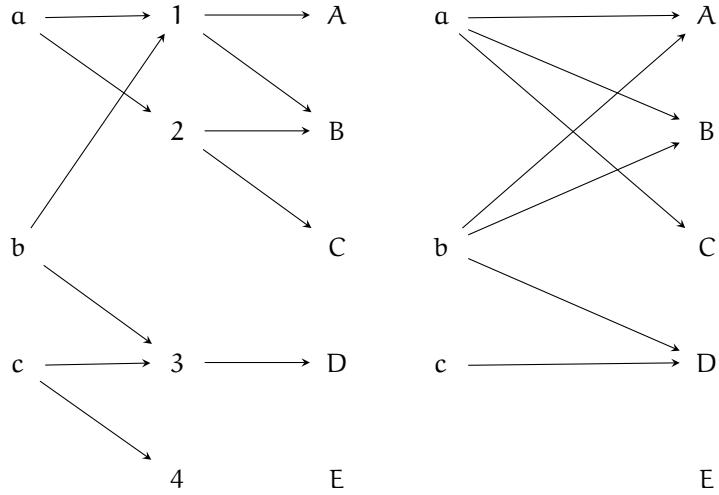


Abbildung 3.6: Auf der linken Seite sind zwei Relationen $R \subseteq M_1 \times M_2$ und $S \subseteq M_2 \times M_3$ dargestellt mit $M_1 = \{a, b, c\}$, $M_2 = \{1, 2, 3, 4\}$, $M_3 = \{A, B, C, D, E\}$. Das Relationenprodukt $R \circ S$ ist auf der rechten Seite zu sehen. Die Kante (a, A) liegt in $R \circ S$, weil $(a, 1) \in R$ und $(1, A) \in S$ gilt und es so einen Weg von a nach A im linken Graphen gibt.

Graphen sind in dem folgenden Sinne auch dienlich zur Veranschaulichung von Mengensystemen. Ist nämlich M eine endliche Menge und \mathfrak{M} ein Mengensystem über M , so kann man mit Knotenmenge $V = M \cup \mathfrak{M}$ einen paaren gerichteten Graphen definieren mit den Kanten $(a, A) \in E \iff a \in A$. Wir werden diese Konstruktion als den *Mengensystemgraph* ansprechen.

3.2.4 Eigenschaften von Relationen

Dieser Abschnitt führt eine ganze Reihe von Begriffen ein, die in den nachfolgenden Teilen entfaltet werden.

Eigenschaften von Funktionen

Die Überschrift deutet schon darauf hin, dass diese Begriffe in Abschnitt 3.3 besonders studiert werden.

Definition 3.2.6 Es seien M_1 und M_2 Mengen und $R \subseteq M_1 \times M_2$.

- R heißt nacheindeutig genau dann, wenn

$$\forall x \in M_1, y \in M_2, z \in M_2 ((x, y) \in R \wedge (x, z) \in R) \implies y = z .$$

- R heißt vortotal genau dann, wenn

$$\forall x \in M_1 \exists y \in M_2 ((x, y) \in R) .$$

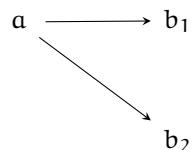
Hinweis: Entsprechend definierbar: *voreindeutig* und *nachtotale*. Wir können auch sagen:

- R ist voreindeutig $\iff R^-$ ist nacheindeutig.
- R ist nachtotal $\iff R^-$ ist vortotal.

Für endliche Grundmengen M_1, M_2 bietet sich die folgende Veranschaulichung als paarer Relationengraph G von R an:

- R ist nacheindeutig \iff Gibt es eine Kante (x, y) , so gibt es keine weitere Kante mit Endknoten y .
- R ist vortotal \iff Zu jedem $x \in M_1$ gibt es eine Kante mit Anfangsknoten x .

Man kann sich diese Deutung gut im Bild einprägen, wenn wir die **verbotenen** Strukturen betrachten:



- R ist **nicht** nacheindeutig \iff es findet sich die Struktur
 $a \in A$ hat also zwei (oder mehr) Partner auf der rechten Seite.
 Im Beispiel von Bild 3.6 sind weder R noch S nacheindeutig.

Diese Charakterisierung lautet allgemein relationenalgebraisch:

Lemma 3.2.8 $R \subseteq M_1 \times M_2$ ist nacheindeutig $\iff R \cap (R \circ \overline{\Delta_{M_2}}) = \emptyset$.

Beweis: Wir zeigen \implies durch Kontraposition. Gibt es nämlich ein $(a, b_1) \in R \cap (R \circ \overline{\Delta_{M_2}})$, so muss es noch ein b_2 geben mit $(a, b_2) \in R$ und $(b_2, b_1) \in \overline{\Delta_{M_2}}$, also $b_2 \neq b_1$. Die Umkehrung sieht man ebenso leicht, wiederum mit Kontraposition. \square

a_1

$(a_2 \longrightarrow b)$

- R ist **nicht** vortotal \iff es findet sich die Struktur
 $a_1 \in A$ hat also keinen Partner auf der rechten Seite. Das Paar (a_2, b) muss es gar nicht geben, weshalb es eingeklammert ist.
 Im Beispiel von Bild 3.6 ist R vortotal, nicht aber S .

Diese Charakterisierung lautet allgemein relationenalgebraisch:

Lemma 3.2.9 $R \subseteq M_1 \times M_2$ ist vortotal $\iff R \circ (M_2 \times M_2) = M_1 \times M_2$.

Beweis: Der Einschluss $R \circ (M_2 \times M_2) \subseteq M_1 \times M_2$ gilt immer. Angenommen, R sei vortotal. Betrachte $(a, b) \in M_1 \times M_2$ beliebig. Da R vortotal, gibt es $b' \in M_2$ mit $(a, b') \in R$. Da (trivialerweise) $(b', b) \in M_2 \times M_2$, ist damit $(a, b) \in R \circ (M_2 \times M_2)$ gezeigt. Gilt $R \circ (M_2 \times M_2) = M_1 \times M_2$, so betrachte $a \in M_1$ und $b \in M_2$ beliebig. Jedenfalls gibt es ein $b' \in M_2$ mit $(a, b') \in R$ (und $(b', b) \in M_2 \times M_2$), also ist R vortotal. \square

Beispiel: Mit $M_1 = \{a, b\}$ und $M_2 = \{1, 2, 3\}$ ist:

- $R_1 = \emptyset$ ist nacheindeutig und voreindeutig, aber weder nachtotal noch vortotal.
- $R_2 = \{(a, 1), (b, 1)\}$ ist vortotal und voreindeutig, aber weder nacheindeutig noch nachtotal.
- $R_3 = \{(a, 1), (b, 2)\}$ ist vortotal, voreindeutig und nacheindeutig, aber nicht nachtotal.
- $R_4 = \{(a, 1), (b, 2), (b, 3)\}$ ist vortotal, nacheindeutig und nachtotal, aber nicht voreindeutig.

Das Relationenprodukt erhält die eingeführten Eigenschaften in folgendem Sinne:

Satz 3.2.10 Es seien M_1, M_2, M_3 Mengen und $R \subseteq M_1 \times M_2$ sowie $S \subseteq M_2 \times M_3$. Betrachte $T := R \circ S$.

1. Sind R und S vortotal, so ist auch T vortotal.
2. Sind R und S nacheindeutig, so ist auch T nacheindeutig.

Den Beweis dieses Satzes überlassen wir zur Übung.

Mit der zuvor eingeführten Schreibweise $[n] = \{m \in \mathbb{N} \mid m < n\}$ können wir jetzt festlegen (und damit die Definition eines Graphen vervollständigen):

Definition 3.2.7 Eine Menge M heißt endlich genau dann, wenn es eine natürliche Zahl n und eine vortotale und voreindeutige Relation $R \subseteq M \times [n]$ gibt.

R ordnet also jedem Element von M eine (oder mehrere) natürliche Zahlen $< n$ zu, und außerdem gibt es keine natürliche Zahl $< n$, der R mehr als ein Element von M zuordnet.

Eigenschaften von Relationen über einer Menge

Definition 3.2.8 Es sei R eine Relation über M .

- R heißt reflexiv genau dann, wenn $\forall x \in M((x, x) \in R)$.
- R heißt irreflexiv genau dann, wenn $\forall x \in M((x, x) \notin R)$.
- R heißt symmetrisch genau dann, wenn

$$\forall x, y \in M((x, y) \in R \implies (y, x) \in R).$$

- R heißt antisymmetrisch genau dann, wenn

$$\forall x, y \in M(((x, y) \in R \wedge (y, x) \in R) \implies x = y).$$

- R heißt transitiv genau dann, wenn

$$\forall x, y, z \in M(((x, y) \in R \wedge (y, z) \in R) \implies (x, z) \in R).$$

Wir haben zum Anfang dieses Abschnitts einige Beispiele für Relationen kennengelernt. Es wäre eine gute Übungsaufgabe, die neuen Begriffe anhand der Beispiele zu studieren. Mehr dazu finden Sie in Abschnitt 5.2.

Aus den Definitionen ergeben sich unmittelbar folgende einfache Aussagen:

Lemma 3.2.11 *Ist $G = (V, E)$ ein gerichteter Graph, so ist $E \subseteq V \times V$ genau dann sowohl irreflexiv als auch symmetrisch, wenn G ein ungerichteter Graph ist.*

Beweis: E ist irreflexiv genau dann, wenn der Graph keine Schlingen besitzt. E ist symmetrisch genau dann, wenn E mit der Kante (x, y) auch immer die “andere Richtung” (y, x) enthält. \square

Lemma 3.2.12 *$R \subseteq M \times M$ ist reflexiv genau dann, wenn $\Delta_M \subseteq R$.*

Beweis: R ist reflexiv (nach Def.) genau dann, wenn für alle $x \in M$ gilt: $(x, x) \in R$, was aber gleichbedeutend ist mit $\Delta_M \subseteq R$ nach Def. der Diagonalen. \square

Lemma 3.2.13 *$R \subseteq M \times M$ ist reflexiv, symmetrisch und antisymmetrisch genau dann, wenn $R = \Delta_M$.*

Beweis: Per Definition ist Δ_M reflexiv. Ist $R = \Delta_M$ und $(x, y) \in R$, so gilt $x = y$, sodass dann R selbstverständlich auch symmetrisch und antisymmetrisch ist. Es sei umgekehrt R reflexiv, symmetrisch und antisymmetrisch. Wegen Lemma 3.2.12 gilt $\Delta_M \subseteq R$. Betrachte $(x, y) \in R$. Da R symmetrisch, folgt $(y, x) \in R$. Da R antisymmetrisch, folgt nun $x = y$, also $(x, y) \in \Delta_M$. Daher gilt $R \subseteq \Delta_M$ und mit Satz 3.1.3 die Behauptung. \square

Der formale Beweis der folgenden Aussagen sei zur Übung überlassen.

Lemma 3.2.14 *$R \subseteq M \times M$ ist irreflexiv genau dann, wenn \bar{R} reflexiv ist.*

Lemma 3.2.15 *$R \subseteq M \times M$ ist symmetrisch genau dann, wenn \bar{R} symmetrisch ist.*

Lemma 3.2.16 *Sowohl Diagonale als auch Allrelation sind reflexiv, symmetrisch und transitiv.*

Mengenoperationen

Nachdem wir bislang vornehmlich die Komplementbildung betrachtet haben, wenden wir uns im folgenden Satz der Durchschnittsbildung zu. Diese ist besonders geeignet, um aus Relationen mit bekannten Eigenschaften neue mit denselben Eigenschaften zu gewinnen.

Satz 3.2.17 *Es seien R_1, R_2 Relationen über M . Setze $R_{\cap} = R_1 \cap R_2$. Dann gilt:*

- Sind R_1 und R_2 reflexiv, so ist auch R_{\cap} reflexiv.
- Sind R_1 und R_2 irreflexiv, so ist auch R_{\cap} irreflexiv.
- Sind R_1 und R_2 symmetrisch, so ist auch R_{\cap} symmetrisch.
- Sind R_1 und R_2 antisymmetrisch, so ist auch R_{\cap} antisymmetrisch.
- Sind R_1 und R_2 transitiv, so ist auch R_{\cap} transitiv.

Am schwierigsten erscheinen Antisymmetrie und Transitivität, die wir deshalb im Folgenden beweisen werden. Die übrigen Eigenschaften sind gute Übungen.

Beweis: (1) Antisymmetrie: Betrachte (x, y) mit $(x, y) \in R_{\cap}$ und $(y, x) \in R_{\cap}$. Da damit $(x, y) \in R_1$ und $(y, x) \in R_1$, folgt bereits $x = y$, da R_1 antisymmetrisch.

(2) Transitivität: Es gelte $(x, y) \in R_{\cap}$ und $(y, z) \in R_{\cap}$. Also gilt $(x, y) \in R_1$ und $(y, z) \in R_1$, d.h., $(x, z) \in R_1$, da R_1 transitiv. Entsprechend: $(x, z) \in R_2$, womit $(x, z) \in R_1 \cap R_2 = R_{\cap}$ folgt. \square

Hinweis: Die Antisymmetrie der zweiten Relation haben wir gar nicht benötigt im Beweis von (1). Daraus folgt, dass eigentlich sogar eine stärkere Aussage gilt als die behauptete. $R_1 \cap R_2$ ist nämlich bereits dann antisymmetrisch, wenn R_1 oder R_2 alleine antisymmetrisch sind.

Hinweis: Bezüglich der Vereinigung gelten längst nicht so schöne “Abschlusseigenschaften” wie beim Durchschnitt. Diese seien Ihnen zum Ergründen überlassen.

Eigentliche Relationenoperationen

Es folgt eine Reihe schöner Kennzeichnungen der wichtigsten Eigenschaften von Relationen mit Hilfe der zuvor betrachteten Relationenoperationen.

Satz 3.2.18 *Es sei R eine Relation über M .*

1. *R ist reflexiv genau dann, wenn $\Delta_M \subseteq R$.*
2. *R ist symmetrisch $\iff R^-$ ist symmetrisch $\iff R^- \subseteq R \iff R^- = R$.*
3. *R ist transitiv genau dann, wenn $R \circ R \subseteq R$.*
4. *R ist antisymmetrisch genau dann, wenn $R \cap R^- \subseteq \Delta_M$.*

Beweis: 1. gilt wegen Lemma 3.2.12.

2. R ist symmetrisch gdw. $\forall x, y \in M ((x, y) \in R \implies (y, x) \in R)$ gdw.

$\forall x, y \in M ((y, x) \in R^- \implies (x, y) \in R^-)$ (gdw. R^- ist symmetrisch) gdw.

$\forall x, y \in M ((y, x) \in R^- \implies (y, x) \in R)$ gdw. $R^- \subseteq R$; Gleichheit gilt aus Symmetriegründen \odot .

3. R ist transitiv gdw. $\forall x, y, z \in M (((x, y) \in R \wedge (y, z) \in R) \implies (x, z) \in R)$.

Betrachte R mit (a) $R \circ R \subseteq R$ und (b) $x, y, z \in M$ bel. mit $(x, y) \in R$ und $(y, z) \in R$, also $(x, z) \in R \circ R$. Wegen (a) folgt aus (b): $(x, z) \in R$.

Betrachte umgekehrt $(x, z) \in R \circ R$. Für ein y gilt dann: $(x, y) \in R \wedge (y, z) \in R$.

Aufgrund der Transitivität von R folgt $(x, z) \in R$.

4. R ist antisymmetrisch gdw. $\forall x, y \in M (((x, y) \in R \wedge (y, x) \in R) \implies x = y)$ gdw.

$\forall x, y \in M ((x, y) \in R \cap R^- \implies (x, y) \in \Delta_M)$. \square

Zum Wesen der Transitivität

Satz 3.2.19 *Es sei R eine transitive Relation über M und $n \in \mathbb{N}$, $n \geq 1$.*

Es seien $a_0, a_1, \dots, a_n \in M$ mit $(a_{i-1}, a_i) \in R$ für alle $1 \leq i \leq n$.

Dann gilt: $(a_0, a_n) \in R$.

Beweis: Wir führen einen Induktionsbeweis.

Die Aussage stimmt sicher für $n = 1$ (IA).

Angenommen, die Aussage stimmt für $n = m$ (IV).

Wir zeigen (im IS), wie daraus die Aussage für $n = m + 1$ (IB) folgt.

Betrachte dazu $a_0, a_1, \dots, a_{m+1} \in M$ mit $(a_{i-1}, a_i) \in R$ für alle $1 \leq i \leq m+1$.
 Insbesondere folgt daraus $(a_{i-1}, a_i) \in R$ für alle $1 \leq i \leq m$ und mit der IV $(a_0, a_m) \in R$.
 Da ferner $(a_m, a_{m+1}) \in R$ und R transitiv, folgt $(a_0, a_{m+1}) \in R$. Dies war zu zeigen.

Nach dem Prinzip der mathematischen Induktion folgt die Satzbehauptung. \square

3.3 Funktionen

Definition 3.3.1 Es seien A und B Mengen. Eine (partielle) Funktion f ist eine nach-eindeutige Relation zwischen A und B .

Eine partielle Funktion f heißt total oder einfach Abbildung gdw. f ist vortotal.

Schreibweise: $f : A \rightarrow B, a \mapsto f(a)$

Wir nennen $f(a)$ Bild von a bei f und a das Urbild von $f(a)$.

A ist Definitionsbereich, B Wertebereich von f .

$f^-(B) = \{a \in A \mid \exists b \in B : f(a) = b\}$ Urbildbereich

$f(A) = \{b \in B \mid \exists a \in A : f(a) = b\}$ Bildbereich

Hinweis: Für Mathematiker sind Funktionen total, für Informatiker sind Funktionen partiell.

Beispiel: Die Diagonale ist eine totale Funktion.

Beispiel: Die Vorschrift, die jedem Studenten der Universität Trier seine DSL-Note zuordnet, ist eine partielle Funktion.

Beispiel: Die Relation, die sämtlichen Elementen aus A stets dasselbe Element aus B zuordnet, ist eine totale Funktion, genannt konstante Funktion.

Beispiel: Ist $A \subseteq B$, so kann man die Diagonale Δ_A auch als Abbildung $\iota : A \rightarrow B$ auffassen: diese heißt auch natürliche Einbettung oder Inklusionsabbildung.

Für $A = \emptyset$ spricht man von der leeren Abbildung.

Gerichtete Graphen gestatten zwei wichtige Abbildungen.

Definition 3.3.2 Ist $G = (V, E)$ ein gerichteter Graph, so bildet $N^- : V \rightarrow 2^V, v \mapsto \{u \in V \mid (u, v) \in E\}$ den Knoten v auf die Menge seiner Vorgänger(knoten) und $N^+ : V \rightarrow 2^V, u \mapsto \{v \in V \mid (u, v) \in E\}$ den Knoten u auf die Menge seiner Nachfolger(knoten) ab. Bei ungerichteten Graphen fallen beide Begriffe zusammen, und $N : V \rightarrow 2^V, v \mapsto \{u \in V \mid uv \in E\}$ bildet den Knoten v auf die Menge seiner Nachbar(knoten) ab. $N(v)$ heißt auch Nachbarschaft von v .

Wegen Satz 3.2.10 gilt:

Folgerung 3.3.1 Sind $f : A \rightarrow B$ und $g : B \rightarrow C$ Funktionen, so ist auch $f \circ g : A \rightarrow C$ eine Funktion. Sind überdies f und g total, so auch $f \circ g$.

Man spricht das Relationenprodukt im Falle von Funktionen auch als Hintereinanderausführung oder Komposition an.

Definition 3.3.3 Ist $f : A \rightarrow B$ eine Funktion und $A' \subseteq A$, so bezeichnet $f|_{A'} : A' \rightarrow B$ die durch $f'(a) = f(a)$ für $a \in A'$ definierte Funktion. Diese heißt Einschränkung oder Restriktion von f auf A' .

Beobachtung 3.3.2 Die Einschränkung einer Abbildung $f : A \rightarrow B$ auf eine Teilmenge $A' \subseteq A$ ist wiederum eine Abbildung.

3.3.1 Eigenschaften von Abbildungen

Definition 3.3.4 Es sei $f : A \rightarrow B$ eine Abbildung.

- f heißt surjektiv oder eine Surjektion, falls f nachtotal ist.
- f heißt injektiv oder eine Injektion, falls f voreindeutig ist.
- f heißt bijektiv oder eine Bijektion, falls f sowohl surjektiv als auch injektiv ist.

Beobachtung 3.3.3 Die Einschränkung einer Injektion $f : A \rightarrow B$ auf eine Teilmenge $A' \subseteq A$ ist wiederum eine Injektion. Dagegen ist die Einschränkung einer Surjektion $f : A \rightarrow B$ auf eine Teilmenge $A' \subseteq A$ nicht notwendig wieder eine Surjektion.

Man veranschauliche sich diese Begriffe an den paaren Relationengraphen. Besonders prägnant ist dies für Bijektionen. Wir halten fest:

Lemma 3.3.4 Der paare Relationengraph einer Bijektion $f : A \rightarrow B$ ist gekennzeichnet durch die folgende Eigenschaft:

- Zu jedem Knoten $a \in A$ gibt es genau eine Kante mit Anfangsknoten a , und
- zu jedem Knoten $b \in B$ gibt es genau eine Kante mit Endknoten b .

Satz 3.3.5 Es sei $f : A \rightarrow B$ eine Abbildung. Die folgenden Aussagen sind logisch äquivalent:

1. f ist surjektiv.
2. $\forall b \in B : f^{-}(\{b\}) \neq \emptyset$.
3. $\exists g : B \rightarrow A : g \circ f = \Delta_B$.
4. Es sei C eine (weitere) Menge und $r, s : B \rightarrow C$ seien beliebige Abbildungen, so gilt die folgende Kürzungsregel: $f \circ r = f \circ s \Rightarrow r = s$.

Wie bei Satz 3.1.12 führen wir wieder einen Ringschluss durch.

Bei der Implikation “2. \implies 3.” machen wir Gebrauch vom *Auswahlaxiom von Zermelo*: Zu jeder Menge M von nichtleeren Mengen eines Universums U gibt es eine Abbildung $f : M \rightarrow U$ mit $f(M) \in U$.

Beweis: “1. \implies 2.”: Da f surjektiv, folgt $f(A) = B$, d.h., für jedes $b \in B$ gibt es ein $a \in A$ mit $f(a) = b$; also folgt $f^{-}(\{b\}) \neq \emptyset$.

“2. \implies 3.”: Mit dem Auswahlaxiom können wir uns wegen $f^{-}(\{b\}) \neq \emptyset$ zu jedem $b \in B$ ein $g(b) \in f^{-}(\{b\})$ auswählen; es gilt nach Definition $f(g(b)) = b$. Damit folgt: $(g \circ f)(b) = f(g(b)) = b$ für alle $b \in B$.

“3. \implies 4.”: Betrachte zwei beliebige Abbildungen $r, s : B \rightarrow C$ mit $f \circ r = f \circ s$. Wegen 3, gibt es $g : B \rightarrow A : g \circ f = \Delta_B$. Mit der Assoziativität der Komposition folgt:

$$r = \Delta_B \circ r = (g \circ f) \circ r = g \circ (f \circ r) = g \circ (f \circ s) = (g \circ f) \circ s = \Delta_B \circ s = s.$$

“4. \implies 1.” zeigen wir mit Kontraposition: Wir nehmen an, f ist nicht surjektiv, d.h., es gibt ein $b_0 \in B \setminus f(A)$. Für $C = \{0, 1\}$ betrachte Abbildungen $r, s : B \rightarrow \{0, 1\}$ mit $r(b) = s(b) = 0$ für alle $b \neq b_0$ und $r(b_0) = 1$ und $s(b_0) = 1$. Offenbar gilt $r \neq s$, aber sehr wohl $f \circ r = f \circ s$, da der Unterschied außerhalb von $f(A)$ auftritt. \square

Satz 3.3.6 Es sei $f : A \rightarrow B$ eine Abbildung. Die folgenden Aussagen sind logisch äquivalent:

1. f ist injektiv.
2. $\forall b \in B : f^{-}(\{b\})$ enthält höchstens ein Element.
3. $\exists g : B \rightarrow A : f \circ g = \Delta_A$.
4. Es sei C eine (weitere) Menge und $r, s : C \rightarrow A$ seien beliebige Abbildungen, so gilt die folgende Kürzungsregel: $r \circ f = s \circ f \Rightarrow r = s$.

Der Beweis verläuft ähnlich zum Vorigen; daher verzichten wir hier darauf.

Satz 3.3.7 Es sei $f : A \rightarrow B$ eine Abbildung. Die folgenden Aussagen sind logisch äquivalent:

1. f ist bijektiv.
2. $\forall b \in B : f^{-}(\{b\})$ enthält genau ein Element.
3. $\exists g : B \rightarrow A : g \circ f = \Delta_B$ und $f \circ g = \Delta_A$.

Der Beweis von Satz 3.3.7 ergibt sich unmittelbar aus der Definition einer Bijektion und den Sätzen 3.3.5 sowie 3.3.6.

Definition 3.3.5 Es sei $f : A \rightarrow B$ eine Bijektion. Die nach Satz 3.3.7 existierende Abbildung $g : B \rightarrow A$ mit $g \circ f = \Delta_B$ und $f \circ g = \Delta_A$ heißt Umkehrabbildung von f . Wir schreiben diese: f^{-1} .

Wegen Punkt 2 von Satz 3.3.7 kann es nur eine Umkehrabbildung gegen, d.h., f^{-1} ist eindeutig durch f festgelegt, und es gilt:

$$a = f^{-1}(b) \iff f(a) = b \iff \{a\} = f^{-}(b).$$

Funktionen können sehr verschiedene Definitions- und Wertebereiche haben. Deshalb definieren wir jetzt noch weitere Mengenschreibweisen.

Definition 3.3.6 Es seien A und B Mengen. B^A bezeichnet die Menge aller Abbildungen von A nach B . $(B \cup \{\perp\})^A$ ist die Menge aller partiellen Funktionen von A nach B . Dies ist so zu deuten, dass, wo immer die partielle Funktion $f : A \rightarrow B$ undefiniert sein mag, wir diese auf das „undefiniert-Symbol“ \perp abbilden. Der Tausch-Operator $\mathcal{T}_{a_1, a_2} : (B \cup \{\perp\})^A \rightarrow (B \cup \{\perp\})^A$ arbeitet wie folgt für zwei verschiedene $a_1, a_2 \in A$:

$$(\mathcal{T}_{a_1, a_2}(f))(a) := \begin{cases} f(a), & \text{falls } a \notin \{a_1, a_2\} \\ f(a_2), & \text{falls } a = a_1 \\ f(a_1), & \text{falls } a = a_2 \end{cases}$$

Die folgenden Eigenschaften des Tausch-Operators sind elementar einzusehen und daher eine Übungsaufgabe.

Satz 3.3.8 Der Tausch-Operator $\mathcal{T}_{a_1, a_2} : (B \cup \{\perp\})^A \rightarrow (B \cup \{\perp\})^A$ hat folgende Eigenschaften:

- Er ist wohldefiniert, d.h., das Bild einer partiellen Funktion ist wieder eine partielle Funktion von A nach B.
- Das Bild einer totalen Funktion ist wieder eine Abbildung.
- Das Bild einer Injektion ist wieder eine Injektion.
- Das Bild einer Surjektion ist wieder eine Surjektion.
- Das Bild einer Bijektion ist wieder eine Bijektion.

Lemma 3.3.9 Mit f ist auch f^{-1} bijektiv, und es gilt: $(f^{-1})^{-1} = f$.

Umkehrungen kann man auch bereits für injektive, aber nicht surjektive Abbildungen definieren. Solche Umkehrungen sind aber im Allgemeinen keine Abbildungen, sondern nur partielle Funktionen.

- Satz 3.3.10**
- (1) Die Komposition von Surjektionen ist surjektiv.
 - (2) Die Komposition von Injektionen ist injektiv.
 - (3) Die Komposition von Bijektionen ist bijektiv.

Der Beweis hierzu ergibt sich rasch aus Satz 3.2.10.

Der im Folgenden formulierte Sachverhalt erscheint auf den ersten Blick völlig einleuchtend, erfordert aber einen nicht-trivialen Beweis. Wir werden hierauf im Haupttext verzichten, ihn aber in den Mathematiken Anmerkungen ausführen. Inhaltlich stellt dieser Satz einen der Höhepunkte der Vorlesung dar.

Satz 3.3.11 (Schröder& Bernstein) Gibt es injektive Abbildungen $f : A \rightarrow B$ und $g : B \rightarrow A$, so gibt es auch eine Bijektion zwischen A und B.

Folgerung 3.3.12 Gilt $A \subseteq B$ und gibt es eine injektive Abbildung $B \rightarrow A$, so gibt es auch eine Bijektion zwischen A und B.

Beweis: Beachte: Die natürliche Einbettung $\iota : A \rightarrow B$ ist injektiv. □

Diese Beobachtungen erleichtern die Angabe von Bijektionen, da Injektionen oft ausreichend sind. Im Folgenden werden wir aber dennoch meist direkt Bijektionen angeben. Das ist aber nicht immer so einfach; versuchen Sie, eine Bijektion $f : [0, 1] \rightarrow [0, 1]$ zu finden, wobei wie üblich $[0, 1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ und $[0, 1) = \{x \in \mathbb{R} \mid 0 \leq x < 1\}$ abgeschlossene bzw. halboffene Intervalle bezeichnen. Mit der Folgerung aus dem Satz von Schröder & Bernstein genügt es jedoch einzusehen, dass $x \mapsto \frac{1}{2}x$ eine Injektion $[0, 1] \rightarrow [0, 1)$ liefert.

3.3.2 Folgen

Definition 3.3.7 • Eine unendliche Folge f mit Gliedern aus einer Menge M ist eine Abbildung $f : \mathbb{N} \rightarrow M$.

- Eine endliche Folge f mit Gliedern aus einer Menge M ist eine Abbildung $f : [n] \rightarrow M$ für ein $n \in \mathbb{N}$. n heißt hier auch Länge der Folge.

Das folgende Beispiel dürfte den Meisten bekannt sein:

Definition 3.3.8 Die Fakultätsfunktion, üblicherweise durch ein nachgestelltes Ausrufezeichen geschrieben, ist eine wie folgt induktiv definierte Abbildung $\mathbb{N} \rightarrow \mathbb{N}$,

$$n \mapsto n! := \begin{cases} 1, & \text{falls } n = 0 \\ n \cdot (n-1)!, & \text{falls } n > 0 \end{cases}$$

Es ergibt sich also (in Listenschreibweise) die sehr schnell wachsende Folge

$$(1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, 39916800, \dots)$$

Kann man diese Folge noch in anderer Weise beschreiben?

Ohne Beweis geben wir an:

Lemma 3.3.13 (Stirlingsche Formel)

$$n! = \sqrt{2\pi n} \left(\frac{n}{e}\right)^n e^{\lambda_n}, \quad \text{wobei } \frac{1}{12n+1} < \lambda_n < \frac{1}{12n}.$$

Folgen dienen zum *Auflisten*, *Abzählen* oder *Nummerieren* von (einigen) Elementen einer Menge. Man beachte, dass die Endlichkeit oder Unendlichkeit einer Folge nichts mit der Endlichkeit oder Unendlichkeit der Menge M zu tun hat. Vielmehr bezieht sich das auf den Definitionsbereich der Folge. Eine surjektive Folge liefert hingegen eine *vollständige Auflistung* des Wertebereichs.

Hinweis: Wir hatten vorher im Haupttext darauf verzichtet, Produkte zwischen beliebig vielen Mengen M_i zu definieren. Für den wichtigen Spezialfall, dass alle Mengen M_i gleich sind, kann man sich damit behelfen, geordnete n -Tupel (als Verallgemeinerung von geordneten Paaren) mit Folgen der Länge n zu identifizieren. Genaueres finden Sie in Satz 4.3.5.

Beispiel: *Listenschreibweise*:

$$\left(1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots, \frac{1}{2^m}, \dots\right)$$

beschreibt die Folge $f : \mathbb{N} \rightarrow \mathbb{Q}$, $i \mapsto 2^{-i}$.

Die Listenschreibweise einer endlichen Folge zeigt ihren engen Zusammenhang mit n -Tupeln als Elementen des Mengenprodukts von n (identischen) Mengen sehr deutlich.

Beispiel: Die ganzen Zahlen lassen sich vollständig auflisten. Betrachte

$$f : \mathbb{N} \rightarrow \mathbb{Z}, \quad n \mapsto \begin{cases} -\frac{n}{2}, & \text{falls } n \text{ gerade} \\ \frac{n+1}{2}, & \text{sonst} \end{cases}$$

Das erste Cantorsche Abzählungsschema Das letzte Beispiel wirft die folgende Frage auf: Wenn sich (schon) die ganzen Zahlen vollständig auflisten lassen, wie sieht es denn mit anderen Zahlerweiterungen aus, z.B. den rationalen oder reellen Zahlen? Diese Fragen hat Cantor beantwortet.

Satz 3.3.14 Es gibt eine vollständige Auflistung von $\mathbb{N} \times \mathbb{N}$.

Beweis: Betrachte das folgende Schema:

	0	1	2	3	4	5	...
0	0	2	5	9	14	20	...
1	1	4	8	13	19	26	...
2	3	7	12	18	25	33	...
3	6	11	17	24	32	41	...
4	10	16	23	31	40	50	...
5	15	22	30	39	49	60	...
							...

Es sollte einleuchten, dass jedes Zahlenpaar (a, b) mit $a, b \in \mathbb{N}$ durch systematisches Ablaufen der Nebendiagonalen der skizzierten unendlichen Matrix genau einmal erreicht wird. \square

Das Schema lässt sich auch formal notieren als *Cantorsche Paarfunktion*:

$$\langle i, j \rangle = (i + j)(i + j + 1)/2 + j$$

Also:

$$\langle 0, 0 \rangle = 0, \langle 1, 0 \rangle = 1, \langle 0, 1 \rangle = 2, \langle 2, 0 \rangle = 3, \dots$$

Hinweis: Geordnete n -Tupel natürlicher Zahlen, also Abbildungen $[n] \rightarrow \mathbb{N}$; lassen sich, sofern $n > 2$, als Paare begreifen, dessen erste Komponente ein $(n - 1)$ -Tupel ist. Daher lässt sich induktiv zeigen, dass die Menge der geordneten n -Tupel natürlicher Zahlen vollständig auflistbar ist.

Beispiel: $n = 3$ (Cantorfunktion für Tripel): $\langle i, j, k \rangle = \langle \langle i, j \rangle, k \rangle$.

Dieses Schema gestattet auch die Beantwortung einer eingangs gestellten Frage.

Satz 3.3.15 Die rationalen Zahlen lassen sich vollständig auflisten.

Beweis: Dies lässt sich zeigen, indem man die (positiven) Brüche folgendermaßen in einem zweidimensionalen Schema anordnet und dann den vorigen Satz anwendet:

1/1	1/2	1/3	1/4	1/5	...
2/1	2/2	2/3	2/4	2/5	...
3/1	3/2	3/3	3/4	3/5	...
4/1	4/2	4/3			...
5/1	5/2				...
					...

Die negativen Brüche sowie die Null kann man dann “dazwischenschlieben”, wie bei der Auflistung der ganzen Zahlen gezeigt wurde. \square

Beispiel 3.3.16 Es gibt Injektionen $f : \mathbb{N} \rightarrow [0, 1]$ mit $f(0) = 1$, z.B.: $i \mapsto 2^{-i}$.

Dies gestattet die Konstruktion einer Bijektion $h : [0, 1] \rightarrow [0, 1]$.

Setze nämlich:

$$h(x) = \begin{cases} x, & \text{falls } x \notin f(\mathbb{N}) \\ f(n+1), & \text{falls } x = f(n) \end{cases}$$

Insbesondere ist also: $h(1) = f(1) = \frac{1}{2}$, $h(\frac{1}{2}) = \frac{1}{4}$.
Überlegen Sie, wo die Injektivität von f eingeht.

Beispiel 3.3.17 Zu jeder Menge $A \subseteq M$ kann man seine Indikatorfunktion oder charakteristische Funktion $\chi_A : M \rightarrow \{0, 1\}$ definieren durch $\chi_A(x) = 1$ gdw. $x \in A$ und $\chi_A(x) = 0$ gdw. $x \notin A$.

Man überlege sich: Die Abbildung $h : 2^M \rightarrow \{0, 1\}^M$, $A \mapsto \chi_A$ ist eine Bijektion.

Für endliche Mengen M kann man χ_A zu $A \subseteq M$ auch als endliche Liste darstellen als sogenannten Bitvektor. Gilt $M = X \times Y$, so ist $A \subseteq M$ eine binäre Relation. Dann kann man (da M endlich) χ_A als Matrix mit Einträgen aus $\{0, 1\}$ auffassen, die sogenannte Relationenmatrix.

3.4 Zur Größe von Mengen

3.4.1 Zum Begriff der Mächtigkeit

Definition 3.4.1 Es seien A und B zwei Mengen.

- A und B heißen gleichmächtig, i.Z. $|A| = |B|$, gdw. es gibt eine Bijektion $f : A \rightarrow B$.
- A heißt höchstens so mächtig wie B , i.Z. $|A| \leq |B|$, gdw. es gibt eine Injektion $f : A \rightarrow B$.
- A heißt weniger mächtig als B , i.Z. $|A| < |B|$, gdw. $|A| \leq |B|$, aber nicht $|A| = |B|$.
- Für $n \in \mathbb{N}$ sagen wir, A hat die Mächtigkeit n , i.Z. $|A| = n$, gdw. $|A| = |[n]|$.

Wir fassen einige wichtige Eigenschaften dieser Begriffe zusammen:

Satz 3.4.1 (Eigenschaften von Mächtigkeiten) Es seien A, B, C Mengen.

1. (Reflexivität) A und A sind gleichmächtig, und A ist höchstens so mächtig wie A .
2. (Symmetrie) Sind A und B gleichmächtig, so sind auch B und A gleichmächtig.
3. (Transitivität 1) Sind A und B gleichmächtig und sind B und C gleichmächtig, so sind auch A und C gleichmächtig.
4. (Transitivität 2) Ist A höchstens so mächtig wie B und ist B höchstens so mächtig wie C , so ist A höchstens so mächtig wie C .
5. (Antisymmetrie) Ist A höchstens so mächtig wie B und ist B höchstens so mächtig wie A , so sind A und B gleichmächtig.
6. Gilt $A \subseteq B$, so folgt $|A| \leq |B|$.

Beweis:

1. Die bijektive Identitätsabbildung zeigt diese Eigenschaften.
2. Ist $f : A \rightarrow B$ bijektiv, so existiert auch die Umkehrabbildung $f^{-1} : B \rightarrow A$, und sie ist ebenfalls bijektiv.
3. Ist $f : A \rightarrow B$ Bijektion und $g : B \rightarrow C$ Bijektion, so ist auch $f \circ g : A \rightarrow C$ eine Bijektion.

4. Ist $f : A \rightarrow B$ Injektion und $g : B \rightarrow C$ Injektion, so ist auch $f \circ g : A \rightarrow C$ eine Injektion.
5. Dies folgt unmittelbar aus dem Satz von Schröder & Bernstein 3.3.11.
6. Die Inklusionsabbildung ist injektiv.

□

Hinweis: Im Allgemeinen gilt nicht, dass aus $A \subsetneq B$ folgt, dass $|A| < |B|$. Das haben wir in Beispiel 3.3.16 konkret gesehen durch Konstruktion einer Bijektion zwischen $[0, 1]$ und $[0, 1)$.

Satz 3.4.2 Es sei $f : A \rightarrow B$ eine Abbildung. Dann gilt: $|f(A)| \leq |A|$.

Beweis: Diskutiere f als Relation: $f \subseteq A \times B$ ist vortotal und nacheindeutig. Nach Def. von $f(A) = \{f(x) \mid x \in A\}$ ist f auch Teilmenge von $A \times f(A)$. Als Relation $f \subseteq A \times f(A)$ ist f zusätzlich nachtotal. Betrachte nun eine beliebige lineare Ordnung \leq auf A . Setze für $x \in f(A)$: $g(x) = \min\{y \in A \mid f(y) = x\}$, wobei sich die Minimumsbildung auf die Ordnung \leq bezieht. Da $f \subseteq A \times f(A)$ nachtotal, ist f vortotal. Die Minimumsbildung auf einer linearen Ordnung hat zur Folge, dass g nacheindeutig ist. Diskutiere x_1, x_2 mit $g(x_1) = g(x_2)$. Also gilt $x_1 = f(g(x_1)) = f(g(x_2)) = x_2$. Mithin ist g auch voreindeutig. Daher ist $g : f(A) \rightarrow A$ injektiv. □

Lemma 3.4.3 A ist endlich $\iff A$ hat die Mächtigkeit n für ein $n \in \mathbb{N}$.

Beweis: Hat A die Mächtigkeit n , so gibt es eine Bijektion $f : A \rightarrow [n]$ und somit ist A endlich nach Def. 3.2.7. Ist A endlich, so gibt es eine vortotale und voreindeutige Relation $R \subseteq A \times [n]$. Aus R gewinnen wir zunächst eine injektive Abbildung g , indem wir $a \in A$ die kleinste Zahl aus $\{m \in [n] \mid (a, m) \in R\}$ zuordnen. Schließlich ist $g(A) \subseteq [n']$ mit einem neuen Wert für n , nämlich $n' = (\max g(A)) + 1$, und falls $g(A) \neq [n']$, ändern wir g zu g' ab, indem wir die größte Zahl $\ell < n'$ finden mit $\ell \notin g(A)$; sodann setzen wir $g'(a) := g(a)$, falls $g(a) < \ell$, und $g'(a) = g(a) - 1$, falls $g(a) > \ell$. Sodann bestimmen wir wieder einen neuen Wert für n , modifizieren evtl. g nochmals usf., bis schließlich $\hat{g}(A) = [\hat{n}]$ für die dann gültigen Abbildungen \hat{g} und Zahlen \hat{n} gilt. Man sieht ein, dass jedes g eine injektive Abbildung ist und das g bei Abbruch der Schleife des Verfahrens sogar bijektiv ist. Da die Zahlenfolge n, n', \dots strikt abnimmt, terminiert das Verfahren, und die Bijektion ist wohldefiniert. □

Dieser Begriff entspricht wohl unserer Intuition, was denn die “Größe” einer Menge angeht. Nach Zermelo sind natürliche Zahlen Mengen. Das bekommt nun einen tieferen Sinn, denn es gilt:

Lemma 3.4.4 Die Menge A hat n Elemente gdw. es gibt eine Bijektion zwischen A und der Menge n_Z .

Definition 3.4.2 Speziell heißt eine Menge

- abzählbar unendlich, wenn sie zu \mathbb{N} gleichmächtig ist,
- abzählbar, wenn sie entweder endlich oder abzählbar unendlich ist,
- überabzählbar, wenn sie unendlich aber nicht abzählbar ist.

3.4.2 Endliche und unendliche Mengen

Wir beschäftigen uns im Folgenden meist mit endlichen Mengen. Daher wollen wir deren Charakter möglichst gut verstehen und uns auch vergewissern, dass unsere sicherlich vorhandene Intuition mit den mathematischen Tatsachen übereinstimmt.

Lemma 3.4.5 *Gilt $n < m$, so ist $|[n]| < |[m]|$.*

Beweis: Wir führen einen Induktionsbeweis über $m \geq 1$.

Für $m = 1$ (IA) muss $n = 0$ gelten. Da $[n] = \emptyset$, gilt für jede Abbildung $f : [n] \rightarrow [m]$: $f([n]) = \emptyset$. Da $0 \in [1]$, kann f nicht surjektiv sein. Also gibt es keine Bijektion zwischen $[0]$ und $[1]$. Da $[0] \subseteq [1]$, gibt es aber eine Injektion von $[0]$ nach $[1]$, die Inklusionsabbildung. Daher gilt $|[0]| < |[1]|$.

Wir nehmen nun an (IV), die Aussage gelte für $m = m'$ und für alle $n < m'$.

Betrachte $m = m' + 1$. Für $n < m'$ folgt die Aussage unmittelbar aus IV, denn wegen $m' \leq m' + 1$ ist $[m'] \subseteq [m' + 1]$, und daher gibt es eine Injektion von $[m']$ nach $[m' + 1]$, die Inklusionsabbildung. Da \leq (nach Satz 3.4.1) transitiv ist, folgt $[n] < [m'] \leq [m' + 1]$.

Für $n = m'$ führen wir nun einen Widerspruchsbeweis und nehmen an, es gäbe eine Bijektion $f : [n] \rightarrow [n + 1]$.

(a) Würde $f(n - 1) = n$ gelten, so wäre die Restriktion von f auf $[n - 1]$ eine Bijektion von $[n - 1]$ nach $[n]$, im Widerspruch zur IV.

(b) Andernfalls sei j durch $f(j) = n$ definiert. Betrachte $g = \tau_{j,n-1}(f)$ (Tauschoperator, siehe Def. 3.3.6). Mit f ist $g : [n] \rightarrow [n + 1]$ ebenfalls bijektiv nach Satz 3.3.8, und $g(n - 1) = n$, also erhält man einen Widerspruch wie in (a). \square

Satz 3.4.6 (*Endlichkeit nach Dedekind*) Eine Menge A ist endlich genau dann, wenn A zu keiner echten Teilmenge von A gleichmächtig ist.

Diese Charakterisierung ist sehr schön, weil sie ohne die natürlichen Zahlen auskommt, und hilft uns, den wichtigen Begriff der Endlichkeit genauer zu verstehen.¹

Beweis: Wir beweisen zunächst \Rightarrow . Betrachte eine endliche Menge A und eine echte Teilmenge B von A . Es gibt also ein $a \in A \setminus B$. Definiere $A' := A \setminus \{a\}$. Klar ist: $B \subseteq A'$ und daher $|B| \leq |A'|$. (Inklusionsabbildung ist injektiv.) Da A endlich, gibt es natürliche Zahl m und eine Bijektion $f : [m] \rightarrow A$. Evtl. nach "Vertauschen" wie im Beweis von Lemma 3.4.5 gilt: $f(m - 1) = a$. Die Restriktion f' von f auf $[m - 1]$ ist daher eine Bijektion von $[m - 1]$ nach A' . Also gilt: $|B| \leq |A'| < |A|$.

Wir zeigen nun \Leftarrow durch einen Widerspruchsbeweis. Betrachte eine unendliche Menge A mit der Eigenschaft, dass sie zu keiner ihrer echten Teilmengen gleichmächtig ist. Man überlege sich, dass dann auch für jede Teilmenge A' von A gilt, dass sie zu keiner ihrer echten Teilmengen gleichmächtig ist. Wir können daher davon ausgehen, dass sämtliche echte Teilmengen von A endlich sind und A sozusagen ein kleinstes Gegenbeispiel zur Behauptung darstellt. Sei nun $B \subset A$ und $a \in A \setminus B$. Die Menge $A' = A \setminus \{a\}$ ist endlich (da wir sonst ein kleineres Gegenbeispiel hätten). Also gibt es eine Bijektion $f' : [n] \rightarrow A'$ für eine natürliche Zahl n . Erweitere nun f' zu $f : [n + 1] \rightarrow A$ durch $f(i) = f'(i)$ für $i \in [n]$ und $f(n) = a$. f ist eine Bijektion, und somit ist A endlich, also (doch) kein Gegenbeispiel zur Behauptung. \square

Satz 3.4.7 Eine Menge ist unendlich genau dann, wenn sie eine abzählbar unendliche Teilmenge besitzt.

¹Es gibt noch weitere Kennzeichnungen des Begriffs der Endlichkeit, die ohne direkten Bezug auf die natürlichen Zahlen auskommen, wie Kuratowski in [28] diskutiert.

Das heißt: Es gibt keine unendliche Menge, die kleiner als \mathbb{N} ist.

Beweis: Ist A_0 unendlich, so besitzt A_0 nach dem Satz 3.4.6 von Dedekind eine unendliche echte Teilmenge A_1 . Wähle $f(0) \in A_0 \setminus A_1$. Sind nun die unendlichen Mengen A_0, \dots, A_n (mit $A_0 \supset A_1 \supset \dots \supset A_n$) und $f(0), \dots, f(n-1) \in A_0$ induktiv festgelegt, sodass $f(i) = f(j) \rightarrow i = j$, so kann man zunächst eine unendliche Teilmenge A_{n+1} von A_n finden und sodann $f(n) \in A_{n+1} \setminus A_n$ wählen. Nach Konstruktion gilt: $f(n) \notin \{f(0), \dots, f(n-1)\}$. Dieser induktive Prozess definiert eine injektive Abbildung $f : \mathbb{N} \rightarrow A_0$, weshalb $f(\mathbb{N})$ eine abzählbar unendliche Teilmenge von A_0 ist. Umgekehrt ist eine abzählbar unendliche Menge A unendlich, denn aus einer Bijektion $f : \mathbb{N} \rightarrow A$ kann man die Injektion $g : \mathbb{N} \rightarrow A$ definieren mit $g(n) := f(n+1)$, sodass $g(\mathbb{N}) = A \setminus \{f(0)\}$ eine abzählbar unendliche Teilmenge von A ist. \square

Hinweis: Varianten des zweiten Beweisteils sind unter Hilberts Hotel bekannt.

Folgerung 3.4.8 *Enthält eine Menge eine unendliche Teilmenge, so ist sie unendlich.*

Beweis: Gilt $A \subseteq B$ und ist A unendlich, so enthält A nach Satz 3.4.7 eine abzählbar unendliche Teilmenge N . Wegen der Transitivität des Einschlusses gilt $N \subseteq B$, also ist B nach Satz 3.4.7 unendlich. \square

Der folgende Satz ist eine Art Nachtrag zum Abschnitt über Funktionen und ihre Eigenschaften, wo uns der geeignete Endlichkeitbegriff noch gefehlt hat.

Satz 3.4.9 *Ist A endlich und $f : A \rightarrow A$, so sind gleichwertig:*

(1) f ist surjektiv, (2) f ist injektiv, (3) f ist bijektiv.

Beweis: Aus den Definitionen ergibt sich unmittelbar, dass nur noch die Äquivalenz von Surjektivität und Injektivität im vorliegenden Fall nachzuweisen ist.

Wir zeigen zunächst die folgende Aussage mit Induktionsbeweis:

$\forall n$: Ist A Menge mit n Elementen und $f : A \rightarrow A$ surjektiv, so ist A injektiv.

Für $n = 0, 1$ sind die Aussagen offenbar richtig.

IV: Die Aussage gilt für alle Mengen mit weniger als n Elementen.

Betrachte Menge A mit $n > 1$ Elementen und Surjektion $f : A \rightarrow A$. Wähle $a \in A$ willkürlich.

(1) Falls $f(a) = a$, so ist $A' = A \setminus \{a\}$ eine Menge mit $n - 1$ Elementen und die Einschränkung von f auf A' surjektiv, nach IV daher injektiv, woraus die Injektivität von f folgt.

(2) Sonst gibt es c mit $f(c) = a$.

Dann ist $f' = T_{a,c}(f)$ (siehe Def. 3.3.6) nach Satz 3.3.8 ebenfalls eine Surjektion. Für sie kann man wie in (1) argumentieren und folgern, dass f' und somit f injektiv sein muss.

Die noch fehlende interessante Beweisrichtung könnte man ganz entsprechend nachweisen, wir argumentieren im Folgenden etwas anders. Sei $f : A \rightarrow A$ injektiv. Per Definition ist f als Abbildung $f : A \rightarrow f(A)$ damit sogar bijektiv. Also gilt $|A| = |f(A)|$ für die Teilmenge $f(A)$ von A . Da A endlich, bedeutet das nach dem Satz 3.4.6 von Dedekind, dass $A = f(A)$ gilt. Daher ist f surjektiv. \square

Satz 3.4.10 *Sei $(M_n)_{n \in \mathbb{N}}$ eine Folge paarweise disjunkter, endlicher, nichtleerer Mengen. Dann ist $\bigcup_{n \in \mathbb{N}} M_n$ abzählbar unendlich.*

Beweis: Gesucht: Bijektion ϕ von \mathbb{N} auf $M^* = \bigcup_{n \in \mathbb{N}} M_n$.

Es bezeichne m_n die Zahl der Elemente von M_n und $m_n^+ = \sum_{0 \leq j < n} m_j$.

Es gibt also Bijektionen $\phi_n : [m_n] \rightarrow M_n$. Da $M_n \neq \emptyset$, gilt stets $m_n > 0$.

Daher gibt es zu jedem $k \in \mathbb{N}$ ein eindeutig bestimmtes $n(k) \in \mathbb{N}$ mit $m_{n(k)}^+ \leq k \leq m_{n(k)+1}^+$.

Da die M_n paarweise disjunkt sind, ist $k \mapsto \phi_{n(k)}(k - m_{n(k)}^+)$ die gesuchte Bijektion ϕ . \square

Folgerung 3.4.11 Sei $M \neq \emptyset$ eine endliche Menge. Die Menge aller endlichen Folgen, gebildet von Elementen aus M , ist abzählbar unendlich.

Dies bedeutet beispielsweise (gemäß Abschnitt 5.3.3), dass die Menge aller Binärwörter abzählbar unendlich ist. Allgemeiner gilt: Programmtexte (in einer fixierten Programmiersprache) lassen sich (rein syntaktisch) als endliche Folgen über einer endlichen Menge (dem *Alphabet*) begreifen. Da wir für jede Funktion $\mathbb{N} \rightarrow \{0, 1\}$, die wir implementieren können, wenigstens einen “eigenen” Programmtext benötigen (in der Regel wird es sogar unendlich viele Programmtexte geben, die dieselbe Funktion implementieren), können wir festhalten:

Folgerung 3.4.12 Die Menge aller Abbildungen $\mathbb{N} \rightarrow \{0, 1\}$, die wir auf Computern implementieren können, ist abzählbar unendlich.

Beweis: Wir müssen uns nur noch überlegen, dass es tatsächlich abzählbar unendlich viele implementierbare Funktionen gibt. Es sollte aber nicht schwerfallen, die Funktion

$$f_n(m) = \begin{cases} 1, & \text{falls } m = n \\ 0, & \text{sonst} \end{cases}$$

zu implementieren. Offenbar gibt es abzählbar unendlich viele derartige Funktionen. \square

Satz 3.4.13 Für jede Menge A gilt: A und 2^A sind nicht gleichmächtig.

Beweis: Andernfalls gäbe es eine Bijektion $f : A \rightarrow 2^A$. Betrachte $S := \{a \in A \mid a \notin f(a)\}$.

Da $S \in 2^A$, gibt es ein $s \in A$ mit $f(s) = S$.

Wäre $s \in S$, so $s \notin f(s)$ nach Def. von S . Da $f(s) = S$, kann das nicht sein.

Wäre $s \notin S$, so wäre nach Def. von S : $s \notin f(s)$, also folgt nach Def. von S : $s \in S$.

Beide möglichen Fälle führen zum Widerspruch. Daher kann es so eine Bijektion nicht geben. \square

Folgerung 3.4.14 Es gibt überabzählbare Mengen.

Beweis: Das folgt mit $A = \mathbb{N}$ aus Satz 3.4.13. \square

Diese Folgerung gestattet noch eine nützlich Veranschaulichung, die auch erklärt, weshalb das (ebenfalls auf Cantor zurückgehende) Beweisprinzip als *Diagonalisierung* bekannt geworden ist. Dazu erinnern wir uns daran, dass $2^{\mathbb{N}}$ und $\{0, 1\}^{\mathbb{N}}$ gleichmächtig sind wegen Beispiel 3.3.17. Angenommen, es gäbe eine Bijektion $f : \mathbb{N} \rightarrow 2^{\mathbb{N}}$.

Dann gäbe es auch eine Bijektion $g : \mathbb{N} \rightarrow \{0, 1\}^{\mathbb{N}}$ mit $\{0, 1\}^{\mathbb{N}} = \{\chi_M \mid M \in 2^{\mathbb{N}}\}$. Wir könnten dann folgende (unendliche) Tabelle erstellen:

	0	1	2	3	4	5	...
$g(0)$	0	1	0	0	0	1	...
$g(1)$	1	1	0	0	0	1	...
$g(2)$	0	1	0	1	1	0	...
$g(3)$	1	0	1	0	1	1	...
\vdots					\ddots		...

Betrachte die Indikatorfunktion, welche durch “Umdrehen” der fettgedruckt hervorgehobenen Bits auf der (Haupt-)Diagonale entsteht. Diese ist “offensichtlich” von jeder der aufgelisteten Indikatorfunktionen verschieden, also gibt es keine vollständige Auflistung aller Indikatorfunktionen der natürlichen Zahlen.

Unsere Überlegungen führen uns zu einer sehr wichtigen Feststellung über die Grenzen der Informatik:

Folgerung 3.4.15 *Nicht jede Abbildung $f : \mathbb{N} \rightarrow \{0, 1\}$ kann durch einen Programmtext beschrieben werden.*

Mit einem ähnlichen Diagonalisierungsargument kann man zeigen (und dies geschieht meist in einer Grundvorlesung über Analysis):

Folgerung 3.4.16 $|\mathbb{Q}| < |\mathbb{R}|$.

3.4.3 Kombinatorik

Die Kunst des Zählens ist von elementarer Wichtigkeit für die Informatik, wie auch das klassische Lehrbuch [20] zeigt.

Dirichletsches Schubfachprinzip

Satz 3.4.17 (*Dirichletsches Schubfachprinzip*)

Gilt $|A| < |B|$, so gibt es keine injektive Abbildung $f : B \rightarrow A$.

Beweis: Es gilt $|A| \leq |B|$. Gäbe es eine injektive Abbildung $f : B \rightarrow A$, dann würde zusätzlich $|B| \leq |A|$ gelten, also $|A| = |B|$ nach Satz 3.4.1 (Antisymmetrie), was $|A| < |B|$ widerspricht. \square

Folgerung 3.4.18 *Gilt $|A| < |B|$, so gibt es zu jeder Abbildung $f : B \rightarrow A$ wenigstens zwei Elemente b, b' mit $f(b) = f(b')$.*

Anwendung: Verteilt man n Gegenstände auf m Fächer mit $m < n$ (und daher $|[m]| < |[n]|$ wegen Lemma 3.4.5), so gibt es ein Schubfach mit mindestens zwei Gegenständen.
Beispiel: Unter 13 Personen finden sich zwei, die im selben Monat Geburtstag haben. Die "Gegenstände" sind die Personen und die "Schubfächer" sind die Monate.

Beispiel: In einer Waschmaschine befinden sich 14 weiße einzelne Socken und 18 schwarze einzelne Socken. Zieht man blind drei Socken heraus, so hat man ein Paar gleichfarbige Socken (Hurra!). Die "Gegenstände" sind die drei Socken und die "Schubfächer" sind die beiden Sockenfarben.

Lemma 3.4.19 *In jedem ungerichteten Graphen $G = (V, E)$ gibt es zwei Knoten $x \neq y$ mit gleich vielen Nachbarn.*

Beweis: Erinnere die Nachbarknotenabbildung N aus Def. 3.3.2. Da $E \cap \Delta_V = \emptyset$, gilt für alle $a \in V$: $d(a) := |N(a)| \in \{0, \dots, |V| - 1\}$. Wir geben jetzt zwei Beweise, einen kürzeren, der mit der Dedekind-Endlichkeit arbeitet, und einen etwas längeren, der mit dem Schubfachprinzip funktioniert.

(A) Wäre d injektiv, so wegen $|V| \leq |d(V)| \leq |\{0, \dots, |V| - 1\}| = |V|$ auch bijektiv, da V endlich. Also gibt es einen Knoten a mit $|N(a)| = |V| - 1$. Da dieser zu allen Knoten benachbart ist, kann es aber keinen Knoten b mit $N(b) = \emptyset$ geben.

(B) Schubfachprinzip-Beweis (mit Fallunterscheidung):

Fall 1: Gibt es ein a mit $|N(a)| = |V| - 1$, so gibt es kein b mit $N(b) = \emptyset$.

V ist dann die Menge der Gegenstände, und $\{1, \dots, |V| - 1\}$ ist die Menge der Schubfächer.

Fall 2: Es gibt kein a mit $|N(a)| = |V| - 1$.

V ist dann die Menge der Gegenstände, und $\{0, \dots, |V| - 2\}$ ist die Menge der Schubfächer. \square

Summenregeln 1

Satz 3.4.20 (*Einfache spezielle Summenregel*)

Sind A und B disjunkte endliche Mengen, so gilt: $|A \cup B| = |A| + |B|$.

Beweis: Da A und B endlich, gibt es natürliche Zahlen n, m und Bijektionen $f : [n] \rightarrow A$ und $g : [m] \rightarrow B$. Definiere

$$h : [n+m] \rightarrow A \cup B, i \mapsto \begin{cases} f(i), & i \in [n] \\ g(i-n), & i \notin [n] \end{cases}$$

Da f, g surjektiv, ist h surjektiv. Da f, g injektiv und da $A \cap B = \emptyset$, ist h injektiv. \square

Satz 3.4.21 (*Mehrfache spezielle Summenregel*) *Sei $k \in \mathbb{N}$ und A_1, \dots, A_k seien endliche, paarweise disjunkte Mengen. Dann gilt:*

$$\left| \bigcup_{i=1}^k A_i \right| = \sum_{i=1}^k |A_i|.$$

Beweis: Die Aussage stimmt für $k \leq 1$.

Angenommen, sie gilt für Vereinigungen von höchstens $k-1$ Mengen, $k \geq 1$. Dann gilt:

$$\begin{aligned} \left| \bigcup_{i=1}^k A_i \right| &= \left| \left(\bigcup_{i=1}^{k-1} A_i \right) \cup A_k \right| \\ &= \left| \left(\bigcup_{i=1}^{k-1} A_i \right) \right| + |A_k| \\ &= \sum_{i=1}^{k-1} |A_i| + |A_k| = \sum_{i=1}^k |A_i|. \end{aligned}$$

Hierbei wurde die einfache spezielle Summenregel und die Induktionsvoraussetzung benutzt. Um die einfache spezielle Summenregel anwenden zu können, müssen wir noch überprüfen, dass $\left(\bigcup_{i=1}^{k-1} A_i \right) \cap A_k = \emptyset$ gilt. Aufgrund der Gültigkeit des in Aufgabe 6.1.10 diskutierten allgemeinen Distributivgesetzes gilt nun

$$\left(\bigcup_{i=1}^{k-1} A_i \right) \cap A_k = \bigcup_{i=1}^{k-1} (A_i \cap A_k).$$

Wegen der paarweisen Disjunkttheit der Mengen A_1, \dots, A_k gilt insbesondere:

$$\forall i \in \{1, \dots, k-1\} : A_i \cap A_k = \emptyset.$$

Daher folgt:

$$\bigcup_{i=1}^{k-1} (A_i \cap A_k) = \bigcup_{i=1}^{k-1} \emptyset = \emptyset,$$

was zu zeigen war. \square

Produkt- und Potenzregeln

Satz 3.4.22 (*Einfache Produktregel*)

Sind A und B endliche Mengen, so gilt: $|A \times B| = |A| \times |B|$.

Beweis: Es sei A beliebig. Wir führen einen Induktionsbeweis über $|B|$.

Für $|B| = 0$ gilt: $|B| = 0$ gdw. $B = \emptyset$, mit den Rechengesetzen des Mengenprodukts gilt also: $|A \times B| = |A \times \emptyset| = |\emptyset| = 0 = |A| \times 0 = |A| \times |B|$, da A endlich.

Im Beweisgang benötigen wir noch die Richtigkeit der Aussage für $|B| = 1$. (*)

In dem Fall ist nämlich $B = \{b\}$, und $f : A \times B \rightarrow A$, $(a, b) \mapsto a$ ist eine Bijektion.

Angenommen (IV), die Aussage gilt für alle Mengen B mit $|B| \leq n$.

Betrachte eine Menge B mit $|B| = n + 1$.

Wähle beliebiges, aber festes Element b und setze $B' = B \setminus \{b\}$.

Wegen $B = B' \cup \{b\}$ und $B' \cap \{b\} = \emptyset$ (nach Konstruktion) gilt mit Satz 3.4.20:

$$n + 1 = |B| = |B'| + |\{b\}| = |B'| + 1, \text{ also } |B'| = n.$$

Daher lässt sich IV auf B' anwenden, und die Rechengesetze des Mengenprodukts liefern:

$$\begin{aligned} |A \times B| &= |A \times (B' \cup \{b\})| = |A \times B' \cup A \times \{b\}| = |A \times B'| + |A \times \{b\}| = |A| \times |B'| + |A| = \\ &= |A| \times (|B'| + 1) = |A| \times |B|. \end{aligned} \quad \text{Hierbei haben wir noch (*) und Satz 3.4.20 angewendet.} \quad \square$$

Analog zur mehrfachen Summenregel kann man zeigen:

Satz 3.4.23 (Mehrfache Produktregel)

Sei $k \in \mathbb{N}$, $k \geq 1$ und A_1, \dots, A_k seien endliche Mengen. Dann gilt:

$$\left| \bigtimes_{i=1}^k A_i \right| = \prod_{i=1}^k |A_i|.$$

Das mehrfache Mengenprodukt wurde in Abschnitt 4.2.1 formal eingeführt. Wichtig ist es vor allem für den Spezialfall $A_1 = \dots = A_k = A$. Dann schreibt man dieses auch A^k (also als Potenz),

Folgerung 3.4.24 (Potenzregel) Ist $A \neq \emptyset$ endlich und $n \in \mathbb{N}$, so gilt: $|A^n| = |A|^n$.

Die Produktregel kann man sich am *Entscheidungsbaum* veranschaulichen. Diese Konzept ist aus der Schule bekannt.

Beispiel: Wie viele Binärwörter mit drei Ziffern gibt es?

Da drei Entscheidungen zu fällen sind (für jede Ziffer eine), haben Pfade von der Wurzel bis zu den Blättern stets die Länge drei.

Da es sich um binäre Entscheidungen jeweils handelt, hat jeder Knoten, der kein Blatt ist, zwei Kinder.

Durch Abzählen der Blätter sehen wir die Lösung: acht.

Dies liefert auch die Produktregel: $|\{0, 1\} \times \{0, 1\} \times \{0, 1\}| = 2^3 = 8$.

Regeln für Funktionen und Mengen

Angesichts bekannter Bijektionen (Satz 4.3.5) beleuchtet der folgende Satz die Potenzregel aus einem anderen Blickwinkel.

Satz 3.4.25 (Funktionenregel) Für endliche Mengen A, B gilt: $|B^A| = |B|^{|A|}$.

Beweis: Jedem Element aus A können $|B|$ verschiedene Elemente zugeordnet werden. Die Zuordnung der Elemente aus B erfolgt unabhängig für verschiedene Elemente aus A . Mit einfacher Induktion über die Größe von A folgt daher:

$$|B^A| = \underbrace{|B| \cdots |B|}_{|A| \text{ mal}} = |B|^{|A|}.$$

□

Wegen Beispiel 3.3.17 folgt hieraus:

Folgerung 3.4.26 (Potenzmengenregel)

Für jede endliche Menge M gilt: $|2^M| = 2^{|M|}$.

Definition 3.4.3 Für eine Menge A und eine natürliche Zahl ℓ (meist: $0 \leq \ell \leq |A|$) bezeichnet

$$\binom{A}{\ell}$$

die Menge der ℓ -elementigen Teilmengen von A . Gilt $n = |A|$, so schreiben wir auch:

$$\binom{n}{\ell} := \left| \binom{A}{\ell} \right|$$

und nennen den linken Ausdruck Binomialkoeffizienten, gelesen n über ℓ .

Satz 3.4.27 $\sum_{\ell=0}^n \binom{n}{\ell} = 2^n$.

Beweis: Wir führen einen *kombinatorischen Beweis*: Es sei A eine n -elementige Menge. Für die Potenzmenge wissen wir: $|2^A| = 2^n$. Die Potenzmenge lässt sich bezüglich der Mächtigkeit in Klassen (paarweise disjunkte Mengen) einteilen. Daher liefert die (mehrfache) Summenregel:

$$\left| \bigcup_{\ell=0}^n \binom{A}{\ell} \right| = \sum_{\ell=0}^n \left| \binom{A}{\ell} \right| = \sum_{\ell=0}^n \binom{n}{\ell} = 2^n.$$

Ein Induktionsbeweis ist viel aufwändiger (siehe [33]). □

Wir wissen bereits, dass es n^n viele Abbildungen einer n -elementigen Menge A auf sich selbst gibt. Wir wissen überdies, dass Eigenschaften wie Bijektivität eine Einschränkung des Begriffs der Abbildung bedeuten. Daher können wir erwarten, dass es weniger Bijektionen $A \rightarrow A$ gibt als n^n . Aber können wir dies genauer angeben?

Satz 3.4.28 Es sei A eine endliche Menge. Die Anzahl der Bijektionen $f : A \rightarrow A$ beträgt $(|A|)!$.

Hinweis: Die Fakultätsfunktion wurde in Abschnitt 3.3 besprochen.

Beweis: Wir zeigen etwas allgemeiner per Induktion: Gilt $|A| = |B| = n$, so gibt es $n!$ verschiedene Bijektionen von A nach B . Für $A = B = \emptyset$ stimmt es; die einzige Abbildung in \emptyset^\emptyset ist bijektiv. Betrachte n -elementige Mengen A, B , $n \geq 1$. Wähle $a \in A, b \in B$ beliebig. $A' = A \setminus \{a\}$ und $B' = B \setminus \{b\}$ sind gleichmächtig. Nach IV gibt es $(n-1)!$ viele Bijektionen von A' nach B' . Jede dieser Bijektionen f' definiert eine Bijektion $f : A \rightarrow B$ durch $f(x) = f'(x)$ für $x \neq a$ und $f(a) = b$. Umgekehrt muss ein fixiertes $a \in A$ auf irgendein $b \in B$ abgebildet werden. Die mehrfache spezielle Summenregel liefert nun die Behauptung:

$$\begin{aligned} |\{f : A \rightarrow B \mid f \text{ ist bijektiv}\}| &= \left| \bigcup_{b \in B} \{f : A \rightarrow B \mid f \text{ ist bijektiv} \wedge f(a) = b\} \right| \\ &= \sum_{b \in B} |\{f : A \rightarrow B \mid f \text{ ist bijektiv} \wedge f(a) = b\}| \\ &= \sum_{b \in B} (n-1)! = |A|(n-1)! = n! \end{aligned}$$

□

Summenregeln 2

Wir wollen jetzt noch eine allgemeinere Form der Summenregel herleiten.

Satz 3.4.29 (allgemeine einfache Summenregel)

Seien A und B endliche Mengen. Dann gilt:

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Beweis: Zu zeigen ist (leicht umgeformt):

$$|A \cap B| + |A \cup B| = |A| + |B|.$$

Da $A \cup B = (A \setminus B) \cup B$ und $(A \setminus B) \cap B = \emptyset$, liefert die einfache spezielle Summenregel:

$$|A \cap B| + |A \cup B| = |A \cap B| + |A \setminus B| + |B|.$$

Da $A = (A \cap B) \cup (A \setminus B)$ und $A \cap B \cap (A \setminus B) = \emptyset$, können wir die einfache spezielle Summenregel nochmals anwenden und erhalten schließlich:

$$|A \cap B| + |A \setminus B| + |B| = |A| + |B|$$

□

Die Idee hinter der allgemeinen Summenregel ist auch als Inklusions-Exklusionsprinzip bekannt. Man muss immer wieder alternierend “zuviel gezählte” Elemente beim nächsten Mal wieder abziehen bzw. zuviel abgezogene Elemente wieder draufzählen. Für drei Mengen sieht die Regel folgendermaßen aus:

Satz 3.4.30 (allgemeine zweifache Summenregel)

Es seien A, B, C endliche Mengen. Dann gilt:

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|.$$

Beweis: $|(A \cup B) \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$
 $= |A| + |B| + |C| - |A \cap B| - |(A \cap C) \cup (B \cap C)|$
 $= |A| + |B| + |C| - |A \cap B| - (|A \cap C| + |B \cap C| - |A \cap B \cap C|).$ □

Die ganz allgemeine Formel sieht etwas unschön aus, zeigt aber das angesproche Alternieren von Zuzählen und Abziehen mit dem Vorfaktor $(-1)^{\ell-1}$ sehr deutlich. Man kann die Formel recht leicht per Induktion beweisen, wobei der Induktionsschritt im Grund im Beweis zu Satz 3.4.30 schon vorgemacht wurde.

Satz 3.4.31 (allgemeine mehrfache Summenregel)

Es seien A_0, \dots, A_{k-1} endliche Mengen. Dann gilt:

$$\left| \bigcup_{i=0}^{k-1} A_i \right| = \sum_{\ell=1}^k (-1)^{\ell-1} \left(\sum_{I \in \binom{[k]}{\ell}} \left| \bigcap_{j \in I} A_j \right| \right) = \sum_{I \subseteq [k], I \neq \emptyset} (-1)^{|I|-1} \left| \bigcap_{j \in I} A_j \right|$$

Mit der Übereinkunft $A_I := \bigcap_{j \in I} A_j$ lässt sich die Formel weiter vereinfachen. Ist nun A_\emptyset eine endliche Obermenge der Mengen A_0, \dots, A_{k-1} und wollen wir zählen, wie viele Elemente in keiner der Mengen A_0, \dots, A_{k-1} liegen, so ergibt sich:

$$\left| A_\emptyset \setminus \left(\bigcup_{i=0}^{k-1} A_i \right) \right| = \sum_{I \subseteq [k]} (-1)^{|I|} |A_I|.$$

Wichtig ist ebenfalls die folgende Abschätzung:

Folgerung 3.4.32 *Es seien A_0, \dots, A_{k-1} endliche Mengen. Dann gilt:*

$$\left| \bigcup_{i=0}^{k-1} A_i \right| \leq \sum_{i=0}^{k-1} |A_i|.$$

3.5 Quasiordnungen

Die folgende Definition fasst die Grundbegriffe dieses Abschnitts zusammen. Es vertieft und baut auf die in Abschnitt 3.2 eingeführten Begrifflichkeiten.

Definition 3.5.1 *Es sei R eine Relation auf M .*

- R heißt Quasiordnung, wenn R reflexiv und transitiv.
- R heißt Äquivalenzrelation, wenn R symmetrische Quasiordnung.
- R heißt Halbordnung, wenn R antisymmetrische Quasiordnung.

Eine recht allgemeine Möglichkeit, sich Beispiele für Quasiordnungen aus einfachen Verknüpfungen zu besorgen, ist in Abschnitt 5.7.2 dargestellt.

Wir zeigen nun, wie man aus einfachen Quasiordnungen kompliziertere zusammensetzen kann.

Satz 3.5.1 *Es sei R_1 eine Quasiordnung auf M_1 und R_2 eine Quasiordnung auf M_2 . Definiere auf $M_1 \times M_2$ die Relation*

$$((x_1, x_2), (y_1, y_2)) \in R : \iff (x_1, y_1) \in R_1 \wedge (x_2, y_2) \in R_2.$$

R ist eine Quasiordnung auf $M_1 \times M_2$.

Wir nennen R auch *komponentenweise Quasiordnung*.

Beweis: Betrachte $(a_1, a_2) \in M_1 \times M_2$ beliebig. Da R_1 und R_2 reflexiv, gilt $(a_1, a_1) \in R_1$ und $(a_2, a_2) \in R_2$ und nach Def. von R : $((a_1, a_2), (a_1, a_2)) \in R$. Also ist R reflexiv.

Betrachte $a_1, b_1, c_1 \in M_1$ und $a_2, b_2, c_2 \in M_2$ mit $((a_1, a_2), (b_1, b_2)), ((b_1, b_2), (c_1, c_2)) \in R$. Nach Def. von R ist damit $(a_1, b_1) \in R_1$, $(a_2, b_2) \in R_2$, $(b_1, c_1) \in R_1$ und $(b_2, c_2) \in R_2$. Da R_1 und R_2 transitiv, folgt $(a_1, c_1) \in R_1$ und $(a_2, c_2) \in R_2$, also nach Def. von R : $((a_1, a_2), (c_1, c_2)) \in R$. Daher ist R transitiv. \square

Wir können diese Konstruktion auch für speziellere Quasiordnungen durchführen.

Folgerung 3.5.2 *Sind R_1 und R_2 Äquivalenzrelationen auf M_1 bzw. M_2 , so ist die hieraus gebildete komponentenweise Quasiordnung R auf $M_1 \times M_2$ eine Äquivalenzrelation.*

Folgerung 3.5.3 *Sind R_1 und R_2 Halbordnungen auf M_1 bzw. M_2 , so ist die hieraus gebildete komponentenweise Quasiordnung R auf $M_1 \times M_2$ eine Halbordnung.*

Die Beweise sind gute Übungsaufgaben.

3.5.1 Äquivalenzrelationen

Wir können aus jeder Quasiordnung in der im Folgenden beschriebenen Weise eine Äquivalenzrelation machen.

Definition 3.5.2 Es sei R eine Quasiordnung auf M . Definiere $x \sim_R y : \iff (x, y) \in R \wedge (y, x) \in R$ als zugeordnete Äquivalenzrelation.

Satz 3.5.4 Jede einer Quasiordnung zugeordnete Äquivalenzrelation ist tatsächlich eine Äquivalenzrelation.

Beweis: Wir müssen also zeigen: Ist R eine Quasiordnung auf M , so ist \sim_R eine Äquivalenzrelation über M .

Reflexivität: $x \sim_R x$, denn $(x, x) \in R$, da R reflexiv.

Symmetrie: Gilt $x \sim_R y$, so heißt das: $(x, y) \in R$ und $(y, x) \in R$, also auch $(y, x) \in R$ und $(x, y) \in R$, d.h., $y \sim_R x$.

Transitivität: Gilt $x \sim_R y$ und $y \sim_R z$, so $\{(x, y), (y, x), (y, z), (z, y)\} \subseteq R$. Da R transitiv, folgt $\{(x, z), (z, x)\} \subseteq R$, also $x \sim_R z$. \square

Beispiel 3.5.5 Es sei \mathcal{U} ein festes Universum. Unsere Überlegungen aus Abschnitt 3.4 zeigen:

- Die Relation $\equiv_{\mathcal{U}} \subseteq 2^{\mathcal{U}} \times 2^{\mathcal{U}}: A \equiv_{\mathcal{U}} B : \iff |A| = |B|$ ist eine Äquivalenzrelation auf $2^{\mathcal{U}}$.
- Die Relation $\leq_{\mathcal{U}} \subseteq 2^{\mathcal{U}} \times 2^{\mathcal{U}}: A \leq_{\mathcal{U}} B : \iff |A| \leq |B|$ ist eine Quasiordnung auf $2^{\mathcal{U}}$.
- Die der Quasiordnung $\leq_{\mathcal{U}} \subseteq 2^{\mathcal{U}} \times 2^{\mathcal{U}}$ zugeordnete Äquivalenzrelation ist $\equiv_{\mathcal{U}}$.

Eine gute Wiederholung ist es, diese drei Behauptungen genau mit Ergebnissen aus Abschnitt 3.4 zu belegen.

Zerlegungen und Äquivalenzrelationen

Diese beiden Begriffe hängen sehr eng zusammen, wie wir jetzt sehen werden.

Satz 3.5.6 Es sei Z eine Zerlegung von M . Definiere eine Relation \sim_Z auf M durch:
 $a \sim_Z b : \iff a$ und b liegen in derselben Z -Klasse.
Dann ist \sim_Z eine Äquivalenzrelation.

Diese Relation \sim_Z heißt auch die von Z induzierte Äquivalenzrelation.

Beweis: 0. Klar: $\sim_Z \subseteq M \times M$.

1. Reflexivität: Wegen $M = \bigcup_{A \in Z} A$ folgt für jedes a : $a \sim_Z a$.

2. Symmetrie: trivial

3. Transitivität: Betrachte a, b, c mit $a \sim_Z b$ und $b \sim_Z c$.

Also gibt es Klassen J und K mit $a, b \in J$ und $b, c \in K$. Daher ist: $J \cap K \neq \emptyset$.

Da Z Zerlegung, folgt $J = K$, woraus sich ergibt, dass a und c in derselben Z -Klasse liegen, also $a \sim_Z c$ gilt. \square

Definition 3.5.3 Es sei R eine Äquivalenzrelation über M .

$[b]_R := \{a \in M \mid aRb\}$ bezeichnet die Äquivalenzklasse von b .

b heißt auch Repräsentant oder Vertreter von $[b]_R$.

$M/R := Z_R := \{[b]_R \mid b \in M\}$ ist die Quotientenmenge von R .

Die Abbildung $M \rightarrow M/R$, $b \mapsto [b]_R$ heißt auch kanonische Abbildung von R .

Beispiel: Die Allrelation ist eine Äquivalenzrelation. $[x]_{M \times M} = M$ für alle $x \in M$.

Es gibt also nur eine Äquivalenzklasse.

Beispiel: Die Diagonale ist eine Äquivalenzrelation. $[x]_{\Delta_M} = \{x\}$ für alle $x \in M$. Es gibt maximal viele Äquivalenzklassen.

Beispiel 3.5.7 Es sei \mathcal{U} ein festes Universum. In Fortführung von Beispiel 3.5.5 und als Ergänzung von Abschnitt 3.4 halten wir fest: Die Äquivalenzklasse $[A]_{\equiv_U}$ heißt Mächtigkeit oder Kardinalität von A , geschrieben $|A|$.

$|\cdot|$ kann also als kanonische Abbildung von \equiv_U aufgefasst werden.

Es bezeichne $\mathfrak{Card}(\mathcal{U}) := 2^{\mathcal{U}} / \equiv_U$ die Mächtigkeiten von Teilmengen von \mathcal{U} .

Die Elemente von $\mathfrak{Card}(\mathcal{U})$ heißen auch Kardinalzahlen (über \mathcal{U}).

Beispiel 3.5.8 $R_m = \{(a, b) \in \mathbb{Z}^2 : m \mid (a - b)\}$ ist eine Äquivalenzrelation. Zwei ganze Zahlen sind äquivalent gdw. sie lassen beim Teilen durch m denselben Rest.

Schreibweise: $a \equiv b \pmod{m}$ statt $aR_m b$.

$R_m \subset \mathbb{Z} \times \mathbb{Z}$: Äquivalenzklassen sind $[0]_{R_m}, [1]_{R_m}, \dots, [m-1]_{R_m}$.

Schreibweise: (für die Menge der Restklassen) $\mathbb{Z}_m := \mathbb{Z}/R_m$.

Die Restklassen $[n]_{R_m}$ notiert man meist durch die kleinste Zahl aus $[n]_{R_m} \cap \mathbb{N}$.

Als Hilfsüberlegung stellen wir auf:

Lemma 3.5.9 Ist $R \subseteq M \times M$ eine Äquivalenzrelation, dann gilt für beliebige Äquivalenzklassen $[b]_R$ und beliebige $x, y \in M$: Falls $\{x, y\} \subseteq [b]_R$, so $\{(x, y), (y, x)\} \subseteq R$.

Satz 3.5.10 Ist R eine Äquivalenzrelation über M , so ist Z_R eine Zerlegung von M .

Wiederum könnte man daher Z_R als die von R induzierte Zerlegung ansprechen.

Beweis: 1. Jedes Element ist in einer ÄK von Z_R enthalten.

Betrachte $a \in M$. Wegen $(a, a) \in R$ gilt: $[a]_R \neq \emptyset$.

2. $\emptyset \notin Z_R$.

Dies folgt mit dem vorigen Argument, da ÄK nur von der Gestalt $[a]_R$ sind.

3. Gilt $[a]_R \cap [b]_R \neq \emptyset$, so ist $[a]_R = [b]_R$.

Vorüberlegung: Da $[a]_R \cap [b]_R \neq \emptyset$, gibt es ein $y \in [a]_R \cap [b]_R$.

Betrachte irgendein $x \in [a]_R$. Da $\{x, y\} \subseteq [a]_R$, gilt $(x, y) \in R$ wegen Lemma 3.5.9.

Betrachte ferner irgendein $z \in [b]_R$. Mit $\{y, z\} \subseteq [b]_R$ gilt $(y, z) \in R$ wegen Lemma 3.5.9.

Da R transitiv, gilt $(x, z) \in R$ (*).

Mithin ist: $(z, b) \in R$ (da $z \in [b]_R$), also $(x, z) \in R$ (wegen (*)) und da R transitiv) und so $x \in [b]_R$ und (ähnlich) $z \in [a]_R$.

Nach Def. der Quotientenmengen und da x, z bel., folgt $[a]_R = [b]_R$. □

3.5.2 Halbordnungen

Beispiel: \leq oder \geq auf \mathbb{R} sind Halbordnungen.

Beispiel: Die Teilerrelation ist eine Halbordnung auf \mathbb{N} , aber nicht auf \mathbb{Z} .

Beispiel: Auf der Potenzmenge von M ist \subseteq oder auch \supseteq eine Halbordnung.

Beispiel: Es gibt einfache Quasiordnungen, die weder symmetrisch noch antisymmetrisch sind, z.B.: $R := \{(a, a), (b, b), (c, c), (a, b), (a, c), (b, a), (b, c)\}$ über $\{a, b, c\}$.

Halbordnungen aus Quasiordnungen Es sei R eine Quasiordnung auf M und \sim_R die vor Satz 3.5.4 definierte induzierte Äquivalenzrelation. Wir definieren auf M / \sim_R nun:

$$A \leq_R B : \iff \exists a \in A \exists b \in B : (a, b) \in R.$$

Lemma 3.5.11 \leq_R ist vertreterunabhängig und somit wohldefiniert.

Beweis: Diskutiere $a, a' \in A$ und $b, b' \in B$ mit $(a, b) \in R$.

Da $a \sim_R a'$, gilt $(a', a) \in R$.

Da $b \sim_R b'$, gilt $(b, b') \in R$.

Zusammen folgt mit der Transitivität von R : $(a', b') \in R$. \square

Wegen dieses Lemmas ist \leq_R eine Binärrelation auf M / \sim_R . Außerdem gilt:

$$A \leq_R B \iff \forall a \in A \forall b \in B : (a, b) \in R.$$

Mit den soeben eingeführten Begriffen können wir aussprechen:

Satz 3.5.12 Ist R eine Quasiordnung auf M , so ist \leq_R eine Halbordnung auf M / \sim_R .

Beweis: Reflexivität: $A \leq_R A$, da für $a \in A$ gilt: $(a, a) \in R$.

Antisymmetrie: Betrachte A, B mit $(A \leq_R B)$ und $(B \leq_R A)$. Wähle $a \in A, b \in B$ beliebig.

Wegen der Vertreterunabhängigkeit (Lemma 3.5.11) ergibt sich dann aus $A \leq_R B$: $(a, b) \in R$ und aus $B \leq_R A$: $(b, a) \in R$. Also folgt $a \sim_R b$.

Da A und B Äquivalenzklassen und a, b beliebig, gilt also $A = B$.

Transitivität: Gilt $(A \leq_R B)$ und $(B \leq_R C)$, so gibt es $a \in A, b \in B$ und $c \in C$ mit $(a, b) \in R$ und $(b, c) \in R$. Da R transitiv, folgt $(a, c) \in R$ und somit $A \leq_R C$ nach Def. von \leq_R . \square

Beispiel 3.5.13 Es sei \mathcal{U} ein festes Universum. In Fortführung von Beispielen 3.5.5 und 3.5.7 sowie als Ergänzung von Abschnitt 3.4 halten wir fest: Da $\leq_{\mathcal{U}}$ eine Quasiordnung auf $2^{\mathcal{U}}$ ist, ist die durch $|A| \leq |B| : \iff A \leq_{\mathcal{U}} B$ auf den Kardinalzahlen über \mathcal{U} definierte Relation eine Halbordnung.

Abgeleitete Begriffe Wir wollen jetzt eine ganze Sammlung von Begriffen bereitstellen, die Sie sicherlich im Zusammenhang mit einigen konkreten Halbordnungen bereits gehört haben oder aber noch hören werden. Für diesen Kursus sind sie allerdings weniger von Belang, mit Ausnahme vom Begriff des Supremums.

Definition 3.5.4 Es sei (M, \leq) eine Halbordnung und $N \subseteq M$.

• $x \in N$ heißt größtes Element von N gdw. $\forall y \in N : y \leq x$.

• $x \in N$ heißt kleinstes Element von N gdw. $\forall y \in N : x \leq y$.

- $x \in N$ heißt maximales Element in N gdw. $\forall y \in N : x \leq y \implies y = x$.
- $x \in N$ heißt minimales Element in N gdw. $\forall y \in N : y \leq x \implies y = x$.
- $x \in M$ heißt obere Schranke von N gdw. $\forall y \in N : y \leq x$.
Sei $OS(N)$ die Menge aller oberen Schranken von N .
- $x \in M$ heißt untere Schranke von N gdw. $\forall y \in N : x \leq y$.
- Eine kleinste obere Schranke von N heißt auch obere Grenze oder Supremum von N , geschrieben $\sup(N)$. $\sup(N)$ ist also ein kleinstes Element in $OS(N)$.
- Eine größte untere Schranke von N heißt auch untere Grenze oder Infimum von N , geschrieben $\inf(N)$.

Aus diesen Definitionen folgt sofort:

Satz 3.5.14 Eine Menge N besitzt ein größtes Element gdw. eine obere Grenze liegt in N gdw. eine obere Schranke liegt in N .
Größte Elemente und obere Grenzen einer Menge sind eindeutig bestimmt (so es sie gibt).

Abgeleitete Relationen und Hasse-Diagramme Man kann von einer Halbordnung verschiedene (andere) Relationen ableiten. Solche Begriffe führen wir jetzt ein.

Definition 3.5.5 Es sei \leq eine Halbordnung auf M . Ferner seien $x, y, z \in M$.

Gilt $(x, y) \in R$, so heißt x auch Vorgänger von y und y Nachfolger von x .

z heißt echter Nachfolger von x , i.Z. $x < z$, gdw. (1) $x \leq z$ und (2) $x \neq z$.

Ein echter Nachfolger z von x heißt unmittelbarer Nachfolger von x , falls

(3) aus $x \leq y \leq z$ folgt: $y = x$ oder $y = z$.

Hinweis: Entsprechend definierbar: echter Vorgänger, unmittelbarer Vorgänger

Zwei Elemente $x, y \in M$ heißen vergleichbar gdw. ($x \leq y \vee y \leq x$);

andernfalls heißen sie unvergleichbar.

Lineare Ordnungen und Sortieren

Definition 3.5.6 Es sei \leq eine Halbordnung auf M .

\leq heißt lineare (oder totale) (Halb-)Ordnung gdw.

alle Elemente von M sind untereinander paarweise vergleichbar.

Beispiel: Zahlenstrahl: Lineare Ordnung der reellen Zahlen.

Beispiel: Lexikalische Ordnung in einem Wörterbuch

Achtung: Die "Struktur" dieser Ordnung ist "anders" als beim Zahlenstrahl.

Wir können beobachten:

Lemma 3.5.15 Eine Halbordnung auf M ist linear genau dann, wenn die zugehörige Vergleichbarkeitsrelation V gleich $M \times M$ ist, was gleichbedeutend damit ist, dass V eine Äquivalenzrelation mit genau einer Äquivalenzklasse ist.

Vergleichbarkeitsrelationen zu Halbordnungen werden in Aufgabe 6.5.10 näher beleuchtet.

Hinweis: Wir hatten in Beispiel 3.5.13 ausgesprochen, dass für die Kardinalzahlen über einem festen Universum \leq eine Halbordnung ist; diese Aussage ließe sich verschärfen. Genauer gesagt ist die Aussage, dass \leq sogar stets eine Lineare Ordnung bildet, zum Auswahlaxiom äquivalent. Mehr dazu finden Sie in Abschnitt 4.5.1.

Rechner werden heutzutage weniger zum Rechnen denn zum Suchen und Sortieren verwendet. Hierbei spielen Ordnungen eine wesentliche Rolle, um die Grundprinzipien zu verstehen.

Es sei (M, \leq) eine totale Ordnung (z.B.: lexikalische Ordnung oder Zahlenstrahl-Anordnung der ganzen Zahlen) und $N \subseteq M$ eine endliche Menge mit totaler Ordnung Mem (z.B.: lineare Anordnung im Speicher).

N heißt *sortiert bzgl. \leq* gdw. $\text{Mem} = \leq \cap N \times N$.

Die Definition motiviert einen einfachen *Sortieralgorithmus*:

Solange $\exists x, y \in N, x \neq y : (x, y) \in \text{Mem} \wedge y \leq x$, **tue:**
 $\text{Mem} \leftarrow (\text{Mem} \setminus \{(x, y)\}) \cup \{(y, x)\}$.

Wir beobachten:

- Sollte der Algorithmus jemals anhalten, so gilt $\text{Mem} = \leq \cap N \times N$, d.h., N wurde sortiert.
- Als Teilmenge von $N \times N$ kann Mem ursprünglich höchstens $|N|^2$ viele “falsch sortierte” Paare von Elementen aus N enthalten, d.h., der Schleifenrumpf wird höchstens $|N|^2$ of ausgeführt.
- Wenn das Auffinden und Reparieren “falsch sortierter Paare” schnell genug geht (recht naiv z.B. mit höchstens $|N|^2$ Schritten), so hält der Algorithmus insgesamt nach höchstens $|N|^4$ Schritten.
- Sollte dieses Auffinden und Reparieren überhaupt auf Rechnern möglich sein², so wird das Verfahren aufgrund der ersten beiden Beobachtungen jedenfalls *terminieren*, d.h. anhalten.

Wer Zweifel an der zweiten Behauptung hat, die ja wesentlich für die in der vierten Behauptung explizierten Terminierungseigenschaft ist, kann die folgende Behauptung per Induktion beweisen:

Lemma 3.5.16 *Es sei m eine natürliche Zahl. Nach dem m -ten Durchlauf des Schleifenrumpfes gilt (so es diesen überhaupt gibt): es gibt wenigstens m Paare $(x, y) \in N \times N, x \neq y$, für die gilt: $(x, y) \in \text{Mem} \wedge x \leq y$.*

Eine der wichtigen Zweige der (Theoretischen) Informatik ist die Algorithmik; sie beschäftigt sich mit dem Auffinden guter Algorithmen (und Datenstrukturen), die möglichst schnelle Lösungen für (wichtige) Aufgabenstellungen. Hierbei sind oft gute mathematische Beobachtungen hilfreich. Unser (naiver) Sortieralgorithmus lässt sich beispielsweise durch folgende Aussage verbessern:

²Diese Bedingung mag Manchem unnötig erscheinen, aber man kann auch in solche Dinge zumindest künstlich Probleme hineinkodieren, die auf Rechnern nicht lösbar sind. Dies ist im Wesentlichen der allgemeinen Natur unserer Darstellung geschuldet. Mehr über derartige Grenzen von Computern erfahren Sie in “Berechenbarkeit und Komplexität”.

Lemma 3.5.17 Gilt für alle $a, b \in N$, für die b unmittelbarer Nachfolger von a bezüglich \leq ist, dass $a \leq b$ gilt, so ist N sortiert.

Beweis: Wir führen einen Induktionsbeweis über $|N|$. Die Aussage gilt sicher für $|N| = 1$ und $|N| = 2$.

Wir nehmen an, die Aussage gilt für N mit $|N| = n \geq 2$.

Betrachte eine Menge N mit $n+1$ Elementen, für die gilt, dass, falls b unmittelbarer Nachfolger von a bezüglich \leq ist, so gilt $a \leq b$. Sei $c \in N$ das größte Element von N bzgl. \leq . Sei $N' = N \setminus \{c\}$. Nach Induktionsvoraussetzung können wir annehmen, dass N' sortiert ist. Daher sind $\leq \cap (N' \times N')$ und $\leq \cap (N' \times N')$ totale Ordnungen. Fügen wir nun c wieder (ans Ende) ein, so ist N' eine totale Ordnung. Das größte Element c' von N' bzgl. \leq ist darin unmittelbarer Vorgänger von c . Also gilt $c' \leq c$. Wegen $\leq \cap (N' \times N') = \leq \cap (N' \times N')$ und da \leq transitiv, folgt, dass c größtes Element von N bzgl. \leq ist. Daher ist N sortiert. \square

Damit können wir unseren Algorithmus schon in Richtung “Bubblesort” entwickeln, was Etliche von Ihnen vermutlich auch kennen. Wir erkennen an diesem Beispiel auch die Wichtigkeit induktiver Beweisgänge bei der Analyse von Algorithmen.

3.6 Ungerichtete Graphen

Wir hatten wichtige Begriffe zu diesem Thema verstreut über die vorigen Abschnitte bereits kennengelernt. Im Folgenden fassen wir diese zur Erinnerung zusammen. Gleichzeitig führen wir einige neue Sprechweisen ein.

- Ein gerichteter Graph $G = (V, E)$ heißt *ungerichtet*, falls $E \subseteq V \times V$ irreflexiv und symmetrisch ist.
- $|V|$ heißt auch *Ordnung*, $|E|$ *Größe* von G .

Im Folgenden sind (wenn nicht ausdrücklich anders vermerkt) in diesem Abschnitt Graphen bei uns stets ungerichtet. Alternativ findet man für ungerichtete Graphen der Literatur die Darstellung der Kantenmenge als

$$E \subseteq \binom{V}{2}.$$

Das folgende Lemma zeigt, dass beide Darstellungen äquivalent sind.

Lemma 3.6.1 $|2^{\binom{V}{2}}| = 2^{\binom{|V|}{2}} = |\{E \subseteq V \times V \mid E \text{ irreflexiv und symmetrisch}\}|$.

Beweis: Die linke Gleichheit folgt aus bekannten kombinatorischen Gesetzen (s. Folg. 3.4.26 und Def. des Binomialkoeffizienten), also gibt es mit Übung 6.4.8 $2^{\frac{n(n-1)}{2}}$ ungerichtete Graphen mit $|V| = n$ in der “Mengendarstellung” der Kanten.

Andererseits ist eine symmetrische irreflexive Relation durch die Nullen und Einsen oberhalb der Hauptdiagonalen der Relationenmatrix festgelegt. Für $|V| = n$ gibt es $n - 1$ festzulegende Werte in der ersten Zeile, $n - 2$ viele in der zweiten usf. bis zu 0 Werten in der n -ten Zeile. Es gilt (siehe Übung 6.1.6) $\sum_{i=0}^{n-1} = \frac{n(n-1)}{2}$. \square

Übereinkunft: Tatsächlich ist die “Mengenauffassung” der Kanten heutzutage die üblichere. Die Mächtigkeit der Menge der Kanten (also die Größe eines Graphen) wird

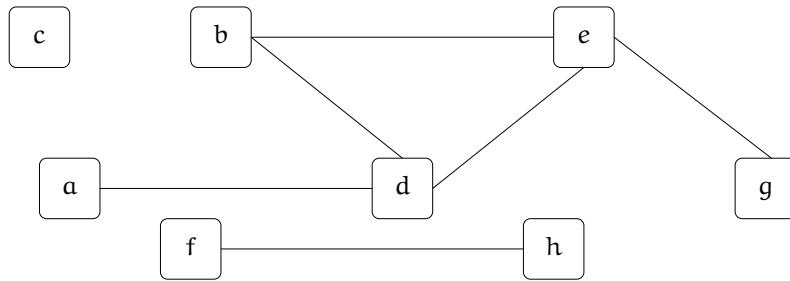


Abbildung 3.7: Ein gezeichneter Graph

hiervon beeinflusst, da ‘‘Kanten in beide Richtungen’’ nur einmal gezählt werden. Der üblicheren Literatur folgend, soll für uns im Folgenden $|E|$ auch so auffassen, dass die Kanten $(x, y), (y, x)$ nur als eine Kante $\{x, y\}$ gezählt werden und dann auch gerne vereinfacht xy geschrieben werden.

Beispiele

- $G_1 = (\{a, b, c\}, \{ab\})$,
- $G_2 = (\{a, b, c\}, \{bc\})$,
- $G_3 = (\{x, y\}, \{xy\})$,
- $G_4 = (\{1, 2, 3\}, \{12, 23\})$,
- $G_5 = (\{1, 2, 3\}, \{12, 23, 13\})$,
- $G_6 = (V_6 := \{(1;3), (2;4), (3;5)\}, \{IJ \mid I, J \in V_6, I \cap J \neq \emptyset, I \neq J\})$.

Bild 3.7 ist eine graphische Darstellung für $G = (V, E)$ mit $V = \{a, b, c, d, e, f, g, h\}$ und $E = \{ad, bd, be, de, eg, fh\}$.

Es sei $G = (V, E)$ ein Graph.

- $G = (V, E)$ definiert die *Inzidenzrelation* $I_G \subseteq V \times E$ durch $(v, e) \in I_G$ gdw. $v \in e$ gdw. v ist mit e inzident, d.h., $v \in e$.
- Sind $u, v \in V$ zwei Knoten, so heißen u, v *benachbart* oder *adjazent*, falls $uv \in E$ gilt. u heißt dann auch *Nachbar* von v .
- $N(v)$ ist die Menge aller Nachbarn von v , und $d(v) = |N(v)|$ ist der *Grad* von v .

Lemma 3.6.2 $d(v) = |\{e \in E \mid v \in e\}|$.

Beweis: Da G keine Mehrfachkanten enthält, gibt es eine Bijektion zwischen der Menge der Kanten mit Endknoten v und der Menge $N(v)$. \square

Satz 3.6.3 (Handschlaglemma) Es sei $G = (V, E)$ ein Graph. Dann gilt:

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

Beweis: Nach Lemma 3.6.1 können wir sagen: E besteht aus zweielementigen Teilmengen von V . Nach dem vorigen Lemma wird daher jede Kante in der Summe $\sum_{v \in V} d(v)$ genau zweimal angesprochen. \square

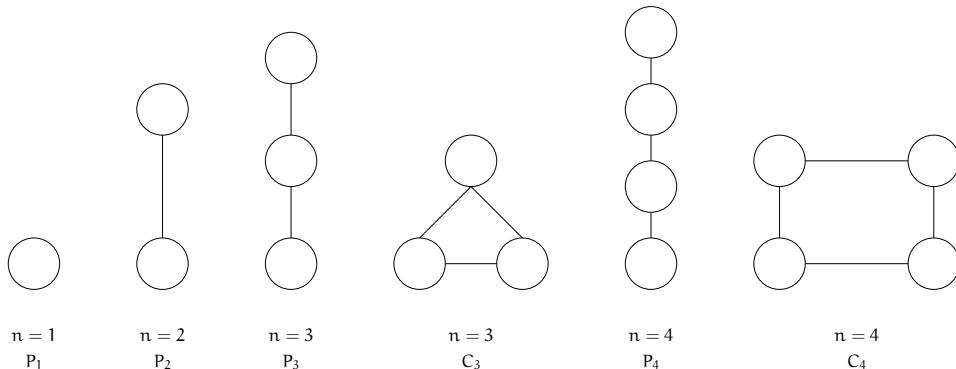


Abbildung 3.8: Viele kleine Graphen (mit Namen)

Die im Beweis (eher implizit) vorgenommene Technik des Doppelten Abzählens kann man auch allgemeiner erfassen und formulieren. Es ist eine der bekanntesten fortgeschritteneren Techniken der Kombinatorik, und so kann Abschnitt 4.6.1 als Nachtrag von Abschnitt 3.4 angesehen werden.

Folgerung 3.6.4 *Jeder Graph hat eine gerade Anzahl von Knoten ungeraden Grades.*

Folgerung 3.6.5 *Haben alle Knoten in einem Graphen G ungeraden Grad k, so teilt k die Anzahl der Kanten von G.*

Isomorphie und Spezielle Graphen Isomorphie heißt im Griechischen “Gleichgestaltigkeit”. Bei Graphen meint dies Folgendes:

Definition 3.6.1 $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ heißen isomorph gdw. es gibt eine Bijektion $\phi : V_1 \rightarrow V_2$ mit:

$$\{u, v\} \in E_1 \iff \{\phi(u), \phi(v)\} \in E_2$$

Die Abbildung ϕ heißt dann auch Graphisomorphismus oder kurz Isomorphismus.

Isomorphe Graphen sehen also genauso aus bis auf die Knotenbenennungen. Formal kann man zeigen (wenn Knotenmengen als Teilmengen eines festen Universum gewählt werden):

Satz 3.6.6 Isomorphie liefert eine Äquivalenzrelation für Graphen.

Auf den nächsten Folien werden daher Knotennamen oft fortgelassen.

Beispiel 3.6.7 In Bild 3.8 sind viele kleine Graphen (mit höchstens vier Knoten) ohne Knotennamen abgebildet, um ihre jeweilige Struktur erkennen zu lassen. Dafür sind offenbar die (gemäß der Definition von Graphen) eigentlich notwendigen Knotennamen nicht nötig. Tatsächlich befasst sich die Graphentheorie genauer meist mit Äquivalenzklassen von Graphen und nicht mit individuellen Graphen (gemäß Satz 3.6.6). In Aufgabe 6.6.3 dürfen Sie sich mit dieser Graphenansammlung näher beschäftigen.

Wollen wir das “Aussehen” eines Graphen beschreiben, so genügt es, einen Vertreter aus der Äquivalenzklasse aller isomorphen Graphen genau zu kennen. So einen Vertreter werden wir im Folgenden für sogenannte Pfade und Kreise konkret angeben.

Definition 3.6.2 Ein Pfad der Länge ℓ , $\ell \geq 0$, kurz $P_{\ell+1}$, ist beschrieben auf der Knotenmenge $[\ell + 1]$ durch die Kantenmenge $\{(i, i + 1) \mid i \in [\ell]\}$.

Ein Kreis der Länge ℓ , $\ell \geq 3$, kurz C_ℓ , ist beschrieben auf der Knotenmenge $[\ell]$ durch die Kantenmenge $\{(i, (i + 1) \bmod \ell) \mid i \in [\ell]\}$.

Zeichnerische Darstellungen kleiner Pfade und Kreise sehen Sie in Bild 3.8. Diese verdeutlichen, dass es auf die gewählten Knotennamen überhaupt nicht ankommt. Versuchen Sie dennoch einmal, Knotennamen zu finden, die mit obiger Definition 3.6.2 in Einklang sind.

Man kann Graphen auch induktiv definieren. Das sehen wir am folgenden Beispiel:

Definition 3.6.3 Wir beschreiben im Folgenden, was ein Baum (als Graph) sein soll.

Anker: Für jeden Knoten v gilt: $(\{v\}, \emptyset)$ ist ein Baum.

Induktionsschritt: Ist (V, E) ein Baum und $v \notin V$ ein neuer Knoten sowie $u \in V$ beliebig, so ist $(V \cup \{v\}, E \cup \{uv\})$ ein Baum.

Vollständigkeit: Nichts Weiteres sind Bäume.

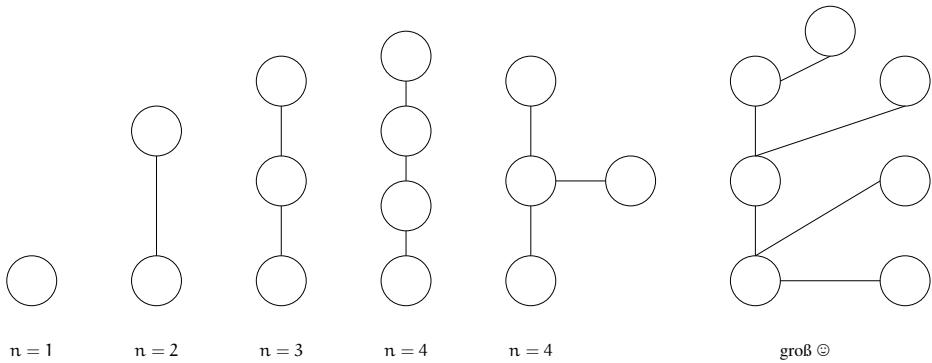


Abbildung 3.9: Einige kleine Bäume

Im Gegensatz zur Definition von Paden und Kreisen haben wir bei den Bäumen keine Vertreter angegeben, sondern eher eine Konstruktionsvorschrift. Diese Vorschrift ist ähnlich wie die induktive Definition der natürlichen Zahlen insofern, als dass von einfachsten Dingen (dem Anker) ausgehend kompliziertere aufgebaut werden (im Induktionsschritt). Da aber nicht direkt über Zahlen gearbeitet wird, nennt man derartige induktive Definitionen auch Definitionen gemäß *struktureller Induktion*. Die entsprechenden induktiven Beweise sind aber wieder völlig analog zu den bekannten aufgebaut: Zunächst zeigt man die Eigenschaft für den Anker und dann führt man den Induktionsschritt durch. Wie sehen Bäume aus? Die Konstruktionsvorschrift macht man sich am einfachsten anhand von Beispielen klar, siehe Bild 3.9

Lemma 3.6.8 Jeder Pfad ist ein Baum.

Beweis: Das sieht man am einfachsten, indem man (induktiv) beweist, dass die folgende Vorschrift die Graphen P_ℓ mit Knotenmenge $[\ell + 1]$ beschreibt; wir haben der Einfachheit halber dazugeschrieben, wieso dies die Baumeigenschaft beweist.

- $P_1 = ([1], \emptyset)$ ist wegen $[1] = \{0\}$ ein Baum.
- Ausgehend von P_n ist P_{n+1} ein Graph mit neuem Knoten n und neuer Kante $(n - 1, n)$ (im Vergleich zur Knotenmenge von P_n); also ist P_{n+1} ein Baum, falls P_n ein Baum ist.

Induktiv sieht man daher, dass alle P_ℓ Bäume sind. \square

Untergraphen und Zusammenhang

Lemma 3.6.9 *Jeder Baum mit n Knoten hat $n - 1$ Kanten.*

Beweis: Induktion (zur Übung) \square

Definition 3.6.4 *Sind $G = (V, E)$ und $G' = (V', E')$ Graphen, so heißt G Untergraph von (oder in) G' und G' Obergraph von G gdw. $V \subseteq V'$ und $E \subseteq E'$.*

Speziell: Ein Untergraph $G = (V, E)$ von $G' = (V', E')$ heißt Pfad von x nach y in G' , mit $x, y \in V$, wenn x und y in G beide den Grad höchstens Eins haben und G ein Pfad ist.

Lemma 3.6.10 *Es sei $G = (V, E)$ ein Graph. Gibt es in G Pfade $P_1 = (V_1, E_1)$ von x nach y und $P_2 = (V_2, E_2)$ von y nach z , so gibt es auch einen Pfad von x nach z in G .*

Beweis: Es sei $u_0, \dots, u_{\ell-1}$ eine Knotenfolge, die den Pfad P_1 beschreibt, d.h., $V_1 = \{u_0, \dots, u_{\ell-1}\}$, $u_0 = x$ und $u_{\ell-1} = y$ sind die einzigen Knoten in P_1 vom Grad höchstens Eins, und $u_i u_{i+1} \in E_1$ für $i \in [\ell - 1]$. Entsprechend sei v_0, \dots, v_{k-1} eine Knotenfolge für P_2 mit $v_0 = y$ und $v_{k-1} = z$. Sei nun $L = \min\{j \in [\ell] \mid \exists i \in [k] : u_j = v_i\}$ und K der entsprechende Index in P_2 , d.h., $u_L = v_K$. Das Minimum existiert, da $u_{\ell-1} \in V_2$ gilt, und da P_2 Pfad, ist K eindeutig bestimmt. Nach Konstruktion gilt für die Knotenfolge

$$KF := u_0, \dots, u_{L-1}, u_L = v_K, v_{K+1}, \dots, v_{k-1},$$

dass aufeinanderfolgende Knoten in G benachbart sind. Gäbe es einen Index $i \in [k] \setminus [K + 1] = \{K + 1, \dots, k - 1\}$ mit $v_i \in V_1$, also $v_i = u_j$ mit $j \in [\ell]$, so muss aufgrund der Wahl von L gelten: $j > L$. Daher gibt keine Wiederholungen in der Folge KF , und also beschreibt KF einen Pfad von x nach z . \square

Definition 3.6.5 *Es sei $G = (V, E)$ ein Graph. Wir definieren die folgende Binärrelation auf V :*

$$(x, y) \in \text{Pfad}(G) \iff \text{es gibt einen Pfad von } x \text{ nach } y \text{ in } G.$$

Satz 3.6.11 *Für jeden Graph $G = (V, E)$ ist $\text{Pfad}(G)$ eine Äquivalenzrelation auf V .*

Beweis: Die Transitivität ergibt sich mit Lemma 3.6.10. Die übrigen Eigenschaften seien zur Übung überlassen. \square

Definition 3.6.6 *$G = (V, E)$ heißt zusammenhängend gdw. zu jedem Paar von Knoten $x, y \in V$ gibt es einen Pfad in G von x nach y .*

Lemma 3.6.12 *Ein Graph G ist zusammenhängend gdw. $\text{Pfad}(G)$ hat nur eine Äquivalenzklasse.*

Unmittelbar aus den Definitionen ergibt sich:

Lemma 3.6.13 *Sind $G = (V, E)$ und $G' = (V', E')$ Graphen mit $V = V'$ und ist G zusammenhängender Untergraph von G' , so ist G' zusammenhängend.*

Lemma 3.6.14 *Jeder Baum ist zusammenhängend.*

Beweis: Es sei $G = (V, E)$ ein Baum. Das bedeutet, dass die Knoten gemäß unserer Definition in einer bestimmten Reihenfolge eingeführt wurden; sei v_0, \dots, v_{n-1} eine Nummerierung der Knoten von V in eben dieser Weise.

Beobachte: Für jedes $i \in [n]$ beschreibt v_0, \dots, v_i den Aufbau eines Baums G_i mit Anker v_0 , der ein Untergraph von G ist.

Behauptung: Für jedes $v \in V$ gibt es einen Pfad von v_0 nach v in G .

Wir beweisen diese Behauptung induktiv, indem wir genauer beweisen:

Für jedes $i \in [n]$ gibt es einen Pfad von v_0 nach v_i in G_i .

Daraus folgt die Behauptung sofort.

Das stimmt trivial für $i = 0$. Angenommen, die Behauptung gilt für alle i , $i < I < n$. Betrachte v_1 in G_I . Nach Baumdefinition gibt es einen Index $J < I$, sodass v_1 bei seiner Einführung mit v_J verbunden wurde. Nach Induktionsvoraussetzung gibt es einen Pfad von v_0 nach v_J in G_J und mithin in G_I . Durch Hinzunahme der Kante $v_J v_1$ wird hieraus ein Pfad von v_0 nach v_1 (in G_I), was zu zeigen war.

Betrachte nun zwei Knoten v_i, v_j . Wir müssen zeigen: es gibt einen Pfad von v_i nach v_j . Je- denfalls gilt nach der gezeigten Behauptung: $(v_0, v_i) \in \text{Pfad}(G)$ und $(v_0, v_j) \in \text{Pfad}(G)$. Mit Satz 3.6.11 folgt: $(v_i, v_j) \in \text{Pfad}(G)$. \square

Der Begriff des Zusammenhangs gestattet eine schöne Kennzeichnung von Kreisen.

Satz 3.6.15 *Ein Graph G ist ein Kreis gdw. G ist zusammenhängend und alle seine Knoten haben Grad zwei.*

Beweis: Es sollte leicht einzusehen sein, dass Kreise zusammenhängend sind und alle Knoten Grad zwei haben. Sei nun umgekehrt $G = (V, E)$ ein zusammenhängender Graph mit n Knoten, und alle Knoten haben Grad zwei. Wir konstruieren eine Bijektion $\phi : [n] \rightarrow V$ folgendermaßen induktiv. Wähle $\phi(0) \in V$ willkürlich. Sei (ebenfalls willkürlich) $\phi(1)$ einer der beiden Nachbarn von $\phi(0)$ in G . Wir nehmen nun an, ϕ sei für alle i mit $i < I < n$ festgelegt, $I \geq 2$. Da $\phi(I-1)$ nach Konstruktion den Nachbarn $\phi(I-2)$ besitzt, kann man in eindeutiger Weise (da $\phi(I-1)$ den Grad 2 hat) $\{\phi(I)\} := N_G(\phi(I-1)) \setminus \{\phi(I-2)\}$ festlegen. Da G zusammenhängend ist und alle Knoten Grad zwei haben, darf für kein $I < n$ bei dieser Festlegung $\phi(I) \in \{\phi(i) \mid i < I\}$ gelten. Genauer widersprüche $\phi(I) \in \{\phi(i) \mid 0 < i < I\}$ der Gradbeschränkung für $\phi(i)$ ³ und $\phi(I) = \phi(0)$ widersprüche dem Zusammenhang. Da alle Knoten von G den Grad zwei haben, muss aber am Ende $\phi(0)\phi(n-1) \in E$ gelten. Die so konstruierte Abbildung ϕ ist ein Isomorphismus von C_n auf G . \square

Lemma 3.6.16 *Zwischen je zwei verschiedenen Knoten eines Kreises gibt es zwei verschiedene Pfade.*

Beweis: C_n hat die Knotenmenge $[n]$. Betrachte $i < j$. Dann gibt es einerseits den Pfad $i, i+1, \dots, j$ zwischen i und j , andererseits aber auch $i, i-1, \dots, 0, n-1, \dots, j+1, j$. \square

³bzw. auch der Tatsache, dass wir keine Mehrfachkanten zulassen; hieraus ergibt sich auch, dass $n \geq 3$ gelten muss

Definition 3.6.7 Ein Graph G heißt kreisfrei, wenn G keinen Kreis als Untergraph enthält.

Lemma 3.6.17 Bäume sind kreisfrei.

Beweis: Bei der Konstruktion eines Baumes wird jede Kante erzeugt durch Verbinden eines „neuen“ mit einem „alten“ Knoten. Um einen Kreis dabei zu konstruieren, müsste man aber irgendwann zwei „alte Knoten“ miteinander verbinden, was offenbar nicht geht. \square

Satz 3.6.18 Ein Graph G ist genau dann nicht kreisfrei (d.h., G enthält einen Kreis als Untergraph), wenn es zwei verschiedenen Knoten u, v gibt und zwei verschiedene Pfade von u nach v .

Beweis: Wegen Lemma 3.6.16 müssen wir noch zeigen: Gibt es in G zwei verschiedene Knoten u, v mit zwei verschiedenen Pfaden von u nach v , dann enthält G einen Kreis. Wir wählen jetzt die Knoten u und v und die Pfade $p_1 = x_0x_1 \dots x_k$ und $p_2 = y_0y_1 \dots y_\ell$ (mit $x_0 = y_0 = u$ und $x_k = y_\ell = v$) so, dass $k + \ell$ kleinstmöglich ist. Wir nennen dann (p_1, p_2) ein kürzestes Pfadpaar. Wäre $\{x_1, \dots, x_{k-1}\} \cap \{y_1, \dots, y_{\ell-1}\} \neq \emptyset$, so gäbe es ein kürzeres Pfadpaar, im Gegensatz zur Wahl der Pfade. Daher ist $x_0x_1 \dots x_k y_{\ell-1} y_{\ell-2} \dots y_1 y_0$ ein Kreis. \square

Eine hübsche Operation, nämlich das Löschen einer Kante, kommt in dem Beweis zum folgenden Lemma zum Einsatz:

Lemma 3.6.19 Enthält der Graph $G = (V, E)$ einen Kreis v_0, \dots, v_{k-1} der Länge $k \geq 3$, so ist $G' = (V, E \setminus \{v_0v_1\})$ zusammenhängend gdw. G zusammenhängend ist.

Beweis: Wegen Lemma 3.6.13 ist G zusammenhängend, wenn G' zusammenhängend ist. Sei also G zusammenhängend und $u, v \in V$ bel. Klar: $(u, v) \in \text{Pfad}(G)$. Zu zeigen ist: $(u, v) \in \text{Pfad}(G')$. Wenn $(u, v) \in \text{Pfad}(G)$ durch eine Pfad p bezeugt wird, der die Kante v_0v_1 nicht verwendet, so ist p auch ein Pfad in G' . Für den anderen Fall betrachte einen Pfad $p = x_0x_1 \dots x_\ell$ mit $x_0 = u$ und $x_\ell = v$, sowie $x_i = v_0$ und $x_{i+1} = v_1$ (der Fall $x_i = v_1$ und $x_{i+1} = v_0$ ist analog). Die Knotenfolge $x_0x_1 \dots x_i v_{k-1} v_{k-2} \dots v_1 = x_{i+1} x_{i+2} \dots x_\ell$ beschreibt nicht notwendigerweise einen Pfad, da die Knoten v_j mit einem der aufgelisteten Knoten x_r übereinstimmen könnten. Diese Dopplungen müssen rausgekürzt bzw. von vornherein vermieden werden. Dazu sei zunächst $L := \min\{l \in [i+1] : x_l \in \{v_0, \dots, v_{k-1}\}\}$. Sei nun L' der Index, sodass $x_L = v_{L'}$. Setze entsprechend $R := \max\{r \in [i+1, \dots, \ell] : x_r \in \{v_0, \dots, v_{k-1}\}\}$. Sei nun R' der Index, sodass $x_R = v_{R'}$. Da p Pfad in G , gilt $L' \neq R'$. Daher ist $x_0 \dots x_L = v_L v_{L'-1} \dots v_{R'} = x_R \dots x_\ell$ ein Pfad von u nach v in G' . (Hierbei ist „modulo k “ beim Rückwärtsläufen in den Indizes der v_i -Knoten zu rechnen, falls $L' < R'$; speziell ist daher für $L' = 0$ der auf v_0 folgende Knoten v_{k-1} .) Der einzige Problemfall ist noch $R' = 0 < L'$; in dem Fall muss andersherum der Kreis durchlaufen werden; dann ist also $x_0 \dots x_L = v_L v_{L'+1} \dots v_{k-1} v_{R'} = x_R \dots x_\ell$ ein Pfad von u nach v in G' . Deshalb ist G' zusammenhängend. \square

Kennzeichnungen von Bäumen

Satz 3.6.20 Sei $G = (V, E)$ ein Graph. G ist ein Baum gdw. G ist zusammenhängend und kreisfrei.

Beweis: Lemmas 3.6.14 und 3.6.17 zeigen: Jeder Baum ist zusammenhängend und kreisfrei. Wir zeigen nun die Umkehrung. Sei G ein zusammenhängender kreisfreier Graph, der kein Baum ist, mit der kleinsten Anzahl von Knoten (kleinstes Gegenbeispiel). Sicher hat G mindestens zwei

Knoten. Sei v_1 ein Knoten von G . v_1 hat in G mindestens einen Nachbarn. Wähle $v_2 \in N(v_1)$. Wenn möglich, wähle nun $v_3 \in N(v_2)$, dann $v_4 \in N(v_3)$, usf. Da G kreisfrei ist, sind alle so “angesteuerten” Knoten voneinander verschieden. Da G nur endlich viele Knoten enthält, erhalten wir so tatsächlich einen Pfad v_1, \dots, v_k . Da es bei v_k nicht weiterging, gilt $d(v_k) = 1$. Entfernt man nun v_k , so erhält man wieder einen zusammenhängenden kreisfreien Graphen G' . Da G ein kleinstes Gegenbeispiel war, ist G' ein Baum. Das Hinzufügen eines neuen Knotens (also v_k) führt auch nur eine neue Kante ein, die ihn mit G' verbindet. Das entspricht genau der induktiven Definition der Bäume, also wäre G doch ein Baum, im Gegensatz zur Annahme. Daher gibt es keinen zusammenhängenden kreisfreien Graph, der kein Baum ist. \square

Satz 3.6.21 *Sei $G = (V, E)$ ein Graph. G ist ein Baum gdw. zwischen je zwei verschiedenen Knoten u, v gibt es einen eindeutig bestimmten Pfad.*

Beweis: Sei G ein Baum und u, v seien verschiedene Knoten. Wegen Lemma 3.6.14 ist G zusammenhängend, es gibt also einen Pfad zwischen u und v in G . Wegen Lemma 3.6.17 ist G kreisfrei, es gibt also gemäß Satz 3.6.18 sogar dann einen eindeutig bestimmten Pfad von u nach v .

Sei nun $G = (V, E)$ ein Graph, für den gilt, dass es zwischen je zwei verschiedenen Knoten u, v stets einen eindeutig bestimmten Pfad gibt. Daher ist G jedenfalls zusammenhängend und mit Satz 3.6.18 auch kreisfrei, also wegen Satz 3.6.20 ein Baum. \square

Den Beweis für den folgenden Kennzeichnungssatz sei als Übung gestellt.

Satz 3.6.22 *Es sei G ein zusammenhängender Graph der Ordnung n . G ist ein Baum gdw. G hat Größe $n - 1$.*

Aufspannende Untergraphen

Definition 3.6.8 *in Untergraph $G' = (V', E')$ eines Graphen $G = (V, E)$ heißt aufspannend, falls $V = V'$ gilt. Von besonderem Interesse sind hier aufspannende Bäume, auch Spannbäume oder Gerüste genannt.*

Spannbäume gestatten eine weitere Kennzeichnung des Begriffs “Zusammenhang”:

Satz 3.6.23 *Ein Graph G ist zusammenhängend gdw. G besitzt einen Spannbaum.*

Beweis: Wegen Lemma 3.6.13 bleibt zu zeigen: “ \Rightarrow ”.

Hierfür geben wir einen Induktionsbeweis an, der über die Zahl $k = |E| - (|V| - 1)$ arbeitet.

IA: Für $k = 0$ folgt die Behauptung mit Satz 3.6.22, denn G ist bereits ein Baum.

IV: Die Beh. gilt für alle zusammenhängenden Graphen $G = (V, E)$ mit $K = |E| - (|V| - 1)$. Für den IS betrachten wir einen zusammenhängenden Graph $G' = (V', E')$ mit $K + 1 = |E'| - (|V'| - 1)$. Wegen $K + 1 > 0$ ist G' mit Satz 3.6.22 kein Baum und ist daher wegen Satz 3.6.20 nicht kreisfrei. Lemma 3.6.19 zeigt, dass das Löschen einer Kante aus einem Kreis in G' nicht den Zusammenhang zerstört. Wähle daher eine beliebige Kante e aus einem beliebigen Kreis in G' . Mit $V = V'$ und $E = E' \setminus \{e\}$ folgt, dass für den zusammenhängenden Graph $G = (V, E)$ gilt: $K = |E| - (|V| - 1) = (|E'| - 1) - (|V'| - 1)$. Nach IV besitzt G einen Spannbaum. Dieser ist auch ein Spannbaum für G' . \square

Hinweis: In dem Beweis versteckt sich übrigens ein hübscher Polynomzeit-Algorithmus zur Berechnung eines Spannbaums. Versuchen Sie, ihn zu erkennen. Mehr zu diesem Thema finden Sie in Abschnitt 5.6.1.

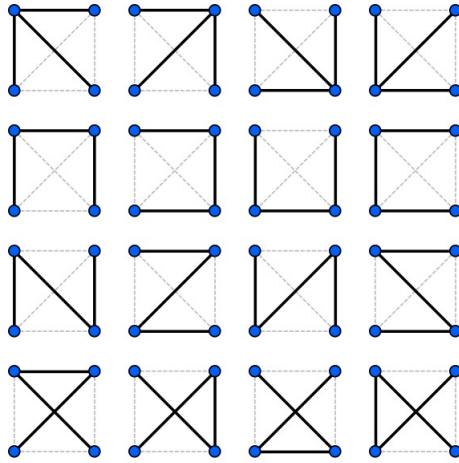


Abbildung 3.10: Es gibt $4^{4-2} = 16$ verschiedene Gerüste des vollständigen Graphs der Ordnung vier, K_4 .

Kombinatorische Frage: Wie viele verschiedene (markierte) Gerüste kann denn ein Graph der Ordnung n maximal haben?

“Markierung” meint, dass wir die “Namen” der Knoten bei der Frage berücksichtigen, ob zwei Bäume “verschieden” sind.

Die meisten Gerüste hat offensichtlich der *vollständige Graph* K_n , der genau $\binom{n}{2} = \frac{n(n-1)}{2}$ viele Kanten bei n Knoten enthält.

Satz 3.6.24 K_n besitzt n^{n-2} verschiedene markierte Gerüste.

In Bild 3.10⁴ ist der Fall $n = 4$ illustriert. Dieser Tatbestand ist auch als Cayley-Formel bekannt. In alternativer Sicht werden hierbei alle markierten Bäume der Ordnung n gezählt (also, ohne auf Isomorphismen Rücksicht zu nehmen; beachten Sie nämlich, dass Bild 3.10 etliche zueinander isomorphe Bäume listet).

Beweis: Der Beweis der Cayley-Formel durch Prüfer (Skizze):

Grundidee: Konstruiere Bijektion zwischen markierten Gerüsten von K_n und der Menge $[n]^{n-2}$.

Wir geben hier nur den Algorithmus an. Sei $[n]$ die Knotenmenge von K_n .

Für einen Baum G mit Knotenmenge $[n]$ wird wie folgt eine Folge $x_1 \dots x_{n-2}$ der Länge $n - 2$ konstruiert:

Für $i = 1$ bis $n - 2$:

Wähle Knoten v aus G mit $d(v) = 1$ mit “kleinstem Namen”.

Sei u der (einzig) Nachbar von v .

Setze $x_i \leftarrow u$.

Lösche v aus G .

Zu zeigen bliebe: Der Algorithmus beschreibt eine Bijektion (zur Übung).

Die Korrektheit der Cayley-Formel folgt dann mit unserem Kombinatorik-Wissen. \square

⁴Quelle: Wikipedia über Spannbäume

```

Data :  $G = (V, E)$ : a connected graph with edge weights  $w : E \rightarrow \mathbb{R}_{>0}$ 
Result :  $F$ : set of edges such that  $(V, F)$  is a minimum-weight spanning tree of  $G$ 
1  $k$ : integer;
2 Order the edges increasingly such that  $E = \{e_1, \dots, e_m\}$  with  

 $w(e_1) \leq w(e_2) \leq \dots \leq w(e_m)$ ;
3 Initialize  $F \leftarrow \emptyset$ ;
4 for  $k \leftarrow 1$  to  $m$  do
5   if  $(T \cup \{e_k\})$  has no cycle then
6      $T \leftarrow T \cup \{e_k\}$ ;

```

Abbildung 3.11: Kruskal's minimum spanning tree algorithm KMST

Ein Spannbaumproblem Abstrakte Aufgabe: Gegeben ein zusammenhängender Graph $G = (V, E)$ mit Kantengewichtsfunktion $w : E \rightarrow \mathbb{R}_{>0}$, finde Gerüst mit Kantenmenge T , sodass $w(T) = \sum_{e \in T} w(e)$ kleinstmöglich ist unter allen Gerüsten von G .

Eine nette Einkleidung des Spannbaumproblems in eine kleine Geschichte findet sich beim Algorithmus der Woche von M. Skutella und K. Langkau.

Greedy: Ein naheliegendes Vorgehen (nach Kruskal)

Gierige (Greedy) Algorithmen bieten sich für viele Optimierungsprobleme an. Nur selten führen sie (wie in diesem Fall) stets zur besten Lösung. Der in Bild 3.11 gezeigte Algorithmus ist so ein gieriges Verfahren, von dem wir gleich zeigen wollen, dass es tatsächlich einen Spannbaum mit kleinstem Gewicht liefert. Dahinter steckt ein allgemeineres Prinzip, das durch sogenannte Matroide formalisiert werden kann. Mehr dazu können Sie in Abschnitt 4.6.4 erfahren.

Satz 3.6.25 *Der Algorithmus von Kruskal liefert ein minimales Gerüst.*

Beweis: Der Graph $G_K = (V, T)$ ist sicher kreisfrei.

Wäre G_K nicht zusammenhängend, so gäbe es zwei Knoten $x, y \in V$, die in G_K nicht durch einen Pfad verbunden sind. Da G zusammenhängend ist, existiert aber ein Pfad von x nach y in G . Wenigstens eine Kante dieses Pfades, z.B. e , ist nicht in T enthalten. Der Algorithmus betrachtet jedoch alle Kanten von G , also insbesondere e . Zu dem Zeitpunkt, an dem er e besah, hätte er e in $T' \subseteq T$ einzufügen können, ohne einen Kreis zu erzeugen, und dies somit auch gemacht, im Gegensatz zur Annahme, G_K wäre nicht zusammenhängend.

Es seien in $T = \{t_1, \dots, t_{n-1}\}$, $n = |V|$, die Kanten von G_K so durchnummieriert, wie sie vom Algorithmus in T eingefügt wurden. Sei nun $G^* = (V, T^*)$ ein minimales Gerüst, das unter allen minimalen Gerüsten j mit der Eigenschaft $\{t_1, \dots, t_j\} \subseteq T^*$ maximiert. Wäre $j = n - 1$, so wäre $G^* = G_K$ minimal. Andernfalls betrachte $G' = (V, T^* \cup \{t_{j+1}\})$. G' enthält einen Kreis C , der $t_{j+1} = uv$ enthält, denn u und v sind ja bereits in G^* durch einen Pfad verbunden. Durch Löschen irgendeiner Kante e aus C wird G' wieder zu einem Gerüst von G . Da unser Algorithmus e nicht gewählt hat, gilt $w(e) \geq w(t_{j+1})$. Da G^* minimal, ist $G^+ = (V, (T^* \setminus \{e\}) \cup \{t_{j+1}\})$ ebenfalls minimal, im Widerspruch zur Maximalität von j . \square

3.7 Verknüpfungen

3.7.1 Gruppoide

Definition 3.7.1 Es sei M eine Menge, hier oft Grundmenge genannt. Eine Abbildung $f : M \times M \rightarrow M$ wird auch (zweistellige) Verknüpfung oder (zweistellige) Operation genannt. Hierbei wird meist die Infixnotation verwendet, d.h., man schreibt xy statt $f(x, y)$. f heißt dann auch Operator.

Zur Unterscheidung von Funktionen werden dann meist andere Symbole verwendet zur Bezeichnung von Operatoren, z.B.: $+$, \cdot , \circ usf.

Eine Grundmenge M zusammen mit einem Operator \circ heißt auch Gruppoid oder Magma und wird als (M, \circ) notiert.

Hinweis: Verknüpfungen werden meist so angegeben, dass zunächst zu zeigen ist, dass das Ergebnis der Verknüpfung zweier Elemente der Grundmenge wieder in der Grundmenge liegt. Diese Eigenschaft einer Verknüpfung bezeichnet man auch als *Abgeschlossenheit*.

- Im Abschnitt 4.1 hatten wir für die Addition von Zermelozahlen gezeigt: Für $n_z, m_z \in \mathbb{N}_Z$ gilt stets: $(n_z +_z m_z) \in \mathbb{N}_Z$. Also ist $(\mathbb{N}_Z, +_z)$ ein Gruppoid.
- Allgemeiner könnten wir für $k \in \mathbb{N}$ definieren:
 $n_z +_z^k m_z := (n_z +_z m_z) +_z k_z$.
Klar (?): Für jedes $k \in \mathbb{N}$ ist $(\mathbb{N}_Z, +_z^k)$ ein Gruppoid.
- Es sei \mathcal{U} ein Universum. Dann sind $(2^\mathcal{U}, \cup)$ und $(2^\mathcal{U}, \cap)$ Gruppoide.

Gruppoide lassen sich auch gut mit Hilfe von *Verknüpfungstafeln* angeben, sofern die betreffende Grundmenge endlich ist. So können wir die üblichen logischen Verknüpfungen beschreiben:

\wedge	0	1	\vee	0	1	\Rightarrow	0	1
0	0	0	0	0	1	0	1	1
1	0	1	1	1	1	1	0	1

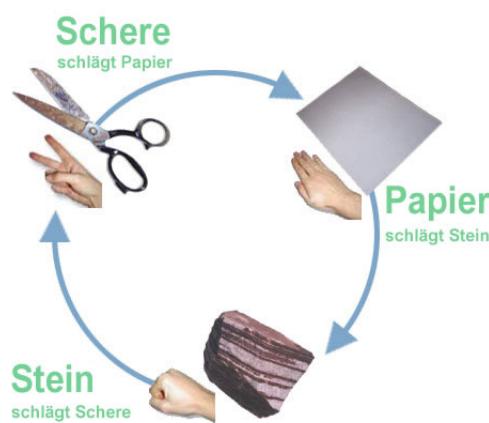


Abbildung 3.12: Die Regeln von Schnick-Schnack-Schnuck

Quelle: http://de.wikipedia.org/wiki/Datei:Schere_Stein_Papier.jpg

Die Idee zu folgendem Beispiel stammt aus [3].

Beispiel: Das Schnick-Schnack-Schnuck-Gruppoid:

In Bild 3.12 sind die Regeln dieses weit verbreiteten Kinderspiels zusammengefasst. Eine andere Darstellung der Information, wer gegen wen gewinnt, liefert die folgende Tabelle.

	.	r	p	s
rock:	r	r	p	r
paper:	p	p	p	s
scissor:	s	r	s	s

Diese Tabelle lässt sich auch als Verknüpfungstafel lesen. Wir erhalten so ein Gruppoid. Die Beziehung

$$(r \cdot p) \cdot s = s \neq r = r \cdot (p \cdot s)$$

zeigt: Dieses Gruppoid ist nicht assoziativ.

Definition 3.7.2 Es sei M eine nicht-leere Menge sowie (und) zwei Symbole (Klammern), die nicht in M liegen. Dann definieren wir die Menge $\mathcal{T}(M)$ der Terme (über M) induktiv wie folgt:

- Jedes Element a aus M ist ein Term.
- Sind s und t Terme über M , so auch (st) .
- Nichts Weiteres sind Terme über M .

Das Term-Gruppoid $(\mathcal{T}(M), \cdot)$ ist gegeben durch die Verknüpfung $s \cdot t := (st)$.

Besondere Elemente

Definition 3.7.3 Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid.

$\alpha \in M$ heißt absorbierend gdw. $\forall x \in M : \alpha \circ x = x \circ \alpha = \alpha$.

$\epsilon \in M$ heißt neutral gdw. $\forall x \in M : \epsilon \circ x = x \circ \epsilon = x$.

Lemma 3.7.1 Ein Gruppoid besitzt höchstens ein neutrales Element.

Beweis: Angenommen, es gibt in (M, \circ) neutrale Elemente e, e' . Dann gilt: $e = e \circ e' = e'$; die erste Gleichheit gilt, weil e' neutrales Element ist, und die zweite, da e neutrales Element ist. \square

Ähnlich zeigt man:

Lemma 3.7.2 Ein Gruppoid besitzt höchstens ein absorbierendes Element.

Zur Konstruktion von Gruppoiden Wir haben verschiedene Konstruktionen kennengelernt, mit denen man aus “einfacheren” Mengen “kompliziertere” bauen kann. Entsprechend kann man auch aus einfacheren Gruppoiden neue konstruieren.

Potenzmengen Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. Dann definiere auf 2^M die folgende zweistellige Operation \circ_K , Komplexprodukt zu \mathbb{G} genannt:

$$M_1 \circ_K M_2 := \{x_1 \circ x_2 \mid x_1 \in M_1, x_2 \in M_2\} \quad \text{für } M_1, M_2 \subseteq M.$$

Unter den beschriebenen Umständen gilt:

Satz 3.7.3 $2^{\mathbb{G}} := (2^M, \circ_K)$ ist ein Gruppoid mit absorbierendem Element \emptyset .
 $2^{\mathbb{G}}$ hat ein neutrales Element gdw. \mathbb{G} hat ein neutrales Element.

Produktmengen Es seien $\mathbb{G}_1 = (M_1, \circ_1)$ und $\mathbb{G}_2 = (M_2, \circ_2)$ Gruppoide. Definiere auf $M_1 \times M_2$ die folgende zweistellige Operation \circ , um damit das *Produktgruppoid* $\mathbb{G}_1 \times \mathbb{G}_2 := (M_1 \times M_2, \circ)$ zu beschreiben:

$$(x_1, x_2) \circ (y_1, y_2) := (x_1 \circ_1 y_1, x_2 \circ_2 y_2)$$

Recht einfach sieht man ein:

Satz 3.7.4 $\mathbb{G}_1 \times \mathbb{G}_2$ ist ein Gruppoid.

Der Spezialfall $M_1 = M_2$ wird im Folgenden erheblich in eine andere Richtung verallgemeinert.

Funktionenmengen Es seien $\mathbb{G} = (M, \circ)$ ein Gruppoid und N eine beliebige Menge. Erweitere nun \circ "punktweise" zu einer Operation auf M^N : $h := f \circ_N g$ mit

$$h(n) := f(n) \circ g(n)$$

für alle $n \in N$.

Satz 3.7.5 $\mathbb{G}^N := (M^N, \circ_N)$ ist ein Gruppoid.

Dieses werden wir auch als *Funktionengruppoid* ansprechen.

Beispiel: Betrachte das Gruppoid $\text{REALPLUS} = (\mathbb{R}, +)$. Vektoren $\vec{x} \in \mathbb{R}^m$ "entsprechen" Abbildungen $[m] \rightarrow \mathbb{R}$. Die im Funktionengruppoid $\text{REALPLUS}^{[m]}$ definierte Addition ist die bekannte Vektoraddition. Entsprechend kann man die Addition von Matrizen (Funktionengruppoid $\text{REALPLUS}^{[m] \times [n]}$) begreifen. Aufbauend auf dem Gruppoid $(\mathbb{N}, +)$ modelliert \mathbb{N}^N zu N gehörende *Multimengen*.

3.7.2 Unterstrukturen und strukturerhaltende Abbildungen

Definition 3.7.4 Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. Eine Teilmenge $N \subseteq M$ beschreibt ein Untergruppoid von \mathbb{G} gdw. die Einschränkung $\circ_{N \times N} : N \times N \rightarrow M$ von $\circ : M \times M \rightarrow M$ auf $N \times N$ ist eine Verknüpfung auf N , d.h., $(N, \circ_{N \times N})$ ist ein Gruppoid.

Lemma 3.7.6 $N \subseteq M$ beschreibt ein Untergruppoid von (M, \circ) gdw. $\forall x, y \in N : (x \circ y) \in N$.

Zu überprüfen bleibt daher die *Abgeschlossenheit* von N unter \circ . Ist diese gewährleistet, so schreibt man die Untergruppoid-Operation meist genauso wie die des "ursprünglichen" Gruppoids.

Beispiel: Die Menge der geraden Zahlen beschreibt ein Untergruppoid von $(\mathbb{N}, +)$, die Menge der ungeraden Zahlen aber nicht, denn die Summe zweier ungerader Zahlen ist gerade.

Definition 3.7.5 Es seien (M, \circ) und (N, \square) Gruppoide und $h : M \rightarrow N$ eine Abbildung. Dann heißt h ein (Homo-)morphismus gdw. Folgendes gilt:

$$\forall x, y \in M : h(x \circ y) = h(x) \square h(y).$$

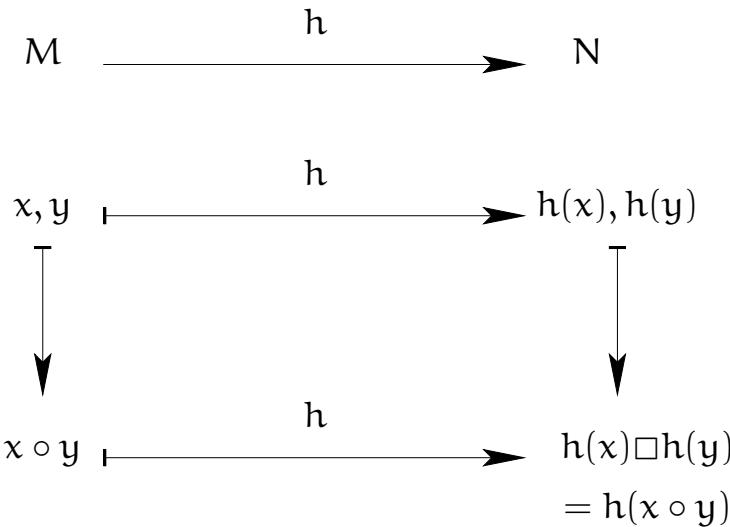


Abbildung 3.13: Ein kommutatives Diagramm für die Homomorphiebedingung.

Einprägsam ist die Darstellung als *kommutatives Diagramm* in Bild 3.13.

Beispiel: Zur Implementierung von Mengenoperationen

$(\{0, 1\}, \min)$ und $(\{0, 1\}, \max)$ sind Gruppoide. Daher sind für beliebige Mengen M ebenfalls Gruppoide: $(\{0, 1\}^M, \min_M)$ und $(\{0, 1\}^M, \max_M)$ (Funktionengruppoide). Zu jeder Menge $A \subseteq M$ kann man seine (bereits zuvor, z.B. in Bsp. 3.3.17 betrachtete) Indikatorfunktion $\chi_A : M \rightarrow \{0, 1\}$ beschreiben durch $\chi_A(x) = 1$ gdw. $x \in A$.

Satz: Die Abbildung $h : 2^M \rightarrow \{0, 1\}^M$, $A \mapsto \chi_A$ ist ein Homomorphismus sowohl von $(2^M, \cup)$ auf $(\{0, 1\}^M, \max_M)$ als auch von $(2^M, \cap)$ auf $(\{0, 1\}^M, \min_M)$.

Beweis: Betrachte $A, B \subseteq M$. Wir diskutieren nur den ersten Fall.

$$h(A \cup B) = \chi_{A \cup B} \text{ mit } \chi_{A \cup B}(x) = 1 \text{ gdw. } x \in A \cup B, \text{ d.h., } x \in A \text{ oder } x \in B.$$

Die Funktion $\max_M(\chi_A, \chi_B)$ entsteht durch ‘punktweises Maximum’ der Argumente.

Wenn also $x \in A$, so gilt $\chi_A(x) = 1$ und somit $\max_M(\chi_A, \chi_B)(x) = 1$, unabhängig vom Wert $\chi_B(x)$.

Für $x \in B$ überlegt man entsprechend.

Liegt x weder in A noch in B , gilt $\chi_A(x) = \chi_B(x) = 0$, also $\max_M(\chi_A, \chi_B)(x) = 0$.

Daher gilt die Homomorphiebedingung, hier also $\chi_{A \cup B} = \max_M(\chi_A, \chi_B)$. \square

Dieser Satz gestattet die Implementierung von Mengenoperationen mit der Hilfe von Bitvektorenoperationen, wie sie auf Maschinensprachenebene bei Mikroprozessoren zumeist vorliegen.

Definition 3.7.6 Es sei (M, \circ) ein Gruppoid und $(T(M), \cdot)$ das Term-Gruppoid. Die Auswertefunktion $\text{eval}_{(M, \circ)} : T(M) \rightarrow M$ wird induktiv definiert durch:

- Für $a \in M$ sei $\text{eval}_{(M, \circ)}(a) = a$.
- Für $s, t \in T(M)$ sei $\text{eval}_{(M, \circ)}((st)) := \text{eval}_{(M, \circ)}(s) \circ \text{eval}_{(M, \circ)}(t)$.

Satz 3.7.7 $\text{eval}_{(M, \circ)}$ ist ein Gruppoid-Morphismus.

Beweis: Nach Definition gilt für beliebige Terme s, t :

$$\text{eval}_{(M,o)}(s \cdot t) = \text{eval}((st)) = \text{eval}_{(M,o)}(s) \circ \text{eval}_{(M,o)}(t). \quad \square$$

In gewissem Sinne liefert das Term-Gruppoid also eine Blaupause für sämtliche möglichen Berechnungen in irgendeinem Gruppoid.

Satz 3.7.8 Es seien (M, o) und (N, \square) Gruppoide. Ist $h : M \rightarrow N$ ein Homomorphismus, so beschreibt $h(M)$ ein Untergruppoid von N .

Beweis: Für $x', y' \in h(M)$ gibt es $x, y \in M$ mit $x' = h(x)$ und $y' = h(y)$. Außerdem gilt:

$$x' \square y' = h(x) \square h(y) = h(x \circ y) \in h(M),$$

da h Homomorphismus. \square

Beispiel: Wir wissen bereits: Die Menge der geraden Zahlen beschreibt ein Untergruppoid von $(\mathbb{N}, +)$. Dies lässt sich auch anders beschreiben:

$h : \mathbb{N} \rightarrow \mathbb{N}, x \mapsto 2 \cdot x$ ist ein Homomorphismus.

Denn: $h(x + y) = 2 \cdot (x + y) \stackrel{\text{DG}}{=} 2x + 2y = h(x) + h(y)$.

$h(\mathbb{N})$ ist die Menge der geraden Zahlen.

Definition 3.7.7 Ist $h : M \rightarrow N$ ein bijektiver Homomorphismus von (M, o) auf (N, \square) , so heißt h auch Isomorphismus. (M, o) und (N, \square) heißen isomorph, wenn es einen Isomorphismus von (M, o) auf (N, \square) gibt.

Satz 3.7.9 Ist $h : M \rightarrow N$ ein Isomorphismus von (M, o) auf (N, \square) , so ist ebenfalls $h^{-1} : N \rightarrow M$ ein Isomorphismus.

Beweis: Es seien $a, b \in N$.

$$h^{-1}(a \square b) = h^{-1}(h(h^{-1}(a)) \square h(h^{-1}(b))) = h^{-1}(h(h^{-1}(a) \circ h^{-1}(b))) = h^{-1}(a) \circ h^{-1}(b).$$

Klar: Die Umkehrung einer Bijektion ist bijektiv. \square

Das bedeutet insbesondere, dass unsere obige Festlegung sprachlich sinnvoll ist: Sind (M, o) und (N, \square) isomorph, so sind auch (N, \square) und (M, o) isomorph; siehe auch Aufgabe 6.7.5.

Beispiel: $h : 2^M \rightarrow \{0, 1\}^M, A \mapsto \chi_A$ ist bijektiv. Mit den vorigen Überlegungen gestattet dies die Implementierung von Mengenoperationen durch Bitvektorverknüpfungen. Man vergleiche auch Aufgabe 6.7.4.

Satz 3.7.10 Es seien $(M, +)$, (N, \square) und (O, \diamond) Gruppoide. Ferner seien $h : M \rightarrow N$ und $g : N \rightarrow O$ Homomorphismen. Dann ist $f = h \circ g : M \rightarrow O$ ein Homomorphismus. Sind h und g sogar Isomorphismen, so auch f .

Beweis: Es seien zunächst $h : M \rightarrow N$ und $g : N \rightarrow O$ Homomorphismen und $x, y \in M$ beliebig. Dann gilt:

$$\begin{aligned} f(x + y) &= (h \circ g)(x + y) &= g(h(x + y)) \\ &\stackrel{h \text{ Hom.}}{=} g(h(x) \square h(y)) \\ &\stackrel{g \text{ Hom.}}{=} g(h(x)) \diamond g(h(y)) \\ &= (h \circ g)(x) \diamond (h \circ g)(y) = f(x) \diamond f(y) \end{aligned}$$

Also ist f ein Homomorphismus. Die Aussage zu Isomorphismen folgt aus Satz 3.3.10. \square

3.7.3 Eigenschaften von Verknüpfungen

Assoziativität, Halbgruppen und Monoide

Definition 3.7.8 Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. \mathbb{G} (oder auch \circ) heißt assoziativ gdw.

$$\forall x, y, z \in M : ((x \circ y) \circ z) = (x \circ (y \circ z))$$

Ein assoziatives Gruppoid heißt auch Halbgruppe. Ein Untergruppoid einer Halbgruppe heißt auch Unterhalbgruppe.

Beispiel: Vereinigung und Durchschnitt sind assoziative Mengen-Verknüpfungen, siehe Satz 3.1.16 bzw. die nachfolgende Anmerkung.

Zur Rechtfertigung unserer Definition zeigen wir zunächst:

Satz 3.7.11 Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. $N \subseteq M$ beschreibe ein Untergruppoid \mathbb{G}' . Ist \mathbb{G} assoziativ, so auch \mathbb{G}' .

Dies zeigt, dass Unterhalbgruppen tatsächlich auch Halbgruppen sind.

Beweis: Wir wissen:

$$\forall x, y, z \in M : ((x \circ y) \circ z) = (x \circ (y \circ z)).$$

Da $N \subseteq M$, gilt auch:

$$\forall x, y, z \in N : ((x \circ y) \circ z) = (x \circ (y \circ z)).$$

Also ist \mathbb{G}' assoziativ. \square

Anwendung: Wir hatten in Satz 3.1.16 die Assoziativität von \cap nicht bewiesen, nur die von \cup . Mit Aufgabe 6.7.4 ist alles klar.

Satz 3.7.12 Es seien (M, \circ) und (N, \square) Gruppoiden. Ferner sei \circ assoziativ.

Ist $h : M \rightarrow N$ ein Homomorphismus, so beschreibt $h(M)$ ein assoziatives Untergruppoid von N .

Deshalb heißen Homomorphismen auch “strukturerhaltende Abbildungen”.

Beweis: Wir wissen aus Satz 3.7.8, dass $h(M)$ ein Untergruppoid von N beschreibt. Zu zeigen bleibt dessen Assoziativität. Betrachte also $x', y', z' \in h(M)$.

Es gibt $x, y, z \in M$ mit $x' = h(x), y' = h(y)$ und $z' = h(z)$. Ferner gilt:

$$\begin{aligned} (x' \square (y' \square z')) &= (h(x) \square (h(y) \square h(z))) = (h(x) \square h(y \circ z)) \\ &= h((x \circ (y \circ z))) = h((x \circ y) \circ z) \\ &= (h(x \circ y) \square h(z)) = ((h(x) \square h(y)) \square h(z)) \\ &= ((x' \square y') \square z') \end{aligned}$$

Das zeigt die behauptete Assoziativität. \square

Beispiel: Man überlege sich, dass (\mathbb{N}, \max) ein assoziatives Gruppoid bildet. Jede Teilmenge $\bar{N} \subseteq \mathbb{N}$ beschreibt ein Gruppoid. (Klar?) Also liefert Satz 3.7.12: (\mathbb{N}, \max) ist stets assoziativ.

Definition 3.7.9 Es sei M eine Menge. $M^{[n]}$ bezeichnet die Menge aller n -elementigen Folgen von Elementen aus M . Es sei

$$M^* := \bigcup_{n \in \mathbb{N}} M^{[n]}$$

die Menge aller endlichen Folgen. Dann definiere folgende Operation \cdot , genannt Konkatenation, auf M^* ; dazu seien $f \in M^{[n]}$ und $g \in M^{[m]}$, $f \cdot g \in M^{[n+m]}$ ist festgelegt durch:

$$(f \cdot g)(i) = \begin{cases} f(i), & \text{falls } i \in [n] \\ g(i-n), & \text{sonst} \end{cases}$$

Beachte die Sonderrolle von $n = 0$: $M^{[0]} = M^\emptyset$ enthält genau eine Abbildung, nämlich die leere Abbildung. (Erinnere für M endlich: $|M^\emptyset| = |M|^{\emptyset} = |M|^0 = 1$.) Wir definieren zusätzlich: $M^+ := M^* \setminus M^\emptyset$.

Lemma 3.7.13 (M^*, \cdot) ist eine Halbgruppe. (M^+, \cdot) ist eine Unterhalbgruppe.

Den Beweis überlassen wir dem Leser als Übungsaufgabe. Mehr zu der Verbindung zum Gebiet der Formalen Sprachen erfahren Sie in Abschnitt 5.7.5.

Zur Auswertefunktion bei Halbgruppen Ist (M, \circ) eine Halbgruppe, so kann man die Auswertung von Termen natürlich wieder über $\mathcal{T}(M)$ definieren (mit $\text{eval}_{(M, \circ)}$).

Intuition: Assoziativität "meint" doch, man kann Klammern weglassen.

Das genau macht die Auswertefunktion von (M^+, \cdot) , wenn wir M mit Folgen der Länge Eins über M identifizieren. Damit ist auch $\mathcal{T}(M) \subset \mathcal{T}(M^+)$ auffassbar.

Ziel: Definiere Auswertefunktion $\text{eval}_{(M, \circ)}^{\text{ass}} : M^+ \rightarrow M$, sodass für $t \in \mathcal{T}(M)$ gilt:

$$\text{eval}_{(M, \circ)}(t) = \text{eval}_{(M, \circ)}^{\text{ass}}(\text{eval}_{(M^+, \cdot)}(t))$$

Idee: Wähle zu $w \in M^+$ willkürlich $t \in \text{eval}_{(M^+, \cdot)}^-(w) \cap \mathcal{T}(M)$ und definiere $\text{eval}_{(M, \circ)}^{\text{ass}}(w) := \text{eval}_{(M, \circ)}(t)$.

Bedeutung: t setzt willkürlich "vollständig" Klammern.

Mathematisches Problem: Vertreterunabhängigkeit / Wohldefiniertheit; was ist also zu zeigen?

Satz 3.7.14 Es sei (M, \circ) eine Halbgruppe. Sind $t, t' \in \mathcal{T}(M)$ mit $\text{eval}_{(M^+, \cdot)}(t) = \text{eval}_{(M^+, \cdot)}(t')$, so gilt: $\text{eval}_{(M, \circ)}(t) = \text{eval}_{(M, \circ)}(t')$.

Beweis: Es ist klar, dass $\text{eval}_{(M^+, \cdot)}(t) = \text{eval}_{(M^+, \cdot)}(t')$ nur dann gelten kann, wenn es eine natürliche Zahl n gibt, sodass sowohl t als auch t' aus n Elementen von M aufgebaut sind. Wir führen einen Induktionsbeweis über diese Zahl n .

$n = 1$ bedeutet, es gibt $m, m' \in M$ mit $t = m$ und $t' = m'$.

Die "Auswertung" in M^+ bedeutet die Identifikation von t mit der Folge m der Länge Eins, und ebenso von t' mit m' . Da $m = m'$, folgt $t = t'$, und somit die Behauptung.

Betrachte nun $n > 1$. Induktionsvoraussetzung: Die Behauptung gilt für alle Terme, die aus weniger als n Elementen aufgebaut sind.

Induktionsschritt: Betrachte Terme t, t' , die jeweils aus $n > 1$ Elementen von M aufgebaut sind. Nach der induktiven Definition von Termen gilt $t = (t_1 t_2)$ und $t' = (t'_1 t'_2)$, wobei sich auf die Terme t_1, t_2, t'_1, t'_2 jeweils die IV anwenden ließe, wenn $\text{eval}_{(M^+, \cdot)}$ gleiche Werte lieferte.

Da $\text{eval}_{(M^+, \cdot)}(t) = \text{eval}_{(M^+, \cdot)}(t')$, beginnen t, t', t_1, t_2 jeweils mit demselben Element $m \in M$. Wähle willkürlich Terme s_1, s'_1 , sodass

$$\text{eval}_{(M^+, \cdot)}((ms_1)) = \text{eval}_{(M^+, \cdot)}(t_1) \text{ sowie } \text{eval}_{(M^+, \cdot)}((ms'_1)) = \text{eval}_{(M^+, \cdot)}(t'_1).$$

(Die Spezialfälle $m = t_1$ bzw. $m = t'_1$ wären gesondert abzuhandeln \sim Übung!)

Nach IV gilt: $\text{eval}_{(M, \circ)}((ms_1)) = \text{eval}_{(M, \circ)}(t_1)$ sowie $\text{eval}_{(M, \circ)}((ms'_1)) = \text{eval}_{(M, \circ)}(t'_1)$.

Da $\text{eval}_{(M, \circ)}$ Homomorphismus, ist überdies:

$$\begin{aligned} \text{eval}_{(M, \circ)}(t) &= \text{eval}_{(M, \circ)}((t_1 t_2)) = \text{eval}_{(M, \circ)}(t_1) \circ \text{eval}_{(M, \circ)}(t_2) \\ &= \text{eval}_{(M, \circ)}((ms_1)) \circ \text{eval}_{(M, \circ)}(t_2). \end{aligned}$$

Wegen der Assoziativität von \circ haben wir außerdem:

$$\begin{aligned}\text{eval}_{(M,\circ)}(t) &= (\text{eval}_{(M,\circ)}(m) \circ \text{eval}_{(M,\circ)}(s_1)) \circ \text{eval}_{(M,\circ)}(t_2) \\ &= \text{eval}_{(M,\circ)}(m) \circ (\text{eval}_{(M,\circ)}(s_1) \circ \text{eval}_{(M,\circ)}(t_2)).\end{aligned}$$

Ganz Entsprechendes gilt für t' , t'_1 , t'_2 und s'_1 .

Nach Voraussetzung bzw. Definition gilt: $\text{eval}_{(M^+, \cdot)}((s_1 t_2)) = \text{eval}_{(M^+, \cdot)}((s'_1 t'_2))$.

Nach IV gilt daher: $\text{eval}_{(M,\circ)}((s_1 t_2)) = \text{eval}_{(M,\circ)}((s'_1 t'_2))$.

Aus der Homomorphismus-Eigenschaft folgt schließlich:

$$\begin{aligned}\text{eval}_{(M,\circ)}(t) &= \text{eval}_{(M,\circ)}(m) \circ (\text{eval}_{(M,\circ)}(s_1) \circ \text{eval}_{(M,\circ)}(t_2)) \\ &= \text{eval}_{(M,\circ)}(m) \circ \text{eval}_{(M,\circ)}((s_1 t_2)) \\ &= \text{eval}_{(M,\circ)}(m) \circ \text{eval}_{(M,\circ)}((s'_1 t'_2)) \\ &= \text{eval}_{(M,\circ)}(m) \circ (\text{eval}_{(M,\circ)}(s'_1) \circ \text{eval}_{(M,\circ)}(t'_2)) \\ &= \text{eval}_{(M,\circ)}(t').\end{aligned}$$

Nach dem Prinzip der vollständigen Induktion folgt die Behauptung. \square

Beispiel: Betrachte $M = \{a, b, c\}$ und die folgenden Abbildungen $M \rightarrow M$:

$\text{id} : a \mapsto a, b \mapsto b, c \mapsto c$

$\sigma_1 : a \mapsto b, b \mapsto c, c \mapsto a$

$\sigma_2 : a \mapsto c, b \mapsto a, c \mapsto b$

$\tau_{a,b} : a \mapsto b, b \mapsto a, c \mapsto c$

$\tau_{a,c} : a \mapsto c, b \mapsto b, c \mapsto a$

$\tau_{b,c} : a \mapsto a, b \mapsto c, c \mapsto b$.

σ_i : "Verschiebung" um i

$\tau_{x,y}$: "Vertauschung" von x, y .

$X = \{\text{id}, \sigma_1, \sigma_2, \tau_{a,b}, \tau_{a,c}, \tau_{b,c}\}$ ist die Menge der Bijektionen von M auf M .

(X, \circ) ist eine Halbgruppe.

$t := ((\sigma_1 \sigma_2)(\tau_{a,b} \tau_{a,b})) \in T(X)$.

$\text{eval}_{(X,\circ)}(t) = \dots = \text{id}$.

$f := \text{eval}_{(X^+, \cdot)}(t)$ lässt sich in Listenschreibweise kürzer notieren als

$f = (\sigma_1, \sigma_2, \tau_{a,b}, \tau_{a,b}) \in X^{[4]}$.

Das zugehörige $\text{eval}_{(X,\circ)}^{\text{ass}}$ liefert $\text{eval}_{(X,\circ)}^{\text{ass}}(f) = \text{id}$.

So wie Term-Gruppoide eine Blaupause für Gruppoide liefert, dient die *freie Halbgruppe* (M^+, \cdot) als Blaupause für jede Halbgruppe mit Grundmenge M .

Homomorphismen $h : (M^+, \cdot) \rightarrow (N, \circ)$ sind bereits durch die Bilder $h(a)$ für $a \in M$ festgelegt.

Definition 3.7.10 Es sei (M, \circ) eine Halbgruppe und $a \in M$ beliebig. Dann definiere die n -te Potenz von a , $n > 0$, wie folgt induktiv:

$$a^n := \begin{cases} a & \text{falls } n = 1 \\ a \circ a^{n-1} & \text{sonst} \end{cases}$$

Bemerkungen:

- Natürliche könnte man Potenzen auch in Gruppoiden definieren, in Halbgruppen gilt aber wegen des vorigen Satzes, dass man die zweite Zeile der Definition auch ersetzen könnte durch $a^{n-1} \circ a$, ohne am Ergebnis etwas zu ändern. Das wäre bei Gruppoiden anders.
- Besitzt die Halbgruppe ein neutrales Element e , so setzt man $a^0 := e$. Dies passt zur induktiven Definition, wie man leicht sieht.

- Schreibt man die Gruppoid-Operation als Addition, so spricht man auch vom *n-ten Vielfachen* eines Elements a und notiert dies auch gerne als $n \cdot a$.

Wie wir wissen, bildet für jede Menge M ($2^{M \times M}, \circ$) eine Halbgruppe mit neutralem Element Δ_M und absorbierendem Element \emptyset . Daher sind die Potenzen R^n für $n \in \mathbb{N}$ definiert.

Satz 3.7.15 Es sei $R \subseteq M \times M$. Für jede natürliche Zahl $n \geq 2$ gilt:

$$R^n = \{(x_0, x_n) \in M \times M \mid \exists x_1, \dots, x_{n-1} \in M \forall j \in \mathbb{N} (j < n \implies (x_j, x_{j+1}) \in R)\}.$$

Der Beweis ist eine hübsche Übungsaufgabe für Induktion. Vergleichen Sie auch mit Satz 3.2.19. $(x, y) \in R^n$ kann man also durch Angabe geeigneter *Brückenelemente* nachweisen.

Definition 3.7.11 Es sei M eine Menge. (M, \circ, e) heißt ein Monoid, wenn (M, \circ) Halbgruppe und e das neutrale Element von (M, \circ) ist.

Wir diskutieren ein Monoid (M, \circ, e) . Eine durch $N \subseteq M$ beschriebene Unterhalbgruppe von (M, \circ) ist nicht notwendigerweise ein Monoid (z.B., weil $e \notin N$). Man legt daher fest: (N, \circ, e) ist Untermonoid von (M, \circ, e) , falls (N, \circ) Untergruppoid von (M, \circ) ist und $e \in N$ gilt. Beachte: Eine Unterhalbgruppe von (M, \circ) muss selbst dann nicht Untermonoid sein, wenn sie selbst ein neutrales Element besitzt. Beispielsweise beschreibt jede Teilmenge N von $\mathbb{N} \cup \{\infty\}$ eine Unterhalbgruppe von $(\mathbb{N} \cup \{\infty\}, \min)$, die ein Monoid ist, falls $\infty \notin N$ oder falls N endlich. Im letzteren Fall beschreibt N aber kein Untermonoid von $(\mathbb{N} \cup \{\infty\}, \min, \infty)$. Das Beispiel zeigt noch etwas Anderes: Ist (M, \circ) eine Halbgruppe ohne neutrales Element, so kann man (M, \circ) durch Hinzufügen eines neutralen Elementes zu einem Monoid machen. Genauer bedeutet dies, dass man ein $e \notin M$ wählt, $M' = M \cup \{e\}$ setzt und \circ durch $e \circ x = x \circ e = x$ für alle $x \in M'$ zu einer Verknüpfung auf M' erweitert. Dann ist (M', \circ, e) ein Monoid. Das freie Monoid über einer Menge ist wieder eine Art Blaupause für alle Monoide auf dieser Menge.

Kommutativität, Idempotenz und Halbverbände

Definition 3.7.12 Es sei $G = (M, \circ)$ ein Gruppoid. G (oder auch \circ) heißt kommutativ gdw.

$$\forall x, y \in M : (x \circ y) = (y \circ x)$$

Mit Satz 3.1.15 sind \cup und \cap kommutative Mengen-Verknüpfungen.

Ganz ähnlich zur Assoziativität kann man zeigen:

Satz 3.7.16 Es sei $G = (M, \circ)$ ein Gruppoid. $N \subseteq M$ beschreibe ein Untergruppoid G' . Ist G kommutativ, so auch G' .

Satz 3.7.17 Es seien (M, \circ) und (N, \square) Gruppoiden. Ferner sei \circ kommutativ. Ist $h : M \rightarrow N$ ein Homomorphismus, so beschreibt $h(M)$ ein kommutatives Untergruppoid von N .

Definition 3.7.13 Es sei $G = (M, \circ)$ ein Gruppoid. G (oder auch \circ) heißt idempotent gdw.

$$\forall x \in M : (x \circ x) = x$$

Nach Satz 3.1.14 gilt: \cup und \cap sind idempotente Mengen-Verknüpfungen.

Satz 3.7.18 Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. $N \subseteq M$ beschreibe ein Untergruppoid \mathbb{G}' . Ist \mathbb{G} idempotent, so auch \mathbb{G}' .

Satz 3.7.19 Es seien (M, \circ) und (N, \square) Gruppoide. Ferner sei \circ idempotent. Ist $h : M \rightarrow N$ ein Homomorphismus, so beschreibt $h(M)$ ein idempotent Untergruppoid von N .

Definition 3.7.14 Ein Gruppoid (M, \sqcup) heißt Halbverband, wenn es assoziativ, kommutativ und idempotent ist.

Halbordnungen und Halbverbände Wir haben in Abschnitt 5.7.2 eine Möglichkeit beschrieben, Quasiordnungen (und oft auch Halbordnungen) aus Verknüpfungen zu gewinnen. Wir beschreiben im Folgenden eine weitere derartige Möglichkeit.

Definition 3.7.15 Es sei (M, \sqcup) ein Halbverband. Dann heißt die Relation $\sqsubseteq \subseteq M \times M$ mit

$$a \sqsubseteq b : \iff a \sqcup b = b$$

die von \sqcup induzierte Halbordnung.

Beispiele:

- Die vom Halbverband $(\mathbb{N} \setminus \{0\}, kgV)$ induzierte Halbordnung ist die Teilerrelation.
- Die vom Halbverband $(2^M, \cup)$ induzierte Halbordnung ist die Teilmengenrelation.
- Die vom Halbverband (\mathbb{R}, \max) induzierte Halbordnung ist \leq .

Satz 3.7.20 Die von einem Halbverband (M, \sqcup) induzierte Halbordnung (M, \sqsubseteq) ist (tatsächlich) eine Halbordnung.

Beweis: Es seien $a, b, c \in M$ beliebig.

Reflexivität: $a \sqsubseteq a$, denn $a \sqcup a = a$, da \sqcup idempotent.

Symmetrie: Gilt $a \sqsubseteq b$ und $b \sqsubseteq a$, so ist: $b = a \sqcup b = b \sqcup a = a$ aufgrund der Kommutativität von \sqcup .

Transitivität: Gilt $a \sqsubseteq b$ und $b \sqsubseteq c$, so ist: $c = b \sqcup c = (a \sqcup b) \sqcup c = a \sqcup (b \sqcup c) = a \sqcup c$, da \sqcup assoziativ. \square

Die in Satz 3.1.13 für Vereinigung und Teilmengenrelation formulierte Monotonie (Verträglichkeit) gilt auch allgemeiner:

Lemma 3.7.21 Sei (M, \sqcup) ein Halbverband mit induzierter Halbordnung \sqsubseteq und $a, b, c \in M$ beliebig. Gilt $a \sqsubseteq b$, so auch $a \sqcup c \sqsubseteq b \sqcup c$.

Beweis: $b \sqcup c = (a \sqcup b) \sqcup c = (a \sqcup b) \sqcup (c \sqcup c) = (a \sqcup c) \sqcup (b \sqcup c)$ aufgrund der Idempotenz, Assoziativität und Kommutativität von \sqcup . \square

Ist (M, \sqsubseteq) eine Halbordnung, bei der (*) zu zwei Elementen $a, b \in M$ stets eine obere Grenze (Supremum) von $\{a, b\}$ existiert, so definiere

$$a \sqcup b := \sup\{a, b\}$$

Def.: \sqcup ist die von \sqsubseteq induzierte Supremumsoperation.

Satz 3.7.22 Unter der Bedingung (*) ist (M, \sqcup) ein Halbverband.

Beweis zur Übung.

Die beiden Induktionsbegriffe "passen zusammen":

So ist die von einer Halbverbandsoperation \sqsubseteq induzierte Halbordnung derart, dass sie (*) erfüllt und wiederum eine Supremumsoperation induziert, die mit \sqsubseteq identisch ist.

3.7.4 Kongruenzrelationen

Wir stellen im Folgenden Beziehungen zum Abschnitt über Äquivalenzrelationen her.

Definition 3.7.16 Es sei $M = (M, \circ)$ ein Gruppoid und \equiv eine Äquivalenzrelation auf M . Die Verknüpfung \circ heißt verträglich mit \equiv gdw.

$$\forall a, b, a', b' \in M : ((a \equiv a') \wedge (b \equiv b')) \implies (a \circ b) \equiv (a' \circ b').$$

Dann heißt \equiv auch Kongruenzrelation auf M .

Die Äquivalenzklassen einer Kongruenzrelation heißen Kongruenzklassen.

Beispiel: Diagonale Δ_M und Allrelation $M \times M$ sind stets Kongruenzrelationen.

Die Identität, konstante Abbildungen und Projektionen sind stets verträglich mit jeder Äquivalenzrelation.

Wir werden diese Begriffe auch auf speziellere Gruppoide wie z.B. Halbgruppen oder Monoide anwenden.

Lemma 3.7.23 Für $m > 1$ gilt: Die in Beispiel 3.5.8 eingeführte Relation R_m ist eine Kongruenzrelation auf dem Monoid $(\mathbb{Z}, +, 0)$.

Beweis: Die bekannten Rechengesetze zeigen: $(\mathbb{Z}, +, 0)$ ist ein Monoid. Aus Übung 6.5.4 wissen wir: R_m ist eine Äquivalenzrelation. Zu überprüfen bleibt die Verträglichkeit. Betrachte also $a, b, a', b' \in \mathbb{Z}$ mit $(a, a'), (b, b') \in R_m$. Also gibt es k_a und k_b mit $(a' - a) = m \cdot k_a$ und $(b' - b) = m \cdot k_b$. Wir haben zu zeigen, dass es ein $k \in \mathbb{Z}$ gibt mit $((a' + b') - (a + b)) = m \cdot k$. Offenbar gilt:

$$((a' + b') - (a + b)) = ((a' - a) + (b' - b)) = m \cdot k_a + m \cdot k_b = m \cdot (k_a + k_b)$$

Mit $k = k_a + k_b$ folgt die Behauptung. \square

Hinweis: Das Rechnen in Restklassen hat wichtige Anwendungen in der Kryptographie.

Homomorphismen liefern Kongruenzrelationen Es seien $M = (M, \circ)$ und $N = (N, \square)$ zwei Gruppoide. $h : M \rightarrow N$ sei ein Homomorphismus. Wir wissen bereits aus unseren Untersuchungen aus Übung 6.3.2:

$\text{Kern}(h) := \{(a, a') \in M \times M \mid h(a) = h(a')\}$ ist eine Äquivalenzrelation.

Lemma 3.7.24 In der beschriebenen Lage ist $\text{Kern}(h)$ eine Kongruenzrelation auf M .

Beweis: Zu zeigen ist lediglich noch die Verträglichkeit.

Betrachte also $a, b, a', b' \in M$, sodass $(a, a') \in \text{Kern}(h)$ und $(b, b') \in \text{Kern}(h)$.

Also gilt: $h(a) = h(a')$ und $h(b) = h(b')$.

Da h Homomorphismus, gilt: $h(a \circ b) = h(a) \square h(b) = h(a') \square h(b') = h(a' \circ b')$.

Somit folgt die Verträglichkeit. \square

Definition 3.7.17 Es sei $\mathbb{M} = (M, \circ)$ ein Gruppoid und \equiv eine Kongruenzrelation auf \mathbb{M} . M/\equiv bezeichnet die Menge aller Kongruenzklassen von \equiv . Wir definieren das Faktorgruppoid $\mathbb{M}/\equiv = (M/\equiv, \circ_\equiv)$ wie folgt:

Für $A, B \in M/\equiv$ sei $A \circ_\equiv B := \{c \in M \mid \exists a \in A \exists b \in B : c = a \circ b\}$.

Lemma 3.7.25 Die Operation \circ_\equiv ist wohldefiniert.

Beweis: Betrachte $A, B \in M/\equiv$, z.B. $A = [a]_\equiv$ und $B = [b]_\equiv$. Wir behaupten: $A \circ_\equiv B = [a \circ b]_\equiv$. Problematisch ist einzig die Vertreterunabhängigkeit.

Betrachte $[a]_\equiv = [a']_\equiv, [b]_\equiv = [b']_\equiv$, also $a \equiv a', b \equiv b'$.

Da \equiv Kongruenzrelation, folgt $a \circ b \equiv a' \circ b'$, also $[a \circ b]_\equiv = [a' \circ b']_\equiv$. \square

Entsprechend kann man Faktorhalbgruppen, Faktormonoide usf. betrachten.

Beispiel: Betrachte das Monoid $(\mathbb{Z}, +, 0)$ und die Zerlegung $\mathbb{Z} = G \cup U$ in die geraden und ungeraden Zahlen. Dieser Zerlegung entspricht die Äquivalenzrelation R_2 . Wir haben gesehen, dass R_2 sogar eine Kongruenzrelation ist.

Betrachte das Faktormonoid mit der Grundmenge $\mathbb{Z}/R_2 = \{G, U\}$.

Die Addition ist hier gegeben durch: $G + G = U + U = G$ und $G + U = U + G = U$. Beachte: Dies entspricht der Monoidoperation auf dem Komplex "produkt" $+_K$ auf der Grundmenge $2^\mathbb{Z}$.

M.a.W.: $(\mathbb{Z}/R_2, +)$ ist eine Unterhalbgruppe von $(2^\mathbb{Z}, +_K)$, allerdings mit unterschiedlichen neutralen Elementen, nämlich G bzw. $\{0\}$.

Erinnere: $f_\equiv : A \rightarrow A/\equiv, a \mapsto [a]_\equiv$ ist die kanonische Abbildung von der ÄR \equiv .

Lemma 3.7.26 Ist \equiv Kongruenzrelation auf dem Gruppoid $\mathbb{M} = (M, \circ)$, so ist f_\equiv ein surjektiver Homomorphismus von \mathbb{M} auf das Faktorgruppoid \mathbb{M}/\equiv .

Ferner gilt: $\text{Kern}(f_\equiv) = \equiv$.

Beweis zur Übung.

Entsprechende Aussagen gelten für Faktorhalbgruppen und Faktormonoide.

3.8 Hullen

Definition 3.8.1 Es sei U ein Universum. Ein Hullenoperator ist eine extensive, monotone und idempotente Abbildung $H : 2^U \rightarrow 2^U$, die A ihre Hülle $H(A)$ zuordnet.

Extensivität $A \subseteq H(A)$,

Monotonie $A \subseteq B \implies H(A) \subseteq H(B)$,

Idempotenz $H(H(A)) = H(A)$.

Eine Menge A mit $H(A) = A$ heißt auch abgeschlossen. (Fixpunkteigenschaft)

Hinweis: Man könnte auch (nur) $H(H(A)) \subseteq H(A)$ fordern,

da $H(H(A)) \supseteq H(A)$ aus Extensivität und Monotonie folgt.

Allgemeiner könnte man auch Hullenoperatoren für Halbordnungen definieren.

Einfachste Beispiele: H als Identität oder $H : A \mapsto U$ (konstante Abbildung).

Wir betrachten im Folgenden noch etliche Beispiele.

- Sei $U = [0, 1]$ (Einheitsintervall). Zu $A \subseteq U$ setze:
 $\inf A := \sup \{x \in U \mid \forall a \in A : x \leq a\}$,
 $\sup A := \inf \{x \in U \mid \forall a \in A : x \geq a\}$, sowie

$$H(A) := [\inf A, \sup A].$$

Die abgeschlossenen Mengen sind hier die *abgeschlossenen Intervalle*.

- Sei $U = \mathbb{R} \times \mathbb{R}$ (Ebene). Zu $A \subseteq U$ sei:

$$\text{conv}(A) := \left\{ \left(\sum_{i=1}^n \alpha_i x_i, \sum_{i=1}^n \alpha_i y_i \right) \mid n \in \mathbb{N}, \sum_{i=1}^n \alpha_i = 1, \forall 1 \leq i \leq n : (x_i, y_i) \in A \wedge \alpha_i \geq 0 \right\}.$$

Die abgeschlossenen Mengen sind hier die *konvexen Mengen*.

Anschaulicher: Mit zwei Punkten ist auch die Verbindungsstrecke in einer konvexen Menge.

Andere Kennzeichnung: als Schnitt von (beliebig vielen) Halbebenen.

Dieser Begriff ist **wichtig** für geometrische Algorithmen, z.B. zur Bestimmung des größten paarweisen Abstands zwischen n Punkten schneller als mit n^2 vergleichen, siehe hier.

- Sei $U = [0, 1]$ (Einheitsintervall). Zu $A \subseteq U$ setze:

$$\text{cl}(A) := \{\lim_{n \rightarrow \infty} f(n) \mid f : \mathbb{N} \rightarrow A, f \text{ konvergiert}\}.$$

Die abgeschlossenen Mengen sind hier die auch in Analysis bzw. Topologie so genannten.

- Sei U eine Menge von Aussagen.

$\text{Th}(A)$ seien die aus $A \subseteq U$ beweisbaren Aussagen aus U .

Deutung (z.B. Monotonie): Sind A_1 und A_2 zwei Axiomenmengen mit $A_1 \subseteq A_2$, so ist die Menge der aus A_1 beweisbaren Aussagen eine Teilmenge der aus A_2 beweisbaren. Je kleiner die zugrunde liegende Axiomenmenge, desto allgemeiner sind die beweisbaren Aussagen.

- Sei (U, \leq) eine Quasiordnung. Definiere:

$$O_{\leq}(A) := \{a' \mid \exists a \in A : a \leq a'\}.$$

Die abgeschlossenen Mengen heißen auch *Oberhalbemengen* (von (U, \leq)).

Satz 3.8.1 $H : 2^U \rightarrow 2^U$ ist ein Hüllenoperator gdw. $(A \subseteq H(B) \iff H(A) \subseteq H(B))$.

Beweis: Ist H ein Hüllenoperator, so folgt aus $A \subseteq H(B)$: $H(A) \subseteq H(H(B)) = H(B)$ wegen der Monotonie und Idempotenz von H .

Umgekehrt folgt aus $H(A) \subseteq H(B)$: $A \subseteq H(B)$ wegen der Extensivität von H und da \subseteq transitiv. Es gelte nun $(A \subseteq H(B) \iff H(A) \subseteq H(B))$ für alle $A, B \subseteq U$.

Für $A = B$ gilt $H(A) \subseteq H(B)$ in trivialer Weise (\subseteq ist reflexiv). Daher folgt $A \subseteq H(B) = H(A)$ (Extensivität).

Aus der Extensivität folgt nun auch $H(A) \subseteq H(H(A))$.

Liest man $H(A) \subseteq H(A)$ als (gültige) linke Seite der (als gültig angenommenen) Äquivalenz, folgt $H(H(A)) \subseteq H(A)$ (und mithin die Idempotenz).

Falls $A \subseteq B$, so auch $A \subseteq H(B)$ (wegen der Extensivität von H und der Transitivität von \subseteq), so gilt $H(A) \subseteq H(B)$ (Monotonie). \square

Hüllen und Halbordnungen

Satz 3.8.2 Es sei $H : 2^U \rightarrow 2^U$ ein Hüllenoperator. Setze $V := H(2^U) = \{H(A) \mid A \subseteq U\}$. Dann ist

- (V, \cap) ein Halbverband und
- (V, \supseteq) die induzierte Halbordnung.

Beweis: Wie aus dem Kapitel über Verknüpfungen bekannt, müssen wir nur zeigen:

Für beliebige $A, B \subseteq U$ gilt: $H(A) \cap H(B) \in V$ (Abgeschlossenheit).

Damit ist nämlich (V, \cap) ein Unterhalbverband von $(2^U, \cap)$.

Aus Monotonie und Idempotenz folgt:

$H(H(A) \cap H(B)) \subseteq H(H(A)) = H(A)$ sowie $H(H(A) \cap H(B)) \subseteq H(H(B)) = H(B)$, d.h.

$H(H(A) \cap H(B)) \subseteq H(A) \cap H(B)$. Die Extensivität liefert die andere Inklusion.

Also gilt: $H(A) \cap H(B) = H(X)$ für ein $X \subseteq U$, nämlich $X = H(A) \cap H(B)$. \square

Ist zur Halbordnung $(H(2^U), \subseteq)$ stets eine Supremumsoperation definiert?

Wie das Beispiel der abgeschlossenen Intervalle lehrt, muss die Vereinigung zweier abgeschlossener Intervalle kein abgeschlossenes Intervall sein.

Wir definieren hingegen:

$$\sup_H(A, B) := \bigcap_{X \in O \subseteq (A \cup B), X \in H(2^U)} X$$

Satz 3.8.3 Es sei $H : 2^U \rightarrow 2^U$ ein Hüllenoperator.

Setze $V := H(2^U) = \{H(A) \mid A \subseteq U\}$. Dann ist $\sup_H(A, B) \in V$, falls $A, B \in V$.

Beweis: Die Argumentation folgt fast wörtlich dem zweiten Teil des vorigen Beweises.

Insbesondere folgt aus Monotonie und Idempotenz:

$H(\sup_H(A, B)) \subseteq H(C)$ für jedes $C \in H(2^U)$ mit $C \supseteq A \cup B$, also $H(\sup_H(A, B)) \subseteq \sup_H(A, B)$. \square

Folgerung 3.8.4 (V, \sup_H) ist ein Halbverband.

Satz 3.8.5 Es sei $H : 2^U \rightarrow 2^U$ ein Hüllenoperator. Dann ist $\sup_H(A, B) = H(A \cup B)$.

Beweis: Da $H(A \cup B) \in H(2^U)$ und $A \cup B \subseteq H(A \cup B)$ (Monotonie), folgt $\sup_H(A, B) \subseteq H(A \cup B)$.

Da H Hüllenoperator, folgt weiter aus $A \cup B \subseteq \sup_H(A, B)$:

$$H(A \cup B) \subseteq H(\sup_H(A, B)) = \sup_H(A, B) \subseteq H(A \cup B),$$

also $H(A \cup B) = \sup_H(A, B)$. \square

$H(A \cup B)$ ist also die kleinste abgeschlossene Obermenge von A und B .

Dies motiviert die folgenden Betrachtungen.

Abgeschlossene Systeme als Kennzeichnung für Hüllen

Definition 3.8.2 Ein Mengensystem $\mathfrak{M} \subseteq 2^U$ heißt abgeschlossenes System gdw. für jede Indexmenge I derart, dass $M_i \in \mathfrak{M}$ für alle $i \in I$, auch $\bigcap_{i \in I} M_i \in \mathfrak{M}$ liegt.
Bem.: Mit der leeren Indexmenge folgt per Konvention: $U \in \mathfrak{M}$.

Satz 3.8.6 Es sei U ein Universum.

1. Ist H ein Hüllenoperator, dann definiert $\mathfrak{M}_H := \{H(A) \mid A \subseteq U\}$ ein abgeschlossenes System.
2. Ist $\mathfrak{M} \subseteq 2^U$ ein abgeschlossenes System, so definiert $H_{\mathfrak{M}}(A) := \bigcap_{B \in \mathfrak{M}, A \subseteq B} B$ einen Hüllenoperator.

Überlegen Sie: Was wäre noch zu beweisen?

Beispiele

1. Ist $\mathbb{G} = (M, \circ)$ ein Gruppoid, so gibt es zwei zugeordnete abgeschlossene Systeme:
 - (a) Die Menge $\text{Sub}(\mathbb{G})$ der Untergruppoide von \mathbb{G} ,
 - (b) Die Menge $\text{Con}(\mathbb{G})$ der Kongruenzrelationen von \mathbb{G} .
2. Ist M eine Menge, so ergeben sich folgende abgeschlossene Systeme:
 - (a) Die Menge $\text{Tr}(M)$ der transitiven Relationen auf M ,
 - (b) Die Menge $\text{QO}(M)$ der Quasiordnungen auf M ,
 - (c) Die Menge $\text{Eq}(M)$ der Äquivalenzrelationen auf M ,
 - (d) Die Menge $\text{PO}(M)$ der Halbordnungen auf M .

Überlegen Sie: Was muss man (noch) zeigen? Was folgt aus dem bisher Gesagten?
Hierzu folgen einige Hinweise.

Lemma 3.8.7 *Beschreiben M_i , $i \in I$, Untergruppoide von $\mathbb{G} = (M, \circ)$, so beschreibt $M_{\cap} := \bigcap_{i \in I} M_i$ ein Untergruppoid von \mathbb{G} .*

Beweis: Wir müssen zeigen: Mit $a, b \in M_{\cap}$ liegt auch $a \circ b \in M_{\cap}$.

Da $a, b \in M_{\cap}$, liegt $a, b \in M_i$ für jedes $i \in I$.

Da M_i ein Untergruppoid beschreibt, liegt $a \circ b$ in M_i .

Also liegt $a \circ b$ in allen M_i und mithin in M_{\cap} . □

Lemma 3.8.8 *Der Durchschnitt beliebig vieler transitiver Relationen ist transitiv.*

Beweis: Betrachte die transitiven Relationen R_i , $i \in I$, sowie $R_{\cap} := \bigcap_{i \in I} R_i$.

Diskutiere (x, y) und (y, z) aus R_{\cap} : Für jedes $i \in I$ gilt: $\{(x, y), (y, z)\} \subseteq R_i$.

Da R_i transitiv, folgt $(x, z) \in R_i$. Also liegt (x, z) in allen R_i und mithin in R_{\cap} . □

Die anderen Behauptungen sieht man entsprechend.

Eine natürliche mathematische Frage: Warum sind die Beweise so ähnlich?

Das hat einen tieferen Grund, es gilt nämlich:

Satz 3.8.9 *Ist M eine Menge, so gilt:*

$$\text{Tr}(M) = \{R \subseteq M \times M \mid R \cup \{\perp\} \in \text{Sub}(M \times M \cup \{\perp\}, \circ')\}.$$

Hierbei sei $(a, b) \circ' (b, c) := (a, c)$, während sich sonst das absorbierende Element \perp ergibt. Man sieht, dass so $(M \times M \cup \{\perp\}, \circ')$ eine Halbgruppe bildet.

Beweis: Wir wissen: $R \subseteq M \times M$ ist transitiv gdw. $R \circ R \subseteq R$. Dann gilt aber für alle $x, y \in R \cup \{\perp\}$: $x \circ' y \in R \cup \{\perp\}$, denn der einzige "kritische Fall" ist $x \in R$ und $y \in R$, sodass $x \circ' y \neq \perp$.

Beschreibt R' andererseits eine Unterhalbgruppe von $(M \times M \cup \{\perp\}, \circ')$, so gilt insbesondere, dass mit $\{(a, b), (b, c)\} \subseteq R' \cap M \times M$ auch $(a, c) \in R' \cap M \times M$ gelten muss, d.h., $R = R' \setminus \{\perp\}$ ist eine transitive Relation. □

Hüllenoperatoren aus abgeschlossenen Systemen—wichtige Beispiele

Ist $R \subseteq M \times M$, so bezeichnet

- R^+ die *transitive Hülle* von R (zu $\text{Tr}(M)$ gehörig),

- R^* die reflexiv-transitive Hülle von R (zu $QO(M)$ gehörig).

Ist $\mathbb{G} = (M, \circ)$ ein Gruppoid und $A \subseteq M$, so bezeichnet
 $\langle A \rangle_{\mathbb{G}}$ das von A erzeugte Gruppoid (zu $\text{Sub}(\mathbb{G})$ gehöriger Hüllenoperator).
 A heißt auch Erzeugendensystem des Gruppoids $\langle A \rangle_{\mathbb{G}}$.
Bsp.: $\{0, 1\}$ ist Erzeugendensystem des Gruppoids $(\mathbb{N}, +)$.

Was bedeutet also R^+ , R^* bzw. $\langle A \rangle_{\mathbb{G}}?$... und kann man das evtl. berechnen?

Eine Kennzeichnung erzeugter Strukturen—Hinführung

Definition 3.8.3 Es sei $\mathbb{G} = (M, \square)$ ein Gruppoid.

Zu $A \subseteq M$ arbeitet der Erzeugungsoperator $E : 2^M \rightarrow 2^M$ wie folgt:

$$E(A) := A \cup \{a \square b \mid a, b \in A\} (= A \cup A \square_K A).$$

Wir setzen induktiv $E^0 := \Delta_{2^M}$ und $E^{n+1} := E^n \circ E$ für $n \in \mathbb{N}$.

Lemma 3.8.10 Für jedes $n \in \mathbb{N}$ ist E^n extensiv und monoton, aber im Allgemeinen nicht idempotent.

Beweis: Die Monotonie folgt unmittelbar aus der Definition.

Die Extensivität ergibt sich durch einen einfachen Induktionsbeweis:

IA: $A = E^0(A)$.

IS: Gilt $A \subseteq E^k(A)$, so gilt $A \subseteq E^{k+1}(A) = E(E^k(A)) = E^k(A) \cup E^k(A) \square_K E^k(A)$. \square

Beispiel: Für das Gruppoid $(\mathbb{N}, +)$ und $A = \{0, 1\}$ gilt: $E^n(A) = \{j \in \mathbb{N} \mid j \leq 2^n\}$.

Außer E^0 ist kein E^n idempotent in diesem Beispiel.

Das sieht ganz anders in dem Restklassengruppoid $(\mathbb{Z}_4, +)$ aus!

Satz 3.8.11 Ist $\mathbb{G} = (M, \circ)$ ein Gruppoid und $A \subseteq M$, so gilt: $\langle A \rangle_{\mathbb{G}} = \bigcup_{n \in \mathbb{N}} E^n(A)$.

Beweis: Betrachte $a, b \in \bigcup_{n \in \mathbb{N}} E^n(A)$. Es gibt also Zahlen i, j , sodass $a \in E^i(A)$ und $b \in E^j(A)$. Daher gilt: $\{a, b\} \in E^{\max\{i, j\}}(A)$. Nach Def. ist also

$$a \square b \in E^{\max\{i, j\}}(A) \subseteq \bigcup_{n \in \mathbb{N}} E^n(A).$$

Also beschreibt $\bigcup_{n \in \mathbb{N}} E^n(A)$ ein Gruppoid. Da $A \subseteq \bigcup_{n \in \mathbb{N}} E^n(A)$, folgt $\langle A \rangle_{\mathbb{G}} \subseteq \bigcup_{n \in \mathbb{N}} E^n(A)$. Die umgekehrte Inklusion sieht man per Induktion.

IA: $A = E^0(A) \subseteq \langle A \rangle_{\mathbb{G}}$ (Extensivität).

IH: Es gelte $E^k(A) \subseteq \langle A \rangle_{\mathbb{G}}$.

Betrachte $c \in E^{k+1}(A)$. Wegen IH und Monotonie bleibt $c \notin E^k(A)$ als interessanter Fall übrig.

Nach Def. gibt es $a, b \in E^k(A)$, sodass $c = a \square b$.

Da $a, b \in \langle A \rangle_{\mathbb{G}}$ (nach IH) und da $\langle A \rangle_{\mathbb{G}}$ Untergruppoid von \mathbb{G} , folgt $c \in \langle A \rangle_{\mathbb{G}}$. \square

Spezialfall Halbgruppen—mit Anwendung für transitive Hüllen

Es sei $\mathbb{G} = (M, \circ)$ eine Halbgruppe.

Dann ist $2^{\mathbb{G}} := (2^M, \circ_K)$ eine Halbgruppe (Komplexprodukt).

In diesem Sinne ist für Teilmengen $A \subseteq M$ und natürliche Zahlen $n \geq 1$ die Potenz A^n definiert.

Achtung: Verwechslungsgefahr mit dem Mengenprodukt und entsprechenden Potenzen.

Satz 3.8.12 Ist $\mathbb{G} = (M, \circ)$ eine Halbgruppe und $A \subseteq M$, so gilt:

$$\langle A \rangle_{\mathbb{G}} = \bigcup_{n \in \mathbb{N}, n \geq 1} A^n.$$

Beweis: Per Induktion kann man beweisen: $A^n \subseteq E^n(A) \subseteq \bigcup_{i=1}^{2^n} A^i$. Daraus ergibt sich mit Satz 3.8.11 die Behauptung. \square

Mit Satz 3.8.9 ergibt sich hieraus (Potenzen beziehen sich nun auf das Relationenprodukt):

Satz 3.8.13 Ist M eine Menge und $R \subseteq M \times M$, so gilt: $R^+ = \bigcup_{n \in \mathbb{N}, n \geq 1} R^n$.

Ein einfaches Beispiel für transitive Hüllen

Gegeben sei eine Relation ‘‘Direkter-Vorgesetzter’’ mit folgenden Beziehungen:

C ist direkter Vorgesetzter von D und E.

B ist direkter Vorgesetzter von C.

A ist direkter Vorgesetzter von B.

Die transitive Hülle dieser Relation enthält nun zusätzlich auch die ‘‘indirekten Vorgesetzten’’:

A ist Vorgesetzter von B, C, D, E.

B ist Vorgesetzter von C, D, E.

C ist Vorgesetzter von D und E.

Endliche Mengen Es sei M eine Menge und $R \subseteq M \times M$ eine Binärrelation.

Aus Satz 3.7.15 wissen wir, dass für jede natürliche Zahl $k \geq 2$ gilt:

$$R^k = \{(x_0, x_k) \in M \times M \mid \exists x_1, \dots, x_{k-1} \in M \forall j \in \mathbb{N} (j < k \implies (x_j, x_{j+1}) \in R)\}.$$

Satz: Ist $R \subseteq M \times M$ und M endlich, so gilt $R^+ = \bigcup_{k=1}^{|M|} R^k$.

Das liefert einen einfachen *Algorithmus zur Berechnung von R^+* , siehe Abb. 3.14.

Beweis: Betrachte also $(x, y) \in R^k$ für ein $k > |M|$ (sonst ist die Aussage trivial).

Wir nehmen ferner an, k sei die kleinste Zahl mit $(x, y) \in R^k$ †.

Also gibt es $k - 1$ Brückenelemente $x_1, \dots, x_{k-1} \in M$ mit: $\forall j \in \mathbb{N} (j < k \implies (x_j, x_{j+1}) \in R)$, wobei $x_0 = x$ und $x_k = y$.

Die k Indizes $1, \dots, k$ sind als ‘‘Gegenstände’’ auf $|M| < k$ Fächer (die Elemente von M) zu verteilen. Daher gibt es zwei Indizes $i < j$ und $j - i \leq |M|$ mit $x_i = x_j$. Man kann $(x, y) \in R^{k-(j-i)}$ mit $k > k - (j - i) > |M| - (j - i) \geq 0$ begründen wegen $x = x_0, x_k = y$ und:

$$(x_0, x_1) \in R, (x_1, x_2) \in R, \dots, (x_{i-1}, x_i) \in R, x_i = x_j, (x_j, x_{j+1}) \in R, \dots, (x_{k-1}, x_k) \in R$$

Dies widerspricht der Minimalität von k , siehe †. \square

Informatiker-Frage: Wie soll so ein Algorithmus aus Abb. 3.14 implementiert werden?

Hinweis: Bitvektoren-Darstellung für Mengen, also auch für Relationen.

Was ‘‘bedeutet’’ hier aber das Relationenprodukt? (\sim Matrixprodukt; siehe Übung 6.8.7).

Ein schnellerer Pseudocode (jenseits konkreter Implementierungen) findet sich in Abb. 3.15

Zur Zeitanalyse: Wir brauchen also:

- $m - 1$ Relationenprodukte und Relationenvereinigungen
- m Zuweisungen

Data : R : binary relation on the set M
Result : R^+ : transitive closure of R

- 1 S, H : subset of $M \times M$;
- 2 k : integer;
- 3 $S \leftarrow R$;
- 4 **for** $k \leftarrow 2$ to $|M|$ **do**
- 5 $H \leftarrow R^k$;
- 6 $S \leftarrow H \cup S$;
- 7 **return** S ;

Abbildung 3.14: A first transitive closure algorithm

Data : R : binary relation on the set M
Result : R^+ : transitive closure of R

- 1 S, H : subset of $M \times M$;
- 2 k : integer;
- 3 $S \leftarrow R$;
- 4 **for** $k \leftarrow 2$ to $|M|$ **do**
- 5 $H \leftarrow R \circ H$;
- 6 $S \leftarrow H \cup S$;
- 7 **return** S ;

Abbildung 3.15: An improved transitive closure algorithm

jeweils für Binärrelationen über einer m -elementigen Grundmenge M .
Es ist naheliegend, etwa m^3 Tests einzelner Elemente von M je Relationenprodukt anzusetzen, siehe Übung 6.8.7.

→ Das Ganze kostet etwa m^4 Tests einzelner Elemente von M .

Weitere Informatiker-Frage: Geht das besser?

Die reflexiv-transitive Hülle R^* ist die kleinste R umfassende Quasiordnung.

Diese spielt in vielen Bereichen der Informatik eine hervorragende Rolle.

Dies betrifft auch den Fall unendlicher Grundmengen, wie Sie in “Automaten und Formale Sprachen” sowie “Berechenbarkeit und Komplexität” sehen werden.

Satz 3.8.14 Es sei R eine Binärrelation über M . Dann gilt:

$$R^* = (R \cup \Delta_M)^+ = R^+ \cup \Delta_M = \bigcup_{k \geq 0} R^k.$$

Wir können also Algorithmen zur Berechnung der transitiven Hülle leicht dazu verwenden, reflexiv-transitive Hüllen zu berechnen. Die Komplexität eines Verfahrens für transitive Hüllen überträgt sich (im Wesentlichen) auf eines für reflexiv-transitive Hüllen.

Veranschaulichung in gerichteten Graphen

Erinnere: $G = (V, E)$ ist ein (gerichteter) Graph, wenn $E \subseteq V \times V$ und V endlich.

Wir können nun *Wege* als endliche Knotenfolgen wie folgt induktiv definieren:

1. Ist $v \in V$, so ist v (auch) ein Weg der Länge null von v nach v .

2. Die Knotenfolge $v_0v_1 \dots v_k$ ist ein Weg der Länge $k \geq 1$ von v_0 nach v_k genau dann, wenn $(v_0, v_1) \in E$ und wenn $v_1 \dots v_k$ ein Weg der Länge $k - 1$ von v_1 nach v_k ist.

Alternative Sicht: Weg der Länge k als “kantenfolgende” Abbildung $[k + 1] \rightarrow V$.

Hinweis: Wege gemäß unserer Definition unterscheiden sich in zwei Dingen von Pfaden:

- Sie sind für gerichtete Graphen definiert.
- Sie erlauben Wiederholungen von Knoten.

Der erste Teil ließe sich leicht anpassen, m.a.W., man kann Pfade in gerichteten Graphen als “wiederholungsfreie Wege” einführen. Der zweite Teil ist schwerwiegender und der eigentlich entscheidende Unterschied.

Satz: Es gibt einen Weg der Länge k von v_0 nach v_k gdw. $(v_0, v_k) \in E^k$ gilt.

Hinweis: Die “Brückenknoten” v_1, \dots, v_{k-1} werden bei Wegen also expliziert.

Frage: Was bedeutet also: $(u, v) \in (E \cup \Delta_V)^k$?

Diese eher anschauliche Sichtweise wird auch bei der Darstellung des Algorithmus von Floyd und Warshall in Abschnitt 5.8.1 angenommen.

Algorithmisches zu Äquivalenzen

Da $\text{Eq}(M)$ abgeschlossenes System, gibt es einen entsprechenden Äquivalenzhüllenoperator $\langle \cdot \rangle_{\text{Eq}}$.

Satz 3.8.15 *Es sei R eine Binärrelation über M . Dann gilt: $\langle R \rangle_{\text{Eq}} = (R \cup R^-)^*$.*

Folgerung: Ist M endlich, kann man also die Äquivalenzhülle einer vorgelegten Relation in kubischer Zeit (gemessen in $|M|$) berechnen; dazu verwendet man den Algorithmus von Floyd und Warshall.

Kapitel 4

Mathematische Anmerkungen

4.1 Mengenlehre

4.1.1 Cantor, Dedekind und Russel: Zur Geschichte der Mengenlehre

Definition 3.1.1 geht zurück auf Georg Cantor (1845-1918). Dieser nannte eine “Menge” allerdings “Mannigfaltigkeit”, siehe beispielsweise Cantors Buch “Grundlagen einer allgemeinen Mannigfaltigkeitslehre” von 1883, das den bezeichnenden Untertitel “ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen” trägt. Derlei philosophische, geradezu religiöse Betrachtungen durchziehen die Werke Cantors. So schreibt Cantor im Vorwort zu der erwähnten Arbeit von 1883: “Indem ich diese Blätter der Öffentlichkeit übergebe, will ich nicht unerwähnt lassen, dass ich sie hauptsächlich im Hinblick auf zwei Leserkreise geschrieben habe, für Philosophen, welche der Entwicklung der Mathematik in die neueste Zeit gefolgt und für Mathematiker, die mit den wichtigsten älteren und neueren Erscheinungen der Philosophie vertraut sind.” Wir werden diese “Lehre des Unendlichen” allerdings immer nur streifen. Es geht uns vielmehr um die Verwendung der von Cantor geschaffenen Formalismen und Begrifflichkeiten. Für besonders Interessierte mag es hilfreich sein zu wissen, dass viele Werke Cantors heute in digitalisierter Form zugänglich vorliegen.

Als kulturelle Anmerkung wollen wir auf Folgendes hinweisen: Die Oper “Cantor — Die Vermessung des Unendlichen” von Ingomar Grünauer widmet sich dem Leben und Werk Georg Cantors; Uraufführung aus Anlass des 1200-jährigen Stadtjubiläums am 10. November 2006 im Opernhaus Halle, siehe Seite des Musikverlages Schott.

Wir bemühen uns in diesem Skript darum, alle Sachverhalte zu beweisen oder doch zumindest den Leser in die Lage zu versetzen, einen derartigen Beweis selbst zu führen. Richard Dedekind hat 1888 im Vorwort der ersten Auflage von [10] geschrieben: “Was beweisbar ist, soll in der Wissenschaft nicht ohne Beweis geglaubt werden.” Dieser an und für sich selbstverständlich erscheinende Grundsatz ist oft nur mühevoll vollständig durchzuführen. Das gilt (auf den ersten Blick erstaunlicherweise) insbesondere für die absoluten Grundlagen eines Fachs. Beim zweiten Draufsehen ist dieser Umstand weniger verwunderlich. Dahinter verbirgt sich nämlich ein philosophisches Problem: Mit welchen denn offensichtlich noch “grundlegenderen” Begriffen sollen denn die Grundbegriffe erklärt werden? Diese Schwierigkeiten sieht man auch schon an Definition 3.1.1. Dort werden (notwendigerweise) Wörter verwendet, die formal vorher nicht

eingeführt worden sind. Jedem des Deutschen Mächtigen sollte aber klar sein, was mit dieser Begriffsbildung gemeint ist.

Aufgrund dieser auch philosophisch bedingten Unschärfen prägt sich die Bedeutung und Umfänglichkeit eines Begriffes meist auch erst durch seine Verwendung heraus. Daher möchten wir dazu ermuntern, von Anbeginn alle wesentlichen Definitionen auch dadurch einzuüben, dass Sie sich immer wieder geeignete Beispiele überlegen.

Konkret: Was sind “gute Beispiele” für Mengen?

Oder auch: Was sieht vielleicht auf den ersten Blick aus wie eine Menge, ist dies aber auf den zweiten Blick streng genommen nicht?

Durch die in der Vorlesung getroffene “Übereinkunft” verliert sich etwas von der Strenge der Definition. Wer meint, die mögliche Vielfachheit von Elementen sollte bei der Definition einer Menge Berücksichtigung finden, sei auf den Begriff einer Multimenge verwiesen. Dieser formalisiert die entsprechende Intuition. Einen genaueren Hinweis finden Sie in Abschnitt 4.3.

4.1.2 Mengenangaben

Wir müssen aber dennoch zur *Vorsicht bei Mengenangaben* gemahnen. Ein allzu naiver Umgang mit Definitionen, welche Mengen durch gewisse Eigenschaften beschreiben wollen, kann zu Widersprüchen führen (die bekannteste ist die Russellsche Antinomie).

Dies vermeiden wir im Folgenden

- einmal dadurch, dass wir Mengen aus “sehr einfachen” Mengen aufbauen
- und dadurch, dass wir (oft) die Menge aller Elemente angeben, aus denen wir überhaupt Mengen aufbauen dürfen, das sogenannte *Universum*.

So kann die Mengenlehre zur *Grundlage aller Mathematik* werden. Diese Stützfunktion innerhalb der Mathematik kann alternativ von der Logik übernommen werden. In Trier hören Sie dazu eine eigene Vorlesung.

Um diese Aussage noch auf der alleruntersten Ebene zu stützen, überlegen wir uns noch folgende Aussage:

Es gibt nur eine Menge, die keine Elemente enthält.

Angenommen nämlich, M und N seien beide Mengen, die keine Elemente enthalten. Ist x nun ein “Ding unserer Anschauung oder unseres Denkens”, welches nicht in M enthalten ist, so kann es auch nicht in N enthalten sein, denn sonst enthielte N ja ein Element. Genausowenig darf ein Ding, welches nicht in N liegt, in M enthalten sein. Damit haben wir gezeigt: $x \notin M \iff x \notin N$, und dies ist logisch gleichwertig mit $x \in M \iff x \in N$. Nach Definition 3.1.2 folgt damit $M = N$.

Da wir aber bereits eine Menge benannt haben, die keine Elemente enthalten soll, nämlich \emptyset , folgt aus unserer Überlegung, dass \emptyset die einzige Menge ist, die keine Elemente enthält. Das rechtfertigt also (im Nachhinein) den Namen, den wir dieser Menge gegeben haben: es ist die leere Menge.

Eine kürzere Begründung dieses wichtigen Sachverhaltes könnte wie folgt ausspielen: Es sei N eine Menge, die keine Elemente enthält. Der Beweis zu Lemma 3.1.2, zeigt, dass dann für jede Menge M gilt: $N \subseteq M$. Speziell trifft das für $M = \emptyset$ zu, also $N \subseteq \emptyset$. Umgekehrt lautet Lemma 3.1.2: “Es sei A einen Menge. Dann gilt: $\emptyset \subseteq A$.” Für $A = N$ erhalten wir somit $\emptyset \subseteq N$. Mit Satz 3.1.3 folgt die Behauptung.

Außerdem ist damit (nochmals) klar, dass die im Haupttext diskutierte Menge $M = \{\emptyset, \{\emptyset\}\}$ tatsächlich zwei unterschiedliche Elemente enthält, denn beides sind Mengen, und nur eine davon kann leer sein.

4.1.3 Zum Aufbau der Zahlen

Auf Richard Dedekind und Giuseppe Peano geht die folgende Definition der natürlichen Zahlen zurück. Diese Peano-Axiome sind ein klassisches Beispiel einer *induktiven Definition*. Die folgende axiomatische Definition der Menge der natürlichen Zahlen \mathbb{N} durch Giuseppe Peano (1889) ist eigentlich von Richard Dedekind bereits in [10] 1888 beschrieben worden.

- 0 ist eine natürliche Zahl.
- Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n' , der ebenfalls eine natürliche Zahl ist.
- Es gibt keine natürliche Zahl, deren Nachfolger 0 ist.
- Zwei verschiedene natürliche Zahlen n und m besitzen stets verschiedene Nachfolger n' und m' .
- Enthält eine Menge X die Zahl 0 und mit jeder natürlichen Zahl n auch stets deren Nachfolger n' , so enthält X bereits alle natürlichen Zahlen.

Aus der letzten Forderung – dem *Induktionsaxiom* – ergibt sich: Ist X dabei selbst eine Teilmenge der natürlichen Zahlen, dann ist $X = \mathbb{N}$.

Peano verwendet dabei die Begriffe 0, Zahl und *Nachfolger*, um die natürlichen Zahlen zu beschreiben.

Wie sehen natürliche Zahlen aus? (nach Dedekind / Peano)

$0, 0', 0'', 0''', 0''''$, ...

Es ist jedoch bequemer, bei der gewohnten Schreibweise zu bleiben:

$0, 1, 2, 3, 4, \dots$

Diese ist überdies deutlich kürzer als die induktiv definierte.

Addition von Zermelo-Zahlen Diese kann man induktiv wie folgt definieren:

$$n_Z +_Z m_Z := \begin{cases} n_Z, & \text{falls } m_Z = \emptyset \\ (n_Z +_Z k_Z)', & \text{falls } m_Z = k_Z' \end{cases}$$

Induktive Definitionen laden zu Induktionsbeweisen geradezu ein. Wir fragen nun zunächst: Ist diese Definition der Addition “sinnvoll”? Dazu zeigen wir, dass zumindest eine Grundvoraussetzung dafür gegeben ist, dass wir $+_Z$ als Verknüpfung ansehen können (mehr dazu in Abschnitt über Verknüpfungen unten), nämlich die sogenannte *Abgeschlossenheit*. Das heißt, die Addition zweier Zermelo-Zahlen soll wieder eine Zermelo-Zahl liefern. Formal behaupten wir also:

Aussage: Sind $n_Z, m_Z \in \mathbb{N}_Z$, so auch $n_Z +_Z m_Z \in \mathbb{N}_Z$.

Beweis: Es sei $n_Z \in \mathbb{N}_Z$ beliebig aber fest.

Betrachte für $m_Z \in \mathbb{N}$ die Aussageform $p(m)$: “ $n_Z +_Z m_Z \in \mathbb{N}_Z$ ”.

IA: $p(0)$ gilt, denn nach Definition der Addition gilt: $n_Z +_Z 0_Z = n_Z$, und $n_Z \in \mathbb{N}_Z$ ist bekannt.

IS: Angenommen, für $k \in \mathbb{N}$ wäre $p(k)$ schon gezeigt. D.h., $n_Z +_Z k_Z \in \mathbb{N}_Z$ kann vorausgesetzt

werden als IV. Als IB ist zu zeigen: $n_Z + z k'_Z \in \mathbb{N}_Z$.

Nach Definition der Addition gilt: $n_Z + z k'_Z = (n_Z + z k_Z)'$.

Mit dem Induktionsaxiom folgt aus $n_Z + z k_Z \in \mathbb{N}_Z$, dass der Nachfolger $(n_Z + z k_Z)'$ in \mathbb{N}_Z liegt. Daher folgt die IB.

Nach dem Prinzip der mathematischen Induktion folgt die behauptete Aussage. \square

4.1.4 Beweistechniken

Beweise sind der Kern mathematischer Gedankengänge. Nur wer sie nachvollziehen kann, ist in der Lage, auch eigenständig mathematische Beweise zu führen. Nur diese Fähigkeit ermöglicht ein tieferes Verständnis der verwendeten Begriffe. Da Letzteres Ziel jeder mathematisch orientierten Veranstaltung sein muss, ist es unumgänglich, dass Sie frühestmöglich in die Lage kommen, selbst Beweise führen zu können.

Modus Ponens Die vielleicht elementarste Regel, die immer wieder in Beweisen (unausgesprochen) angewendet wird, ist der Modus Ponens. In Worte gefasst, handelt es sich dabei um Folgendes. Wir wollen in einem Beweis zeigen, dass eine Aussage q gilt, wenn (als Voraussetzung) die Aussage p wahr ist. Dazu beweisen wir die Richtigkeit der Implikation $p \implies q$ unter der Annahme der Richtigkeit von p .

Wir können diese Regel auch als Tautologie verstehen:

$$(p \wedge (p \implies q)) \implies q$$

Beweisketten Im Modus Ponens “steckt” ja sozusagen der Nachweis einer Implikation, nämlich $p \implies q$. Diese wiederum zeigt man oft durch Zwischenbehauptungen, die dann zu Beweisketten zusammengefügt werden können. Im einfachsten Fall findet man also eine Aussage r und beweist dann zunächst $p \implies r$, wobei (als Voraussetzung) die Aussage p wahr ist. Sodann zeigt man $r \implies q$, wobei wir nun p und r als wahr annehmen können. Daraus können wir die Richtigkeit von q schlussfolgern unter der Annahme der Richtigkeit von p .

Wir können diese Regel auch wieder als Tautologie verstehen:

$$((p \wedge (p \implies r)) \wedge (r \implies q)) \implies q$$

Die Richtigkeit sieht man durch zweimalige Anwendung des Modus Ponens ein.

Noch allgemeiner ist die folgende Situation: Wir betrachten $n \geq 1$ Aussagen p_1, \dots, p_n . Dann können wir aus der Richtigkeit von p_1 und der der Implikationen $p_i \implies p_{i+1}$ für $i \in \{1, \dots, n-1\}$ die Richtigkeit von p_n schlussfolgern. Wir können also beliebig lange Beweisketten in Beweisgängen benutzen. Die Gültigkeit dieser Regel zeigt man durch vollständige Induktion sehr ähnlich wie im Beweis von Satz 3.2.19.

Kontraposition ist eine hilfreiche Technik, wenn der direkte Nachweis von $(p \implies q)$ nicht klappt. Gleichwertig kann man nämlich zeigen, dass $(\neg q \implies \neg p)$ gilt. Dahinter verbirgt sich die folgende Tautologie:

$$(p \implies q) \iff (\neg q \implies \neg p).$$

Wie beweist man Mengengleichheit? Der logische Hintergrund für die übliche Art von Beweis (elementweise Argumentation mit zwei Beweisrichtungen) ist die Tautologie

$$(p \iff q) \iff ((p \Rightarrow q) \wedge (q \Rightarrow p)).$$

Diejenigen unter Ihnen, die die “Einführung in die Logik” bereits gehört haben, werden diese wiedererkennen. Wir werden diese Tautologie auch noch im Zusammenhang mit dem Einschluss wiedersehen.

Ringschluss Wenn mehrere Aussagen zueinander äquivalent sind, so ist es meist am einfachsten, diese Äquivalenz dadurch nachzuweisen, indem man zeigt, dass aus der ersten Aussage die zweite folgt, aus der zweiten die dritte usf. und man schließlich aus der Gültigkeit der letzten Aussage die der ersten folgern kann.

Wenn wir also die Äquivalenz dreier Aussagen p, q, r beweisen wollen, genügt es, die drei Implikationen $p \Rightarrow q, q \Rightarrow r$ und $r \Rightarrow p$ zu beweisen. Logischer Hintergrund ist hier die folgende Tautologie:

$$((p \iff q) \wedge (q \iff r)) \iff ((p \Rightarrow q) \wedge (q \Rightarrow r) \wedge (r \Rightarrow p))$$

Dieses Argument gilt auch allgemeiner: Sind p_1, \dots, p_n n viele Aussagen (mit $n \geq 2$), deren Äquivalenz wir beweisen wollen, so genügt es, die n Implikationen $p_1 \Rightarrow p_2, p_2 \Rightarrow p_3, \dots, p_{n-1} \Rightarrow p_n$ sowie $p_n \Rightarrow p_1$ nachzuweisen. Dies beruht auf folgender Tautologie:

$$\left(\bigwedge_{i=1, \dots, n; j=1, \dots, n} (p_i \iff p_j) \right) \iff \left(\left(\bigwedge_{i=1}^{n-1} (p_i \Rightarrow p_{i+1}) \right) \wedge (p_n \Rightarrow p_1) \right)$$

Diese sieht man leicht mit vollständiger Induktion ein. (Das ist eigentlich eine schöne Übungsaufgabe.) Die zuvor angegebene Tautologie ist übrigens nicht genau der Fall $n = 3$. Sehen Sie den Unterschied?

Als Anwendung könnte man mit elementweiser Argumentation hieraus folgendes Beweisprinzip für Mengengleichheit ableiten: Es seien A_1, \dots, A_n Mengen. Aus

$$\forall i \in \{1, \dots, n-1\}: A_i \subseteq A_{i+1}$$

sowie $A_n \subseteq A_1$ folgt:

$$\forall i, j \in \{1, \dots, n\}: A_i = A_j.$$

4.1.5 Zu den Rechengesetzen

Viele der für die Mengenoperationen bewiesenen Rechenregeln werden Ihnen bekannt vorkommen aus Ihrem Umgang mit Zahlen, einige jedoch nicht. In der Mathematik ist es die Algebra, die sich mit derartigen Rechenregeln beschäftigt. Zum Beispiel lernen Sie in der “Linearen Algebra” Strukturen wie Vektorräume kennen, die die “geometrischen Vektoren” verallgemeinern, welchen Sie in der Schule (z.B. auch im Physikunterricht) begegnet sind. Wir werden uns ebenfalls mit sehr einfachen Strukturen später noch beschäftigen.

Beim Umgang mit algebraischen Strukturen ist es von großer Wichtigkeit, sich stets darüber im Klaren zu sein, welche Regeln angewendet werden dürfen (und welche im Allgemeinen im konkreten Fall nicht gelten). So wäre es fatal, das Idempotenzgesetz

unüberlegt beim Rechnen mit Zahlen anzuwenden. Deshalb müssen bei algebraischen Umformungen auch immer alle Einzelschritte begründet werden.

Es gibt aber auch Rechengesetze für Mengen, zu denen es bei den “normalen Zahlen” kaum eine Entsprechung gibt. Betrachten wir einmal folgende Aussage:

Lemma 4.1.1 *Es seien A, B, C Mengen. Dann gilt:*

$$A \setminus B \subseteq C \iff A \subseteq B \cup C \iff A \setminus C \subseteq B.$$

Welche Entsprechung sollte es hierfür im Reich der Zahlen geben? Wenn die Mengendifferenz der üblichen Differenzbildung entspricht und die Teilmengenbeziehung dem Kleiner-Gleich (wie das zu verstehen sein könnte, werden wir in Abschnitt über Quasiordnungen sehen), so stünde dort $(a - b) \leq c \iff a \leq (b + c) \iff (a - c) \leq b$; das wäre ja soweit in Ordnung. Der nun folgende Beweis zeigt aber, dass die Begründung hierfür doch in der Mengenalgebra anders aussieht als bei den Zahlen.

Wir wollen bei dem nun folgenden elementweisen Beweis auch noch die Nähe der Argumentation zur Logik darstellen und weiter verstehen lernen.

Beweis: Es sei x ein beliebiges Element aus dem zugrundeliegenden Universum \mathcal{U} . Wir müssen zeigen:

$$((x \in A \setminus B) \implies x \in C) \iff (x \in A \implies (x \in B \vee x \in C)) \iff ((x \in A \setminus C) \implies x \in B).$$

Wir betrachten die folgende Kette logischer Äquivalenzen:

$$\begin{aligned} ((x \in A \setminus B) \implies x \in C) &\iff ((x \in A \wedge x \notin B) \implies x \in C) \\ &\iff ((\neg(x \in A \wedge x \notin B)) \vee x \in C) \\ &\iff ((x \notin A \vee x \in B) \vee x \in C) \\ &\iff ((x \notin A) \vee (x \in B \vee x \in C)) \\ &\iff (x \in A \implies (x \in B \vee x \in C)) \quad (*) \\ &\iff (x \in A \implies (x \in C \vee x \in B)) \\ &\iff (x \notin A \vee (x \in C \vee x \in B)) \\ &\iff ((x \notin A \vee x \in C) \vee x \in B) \\ &\iff ((\neg(x \in A \wedge x \notin C)) \vee x \in B) \\ &\iff ((x \in A \wedge x \notin C) \implies x \in B) \\ &\iff ((x \in A \setminus C) \implies x \in B) \end{aligned}$$

Beachten Sie, dass $(*)$ gerade der mittleren Behauptung entspricht. Beobachten Sie, welche Rechengesetze der Aussagenlogik nacheinander angewendet wurden, nachdem die Mengendifferenz als wohl am wenigsten eingängiger Mengenoperation als Konjunktion aufgelöst worden war:

1. das Gesetz von deMorgan;
2. das Gesetz der doppelten Negation;
3. das Assoziativgesetz der Disjunktion;
4. das Kommutativitätsgesetz der Disjunktion;
5. ... (nun wieder rückwärts)

Da x beliebig gewählt wurde, folgt die Behauptung für die Mengenalgebra. \square

Alternativ zur elementweisen Argumentation wäre es möglich, rein mit den Gesetzen der Mengenalgebra zu argumentieren. Dies ist aber oft schwieriger und jedenfalls

ungewohnter. Wir zeigen im Folgenden daher nur eine der insgesamt (selbst bei Ringschluss) drei nötigen Implikationen.

$$\begin{aligned}
 A \setminus B \subseteq C &\implies (A \cap \overline{B}) \subseteq C \\
 &\implies B \cup (A \cap \overline{B}) \subseteq B \cup C \\
 &\implies (B \cup A) \cap (B \cup \overline{B}) \subseteq B \cup C \\
 &\implies (B \cup A) \cap U \subseteq B \cup C \\
 &\implies B \cup A \subseteq B \cup C \\
 &\implies A \subseteq B \cup C
 \end{aligned}$$

Überlegen Sie einmal, welche Sätze bei dieser Argumentation in jedem Schritt verwendet wurden.

4.1.6 Sprachliche Anmerkungen

Mathematische Sprech- und Schreibweisen wandeln sich im Laufe der Zeit, so wie das für Sprache allgemein gilt. Wenn Sie einmal versuchen, ein älteres mathematisches Buch zu lesen, so werden Sie diese Aussage gut nachvollziehen können.

Dazu kommt, dass insbesondere Mengenlehre und Logik zwei Gebiete sind, die ursprünglich dem Bereich der Philosophie eher noch als der Mathematik zuzuordnen sind. Unsere (kurzen) Exkurse zum Wesen der Gleichheit mögen das schon belegen. Noch beredter ist vielleicht das folgende Zitat von Gottlob Frege aus [16].

Die Gleichheit fordert das Nachdenken heraus durch Fragen, die sich daran knüpfen und nicht ganz leicht zu beantworten sind. Ist sie eine Beziehung? eine Beziehung zwischen Gegenständen? oder zwischen Namen oder Zeichen für Gegenstände? Das Letzte hatte ich in meiner Begriffschrift angenommen. Die Gründe, die dafür zu sprechen scheinen, sind folgende: $a = a$ und $a = b$ sind offenbar Sätze von verschiedenem Erkenntniswert: $a = a$ gilt a priori und ist nach Kant analytisch zu nennen, während Sätze von der Form $a = b$ oft sehr wertvolle Erweiterungen unserer Erkenntnis enthalten und a priori nicht immer zu begründen sind. Die Entdeckung, daß nicht jeden Morgen eine neue Sonne aufgeht, sondern immer dieselbe, ist wohl eine der folgenreichsten in der Astronomie gewesen.

Da in der heutigen Zeit das Englische als Wissenschaftssprache praktisch alle anderen Sprachen verdrängt hat und es demgemäß nicht nur üblich geworden ist, wissenschaftliche Fachaufsätze in englischer Sprache abzufassen, sondern auch Lehrbücher, ist es für Sie wichtig, dass Sie auch die englischen Entsprechungen der deutschen Fachausdrücke kennen. Die wichtigsten aus diesem Abschnitt, die sich nicht durch Abändern weniger Buchstaben auseinander ergeben, seien im Folgenden zusammengefasst. Diese Aufstellung können Sie auch gleichzeitig als Überprüfung Ihres Lernerfolges ansehen: Sollten Sie einen der aufgeführten Begriffe nicht gut verstanden haben, so sollten Sie dies nun dringend nachholen, da dies alles Kernbegriffe für den gesamten Kurs sind.

deutsch	englisch
Menge	set
leere Menge	empty set
Teilmenge	subset
Obermenge	superset
Vereinigung	union
Durchschnitt	intersection
Potenzmenge	power set

4.2 Relationen und gerichtete Graphen

Grundsätzlich ist wohl anzumerken, dass dieser Abschnitt, im Gegensatz zum vorigen, mehr konzeptueller Natur ist. Sie finden mehr Begriffe, die eingeführt werden, und dafür verhältnismäßig wenig Sätze und Beweise. Die eingeführten Begriffe sind aber äußerst wichtig für die nachfolgenden Abschnitte, weshalb sie gründlich studiert werden sollten.

4.2.1 Mehrstellige Relationen

Wir könnten Relationen auch allgemeiner definieren:

Definition 4.2.1 Es seien M_1, \dots, M_n Mengen.
 R heißt n -stellige Relation zwischen M_1, \dots, M_n gdw.

$$R \subseteq M_1 \times \dots \times M_n.$$

M_i heißen auch Grundmengen von R .

Gilt $M = M_i$ für $i \in \{1, \dots, n\}$, so heißt R eine n -stellige Relation über M .

In der Literatur findet sich auch: Schreibweise: $R(x_1, \dots, x_n)$ statt $(x_1, \dots, x_n) \in R$ (Prädikatnotation)

Hinweis: Relationen und Prädikate: " $(x_1, \dots, x_n) \in R$ " ist Aussageform mit Variablen x_1, \dots, x_n . Umgekehrt definieren Aussageformen Relationen.

Für unsere Zwecke genügen aber die zweistelligen Relationen, wie sie im Haupttext eingeführt worden sind. Alternativ zur Definition 4.2.1 könnten wir auch eine induktive Definition wählen. An ihr erkennt man auch, dass es im Grunde keinen neuen Begriff z.B. einer dreistelligen Relation bedürfte. Außerdem behebt sie die in der vorigen Definition unschöne Pünktchenschreibweise.

Definition 4.2.2 Es seien M_1, \dots, M_n Mengen.
Definiere zunächst induktiv die Produktmenge

$$\bigtimes_{i=1}^n M_i := \begin{cases} M_1, & \text{falls } n = 1, \\ \left(\bigtimes_{i=1}^{n-1} M_i \right) \times M_n, & \text{falls } n > 1. \end{cases}$$

R heißt n -stellige Relation zwischen M_1, \dots, M_n gdw. $R \subseteq \bigtimes_{i=1}^n M_i$.

Die übrigen Begriffe übertragen sich aus der vorherigen Definition. Wenn wir der induktiven Definition konsequent folgten, müssten wir Tripel z.B. als $((a, b), c)$ schreiben, denn wegen der Induktion sind es ja Paare, dessen erste Komponente wiederum ein Paar ist. Insofern ist diese “Lösung” auch unbefriedigend, zumal wir ja auch durchaus andere Arten von induktiven Definitionen geben können, zum Beispiel:

$$\bigtimes_{i=1}^n M_i := \begin{cases} M_1, & \text{falls } n = 1, \\ M_1 \times \left(\bigtimes_{i=2}^n M_i \right), & \text{falls } n > 1. \end{cases}$$

Nun wären Tripel von der Bauart $(a, (b, c))$. Auch dies wäre nicht die einzige Möglichkeit. Wir möchten wenigstens noch eine weitere angeben:

$$\bigtimes_{i=1}^n M_i := \begin{cases} M_1, & \text{falls } n = 1, \\ \left(\bigtimes_{i=1}^{n-1} M_i \right) \times M_n, & \text{falls } n > 1 \text{ und } n \text{ ungerade}, \\ \left(\bigtimes_{i=1}^{n/2} M_i \right) \times \left(\bigtimes_{i=n/2+1}^n M_i \right), & \text{sonst.} \end{cases}$$

Wir werden im nächsten Abschnitt einen Begriff kennenlernen, der eine schönere, weil symmetrischere und dennoch mathematisch saubere Definition von “ n -Tupeln” als Grundelementen von n -stelligen Relationen gestattet.

4.2.2 Relationenalgebra

Wir haben im Haupttext die Gültigkeit etlicher Formeln zum “Rechnen” mit Relationen hergeleitet. Dies legt die Frage nahe, inwiefern sich nicht auch ein Kalkül angeben lässt, der (im Sinne von Axiomen) die wesentlichen Rechenregeln beinhaltet, sodass sich die Übrigen hieraus erschließen und beweisen lassen. Tatsächlich ist dies auch im Falle der sogenannten Relationenalgebren erfolgt, wie in vielen Bereichen der Algebra.

Uns liegt fern, diese Algebra hier im Einzelnen einzuführen, wollen aber (dem Buch [37] folgend) ein paar Grundlinien skizzieren.

Ansonsten haben wir es nur mit Algebren zu tun, die auf einer einzigen Operation (evtl. plus Konstanten) fußen. Hier jedoch haben wir es mit einer Algebra zu tun, die mehrere Operationen auf einer Grundmenge U (hier $2^{M \times M}$) gleichzeitig betrachtet:

- die Mengenoperationen \cup , \cap und das Komplement sowie
- das Relationenprodukt \circ und die Inversenbildung.

Man fordert nun, dass U zusammen mit den Mengenoperationen einen atomaren, vollständigen Booleschen Verband bildet, wie wir dies kurz am Ende von diesem Skript anreißen. Für das Relationenprodukt fordert man seine Assoziativität und die Existenz eines neutralen Elements (m.a.W., (U, \circ, Δ_M) ist ein Monoid, wie wir noch sehen werden). Ferner benötigt man die Gültigkeit der *Tarski-Regel*

$$\forall R \subseteq M \times M : R \neq \emptyset \implies (M \times M) \circ R \circ (M \times M) = M \times M$$

und die *Schröderschen Umformungen*

$$\forall R, S, T \subseteq M \times M : \bar{R}^- \circ \bar{S}^- \subseteq T \iff \bar{S}^- \circ \bar{T}^- \subseteq R \iff \bar{T}^- \circ \bar{R}^- \subseteq S$$

Hieraus lassen sich alle bislang von uns aufgeführten Sätze zurückführen, ohne wirklich genau das Wesen von konkreten Relationen zu verwenden. Eine der interessanten Resultate ist die *Dedekind-Formel*

$$\forall R, S, T \subseteq M \times M : (R \circ S) \cap T \subseteq (R \cap (T \circ S^-)) \circ (S \cap (R^- \circ T))$$

Der interessierte Leser mag sich daran versuchen, die drei zuletzt genannten Gesetze für unsere (konkreten) Relationen (als Teilmengen von $2^{M \times M}$) nachzurechnen. In leicht abgeänderter Form gelten die Gesetze auch für Relationen zwischen verschiedenen Mengen. Es ist ebenfalls eine gute Übungsaufgabe, die Gesetze in diesem Sinne verallgemeinert aufzuschreiben.

Als eine Anwendung von derlei algebraischen Überlegungen wollen wir uns um eine der bekannteren algebraischen Aufgabenstellungen kümmern, dem Lösen von “linearen” Gleichungen. Vorweg machen wir dazu eine Hilfsüberlegung:

Lemma 4.2.1 *Es seien R, S Relationen auf M . Dann gilt: $R \circ \overline{R^- \circ \overline{S}} \subseteq S$.*

Beweis: Betrachte $(u, w) \in R \circ \overline{R^- \circ \overline{S}}$ beliebig. Also gibt es ein $v \in M$ mit $(u, v) \in R$ und $(v, w) \in \overline{R^- \circ \overline{S}}$. Da $(u, v) \in R$, folgt $(v, u) \in R^-$. Wäre nun $(u, w) \notin S$, so fänden wir $(v, w) \in R^- \circ \overline{S}$, Widerspruch! Also gilt $(u, w) \in S$. \square

Satz 4.2.2 *Es seien R, S Relationen auf M . Dann gilt:*

$$R \circ X = S \text{ besitzt eine Lösung } X \subseteq M \times M \iff S \subseteq R \circ \overline{R^- \circ \overline{S}}.$$

Wegen Lemma 4.2.1 könnten wir anstelle des Einschlusses auch die Gleichheit fordern.

Beweis: Gilt für $X \subseteq M \times M$, dass $R \circ X = S$, so folgt aus den Schröderschen Umformungen, dass gilt:

$$R \circ X \subseteq S \iff \overline{S}^- \circ R \subseteq \overline{X}^- \iff R^- \circ \overline{S} \subseteq \overline{X} \iff X \subseteq \overline{R^- \circ \overline{S}}.$$

Daher folgt: $R \circ X = S \subseteq R \circ \overline{R^- \circ \overline{S}}$.

Gilt umgekehrt $S \subseteq R \circ \overline{R^- \circ \overline{S}}$, so folgt für $X = \overline{R^- \circ \overline{S}}$, dass $R \circ X \supseteq S$ gilt. $R \circ X \subseteq S$ gilt immer wegen Lemma 4.2.1. \square

4.2.3 Bezeichnungen

So wichtig die in diesem Abschnitt behandelten Begriffe sind, so unterschiedlich sind doch die Bezeichnungen. Auch wenn, Hilbert im übertragenden Sinne folgend, Namen in der Mathematik geradezu Schall und Rauch sind, so muss man diese Vielfalt von Bezeichnungen kennen, um sich in anderen Büchern oder auch im Internet ansatzweise orientieren zu können. Die folgende Tabelle gibt “Übersetzungen” der Begriffe an.

bei uns	in der Literatur ebenfalls üblich
Diagonale	Identitätsrelation, Gleichheitsrelation
nacheindeutig	rechtseindeutig, eindeutig
vortotal	linkstotal, total
Relation auf M	homogene Relation
Relation zwischen M_1 und M_2	heterogene Relation
Inverse	Konverse, Transponierte
paar (Graph)	geteilt, bipartit

4.3 Funktionen

4.3.1 Mengenfunktionen

Wir haben Funktionen als spezielle – nämlich nacheindeutige – Relationen eingeführt. Dies ist nicht die einzige Art von Beziehung, die zwischen den Begriffen besteht.

Es sei $R \subseteq A \times B$ eine beliebige Relation. Diese kann man auch als zwei Mengenfunktionen deuten:

$$\begin{aligned} R_1 : 2^A &\rightarrow 2^B, X \mapsto \{y \in B \mid \exists x \in X (x, y) \in R\} \\ R_2 : 2^B &\rightarrow 2^A, Y \mapsto \{x \in A \mid \exists y \in Y (x, y) \in R\} \end{aligned}$$

Satz 4.3.1 $R_1(A_1 \cup A_2) = R_1(A_1) \cup R_1(A_2)$. (entsprechend für R_2)

Beweis: Sei $y \in R_1(A_1 \cup A_2)$. Dann gibt es $x \in A_1 \cup A_2$ mit $(x, y) \in R$. Also: $x \in A_1$ oder $x \in A_2$. Im ersten Fall ist $y \in R_1(A_1)$, im zweiten $y \in R_1(A_2)$. Die Rückrichtung sieht man analog. \square

Satz 4.3.2 $R_1(A_1 \cap A_2) \subseteq R_1(A_1) \cap R_1(A_2)$. (entsprechend für R_2)

Die umgekehrte Inklusion gilt im Allgemeinen nicht.

Beweis: Die Inklusion sieht man wie bei \cup . Gleichheit gilt im Allgemeinen nicht, z.B.: $A = \{a, a'\}, B = \{1\}, R = \{(a, 1), (a', 1)\}, A_1 = \{a\}, A_2 = \{a'\}$. $R_1(A_1 \cap A_2) = R_1(\emptyset) = \emptyset \subsetneq \{1\} = R_1(A_1) \cap R_1(A_2)$. \square

Ist R durch eine Funktion $f : A \rightarrow B$ gegeben, schreibt man auch $f(X)$ statt $R_1(X)$, und $f^-(Y)$ statt $R_2(Y)$.

Satz 4.3.3 $f^-(B_1 \cap B_2) = f^-(B_1) \cap f^-(B_2)$.

Wir verweisen hierbei auf Aufgabe 6.3.1,

Eine weitere interessante Mengenabbildung ist:

$$\text{eindeutig} : 2^{A \times B} \rightarrow 2^{A \times B}, R \mapsto \overline{R \circ \Delta_B}.$$

$\text{eindeutig}(R)$ beschreibt den eindeutigen Anteil von R ; so ist die Relation $\text{eindeutig}(R)$ stets nacheindeutig. Wir verweisen auch auf die Lösungsdiskussion 7.2.7. Daher gilt auch:

Satz 4.3.4 $R \subseteq A \times B$ ist eine Abbildung $\iff \text{eindeutig}(R) \circ (B \times B) = B \times B$.

4.3.2 Der Satz von Schröder und Bernstein

Etwas zur Historie: Der erste Beweis hierzu wurde von Felix Bernstein vorgestellt, damals war F.B. ein Student bei Georg Cantor. Einige Jahre zuvor haben den Satz wohl Richard Dedekind und Ernst Schröder bewiesen, und Cantor hat den Sachverhalt wohl auch schon erkannt. Unser Beweis folgt der Darstellung von Julius König. Wir verweisen auf die Diskussion in http://en.wikipedia.org/wiki/Talk%3ACantor%20%93Bernstein%20%93Schroeder_theorem. Tatsächlich ist die historische Lage recht verworren, was auch dadurch belegt werden kann, da es zu dieser Geschichte ein ganzes Buch [23] gibt.

Wir wollen den folgenden Satz beweisen:

Gibt es injektive Abbildungen $f : A \rightarrow B$ und $g : B \rightarrow A$, so gibt es auch eine Bijektion zwischen A und B .

Beweis: Es seien $f : A \rightarrow B$ und $g : B \rightarrow A$ injektiv. O.E. gehen wir davon aus, dass $A \cap B = \emptyset$. Für jedes $a \in A$ betrachte die Folge

$$\dots \mapsto f^-(g^-(a)) \mapsto g^-(a) \mapsto a \mapsto f(a) \mapsto g(f(a)) \mapsto \dots$$

(und entsprechend für $b \in B$); diese Folgen wechseln zwischen A und B hin und her.

Für gewisse $n \geq 1$ könnte $(f \circ g)^n(a) = a$ gelten.

Dann bildet $a, f(a), g(f(a)), \dots, (g \circ f)^{n-1}(f(a))$ einen “Kreis.”

Andernfalls setzt sich die Folge “nach rechts” unendlich lang fort.

Man unterscheidet “nach links” drei Fälle, da $f^-(x)$ bzw. $g^-(x)$ nicht definiert sein muss:

(a) Die Folge endet in A ; (b) sie endet in B ; (c) sie setzt sich unendlich fort.

Beobachtung: Jedes Element aus A und auch aus B kommt in genau einer dieser Folgen vor.

Daher wird hierdurch eine Zerlegung von $A \cup B$ in Klassen beschrieben.

Wir definieren eine Bijektion $h : A \rightarrow B$ für jede Klasse getrennt:

Liegt $a \in A$ in einer Folge vom Typ (a) oder (c) oder in einem Kreis, so setze $h(a) = f(a)$.

Liegt $a \in A$ in einer Folge vom Typ (b), so setze $h(a) = g^-(a)$.

Zu zeigen bleibt: h ist tatsächlich eine Bijektion.

Klar: $h \subseteq A \times B$ (Relationenschreibweise).

h ist vortotal: Mit der Beobachtung genügt die folgende Bemerkung: Insbesondere wird $h(a) = g^-(a)$ nur im Fall (b) gesetzt, wenn Urbilder von g stets existieren.

h ist vor- und nacheindeutig: Das ergibt sich mit der Beobachtung aus der Nacheindeutigkeit von f und der Voreindeutigkeit von g .

h ist nachtotal: Betrachte ein $b \in B$. Nach der Beobachtung liegt b in einer Folge, die sich (im Ausschnitt) als

$$\dots \mapsto f^-(b) \mapsto b \mapsto g(b) \mapsto \dots$$

darstellt. Je nach Fall ist somit $h(f^-(b)) = b$ oder $h(g(b)) = b$. Also gilt $b \in h(A)$.

Warum stimmt also die Beobachtung (Folgen zerlegen $A \cup B$)?

Würde $a \in A$ in zwei solcher Folgen vorkommen, so wären beide Folgen “nach rechts” ab a identisch aufgrund der Nacheindeutigkeit von f und von g , und sie stimmten auch “nach links” überein ab a wegen der Voreindeutigkeit von f und von g .

Ferner gilt: Da f (und g) vortotal, enthält jede Folge mit $a \in A$ auch $f(a) \in B$ und umgekehrt; also enthält jede Folge mindestens zwei Elemente.

Das gilt insbesondere für mögliche Kreise. □

Eine Illustration des Beweises

Es sei $A \subseteq \mathbb{N}$ die Menge der geraden Zahlen und $B \subseteq \mathbb{N}$ die Menge der ungeraden Zahlen. Die Abbildungen $f : A \rightarrow B$, $n \mapsto n + 3$ und $g : B \rightarrow A$, $n \mapsto 3n - 1$ sind beide injektiv. Folgen in $A \cup B$ sind:

$$0 \mapsto 3 \mapsto 8 \mapsto 11 \mapsto 32 \mapsto \dots$$

$$1 \mapsto 2 \mapsto 5 \mapsto 14 \mapsto 17 \mapsto \dots$$

$$4 \mapsto 7 \mapsto 20 \mapsto 23 \mapsto 68 \mapsto \dots$$

$$6 \mapsto 9 \mapsto 26 \mapsto 29 \mapsto 86 \mapsto \dots$$

⋮

$$h : 0 \mapsto 3, 2 \mapsto 1, 4 \mapsto 7, 6 \mapsto 9, 8 \mapsto 11, 10 \mapsto 13, 12 \mapsto 15, 14 \mapsto 5, \dots$$

Definiert man (in Relationenschreibweise)

$f' := (f \setminus \{(2, 5)\}) \cup \{(2, 1)\}$ und $g' = (g \setminus \{(1, 2), (3, 8)\}) \cup \{(1, 0), (3, 2)\}$, so erhält man den Kreisfall.

$$0 \mapsto 3 \mapsto 2 \mapsto 1 \mapsto 0$$

Ein sehr viel kürzerer Beweis ist über den Fixpunktsatz von Knaster-Tarski möglich, der uns hier allerdings nicht zu Gebote steht. Wir verweisen auf den Eintrag by Mathworld.

4.3.3 Endliche Folgen und das Mengenprodukt

Wir verweisen zunächst auf Definition 4.2.1.

Satz 4.3.5 Es sei M eine Menge und n eine natürliche Zahl.

Wir legen fest: $M_1 = M_2 = \dots = M_n := M$, sowie $N := M_1 \times \dots \times M_n$. Dann gibt es eine Bijektion zwischen N und $M^{[n]}$.

Beweis: Wir definieren $f : N \rightarrow M^{[n]}$ durch $(x_1, \dots, x_n) \mapsto g$ mit $g(j) = x_{j+1}$ für $j \in [n]$.

Zu jeder Folge $h \in M^{[n]}$ gibt es ein $y = (y_1, \dots, y_n) \in N$ mit $f(y) = h$.

Setze nämlich $y_{j+1} := h(j)$ für $j \in [n]$. Also ist f surjektiv.

Angenommen, es gibt $x = (x_1, \dots, x_n) \in N$ und $y = (y_1, \dots, y_n) \in N$ mit $f(x) = f(y)$.

$f(x)$ bezeichne die Folge g und $f(y)$ die Folge h . Wir nehmen an, dass $g = h$.

Nach Definition von f gilt daher:

$$x_{j+1} = g(j) = h(j) = y_{j+1}$$

für alle $j \in [n]$. Also ist $x = y$, und somit ist f injektiv. \square

4.4 Zur Größe von Mengen

4.4.1 Geschichtliches zum Begriff der Mächtigkeit von Mengen

Auch bereits vor der Einführung der Mengenlehre durch Georg Cantor war beispielsweise im Rahmen kombinatorischer Überlegungen untersucht worden, wie die Mächtigkeit einer endlichen Menge zu bestimmen wäre. Nachdem der formale Rahmen der Mengenlehre geschaffen worden ist, hat Cantor selbst auch sogleich begonnen, unendliche (“transfinite”) Mengen genauer zu untersuchen, siehe [7]. Es ist lehrreich, die wesentlichen Gedanken hierzu im Original zu studieren. Wir zitieren auszugsweise:

“Mächtigkeit” oder “Cardinalzahl” von M nennen wir den Allgemeinbegriff, welcher mit Hilfe unseres activen Denkvermögens dadurch aus der Menge M hervorgeht, dass von der Beschaffenheit ihrer verschiedenen Elemente m und von der Ordnung ihres Gegebenseins abstrahiert wird.

In §6 wird nun ausgeführt:

Die Mengen mit endlicher Kardinalzahl heißen “endliche Mengen”, alle anderen wollen wir “transfinite Mengen” und die ihnen zukommenden Cardinalzahlen “transfinite Cardinalzahlen” nennen.

Die Gesamtheit aller endlichen Cardinalzahlen ν bietet uns das nächstliegende Beispiel einer transfiniten Menge; wir nennen die ihr zukommende Cardinalzahl “Alef-null”, in Zeichen \aleph_0 .

Wie Cantor in seiner Arbeit ausführt, kann man auch mit unendlichen Kardinalzahlen ähnlich wie mit den endlichen rechnen, die den vertrauten natürlichen Zahlen entsprechen. Insbesondere kann man sie addieren und untereinander (mit \leq) vergleichen. Der Vergleichbarkeitssatz sagt aus, dass für zwei verschiedene Mächtigkeiten m_1 und m_2 stets $m_1 \leq m_2$ oder $m_2 \leq m_1$. Dieser so selbstverständlich anmutende Satz ist nicht-trivial und, wie schließlich Friedrich Moritz Hartogs zeigen konnte [22], äquivalent zum Auswahlaxiom.

In unserer Sprechweise ist \aleph_0 die Mächtigkeit der natürlichen Zahlen; eine Menge mit einer derartigen Mächtigkeit sprechen wir auch als abzählbar unendlich an. Aus den üblichen Konstruktionen der reellen Zahlen kann man (verhältnismäßig einfach) schlussfolgern, dass die Menge der reellen Zahlen gleichmächtig ist zur Potenzmenge der natürlichen Zahlen. Aus Satz 3.4.13 können wir schließen, dass

$$\aleph_0 = |\mathbb{N}| < |2^{\aleph_0}| = |\mathbb{R}| = 2^{\aleph_0}$$

gilt. Schon Cantor hat die Frage gestellt, ob es eine Teilmenge $X \subseteq \mathbb{R}$ geben kann mit:

$$|\mathbb{N}| < |X| < |\mathbb{R}|.$$

Wenn man mit \aleph_1 die “zweitgrößte” unendliche Mächtigkeit bezeichnet, ist diese Frage gleichwertig zu der Frage, ob $\aleph_1 = 2^{\aleph_0}$ gilt (oder nicht). Die Feststellung “ $\aleph_1 = 2^{\aleph_0}$ ” ist als *Kontinuumshypothese* bekannt. Aus Resultaten von Kurt Gödel und Paul Cohen folgt, dass diese (selbst in verallgemeinerter Form) unabhängig ist von den üblichen Axiomen der Mengenlehre – abgesehen vom Auswahlaxiom, zu dem die allgemeine Kontinuumshypothese sogar äquivalent ist; wir verweisen hier auf den Übersichtsartikel von Leonard Gillman [18].

4.4.2 Pascalsches Dreieck

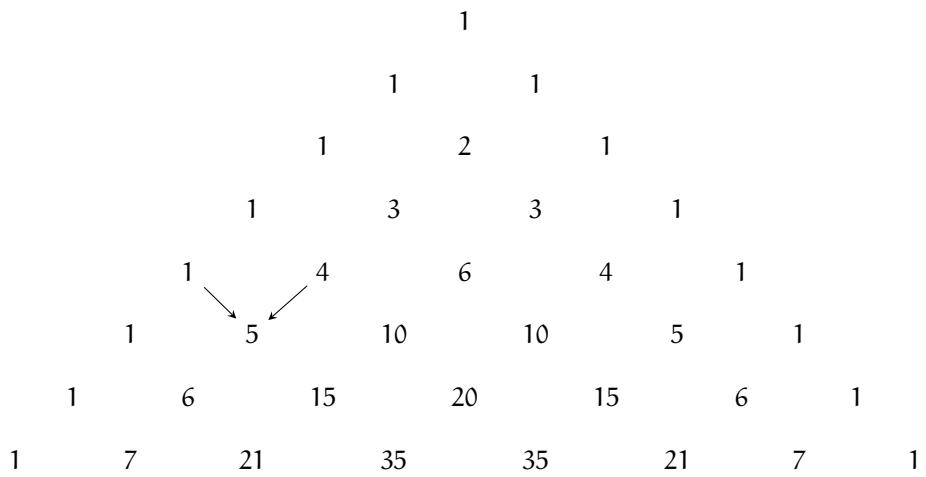


Abbildung 4.1: Die Pfeile veranschaulichen die Bildungsvorschrift beim Pascalschen Dreieck.

Satz 4.4.1 (*Pascalsche Formel*) Es seien $k, m \in \mathbb{N}$, $m \geq 2$, $1 \leq k \leq m$. Dann gilt:

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

Beweis: Wir führen einen kombinatorischen Beweis.

Es sei A eine beliebige $(m+1)$ -elementige Menge und $a \in A$ fest gewählt.

Für jedes k , $1 \leq k \leq m$, lässt sich $\binom{A}{k}$ zerlegen in

$$A_1 = \{X \subseteq A \mid a \in X, |X| = k\} \text{ und } A_2 = \{X \subseteq A \mid a \notin X, |X| = k\}.$$

$$\leadsto \binom{m+1}{k} = \binom{|A|}{k} = \left| \binom{A}{k} \right| = |A_1| + |A_2|.$$

Es gibt offensichtliche Bijektionen von A_1 auf $\binom{A \setminus \{a\}}{k-1}$ und von A_2 auf $\binom{A \setminus \{a\}}{k}$. \leadsto

$$|A_1| + |A_2| = \binom{|A \setminus \{a\}|}{k-1} + \binom{|A \setminus \{a\}|}{k}, \text{ was wegen } |A| = m+1 \text{ die Beh. liefert. } \square$$

4.4.3 Zählen von Färbungen

Ist $G = (V, E)$ ein ungerichteter Graph, so heißt eine Abbildung $c : V \rightarrow [k]$ eine (*echte*) k -Färbung, falls für jede Kante $uv \in E$ gilt: $c(u) \neq c(v)$. Wie viele Möglichkeiten gibt es nun, einen Graphen G zu mit x Farben zu färben? Dieses soll die Funktion $f_G(x)$ angeben. Wenn G gar keine Kanten enthält, ist jede Abbildung $V \rightarrow [k]$ eine k -Färbung, weshalb $f_G(x) = x^n$ gilt, mit $n = |V|$. Um den allgemeinen Fall lösen zu können, betrachten wir zwei Operationen auf Graphen:

- $G - e$ bezeichnet den Graphen, der aus G durch Löschen der Kante $e \in E$ entsteht, d.h., $G - e = (V, E \setminus \{e\})$.
- G/e bezeichnet den Graphen, der aus G durch Verschmelzen der beiden zu e inzidenten Knoten entsteht. Gilt also $e = uv$, so ist $G/e = (V', E')$ mit $V' = V \setminus \{u\}$, $E' = (E \setminus \{xu \mid x \in V\}) \cup \{xv \mid x \in V \wedge xu \in E\}$.

Beachte jetzt, dass

$$f_{G-e}(x) = f_G(x) + f_{G/e}(x)$$

für jede Kante e von G gilt. Jede Färbung von $G - e$ wird nämlich die beiden zu e inzidenten Knoten entweder (wie in G) verschieden färben oder aber (wie in G/e) gleich färben. Daraus ergibt sich:

$$f_G(x) = f_{G-e}(x) - f_{G/e}(x).$$

Da die Graphen $G - e$ und G/e wenigstens eine Kante weniger als G besitzen, können wir diese Vorschrift solange weiter anwenden, bis der Graph keine Kanten mehr besitzt. Von solchen Graphen H wissen wir ja schon, wie f_H aussieht. Mit vollständiger Induktion kann man zeigen:

Satz 4.4.2 Für jeden Graph G mit n Knoten ist $f_G(x)$ ein Polynom vom Grad n .

Beweis: Die Behauptung gilt für jeden kantenlosen Graphen. Das zeigt den Induktionsanfang. Wir nehmen nun an, die Aussage würde für jeden Graphen mit höchstens m Kanten gelten. Betrachte einen Graphen G mit $m+1$ Kanten. Da $G - e$ und G/e höchstens m Kanten besitzen, kann man hierauf die Induktionsvoraussetzung anwenden. Insbesondere ist also $f_{G-e}(x)$ ein Polynom vom Grad n , wobei n die Knotenzahl von G ist, und $f_{G/e}(x)$ ist ein Polynom vom

Grad $n - 1$. Deshalb muss $f_G(x) = f_{G-e}(x) - f_{G/e}(x)$ ein Polynom vom Grad n sein, was die Induktionsbehauptung darstellt. \square

Genauer lässt sich sogar für einen ungerichteten Graphen $G = (V, E)$ mit n Knoten aussagen (Satz von Whitney), dass $f_G(x) = \sum_{i=0}^n (-1)^{n-i} a_{n-i} x^i$ gilt mit $a_0 = 1$, $a_1 = |E|$ und $a_i \geq 0$ für $i = 0, \dots, n$.¹ Aus diesem Grund heißt $f_G(x)$ auch *chromatisches Polynom* von G . Die kleinste natürliche Zahl k mit $f_G(k) > 0$ heißt auch *chromatische Zahl* von G . Sie gibt an, wie viele Farben man zum Färben eines Graphen mindestens benötigt. Mit der chromatischen Zahl hängt ein berühmtes mathematisches Problem zusammen. Ein Graph heißt *planar*, wenn er sich kreuzungsfrei in der Ebene darstellen lässt.² Kenneth Appel und Wolfgang Haken konnten 1976 einen Nachweis darüber führen, dass für jeden planaren Graphen G gilt: $f_G(4) > 0$. Der Vier-Farben-Satz ist das erste (bedeutende) mathematische Resultat, dessen Beweis (nur) mit Computerhilfe gelang.

Ob $f_G(k) > 0$ gilt, kann man für einen Graphen $G = (V, E)$ mit n Knoten selbstverständlich herausbekommen, indem man alle Abbildungen $c : V \rightarrow [k]$ daraufhin überprüft, ob es sich um eine echte Färbung handelt. Ob eine Färbung vorliegt, kann für jede Abbildung c durch $|E|$ viele Vergleiche von Knotenfarben $c(u)$ und $c(v)$ für $uv \in E$ geprüft werden. Das bedeutet aber, k^n solche Überprüfungen im schlimmsten Falle nötig sein müssten. Das ist selbst auf den schnellsten Rechnern für $k = 3$ und $n = 10000$ nicht mehr praktisch durchzuführen. Tatsächlich gehört die Frage, ob $f_G(3) > 0$ gilt, bereits zu einer Art von Problemen, für die man vermutet, dass es keine effizienten Algorithmen hierfür gibt.³

Für sehr kleine k ist die Frage allerdings sehr wohl schnell lösbar. $f_G(1) > 0$ ist offenbar gleichbedeutend damit, dass G gar keine Kanten enthält. Um festzustellen, ob $f_G(2) > 0$ gilt für $G = (V, E)$, kann man zunächst irgendeinen Knoten v mit 0 färben, dann müssen alle Nachbarn von v mit 1 färbbar sein, sodann deren Nachbarn wieder mit 0 usf. Gelingt es, auf diese Weise eine echte Färbung zu konstruieren, ist der Graph zweifärbbar. Falls der Graph zweifärbbar ist, wird das beschriebene Verfahren auch so eine Zweifärbung finden. Ferner gilt (wie man sich überlegen kann):

Lemma 4.4.3 G ist paarer ungerichteter Graph genau dann, wenn $f_G(2) > 0$.

Die chromatische Zahl spielt bei vielen Anwendungen eine Rolle. Nehmen wir an, wir wollen eine gewisse Anzahl von Aufgaben von möglichst wenig Personen erledigen lassen. Konstruieren wir zu den Aufgaben (als Knoten) einen Graphen G , indem wir zwei solche Aufgaben miteinander (durch eine Kante) verbinden, falls sie nicht gleichzeitig von einer Person ausgeführt werden können. Dann ist die chromatische Zahl von G die gesuchte Personenzahl.

4.4.4 Etwas fortgeschrittene Kombinatorik: Das Sonnenblumenlemma von Erdős und Rado

Wir zeigen hier an einem Beispiel, wie kombinatorische Resultate erzielt werden können, die einen anspruchsvoller Beweis erfordern. Das Sonnenblumenlemma von Erdős⁴ und Rado zählt zu den kombinatorischen Lemmas mit den reichhaltigsten An-

¹Etwas mehr hierzu finden Sie z.B. in [8] oder (fast) jedem anderen Buch über Graphtheorie.

²Wir hoffen, diese Erklärung ist verständlich. Eine saubere mathematische Beschreibung dieses scheinbar einfachen Sachverhalts würde diesen Abschnitt deutlich sprengen.

³Technischer gesprochen: Das *Dreifärbungsproblem* für Graphen ist NP-vollständig.

⁴Pál Erdős zählt zu den bedeutendsten Mathematikern des 20. Jahrhunderts; er dürfte der bekannteste Kombinatoriker überhaupt sein.

wendungen in allen Bereichen der Algorithmik und Informatik insgesamt.

Es sei \mathcal{M} eine Menge und $\mathcal{M} \subseteq 2^{\mathcal{M}}$ ein Mengensystem. Ein Teilsystem $\mathcal{S} \subseteq \mathcal{M}$ mit $\emptyset \notin \mathcal{S}$ heißt *Sonnenblume* mit Kern K gdw. $\forall X, Y \in \mathcal{S} : X \cap Y = K \vee X = Y$. Für $X \in \mathcal{S}$ heißt $X \setminus K$ auch *Blütenblatt*.

Satz 4.4.4 (Sonnenblumenlemma) Gibt es ein $s \geq 1$, sodass $\forall X \in \mathcal{M} : |X| = s$, und gilt $|\mathcal{M}| > s!(k-1)^s$, so enthält \mathcal{M} eine Sonnenblume $\mathcal{S} \subseteq \mathcal{M}$ mit wenigstens k Blütenblättern.

Beweis: Wir führen einen Induktionsbeweis über s .

Für $s = 1$ (IA) enthält \mathcal{M} nur einelementige Mengen. Gilt $|\mathcal{M}| > (k-1)$, so ist \mathcal{M} selbst eine Sonnenblume mit leerem Kern und wenigstens k Blütenblättern.

Es sei die Behauptung für $s < t$ gezeigt (IV). Wir zeigen im IS die Gültigkeit für $s = t$.

Betrachte ein Teilsystem $\mathcal{T} \subseteq \mathcal{M}$ mit:

- $\forall X, Y \in \mathcal{T} : X \cap Y = \emptyset \vee X = Y$ sowie
- $\forall Z \in \mathcal{M} \setminus \mathcal{T} \exists X \in \mathcal{T} : Z \cap X \neq \emptyset$.

Gilt $|\mathcal{T}| \geq k$, so ist \mathcal{T} eine Sonnenblume mit leerem Kern und wenigstens k Blütenblättern.

Betrachten wir jetzt den Fall $|\mathcal{T}| < k$.

Bilde die Menge $B = \bigcup\{A \mid A \in \mathcal{T}\}$. Nach Konstruktion gilt: $|B| \leq t \cdot (k-1)$.

Nach dem Schubfachprinzip gibt es ein Element $x \in B$, das in wenigstens

$$\frac{|\mathcal{M}|}{|B|} > \frac{t!(k-1)^t}{t(k-1)} = (t-1)!(k-1)^{(t-1)}$$

vielen Mengen aus \mathcal{M} enthalten ist. Betrachte das Mengensystem

$$\mathcal{M}_x := \{A \setminus \{x\} \mid A \in \mathcal{M} \wedge x \in A\}.$$

Nach Konstruktion gilt $|\mathcal{M}_x| > (t-1)!(k-1)^{(t-1)}$ und $\forall A \in \mathcal{M}_x : |A| = t-1$.

Wir können hierauf also IV anwenden:

\mathcal{M}_x enthält eine Sonnenblume \mathcal{S}_x mit Kern K_x und wenigstens k Blütenblättern.

Damit ist $\mathcal{S} = \{A \cup \{x\} \mid A \in \mathcal{S}_x\}$ eine Sonnenblume in \mathcal{M} mit Kern $K = K_x \cup \{x\}$ mit wenigstens k Blütenblättern. \square

Wir skizzieren jetzt eine Anwendung des Sonnenblumenlemmas. Die Kanten eines ungerichteten Graphen kann man auch als zweielementige Knotenmengen modellieren (siehe auch Lemma 3.6.1). Jeder Graph $G = (V, E)$ beschreibt daher solch ein Mengensystem $\mathcal{M}_E \subseteq 2^V$. Gilt $|E| = |\mathcal{M}_E| > 2 \cdot k^2$, so gibt es eine Sonnenblume $S \subseteq E$ mit wenigstens $k+1$ Blütenblättern. Diese Sonnenblume hängt zusammen mit einem der bekanntesten kombinatorischen Problemen bei Graphen, nämlich der Frage, ob G eine *Knotenüberdeckung* $C \subseteq V$ mit $|C| \leq k$ besitzt. Dabei heißt C Knotenüberdeckung, falls jede Kante von E mindestens einen Knoten aus C als Endknoten hat. Jetzt gibt es zwei Fälle: Falls der Kern K der Sonnenblume leer ist, so haben wir ein System von mindestens $k+1$ Kanten gefunden, die paarweise keinen Endknoten gemein haben. Diese Sonnenblume beweist also, dass G keine Knotenüberdeckung mit höchstens k Knoten haben kann. Falls der Kern K nicht leer ist, so zeigt dasselbe Argument, dass allein zur Überdeckung der $k+1$ Blütenblätter $k+1$ Knoten nötig gewesen wären, was nicht geht, sodass der Kern des Blütenblatts zu C gehören muss. Algorithmisch könnten wir das dadurch ausnutzen, dass wir versuchen, sukzessive immer mehr Knoten in eine Knotenüberdeckung aufzunehmen, zum Beispiel den jeweiligen Kern des Blütenblatts. Wenn wir den Knoten aufgenommen haben, löschen wir ihn samt anliegender Kanten aus dem Graphen und machen mit dem kleineren Graphen und dem kleineren Wert von k weiter. Das Verfahren terminiert, sobald keine genügend großen

Sonnenblumen mehr gefunden werden können. Aus dem Sonnenblumenlemma folgt, dass dann der Graph höchstens $2 \cdot k^2$ viele Kanten besitzen kann. Er ist also (im Vergleich zu k) relativ klein und so hoffentlich verhältnismäßig leicht zu lösen. (Ganz so einfach kann es sowieso nicht werden, da die Problemstellung zu einer Klasse von Problemen gehört, von denen man annimmt, dass es keine (bei jeder Eingabe) effizienten Algorithmen zu ihrer Lösung gibt.)⁵

4.4.5 Etwas fortgeschrittene Kombinatorik: Ramsey-Theorie

Ist $G = (V, E)$ ein ungerichteter Graph, so heißt $G' = (V', E')$ Untergraph von G , falls $V' \subseteq V$ und $E' \subseteq E$. $G = (V, E)$ heißt vollständig, falls $E = V \times V \setminus \Delta_V$, E also größtmöglich ist.

Satz 4.4.5 (Ramsey 1930) Es seien $n_1, n_2 \in \mathbb{N}, n_1, n_2 \geq 2$. Ist $G = (V, E)$ ein vollständiger Graph mit n Knoten, wobei

$$n \geq \binom{n_1 + n_2 - 2}{n_1 - 1},$$

und ist $E_1 \cup E_2 = E$ eine beliebige Zerlegung von E , so enthält $G_1 = (V, E_1)$ einen vollständigen Untergraph mit n_1 Knoten, oder $G_2 = (V, E_2)$ enthält einen vollständigen Untergraph mit n_2 Knoten.

Beweis: Wir führen einen Induktionsbeweis über $N = n_1 + n_2$. Der (kleinste) Fall $N = 4$ ist trivial, da ein vollständiger Graph mit mindestens $\binom{2}{1} = 2$ Knoten eine Kante enthält. Dasselbe Argument gilt für $N = n_1 + n_2 > 4$, sofern $n_1 = 2$ oder $n_2 = 2$ gilt. Betrachten wir also im Induktionsschritt $N = n_1 + n_2 > 4$ unter der Bedingung, dass $n_1 > 2$ und $n_2 > 2$ gilt. Sei also $G = (V, E)$ ein vollständiger Graph mit n Knoten, wobei

$$n = \binom{n_1 + n_2 - 2}{n_1 - 1},$$

und sei $E_1 \cup E_2 = E$ eine beliebige Zerlegung von E . (Wir nehmen jetzt Gleichheit an, da die Satzaussage mit $n \geq \dots$ daraus unmittelbar folgt.)

Wir nehmen als Induktionsvoraussetzung an, dass die Aussage für $N' < N$ gilt bzw. auch im Falle $n_1 = 2$ oder $n_2 = 2$.

Mit Satz 4.4.1 gilt für $n' = \binom{n_1 + (n_2 - 1) - 1}{n_1 - 1}$ und $n'' = \binom{(n_1 - 1) + n_2 - 1}{(n_1 - 1) - 1}$:
 $n = n' + n''$. (*)

Sei $v \in V$ beliebig, sodass v sowohl zu einer Kante aus E_1 als auch zu einer aus E_2 inzident ist. (Gäbe es so ein v nicht, so würden alle Kanten entweder zu E_1 oder zu E_2 gehören, d.h., $E = E_1 \cup E_2$ wäre keine Zerlegung von E .) Für die zu v inzidenten $n - 1$ Kanten gilt wegen (*): (a) wenigstens n' von ihnen gehören zu E_2 oder aber (b) wenigstens n'' von ihnen gehören zu E_1 .

Betrachte Fall (a). Betrachte den vollständigen Untergraph $G' = (V', E')$ von G , der aus den über Kanten aus E_2 zu v benachbarten Knoten besteht. G' hat wenigstens n' viele Knoten. $E'_1 = E_1 \cap E'$ und $E'_2 = E_2 \cap E'$ ist eine Zerlegung von E' aufgrund der Wahl von v . Mit $n'_1 = n_1$ und $n'_2 = n_2 - 1$ gilt $N' = n'_1 + n'_2 < N$ sowie $n'_1, n'_2 \geq 2$, und wir können schließen, dass $G'_1 = (V', E'_1)$ (und damit auch G) einen vollständigen Untergraph mit n'_1 Knoten enthält, oder aber $G'_2 = (V', E'_2)$ enthält einen vollständigen Untergraph H mit n'_2 Knoten; im letzteren Fall bildet H zusammen mit v einen vollständigen Untergraphen von G mit n_2 Knoten, der nur Kanten aus E_2 enthält.

⁵Technischer gesprochen: Das Knotenüberdeckungsproblem für Graphen ist NP-vollständig.

Der Nachweis verläuft im Fall (b) völlig analog. \square

Frank Plumpton Ramsey war äußerst einflussreich in verschiedensten Wissenschaftsbereichen (Logik, Philosophie, Kombinatorik, Volkswirtschaftslehre), was umso erstaunlicher ist, da er schon im Alter von 26 Jahren verstarb. Ein ganzer Zweig der Kombinatorik, die Ramsey-Theorie, geht auf ihn zurück.

Der Satz von Ramsey hat einige erstaunliche Folgerungen bzw. Anwendungen:

- Treffen sich sechs Personen, so gibt es darunter wenigstens drei, die sich gegenseitig kennen oder aber drei, die einander gegenseitig nicht kennen.
- In jeder Folge a_1, \dots, a_n von $n = \binom{2m-2}{m-1}$ paarweise verschiedenen reellen Zahlen gibt es eine monotone Teilfolge der Länge mindestens m .

Betrachte dazu die Knotenmenge $V = \{a_1, \dots, a_n\}$ und die Kanten $E_1 = \{(a_i, a_j) \mid a_i < a_j\}$ (und damit $E_2 = \{(a_i, a_j) \mid a_i > a_j\}$).

- Allgemein definiert man die *Ramsey-Zahl* $R(n_1, n_2)$ als die kleinste Zahl n , für die gilt: Ist $G = (V, E)$ ein vollständiger Graph mit n Knoten und ist $E_1 \cup E_2 = E$ eine beliebige Zerlegung von E , so enthält $G_1 = (V, E_1)$ einen vollständigen Untergraph mit n_1 Knoten, oder $G_2 = (V, E_2)$ enthält einen vollständigen Untergraph mit n_2 Knoten. Der Satz von Ramsey liefert eine obere Schranke für $R(n_1, n_2)$. Die Anwendungen sind natürlich gültig, wenn wir die sich aus den Binomialkoeffizienten ergebenen Ausdrücke ersetzen, z.B. im zweiten Fall durch $R(m, m)$. Genaue Werte für $R(n_1, n_2)$ kennt man nur wenige, z.B. $R(3, 3) = 6$.

4.4.6 Zum Messen von Mengen

Unser Ansatz, die Größe von Mengen im Wesentlichen durch Abzählen zu bestimmen und so Mengen vergleichen zu können, funktioniert anschaulich besonders gut für endliche Mengen. Bei unendlichen Mengen versagt unsere naive Vorstellung aus wenigstens zweierlei Gründen:

- Wir sind es nicht gewohnt, in Kategorien von Kardinalitäten zu denken und uns in diesem Sinne immer größere unendliche Mengen vorzustellen, wie sie ja die Diagonalisierung (Satz 3.4.13) erzeugt.
- Gleichzeitig sind Mengen “gleich groß”, denen wir eher unterschiedliche Größe zugestehen würden, z.B. bildet $f : x \mapsto 2x$ das Einheitsintervall $[0, 1]$ bijektiv auf das “doppelt so große” Intervall $[0, 2]$ ab. Insbesondere scheint dieser Größenbegriff zum Beschreiben und Vergleichen von Längen (oder auch Flächen) ungeeignet zu sein.

In der Mathematik wurde (in Entgegnung des zweiten Einwands) die *Maßtheorie* entwickelt. Diese können und wollen wir hier nicht ausbreiten, aber doch erwähnen, dass sie die theoretische Grundlage sowohl für die Integrations- wie auch für die Wahrscheinlichkeitsrechnung liefert.

Den letztere Bereich wollen wir doch noch etwas vertiefen, indem wir im Folgenden einige Grundlagen zumindest der diskreten Stochastik bereitstellen.

4.4.7 Diskrete Stochastik

Am einfachsten zum Einstieg dürfte sein, zunächst den Abschnitt 5.4.4 über Wahrscheinlichkeitsrechnung, insbesondere bei Gleichverteilungen zu lesen. Grundlegende Definitionen wie Def. 5.4.1 gelten auch allgemeiner als dort verwendet.

Definition 4.4.1 Eine Funktion P , die jedem Elementarereignis $x \in S$ eine nichtnegative Zahl $P(x)$ zuordnet, heißt Wahrscheinlichkeitsfunktion auf S , falls $\sum_{x \in S} P(x) = 1$ gilt. P lässt sich leicht auf Ereignisse verallgemeinern durch $P(A) = \sum_{x \in A} P(x)$.

Satz 4.4.6 Es sei S ein Ereignisraum. Dann gelten die folgenden Eigenschaften:

- $1 \geq P(A) \geq 0$ für jedes Ereignis A .
- $P(A \cup B) = P(A) + P(B)$ für disjunkte Ereignisse A, B .
- $P(B \setminus A) = P(B) - P(A)$ und $P(\bar{A}) \leq P(B)$ für $A \subseteq B$.
- $P(\bar{A}) = P(S \setminus A) = 1 - P(A)$.
- $P(\emptyset) = 0$ und $P(S) = 1$.
- Für jede Folge $(A_n)_{n \in \mathbb{N}}$ paarweise disjunkter Teilmengen von S gilt:

$$P\left(\bigcup_{n \in \mathbb{N}} A_n\right) = \sum_{n \in \mathbb{N}} P(A_n) \quad (\sigma\text{-Additivität})$$

Beweis: Die meisten Eigenschaften folgen unmittelbar aus den Definitionen, wohl mit Ausnahme der σ -Additivität. Hierfür überlegt man sich zunächst die Additivität, also:

$$P\left(\bigcup_{n \in M} A_n\right) = \sum_{n \in M} P(A_n) \quad (\text{Additivität})$$

für alle endlichen Teilmengen M von \mathbb{N} , wobei $(A_n)_{n \in \mathbb{N}}$ paarweise disjunkte Teilmengen von S sind. Daher sind die Folgen $(P(\bigcup_{n \in [N]} A_n))_{N \in \mathbb{N}}$ und $(\sum_{n \in [N]} P(A_n))_{N \in \mathbb{N}}$ identisch. Da sie monoton und beschränkt sind, konvergieren sie gegen einen Grenzwert ≤ 1 . \square

Einfachster Fall: Alle elementaren Ereignisse sind gleichwahrscheinlich und der Ereignisraum ist endlich. Dann gilt: $\forall x \in S : P(x) = 1/|S|$. (Gleichverteilung) Für ein Ereignis $A \subseteq S$ gilt somit:

$$P(A) = \sum_{x \in A} P(x) = \frac{|A|}{|S|}.$$

Mehr, insbesondere Beispiele, finden Sie in Abschnitt 5.4.4.

Bernoulli-Experimente: Münzwürfe mit Wahrscheinlichkeit p für ‘‘Zahl’’ $b(k; n, p)$: Wahrscheinlichkeit, bei n unabhängigen Wiederholungen eines Bernoulli-Versuches mit Wahrscheinlichkeit p für ‘‘Zahl’’ genau k mal ‘‘Zahl’’ zu werfen.

Satz 4.4.7 (Binomialverteilung) $b(k; n, p) = \binom{n}{k} \cdot p^k (1-p)^{n-k}$.

Beweis: durch Induktion über n :

IA: $n = 1 \checkmark$

IV: Die Behauptung gelte für $n = m$.

IB: Die Behauptung gilt für $n = m + 1$.

Es gibt zwei Möglichkeiten, mit $m + 1$ Versuchen genau k Zahlen zu werfen.

1. Im $m + 1$. Versuch wird "Kopf" geworfen, aber in den vorigen m Versuchen genau k -mal Zahl.

2. Im $m + 1$. Versuch wird "Zahl" geworfen und in den vorigen m Versuchen genau $(k - 1)$ -mal Zahl.

$$\begin{aligned} b(k; m+1, p) &= b(k; m, p)(1-p) + b(k-1; m, p)p \\ &= \binom{m}{k} \cdot p^k (1-p)^{m-k} (1-p) + \binom{m}{k-1} \cdot p^{k-1} (1-p)^{m-k+1} p \\ &= \left(\binom{m}{k} + \binom{m}{k-1} \right) p^k (1-p)^{m-k+1} \\ &= \binom{m+1}{k} p^k (1-p)^{(m+1)-k} \end{aligned}$$

Die letzte Gleichung folgt mit Satz 4.4.1. \square

Definition 4.4.2 Es sei S ein Ereignisraum mit Wahrscheinlichkeitsfunktion $P : S \rightarrow \mathbb{R}$. Die bedingte Wahrscheinlichkeit von Ereignis $A \subseteq S$ unter der Voraussetzung, dass Ereignis $P(B) \neq 0$ eintritt, ist definiert als:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Beobachte: $P(A|B) = P(A'|B)$ gdw. $P(A \cap B) = P(A' \cap B)$; dies ist insbesondere dann der Fall, wenn $A \cap B = A' \cap B$ gilt.

\leadsto nur die Wahrscheinlichkeitsverteilung "im Bereich B " ist von Interesse

Lemma 4.4.8 $P_B(x) := P(x)/P(B)$ für $x \in B$ eine ist Wahrscheinlichkeitsfunktion auf dem Ereignisraum B .

Beweis: $\sum_{x \in B} P_B(x) = \sum_{x \in B} P(x)/P(B) = 1$. \square

Diese Deutung der bedingten Wahrscheinlichkeit ist oft bequem.

Beispiel: Münzwurf mit zwei (fairen) Münzen

Ereignisraum $S = \{(Kopf, Kopf), (Kopf, Zahl), (Zahl, Kopf), (Zahl, Zahl)\}$

Wie groß ist die Wahrscheinlichkeit, dass zwei Münzwürfe beide "Kopf" ergeben, wenn man sicher weiß, dass mindestens einer der Würfe "Kopf" ergibt?

$A = \{(Kopf, Kopf)\}$

$B = \{(Kopf, Kopf), (Kopf, Zahl), (Zahl, Kopf)\}$.

$$P(A|B) = \frac{P(A \cap B)}{P(B)} = \frac{P(A)}{P(B)} = \frac{1/4}{3/4} = \frac{1}{3}$$

oder: $P_B((Kopf, Kopf)) = 1/3$ direkt, da $(Kopf, Kopf)$ Elementarereignis der Gleichverteilung über B ist.

Hinweis: Gilt $P(B) \neq 0$, so folgt: A und B sind unabhängig gdw. $P(A|B) = P(A)$.

Dies motiviert: Setze $P(A|B) = P(A)$, falls $P(B) = 0$.

Dann gilt (auch für $P(B) = 0$): $P(A \cap B) = P(B) \cdot P(A|B)$

sowie symmetrisch: $P(A \cap B) = P(A) \cdot P(B|A)$

Aus diesen Überlegungen folgt sofort der *Satz von (Thomas) Bayes*:

$$P(A|B) = \frac{P(A) \cdot P(B|A)}{P(B)}.$$

In der Anwendung oft nützlich:

$$P(B) = P(B \cap A) + P(B \cap \bar{A}) = P(A) \cdot P(B|A) + P(\bar{A}) \cdot P(B|\bar{A}).$$

Beispiel: Eine Anwendung mit (un)fairen Münzen:

Wir haben eine faire Münze und eine unfaire, die immer "Kopf" liefert. Das folgende Zufallsexperiment wird ausgeführt: "Wähle eine der beiden Münzen zufällig (fair) aus und wirf sie zweimal."

Frage: Wie groß ist die Wahrscheinlichkeit dafür, die unfaire Münze ausgewählt zu haben, falls zweimal "Kopf" erscheint ?

A entspricht: die unfaire Münze wurde ausgewählt.

B heißt: Beide Münzwürfe liefern "Kopf".

Wir fragen also nach: $P(A|B)$.

Bekannt: $P(A) = 1/2$; $P(B|A) = 1$; $P(B) = P(A) \cdot P(B|A) + P(\bar{A}) \cdot P(B|\bar{A}) = 5/8$.

Bayes $\leadsto P(A|B) = 4/5$.

Der Satz von Bayes wird in der Praxis in ähnlicher Weise zur Bestimmung von Wahrscheinlichkeiten für nur indirekt beobachtete Ereignisse verwendet.

Erwartungswerte

Satz 4.4.9 (Ungleichung von Markoff) Sei $c > 0$ und X eine ZV mit nichtnegativen Werten. \leadsto

$$P[X \geq c] \leq \frac{E[X]}{c}.$$

Beweis: $P[X \geq c] = \sum_{r \geq c} P[X = r] \leq \sum_{r \geq c} \frac{r}{c} \cdot P[X = r] \leq \sum_{r \geq 0} \frac{r}{c} \cdot P[X = r] = \frac{E[X]}{c}$. \square

Beispiel: (Binomialverteilung)

ZV X : Anzahl der "Erfolge" bei "Erfolgswahrscheinlichkeit" p .

$\leadsto P[X = k] = b(k; n, p)$.

$$\begin{aligned} E[X] &= \sum_{k \in [n+1]} k \cdot b(k; n, p) \\ &= \sum_{k \in [n+1]} k \cdot \binom{n}{k} \cdot p^k (1-p)^{n-k} \\ &= \sum_{k=1}^n k \cdot \frac{n}{k} \cdot \binom{n-1}{k-1} \cdot p^k (1-p)^{n-k} \\ &= n \cdot p \cdot \sum_{k=1}^n \binom{n-1}{k-1} \cdot p^{k-1} (1-p)^{n-k} \\ &= n \cdot p \cdot \sum_{k=0}^{n-1} \binom{n-1}{k} \cdot p^k (1-p)^{n-1-k} \\ &= n \cdot p \cdot \sum_{k=0}^{n-1} b(k; n-1, p) = n \cdot p \end{aligned}$$

Beispiel: (Geometrische Verteilung)

Wir werfen wiederum wiederholt mit einer Münze, die mit Wahrscheinlichkeit p "Kopf" zeigt.

Frage: Wie oft muss man werfen, bis das erst Mal "Kopf" erscheint?

X : ZV, die die Anzahl der nötigen Würfe beschreibt.

Definitionsbereich von X : Menge der endlichen Folgen von Münzwürfen.

$X(e)$ ist dann der Index der ersten Stelle, die "Kopf" ist.

Konkret: $X((\text{Zahl}, \text{Zahl}, \text{Zahl}, \text{Kopf}, \text{Zahl}, \text{Kopf})) = 4$.

Wertebereich von X : Menge der positiven ganzen Zahlen.

$$P[X = k] = (1-p)^{k-1}p$$

$P[X = \cdot]$ ist Wahrscheinlichkeitsfunktion wegen geometrischer Reihe:

$$\sum_{k=1}^{\infty} P[X = k] = \sum_{k=1}^{\infty} (1-p)^{k-1}p = p \cdot \frac{1}{1-(1-p)} = 1.$$

$$E[X] = \sum_{k=1}^{\infty} k \cdot (1-p)^{k-1}p = \frac{p}{1-p} \sum_{k=0}^{\infty} k(1-p)^k = \frac{p}{1-p} \cdot \frac{1-p}{p^2} = \frac{1}{p};$$

erinnere dazu aus der Analysis: $\sum_k \frac{d x^k}{d x} = \frac{d \sum_k x^k}{d x}$.

4.5 Quasiordnungen

4.5.1 Zum Auswahlaxiom der Mengenlehre

Wir haben (wie eingangs erwähnt) einen naiven Zugang zur Mengenlehre gewählt. Das Gegenteil hiervon wäre ein axiomatisch fundierter Zugang gewesen. Das bekannteste derartige Axiomensystem geht auf Zermelo und Fraenkel zurück. In voller Form enthält das dann üblicherweise mit ZFC abgekürzte Axiomensystem auch das Auswahlaxiom. Dieses bedeutet anschaulich, dass man sich aus jeder nicht-leeren Menge jederzeit ein Element "auswählen" kann. Diese scheinbar harmlose Forderung hat tiefgreifende mathematische und auch philosophische Konsequenzen. Dies wollen wir hier nicht vertiefen, aber auf eine äquivalente Forderung eingehen, die sich bei ZFC als Satz ergibt, das (berühmte) Lemma von Zorn.

Jede halbgeordnete Menge, in der jede total geordnete Teilmenge eine obere Schranke besitzt, enthält mindestens ein maximales Element.

Wir wollen jetzt eine Anwendung zeigen; Beweise mit dem Zornschen Lemma folgen nämlich einem typischen Muster. Sie werden diesem Muster noch in mancher Mathematik-Vorlesung begegnen.

Satz 4.5.1 \leq auf den Kardinalzahlen eines festen Universums \mathcal{U} liefert eine lineare Ordnung.

Beweis: Wir verweisen auf Beispiel 3.5.13, was die Halbordnungseigenschaft angeht. Wir müssen noch zeigen, dass für zwei beliebige Mengen $A, B \subseteq \mathcal{U}$ gilt: $|A| \leq |B|$ oder $|B| \leq |A|$. Dazu betrachten wir die Menge

$$\text{einheitig}(A, B) := \{R \subseteq A \times B \mid R \text{ ist vor- und nacheinheitig}\}.$$

Wenn es eine Abbildung in $\text{einheitig}(A, B)$ gibt, dann gibt es eine Injektion $f : A \rightarrow B$, d.h., $|A| \leq |B|$. Nehmen wir also an, eine derartige Injektion gäbe es nicht.

$\text{einheitig}(A, B)$ kann als Menge von Relationen per Inklusion halbgeordnet werden. Wir zeigen jetzt zwei Dinge:

1. Jede total geordnete Teilmenge besitzt eine obere Schranke.

2. Jedes maximale Element ist nachtotal und beschreibt somit eine Injektion $g : B \rightarrow A$.

Sei $K \subseteq \text{eindeutig}(A, B)$ total geordnet (bzgl. Einschluss). Da K eine Menge von Relationen (also von speziellen Mengen) ist, können wir $F = \bigcup\{R \mid R \in K\}$ bilden. Wir zeigen nun, dass $F \in \text{eindeutig}(A, B)$ gilt, woraus folgt, dass F obere Schranke von K ist. Aus Symmetriegründen genügt es zu diskutieren, warum F voreindeutig ist. Betrachte dazu $(a, b), (a', b) \in F$. Aus der Definition von F folgt, dass es R mit $(a, b) \in R$ und R' mit $(a', b) \in R'$ gibt. Da K linear geordnet bezüglich Inklusion ist, gilt $R \subseteq R'$ oder $R' \subseteq R$, also insbesondere gilt: $R \cup R' \in K$. Wir wissen also, dass (a, b) und (a', b) zu der voreindeutigen Relation $R \cup R'$ gehören. Deshalb gilt $a = a'$. Also ist F voreindeutig.

Sei nun G ein maximales Element von $\text{eindeutig}(A, B)$, was nach Punkt 1 und dem Zornschen Lemma existiert. Da wir annehmen, dass $|A| \leq |B|$ nicht gilt, ist G nicht nachtotal. Daher gibt es ein $a_0 \in A$, sodass für kein $b \in B$ gilt, dass $(a_0, b) \in G$. Wir zeigen nun: G ist nachtotal. Wäre das nicht der Fall, so gäbe es ein $b_0 \in B$, sodass für alle $a \in A$ gilt: $(a, b_0) \notin G$. Dann wäre aber $G \cup \{(a_0, b_0)\}$ sowohl vor- als auch nacheindeutig. Daher wäre dann G nicht maximal, im Gegensatz zur Annahme. Daher muss G nachtotal sein. \square

Eine weitere zum Auswahlaxiom äquivalente Aussage ist das *Maximalkettenprinzip von Hausdorff/Birkhoff*: In jeder halbgeordneten Menge gibt es maximale Ketten. Wir geben hierfür jetzt einen Beweis an, fußend auf dem Auswahlaxiom. Dieser wurde zuerst von Frink angegeben [17].

Wir führen einen Widerspruchsbeweis und nehmen an, es gäbe eine Halbordnung (M, \leq) , in der es eine Kette K gibt, die wiederum in keiner maximalen Kette enthalten ist. Da insbesondere K nicht maximal ist, gibt es eine Kette \tilde{K} , die K enthält. Wir können nun Dank des Auswahlaxioms aus $\tilde{K} \setminus K$ ein Element x auswählen, sodass $K' = K \cup \{x\}$ als Restriktion von \tilde{K} eine Kette in M ist. Dieses Argument gilt allgemeiner für alle Ketten C , die K enthalten. Auch hier können wir ein Element $x \notin C$ auswählen, sodass $C' = C \cup \{x\}$ als Restriktion einer C umfassenden Kette \tilde{C} eine Kette in M ist. Wir nennen C' *Nachfolger* von C . Nun wollen wir eine Mengensystem \mathcal{K} vollständig nennen, wenn Folgendes gilt:

- $K \in \mathcal{K}$,
- $C \in \mathcal{K} \implies C' \in \mathcal{K}$ sowie
- Ist $\mathcal{L} \subseteq \mathcal{K}$ ein durch Inklusion linear geordnetes Teilmengensystem von \mathcal{K} , so liegt auch $\bigcup_{L \in \mathcal{L}} L$ in \mathcal{K} . (Vereinigungseigenschaft)

Wir beobachten nun:

1. Die soeben vereinbarte Begriffsbildung ist sinnvoll insofern, als dass ein durch Inklusion linear geordnetes Teilmengensystem $\mathcal{L} \subseteq \mathcal{K}$ tatsächlich erfüllt, dass $\bigcup_{L \in \mathcal{L}} L$ eine K umfassende Kette in M ist.
2. Das aus allen K enthaltenden Ketten bestehende Mengensystem ist vollständig.
3. Ist \mathfrak{K} eine Menge vollständiger Mengensysteme, so ist $\mathcal{J} := \bigcap_{K \in \mathfrak{K}} \mathcal{K}$ ein vollständiges Mengensystem.

\mathcal{J} ist also das kleinste vollständige Mengensystem. Da $K \in \mathcal{J}$, ist $\mathcal{J} \neq \emptyset$.

Wir nennen eine Kette $C \in \mathcal{J}$ *normal*, falls für jede Kette $X \in \mathcal{J}$ gilt: $X \subseteq C \vee C \subseteq X$. C ist also mit jeder Kette aus \mathcal{J} (bzgl. Inklusion) vergleichbar. Beispielsweise ist K normal, denn jede Kette aus \mathcal{J} umfasst K . Wir wollen jetzt zeigen, dass jede Kette in \mathcal{J} normal ist. Für eine normale Kette $C \in \mathcal{J}$ definieren wir das Mengensystem $\mathcal{N}(C) := \{X \in \mathcal{J} \mid X \subseteq C \vee C \subseteq X\}$. Behauptung: $\mathcal{N}(C)$ ist vollständig.

Zunächst ist $K \in \mathcal{N}(C)$, da $K \subseteq C$. Der Nachfolger jeder Kette X aus $\mathcal{N}(C)$ liegt ebenfalls in $\mathcal{N}(C)$. insbesondere gilt daher: $\{C, C'\} \subseteq \mathcal{N}(C)$ (*). Nach Definition von $\mathcal{N}(C)$ gilt für $X \in \mathcal{N}(C)$: $X \subseteq C \vee C' \subseteq X$. Im zweiten Fall ist sicherlich $C' \subseteq X'$. Da C normal und (wegen der Vollständigkeit von \mathcal{J}) $X' \in \mathcal{J}$, folgt $X' \subseteq C \vee C \subseteq X'$. Falls $X' \subseteq C$, so $X' \in \mathcal{N}(C)$. Im einzigen verbliebenen Fall gilt: $X \subseteq C \subseteq X'$. Da sich X und X' nur um ein einziges Element unterscheiden, muss $X = C$ oder $X' = C$ gelten, woraus $X' \in \mathcal{N}(C)$ folgt wegen (*). Die Vereinigungseigenschaft ist offensichtlich.

Da \mathcal{J} minimal war unter allen vollständigen Mengensystemen und $\mathcal{N}(C)$ umfasst, gilt $\mathcal{J} = \mathcal{N}(C)$ für jede normale Kette $C \in \mathcal{J}$. Insbesondere gilt: $\mathcal{J} = \mathcal{N}(K)$.

Wir betrachten nun $\mathcal{N} := \{N \in \mathcal{J} \mid N \text{ ist normal}\}$. Man überlegt sich hierbei rasch, dass \mathcal{N} vollständig ist. Insbesondere ist nämlich jeder Nachfolger einer normalen Kette normal. Da \mathcal{J} minimal, folgt $\mathcal{N} = \mathcal{N}(K) = \mathcal{J}$. \mathcal{J} ist also eine Kette von normalen Ketten. Da \mathcal{J} vollständig, muss sie auch die Vereinigung \bigcup sämtlicher Ketten enthalten, die in \mathcal{J} liegen, und ebenso deren Nachfolger \mathcal{J}' , was aber nicht sein kann. Damit ist der gewünschte Widerspruchsbeweis geführt. \square

4.6 Ungerichtete Graphen

4.6.1 Vom Doppelten Abzählen: Ein kombinatorischer Nachtrag

In der Kombinatorik heißt eine Relation $I \subseteq S \times T$ auch *Inzidenz* und $i = (S, T, I)$ heißt *Inzidenzsystem*. Gilt $(a, b) \in I$, so nennen wir a und b auch (I -)inzident.

Wir führen noch folgende Bezeichnungen ein:

Für $a \in S$ sei $i_1(a)$ die Zahl der mit a inzidenten $b \in T$.

Für $b \in T$ sei $i_2(b)$ die Zahl der mit b inzidenten $a \in S$.

Regel vom Doppelten Abzählen: $\sum_{a \in S} i_1(a) = \sum_{b \in T} i_2(b)$.

Warum gilt die Regel? Veranschaulichung durch *Inzidenzmatrix*:

Für $S = \{a_1, \dots, a_m\}$ und $T = \{b_1, \dots, b_n\}$ stelle $m \times n$ -Matrix $M = (m_{ij})$ auf mit

$$m_{ij} = \begin{cases} 1, & \text{falls } (a_i, b_j) \in I \\ 0, & \text{sonst} \end{cases}$$

$i_1(a_i)$: Zahl der Einsen in der i -ten Zeile

$i_2(b_j)$: Zahl der Einsen in der j -ten Spalte

M ist also, anders gesagt, die Relationenmatrix von I .

Als Anwendung betrachten wir das im Haupttext erwähnte Handschlaglemma: Ist $G = (V, E)$ ein ungerichteter Graph, so gilt: $\sum_{v \in V} d(v) = 2|E|$.

Beweis: Betrachte Inzidenzrelation $I_G = \{(v, e) \in V \times E \mid \exists u \in V : (u, v) = e\}$ für das Inzidenzsystem (V, E, I_G) . Da G ungerichtet, gilt: $i_1(v) = d(v)$, sowie $i_2(e) = 2$ (immer). Daher ist:

$$\sum_{v \in V} d(v) = \sum_{v \in V} i_1(v) = \sum_{e \in E} i_2(e) = 2|E|.$$

\square

Als weitere (vielleicht überraschendere) Anwendung betrachten wir die Aufgabe, die durchschnittliche Anzahl der Teiler der Zahlen $1, \dots, n$ zu bestimmen.

$t(n)$: Zahl der Teiler der Zahl n

$\bar{t}(n) = \frac{1}{n} \sum_{j=1}^n t(j)$: Durchschnittliche Anzahl der Teiler der Zahlen $1, \dots, n$

Inzidenzsystem: $S = T = \{1, \dots, n\}$ mit $I = |$ (Teilerrelation).

Offenbar gilt: $\iota_2(j) = t(j)$ für $j \leq n$.

Ebenso leicht: $\iota_1(j) = \lfloor \frac{n}{j} \rfloor$.

$$\leadsto \bar{t}(n) = \frac{1}{n} \sum_{j=1}^n \iota_2(j) = \frac{1}{n} \sum_{j=1}^n \iota_1(j) \approx \sum_{j=1}^n \frac{1}{j} \approx \ln(n) \text{ (Harmonische Reihe)}$$

Wer mehr über die *Harmonische Reihe* wissen möchte, findet viele Informationen im entsprechenden Wikipedia-Eintrag, einschließlich eines netten Beitrags über die Konstruktion von Türmen von gleichartigen Klötzen mit größtmöglichem Überhang.

4.6.2 Geschichtliche, informatische und sprachliche Anmerkungen zu Graphen

Die Graphentheorie nahm ihren Ausgangspunkt in den Untersuchungen Eulers zum Königsberger Brückenproblem (siehe Abschnitt 5.2.3) und zu der Theorie der Polyeder (Vielfläche). Der Begriff "Graph" selbst wurde aber wohl von englischen Mathematikern geprägt, wie die Ausführungen Petersens [34] andeuten. In der erwähnten Arbeit des dänischen Mathematikers Petersen wird im Übrigen auch erläutert, was der Begriff des "Grades eines Graphens" mit dem den Meisten geläufigen des "Grades eines Polynoms" zu tun haben.

Der Begriff des Zusammenhangs zeigt deutlich die Urverwandtschaft von Graphentheorie und Topologie, wobei letztere heute ein Zweig der Analysis ist. Teile der Graphentheorie wenigstens waren früher unter dem Begriff "Analysis situs", also "Analysis der Lage" bekannt, bevor sich hieraus im Wesentlichen die Topologie entwickelte.

"Zusammenhang" und verwandte Begriffe haben leicht ersichtliche Anwendungen, wenn es z.B. um die Zuverlässigkeit von Computernetzen geht. Weniger naheliegend erscheint vielleicht die Computergraphik, aber man denke daran, dass sich Pixelbilder als gitterartige Graphen auffassen lassen, und dann könnte "Zusammenhang" bei der Interpretation der "Füllfunktion" bei Malprogrammen dienen.

Leider sind die Bezeichnungen im Bereich der Graphentheorie recht uneinheitlich. Wir haben in diesem Skript z.B. das Wort "Pfad" anstelle von dem wohl üblicheren "Weg" gewählt, weil es doch der Abkürzung P_n näher steht. Nicht-Standard ist in dem Zusammenhang, dass konkrete Pfade bzw. Kreise als "Modelle" vorgegeben werden. Die Schwierigkeiten einer sauberen Definition werden offenkundig, wenn man sich einmal die am 29.12.2014 in der deutschen Wikipedia abrufbaren Definitionen anschaut:

- Ein nicht-leerer Graph W , mit der Knotenmenge $\{x_1, x_2, \dots, x_n\}$ und der Kantenmenge $\{\{x_1, x_2\}, \{x_2, x_3\}, \dots, \{x_{n-1}, x_n\}\}$, heißt Weg, wenn die Knoten x_i paarweise verschieden sind.
- Ist $G = (V, E)$ ein Graph, dann heißt ein Weg (v_1, \dots, v_n) mit $v_i \in V$ für $i = 1, \dots, n$ Zyklus, wenn $v_1 = v_n$ gilt. In einem Zyklus müssen also Start- und Endknoten des Weges übereinstimmen.
- Entsprechend dazu heißt ein Zyklus (v_1, \dots, v_n) in einem Graphen Kreis, wenn (v_1, \dots, v_{n-1}) ein Pfad ist. Ein Kreis ist damit ein Zyklus, bei dem nur Start- und Endknoten gleich sind, es gilt also zusätzlich $v_i \neq v_j$ für $i, j \in \{1, \dots, n-1\}$ mit $i \neq j$.

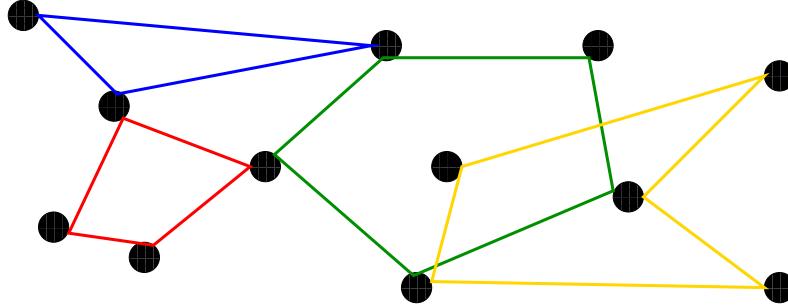


Abbildung 4.2: Ein Eulerscher Graph mit zugehöriger Kreiszerlegung.

In der Definition von "Weg" ist klar gesagt, dass die Knoten paarweise verschieden sein sollen. Wenn wir jetzt man kurzfristig akzeptieren, dass wir solche Wege (also unsere Pfade) gleichwertig mit einer Folge von Knoten beschreiben kann, so sind die nächsten beiden Punkte nur sinnvoll, wenn wir bei Wegen (doch) Wiederholungen von Knoten zulassen, bei Pfaden hingegen nicht, obwohl der Link von "Pfad" auf den Eintrag für "Weg" verweist. Diese Ausführungen sollen nur unterstreichen, dass man oft doch genauer lesen muss, um manche Lexikoneinträge richtig lesen zu können. Konsistenz ist nicht unbedingt eine Stärke solcher nicht zentral koordinierter Systeme.

Sehr unterschiedliche Einführungen in das mitlerweile sehr reiche Gebiet der Graphentheorie findet der Interessierte in [41, 42, 43].

4.6.3 Eulersche Graphen

Wir erinnern zunächst an das Königsberger Brückenproblem in Abschnitt 5.2.3. Dort ging es darum, in einem (Multi-)Graphen einen Rundgang zu finden, der alle Kanten (das sind in der Anwendung die Brücken) genau einmal aufsucht, die Knoten (in der Anwendung die verschiedenen Stadtteile von Königsberg) aber mehrfach besuchen darf.

Das motiviert die folgende Definition:

Definition 4.6.1 Eine Folge e_1, \dots, e_m von Kanten eines Graphen $G = (V, E)$ heißt Eulerzug gdw. (1) $E = \{e_1, \dots, e_m\}$, (2) $m = |E|$, (3) $\forall i \in \{1, \dots, m-1\} : e_i \cap e_{i+1} \neq \emptyset$.

(1) und (2) stellen sicher, dass jede Kante von G genau einmal in der Folge gelistet wird, und (3) besagt, dass in der Folge benachbarte Kanten einen gemeinsamen Knoten haben. Hierbei verwenden wir die Auffassung, dass Kanten zweielementige Teilmengen von V sind.

Definition 4.6.2 Ein zusammenhängender Graph heißt Eulersch gdw. der Grad jedes Knotens ist gerade.

Beispielsweise sind Kreise offenkundig Eulersche Graphen.

Satz 4.6.1 Ein zusammenhängender Graph $G = (V, E)$ der Ordnung $n \geq 3$ ist Eulersch gdw. E lässt sich zerlegen in E_1, \dots, E_k , sodass jeder Graph $G_i = (V, E_i)$ ein Kreis ist.

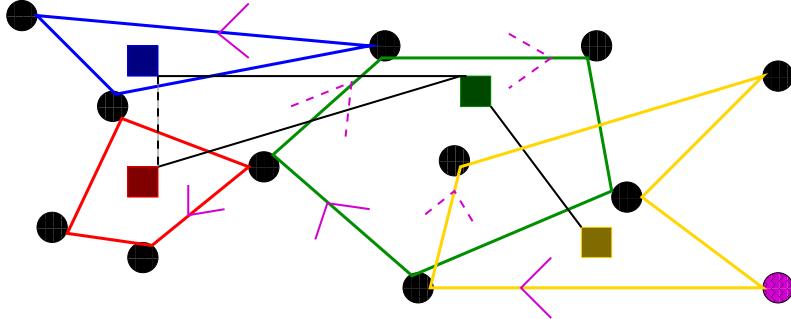


Abbildung 4.3: Ein Eulerscher Graph mit zugehöriger Kreiszerlegung. Weiter ist der Hilfsgraph (bestehend aus den Kreisen als Knoten) aus dem Beweis von Satz 4.6.2 mit quadratischen Knoten eingetragen. Die Kanten des bei Gelb verwurzelten Spannbaums sind durchgezogen gezeichnet. Der Eulerzug startet nun bei dem Magenta gekennzeichneten Knoten des gelben Kreises, wechselt sodann (den durchgezogenen magenta Pfeilen folgend) auf den grünen Kreis und danach auf den roten Kreis. Der Zug kehrt dann auf den grünen Kreis zurück, dem gestrichelten magenta Pfeil folgend, und wechselt dann auf den blauen Kreis und wieder zurück auf den grünen, dem nächsten gestrichelten magenta Pfeil folgend. An dem Knoten, der anfangs den Wechsel vom gelben zum grünen Kreis markiert hatte, wird schließlich der gelbe Kreisdurchlauf wieder aufgenommen (gestrichelter magenta Pfeil), bis der magenta Ausgangspunkt wieder erreicht wird.

Wir sprechen die Zerlegung aus dem Satz auch als “Kreiszerlegung” an. Bild 4.2 soll den Satz illustrieren. Überlegen Sie: Wie könnte hier ein Eulerzug aussehen?

Beweis: Klar: Wenn eine Kreiszerlegung existiert, sind alle Grade gerade.

Ein Kreis der Länge drei ist der kleinste Graph, der Eulersch ist und eine triviale Kreiszerlegung besitzt.

Per Induktion zeigen wir stärker: Jeder Graph mit lauter geradgradigen Knoten, der keinen Knoten vom Grad Null besitzt, hat eine Kreiszerlegung.

Angenommen, jeder Graph mit höchstens m Kanten erfüllt die Behauptung.

Betrachte einen Graphen $G = (V, E)$ mit lauter geradgradigen Knoten ohne Grad-0-Knoten mit $m + 1$ Kanten.

Wähle einen beliebigen Knoten $x_0 = y_0$, zwei seiner Nachbarn x_1, y_1 , und (induktiv) einen Nachbarn x_{i+1} von x_i , der ungleich x_{i-1} ist, sowie einen Nachbarn y_{i+1} von y_i , der ungleich y_{i-1} ist, bis ein Nachbarknoten x_j (oder y_j) gewählt werden kann, der bereits bezeichnet wurde. Dies muss eintreten, da beim “Betreten” eines Knotens nur eine inzidente Kante “benutzt” wurde, ein “Verlassen” dieses Knoten aufgrund seines geraden Grades über eine “unbenutzte” Kante also stets möglich ist, der Prozess aufgrund der Endlichkeit des Graphens aber abbrechen muss.

Ist nun $x_j = x_i$ für $i < j$, so beschreibt die Knotenfolge x_i, x_{i+1}, \dots, x_j einen Kreis.

Ist $x_j = y_i$, so beschreibt $y_i, y_{i-1}, \dots, y_0 = x_0, x_1, \dots, x_j$ einen Kreis.

Entferne die Kanten des so erhaltenen Kreises aus G sowie Knoten, die nunmehr Grad Null haben.

Dieser neue Graph G' besitzt eine Kreiszerlegung nach Induktionsannahme.

Diese liefert zusammen mit dem “neuen Kreis” eine Kreiszerlegung für G . \square

Satz 4.6.2 Sei $G = (V, E)$ ein zusammenhängender Graph. G ist Eulersch gdw. G besitzt einen Eulerzug.

Beweis: Besitzt G einen Eulerzug, so hat jeder Knoten geraden Grad: Jedesmal, wenn ein Knoten auf einem “Rundgang” betreten wird, muss er auch gleich wieder verlassen werden, sodass zu jedem Knoten eine gerade Anzahl von Kanten incident ist.

Ist umgekehrt G Eulersch, so besitzt G nach Satz 4.6.1 eine Kreiszerlegung E_1, \dots, E_k .

Die nun folgende Konstruktion ist in Bild 4.3 illustriert.

Bilde neuen Graphen $G' = (V', E')$ mit $V' = \{E_1, \dots, E_k\}$ und $E_i E_j$ ist eine Kante in E' gdw. die durch E_i und E_j beschriebenen Kreise haben einen gemeinsamen Knoten. Also gibt es eine Abbildung $\kappa : E' \rightarrow V$, die $E_i E_j$ einen gemeinsamen Knoten zuordnet. (Kreuzen sich die Kreise mehrmals, so ist die Auswahl des Knotens durch κ willkürlich.) Da G zusammenhängend ist, ist auch G' zusammenhängend. Sei $G'' = (V'', E'')$ ein Gerüst von G' . Starte in beliebigem Knoten w von G'' (“Wurzel”) und beschreibe einen “Lauf” durch G'' mittels “Tiefensuche”. Beachte hierbei “zyklische Ordnung” auf den Kindknoten, die durch Kreis (in G) vorgegeben ist.

(Wir können G'' also auch als gerichteten geordneten Baum auffassen, wie er uns demnächst häufiger begegnen wird.)

Mithilfe von κ lässt sich der G'' -Lauf als Eulerzug in G deuten. \square

Unsere Kennzeichnungen für Graphen mit Eulerzügen lassen sich auch leicht auf Multigraphen übertragen. Bereits in Abschnitt 5.2.3 wurde gezeigt, wie man einen Multigraphen durch Unterteilung aller Kanten in einen schlichten Graphen überführen kann. Dieser (neue) Graph hat einen Eulerzug genau dann, wenn der ursprüngliche Multigraph einen hatte. Damit können wir schließlich schlussfolgern, dass das Königsberger Brückenproblem keine Lösung besitzt.

4.6.4 Matroide

Wir versuchen, eine allgemeine Form der Probleme zu finden, bei denen ein Greedy-Verfahren anwendbar ist:

Definition 4.6.3 E sei endliche Menge, \mathcal{U} sei eine Menge von Teilmengen von E . Die Struktur (E, \mathcal{U}) heißt Teilmengensystem, wenn

- $\emptyset \in \mathcal{U}$
- $A \subseteq B \wedge B \in \mathcal{U} \Rightarrow A \in \mathcal{U}$

M.a.W.: \mathcal{U} ist (bzgl. \supseteq) eine Oberhalbmenge.

Beispiel: Eine Menge $I \subseteq V$ heißt unabhängig im Graphen $G = (V, E)$ gdw. zwei verschiedene $x, y \in I$ sind nicht durch eine Kante verbunden.

Die unabhängigen Knotenmengen bilden ein Teilmengensystem.

$w : E \rightarrow \mathbb{R}$ sei eine Gewichtsfunktion, gesucht wird eine in \mathcal{U} maximale Menge T (bzgl. \subseteq) mit maximalem Gesamtgewicht

$$w(T) = \sum_{e \in T} w(e)$$

In unserem Beispiel hatten wir im Haupttext ein Minimierungsproblem betrachtet. Dieses lässt sich durch Einführen negativer Gewichte (also z.B. -5 statt 5) leicht in ein offensichtlich äquivalentes Maximierungsproblem überführen.

Charakterisierung der Probleme, die Greedy-Algorithmus optimal löst

Data : (E, \mathcal{U}) : a subset system with weights $w : E \rightarrow \mathbb{R}$
Result : T : set of elements that is maximal in \mathcal{U} such that $w(T) = \sum_{e \in T} w(e)$ is maximum

- 1 k : integer;
- 2 Order the elements decreasingly such that $E = \{e_1, \dots, e_n\}$ with $w(e_1) \geq w(e_2) \geq \dots \geq w(e_n)$;
- 3 Initialize $T \leftarrow \emptyset$;
- 4 **for** $k \leftarrow 1$ **to** n **do**
- 5 **if** $(T \cup \{e_k\}) \in \mathcal{U}$ **then**
- 6 $T \leftarrow T \cup \{e_k\}$;

Abbildung 4.4: A canonical greedy algorithm

Definition 4.6.4 Ein Teilmengensystem (E, \mathcal{U}) heißt Matroid wenn zusätzlich die Austauscheigenschaft gilt:

$$A, B \in \mathcal{U} \wedge |A| < |B| \Rightarrow (\exists x \in B \setminus A) A \cup \{x\} \in \mathcal{U}$$

- ‘Matroid’ verallgemeinert Begriff ‘(lineare) Unabhängigkeit’
- In Matroiden haben maximale Mengen gleiche Mächtigkeit!
- Unabhängige Knotenmengen in Graphen bilden i.Allg. kein Matroid.

Beispiel für Matroide:

- $E = [n]$, $\mathcal{U}_k = \bigcup_{i=0}^k \binom{[n]}{i}$ für $k, n \in \mathbb{N}$ mit $k \leq n$.
- E : endliche Menge von Vektoren,
 \mathcal{U} : linear unabhängige Teilmengen von E
(z.B.: E besteht aus Spalten einer Matrix, daher auch ‘Matroid’)
- E : Kantenmenge eines endlichen Graphen G ,
 \mathcal{U} : kreisfreie Teilmengen von E
(auch *graphisches Matroid* genannt)
Maximale Elemente von \mathcal{U} sind aufspannende Wälder von G .
Ein Wald ist ein Graph, in dem jeder zusammenhängende Untergraph ein Baum ist.

Bedeutung der Austauscheigenschaft:

- A und B seien maximale Elemente im Matroid (E, \mathcal{U})
- Damit $|A| = |B|$
- Falls $A \neq B$:
 - Wähle $a \in A \setminus B$.
 - Zu $A \setminus \{a\}$ gibt es $b \in B \setminus A$ mit $A' := A \setminus \{a\} \cup \{b\} \in \mathcal{U}$.
 - $A' \setminus B$ ist kleiner als $A \setminus B$, $A' \cap B$ ist größer als $A \cap B$.
- Also: Man kann A durch Austausch einzelner Elemente schrittweise in B umwandeln, ohne dabei \mathcal{U} zu verlassen!

Satz 4.6.3 Sei (E, \mathcal{U}) ein Teilmengensystem.

Der kanonische Greedy-Algorithmus liefert beim Optimierungsproblem genau dann für jede beliebige Kostenfunktionen $w : E \rightarrow \mathbb{R}$ die optimale Lösung, wenn (E, \mathcal{U}) ein Matroid ist.

Folgerung 4.6.4 Der beschriebene Greedy-Algorithmus findet Gerüste mit größtmöglichen Gewicht in kantengewichteten Graphen.

Beweis: “ \Leftarrow ”:

Vorausgesetzt wird: (E, \mathcal{U}) Matroid, $w : E \rightarrow \mathbb{R}$ Gewichtsfunktion.

O.B.d.A.: bereits Ordnung $w(e_1) \geq w(e_2) \geq \dots \geq w(e_n)$ vorhanden.

$T = \{e_{i_1}, \dots, e_{i_k}\}$ sei Lösung durch Greedy-Algorithmus.

Annahme: Greedy-Algorithmus liefert nicht die optimale Lösung.

$T' = \{e_{j_1}, \dots, e_{j_k}\}$ sei bessere Lösung, d.h., $w(T') > w(T)$.

O.B.d.A.: $i_1 < i_2 < \dots < i_k$ und $j_1 < j_2 < \dots < j_k$.

Also existiert minimales μ mit $w(e_{j_\mu}) > w(e_{i_\mu})$, insbesondere dabei $j_\mu < i_\mu$.

Wende Austauscheigenschaft auf $A = \{e_{i_1}, \dots, e_{i_{\mu-1}}\}$ und $B = \{e_{j_1}, \dots, e_{j_\mu}\}$ an:

Es gibt daher $e_{j_\sigma} \in B \setminus A$ mit $A \cup \{e_{j_\sigma}\} \in \mathcal{U}$.

Mit $\sigma \leq \mu$ jedoch $w(e_{j_\sigma}) \geq w(e_{j_\mu}) > w(e_{i_\mu})$, d.h.,

Greedy-Algorithmus hätte e_{j_σ} vor e_{i_μ} in T aufnehmen müssen. Widerspruch!

Indirekter Beweis von “ \Rightarrow ”:

- Annahme: Austauscheigenschaft gilt nicht,
aber Greedy liefert für jedes w optimale Lösung.
- Also gibt es $A, B \in \mathcal{U}$ mit $(\forall b \in B \setminus A) A \cup \{b\} \notin \mathcal{U}$.
- Setze $r := |B|$ und betrachte folgende Kostenfunktion w :

$$w(e) := \begin{cases} r+1, & e \in A \\ r, & e \in B \setminus A \\ 0, & \text{sonst} \end{cases}$$

- Greedy-Algorithmus: Lösung T mit $A \subseteq T$ und $T \cap (B \setminus A) = \emptyset$.
- Wegen $B \in \mathcal{U}$ gibt es auch eine Lösung T' mit $B \subseteq T'$
- Dann jedoch

$$\begin{aligned} w(T) &= (r+1) \cdot |A| \leq (r+1) \cdot (r-1) = r^2 - 1 \\ w(T') &\geq r \cdot |B| = r^2 \end{aligned}$$

Also $w(T) < w(T')$, d.h. Greedy versagt bei diesem w . Widerspruch!

□

Rang in Matroiden: Eine Kennzeichnung von Matroiden

Die Austauscheigenschaft besagt, dass man zu einem Matroid $M = (E, \mathcal{U})$ eine Zahl $r(E)$ zuordnen kann, genannt *Rang* oder *Dimension* von M , nämlich die Anzahl von Elementen in einer maximalen unabhängigen Menge von M . Da mit M und $A \subseteq E$ auch $M_A = (A, \{U \in \mathcal{U} \mid U \subseteq A\})$ ein Matroid ist, kann man allgemeiner $r(A)$ definieren. Diese Abbildung $r : 2^E \rightarrow \mathbb{Z}$ erfüllt:

1. $\forall A \subseteq E : 0 \leq r(A) \leq |A|$,
2. $\forall A, B \subseteq E : r(A \cap B) + r(A \cup B) \leq r(A) + r(B)$ (Submodularität)
3. $\forall A \subseteq E, x \in E : r(A) \leq r(A \cup \{x\}) \leq r(A) + 1$ (Monotonie)

Hat man umgekehrt eine Abbildung $r : 2^E \rightarrow \mathbb{Z}$ mit diesen Eigenschaften, so bildet $M = (E, \{A \subseteq E \mid \exists B \subseteq E : A \subseteq B \wedge r(B) = |B|\})$ ein Matroid.

Hüllen in Matroiden: Eine weitere Kennzeichnung von Matroiden

Es sei $M = (E, \mathcal{U})$ ein Matroid und $r : 2^E \rightarrow \mathbb{Z}$ ihre Rangfunktion.

Definiere

$$\text{cl}(A) := \{x \in E \mid r(A) = r(A \cup \{x\})\}.$$

Dann ist $\text{cl} : 2^E \rightarrow 2^E$ ein Hüllenoperator,⁶ der außerdem erfüllt:

$$\forall a, b \in E \forall Y \subseteq E : (a \in \text{cl}(Y \cup \{b\}) \setminus \text{cl}(Y)) \implies (b \in \text{cl}(Y \cup \{a\}) \setminus \text{cl}(Y))$$

Ist andererseits $\text{cl} : 2^E \rightarrow 2^E$ ein Hüllenoperator mit der zuletzt beschriebenen Austauschegenschaft, so definiert

$$M = (E, \{A \subseteq E \mid \forall x \in A : \text{cl}(A \setminus \{x\}) \neq \text{cl}(A)\})$$

ein Matroid.

Abschließende Bemerkungen

Maximale unabhängige Mengen in Matroiden ähneln “Basen” (und werden auch so genannt). Diese werden Ihnen so im Bereich der Linearen Algebra wieder begegnen. Der Begriffs des “Rangs” entspricht dann dem “Rang” einer Matrix im Sinne der Dimension des von den Spaltenvektoren aufgespannten Unterraums; dieser aufgespannte Unterraum ist das “Erzeugnis” im Sinne des assoziierten Hüllenoperators.

Kann man einfach testen, ob eine endliche Menge unabhängig ist, so kann man mit dem Greedy-Algorithmus auch einfach eine Basis eines solchen Unterraums berechnen.

4.7 Verknüpfungen

4.7.1 Anmerkungen zur Algebra

Algebra als “Buchstabenrechnen” ist von der Schule her geläufig. Dort sollte Ihnen auch bewusst geworden sein, wie wichtig es ist, sich genau zu überlegen, unter welchen Umständen welche Rechenoperationen zulässig sind. Ziel derartiger algebraischer Umformungen ist in der Regel das Auflösen von Gleichungen. An und für sich ist diese Methodik seit altersher bekannt: schon Babylonier, Ägypter und Griechen sowie Chinesen, Inder und Araber haben diese studiert. So leitet sich auch der Begriff selbst “Al-gabr” aus dem Arabischen ab, was sich im Titel eines mathematischen Werkes des persischen Gelehrten al-Chwarizmi (Wirkungszeit: erste Hälfte des 9. Jahrhunderts) fand. Für Informatiker mag von Interesse sein, dass sein Name in latinisierter Form zum Hauptgegenstand ihres Faches geworden ist: der Algorithmus.

Die Ihnen von der Schule vertrauten algebraischen Regeln beziehen sich zumeist auf das Rechnen mit Zahlen, auch wenn Sie vermutlich auch das Rechnen mit (Zahl-)Vektoren gelernt haben. In den voranstehenden Kapiteln haben wir auch etliche Rechenregeln für Mengen und Relationen vorgestellt.

Das Studium von Rechengesetzen im Abstrakten lässt sich mathematisch am einfachsten durchführen, wenn wir die wesentlichen (uns aus zahlreichen Beispielen nun vertrauten) Eigenschaften von Operationen (Verknüpfungen) isoliert betrachten. Was können wir schlussfolgern, wenn Operationen assoziativ oder kommutativ sind? Diese minimalistische und möglichst verallgemeinernde Vorgehensweise ist typisch für die moderne Mathematik, kann doch nur so der eigentliche Kern von Einsichten kurz und knapp dargelegt werden, deren Tragweite sich erst erschließt, wenn man beachtet,

⁶Siehe Abschnitt 3.8

dass bei weniger abstrakter Betrachtungsweise die grundlegenden Eigenschaften von Operationen in jedem Spezialfall neu überlegt und begründet werden müssten.

Dieser Abschnitt kann nur einen kleinen Einblick in das weite Feld der Algebra bieten. Kapitel 8 zeigt eine weitergehende Einbettung der Mengenalgebra (und auch der Algebra der Aussagenlogik) als eine mögliche Algebra mit mehr als einer Grundoperation.

Sollten Sie vertieftes Interesse an der Algebra mit Blick auf die Informatik haben, so möchten wir Ihnen anraten, die Bücher von Ihringer [25, 26] oder auch von Dencke [11] oder von Diekert, Kufleitner und Rosenberger [12] zu lesen. Dort werden auch zahlreiche weitere informatische Anwendungen der algebraischen Sprech- und Denkweisen besprochen.

4.8 Hüllen

4.8.1 Topologische Gedanken

Als Erster hat K. Kuratowski einen Begriff der Hülle axiomatisch gefasst [29, 35]. Allerdings ist sein Begriff etwas enger.

Definition 4.8.1 Es sei U ein Universum. Ein Kuratowski-Hüllenoperator ist eine Abbildung $\bar{H} : 2^U \rightarrow 2^U$, die A ihre Kuratowski-Hülle $\bar{H}(A)$ zuordnet und folgende Gesetze erfüllt (für beliebige $A, B \subseteq U$):

1. $\bar{H}(A \cup B) = \bar{H}(A) \cup \bar{H}(B)$;⁷
2. $A \subseteq \bar{H}(A)$;
3. $\bar{H}(\emptyset) = \emptyset$;
4. $\bar{H}(\bar{H}(A)) = \bar{H}(A)$.

Satz 4.8.1 Jeder Kuratowski-Hüllenoperator ist ein Hüllenoperator.

Beweis: Zu zeigen bleibt noch die Monotonie, da sowohl Extensivität als auch Idempotenz ausdrücklich gefordert werden. Gilt $A \subseteq B$, so auch (nach Satz 3.1.12) $A \cup B = B$ und mithin $\bar{H}(A \cup B) = \bar{H}(B)$. Weiter gilt aber $\bar{H}(A \cup B) = \bar{H}(A) \cup \bar{H}(B)$, zusammen also $\bar{H}(A) \cup \bar{H}(B) = \bar{H}(B)$, woraus (nach Satz 3.1.12) $\bar{H}(A) \subseteq \bar{H}(B)$ folgt. \square

Tatsächlich gibt es aber Hüllenoperatoren, die keine Kuratowski-Hüllenoperatoren sind, da sie das dritte Axiom nach der Zählung von Kuratowski verletzen, z.B. sind beliebige konstante Mengenabbildungen Hüllenoperatoren, aber nur die Abbildung, die stets (konstant) auf die leere Menge abbildet, ist ein Kuratowski-Hüllenoperator. Überdies erfüllt jeder Hüllenoperator $H : 2^U \rightarrow 2^U$ aufgrund er Monotonie:

$$H(A) \cup H(B) \subseteq H(A \cup B),$$

aber nicht notwendigerweise die andere Inklusionsrichtung. Betrachte z.B. das Universum $U = \{a, b, 0, 1, 2\}$ und den Operator

$$H(A) = \begin{cases} A, & \text{falls } A \cap \{0, 1, 2\} \neq \emptyset, \\ A \cup [|A|], & \text{falls } A \subseteq \{a, b\} \end{cases}$$

⁷Wenn man den ersten Beweis von Kuratowski liest, merkt man, dass seinem notierten Axiom ein Hüllenoperatorzeichen fehlt; in diesem Sinne steht es auch im erwähnten Buch von Rinow.

Damit gilt:

$$H(\{a\}) \cup H(\{b\}) = \{a, 0, 1\} \cup \{b, 0, 1\} = \{a, b, 0, 1\} \neq H(\{a, b\}) = U.$$

Die Hüllenaxiome weist man leicht nach.

Kuratowski-Hüllen eignen sich zur Definition abstrakter Topologien. Diese wiederum verallgemeinern die topologischen Grundbegriffe, wie Sie sie aus der Analysis (beispielsweise) kennen. Mehr dazu finden Sie in Lehrbüchern über Topologie wie z.B. [15, 35]. Wenn wir (wieder) festlegen, dass eine Menge A abgeschlossen heißen soll, wenn $\bar{H}(A) = A$ gilt, dann kann man zu jedem Kuratowski-Hüllenoperator \bar{H} ein System \mathfrak{M} abgeschlossener Mengen assoziieren. Dieses ist nach den Vorüberlegungen ein abgeschlossenes System, das die leere Menge enthält und überdies erfüllt:

$$\forall A, B \in \mathfrak{M} : A \cup B \in \mathfrak{M}.$$

Es gilt nämlich für $\bar{H}(A)$:

$$\bar{H}(A \cup B) = \bar{H}(A) \cup \bar{H}(B) = A \cup B.$$

Umgekehrt definiert ein abgeschlossenes System, das gegen endliche Vereinigung abgeschlossen ist (und damit auch die leere Menge enthält), eindeutig einen Kuratowski-Hüllenoperator; vgl. auch Satz 3.8.6.

Kapitel 5

Beispiele und Anwendungen

5.1 Mengenlehre

5.1.1 Computer und Mengen

Wozu dienen heutzutage “Computer”? Tatsächlich ist ihre Aufgabe beileibe nicht auf das “Rechnen” beschränkt, wie man bei der Bezeichnung “Rechner” vermuten könnte, die im Deutschen für “Computer” üblich ist. Daran mag es auch liegen, dass die begrifflich weitere englische Bezeichnung sich auch im Deutschen durchgesetzt hat. Eine der bedeutenden und von Vielen genutzten Anwendungen von Computern ist deren Fähigkeit, sich schiere “Unmengen” von Fakten “merken” zu können. Dieses “Merken” umfasst sowohl das Speichern von Daten als auch den problemlosen Zugriff auf selbige. Um dies technisch bewerkstelligen zu können, besitzt ein Computer nicht nur ein “Rechenwerk”, sondern auch einen großen Speicher, den man umgangssprachlich als eine “große Menge von Speicherwörtern” beschreiben kann.

Ist so ein Speicher aber in unserem Sinne überhaupt eine “Menge von Speicherwörtern”, also insbesondere eine Menge? Wenn ein Speicherwort so etwas wie ein Gefäß ist, in dem man ein einzelnes Datum ablegen kann, so ist im strengen Sinne ein Speicher zunächst einmal keine Menge von Speicherwörtern, da diese Datengefäße sozusagen von außen betrachtet alle gleich aussehen. Zumal ist technisch meist festgelegt, welche Art von Daten so ein Gefäß überhaupt aufnehmen kann. Typisch sind “Bytes” als Speicherwörter, die eine Folge von acht Nullen und Einsen als Datum speichern können. Da diese Gefäße von außen gleich aussehen und eben auch alle dieselbe Eigenschaft und Aufgabe haben, nämlich konkret das Aufnehmen von je einer Folge von acht Nullen und Einsen, einem Byte, so ist ihre Zusammenfassung keine Menge, weil ihr die geforderte Unterscheidbarkeit der Gegenstände (also hier der Gefäße, der Bytes) fehlt. Die Bytes sind als Speicherwörter nicht wohlunterschieden, um die in der Definition einer Menge gewählte Wortwahl aufzugreifen.

Dieses ist nicht nur ein Mangel, der sich lediglich anhand der Definition ergibt, sondern auch bezüglich der beabsichtigten Anwendung. Es soll ja nicht möglich sein, Bytes in den Gefäßen abzulegen, sondern man will ja auf die abgelegten Daten auch wieder (schnell) zugreifen können. Versuchen wir das Bild noch weiter auf das alltägliche Leben zu übertragen. Stellen Sie sich vor, die (von außen nicht unterscheidbaren) Gefäße dienten nicht zum Speichern von Bytes, sondern zum Speichern von Küchenzutaten, wie zum Beispiel Gewürzen. Wenn man nun beim Kochen zum Beispiel ein Gericht mit schwarzem Pfeffer würzen will, so wird man beim Öffnen eines

Gefäßes, welches weiße Körner enthält, davon Abstand nehmen, diese dem Gericht zuzuführen, da es sich zweifelsfrei nicht um schwarzem Pfeffer handelt. Möchte man allerdings das Gericht salzen, so ist bei der raschen Anwendung der weißen Körner des besagten Gefäßes Vorsicht geboten, könnte es sich doch gleichermaßen um Zucker handeln. Wie wird mit dieser Schwierigkeit im Alltag umgegangen? Sinnvollerweise werden die Gefäße in der Küche beschriftet, oder wenigstens gibt es andere bekannte Anhaltspunkte, die eine eindeutige und rasche Zuordnung von Gefäßen zu ihrem Inhalt gestatten. Die unterschiedliche kristalline Struktur von Zucker und Salz ist hierfür praktisch ungenügend. Genau diese Art der Individualisierung der Gefäße in Form ihrer Beschriftung verwendet man auch im Rechner, indem man den Speicherwörtern eindeutige Namen zuordnet. Diese Namen nennt man auch "Adressen". So kann man sehr wohl von der Menge der adressierten (oder adressierbaren) Speicherwörter sprechen, die eine wesentliche Rolle in einem heutigen Computer spielt. Dies entspricht der Menge der beschrifteten Gefäße im Gewürzregal der Küche.

Durch die in der Vorlesung getroffene "Übereinkunft" verliert sich etwas von der Strenge der Definition. So könnte man nun doch auch von der Menge der Speicherwörter eines Rechners sprechen, würde damit aber (aufgrund der Ununterscheidbarkeit der "Gefäße") eben nur eine einelementige Menge ansprechen. Dies sollte man stets bedenken, wenn man auf einfache Weise Mengen beschreiben möchte.

5.1.2 Soziale Netzwerke

Der Begriff eines *sozialen Netzwerkes* ist heutzutage weit verbreitet und hat einen recht technischen Sinn. In der Soziologie ist dieser Begriff schon seit über 50 Jahren üblich, um die unterschiedlichen Beziehungen zwischen Menschen zu beschreiben. Wir werden unser Beispiel aber der moderneren, technischen Begriffsprägung entlehnen.

Jeder Teilnehmer eines sozialen Netzwerkes kann sich eine Gruppe anderer Teilnehmer als "Bekannte" zuordnen, die je nach Netzwerk "friends" oder "follower" genannt werden. Zu jedem Teilnehmer ist also die Menge der "Bekannten" zugeordnet. Diese kann man dann auch häufig noch in Teilmengen untergliedern, die zum Beispiel "Kreise" genannt werden. Diese Bezeichnung wird an der bildlichen Darstellung klar, die wiederum Venn-Diagrammen ähnelt. Es gibt oft auch die Möglichkeit, sich "gemeinsame Bekannte" aufzulisten zu lassen, was der Bildung einer Schnittmenge entspricht. Überlegen Sie sich einmal, welche Mengenoperationen noch sinnvoll sind. Wie wird zum Beispiel konkret die Vereinigung interpretiert? Wäre es sinnvoll, beliebige Mengen von Bekannten zu vereinigen? Was wird stattdessen in derlei Systemen angeboten?

5.1.3 Mengen und Datentypen

(Abstrakte) Datentypen sind durch Mengen(namen) und Operationen(namen) gegeben. Diese sind von grundlegender Bedeutung in fast allen Programmiersprachen. Mithilfe von einfachen Operationen lassen sich oft komplexere beschreiben.

In realen Programmiersprachen wie JAVA wird dieses Konzept zu dem von Objekten und Klassen fortentwickelt. Für die verwandte Sprache C++ kann man dies in der Einführung von Peter Müller im Internet nachlesen. Wir wollen aber hier eher den klassischen Ansatz am Beispiel erläutern.

Beispielsweise haben wir die Menge \mathbb{N}_Z der Zermelo-Zahlen und die Nachfolgeroperation n'_Z kennengelernt. Hierdurch lässt sich die Addition $+_Z$ (induktiv) erklären.

Hierzu seien n_Z, m_Z beliebige natürliche (Zermelo-)Zahlen.

$$n_Z +_Z m_Z := \begin{cases} n_Z, & \text{falls } m_Z = \emptyset \\ (n_Z +_Z k_Z)', & \text{falls } m_Z = k_Z' \end{cases}$$

Wir addieren so zwei Zahlen, z.B. $2_Z +_Z 3_Z$. Es gilt also in obigem Formalismus: $n_Z = 2_Z$ und $m_Z = 3_Z$. Da $3_Z \neq \emptyset$, gilt genauer $3_Z = 2'_Z$, in dem Formalismus setzen wir also $k_Z = 2_Z$. Wir erhalten also:

$$2_Z +_Z 3_Z = (2_Z +_Z 2_Z)'$$

Dies ist noch keine befriedigende Lösung, also rechnen wir weiter:

$$2_Z +_Z 2_Z = (2_Z +_Z 1_Z)',$$

woraus die immer noch unbefriedigende Darstellung

$$2_Z +_Z 3_Z = (2_Z +_Z 1_Z)''$$

folgt. Wir müssen also nochmal weiterrechnen:

$$2_Z +_Z 1_Z = (2_Z +_Z 0_Z)'.$$

Unter Beachung von $0_Z = \emptyset$ ergibt sich hieraus:

$$2_Z +_Z 1_Z = (2_Z +_Z \emptyset)' = 2'_Z = 3_Z.$$

Daraus können wir nun das gewünschte Ergebnis ausrechnen:

$$2_Z +_Z 3_Z = (2_Z +_Z 1_Z)'' = 3''_Z = 4'_Z = 5_Z.$$

Wir haben also entlang dieser Definitionen nachgerechnet, dass $2 + 3 = 5$ gilt. Irgendwie wussten wir das wohl schon zuvor.

Entsprechend kann man z.B. die Multiplikation von Zermelo-Zahlen einführen, siehe Abschnitt 6.1.

Rekursion versus Induktion Induktiv können wir “der Reihe nach” die definierten Objekte auflisten, beginnend mit dem Induktionsanker.

Den umgekehrten Weg geht die Rekursion: n'_Z ist eine Zermelo-Zahl, wenn n_Z eine ist, und das ist der Fall, wenn entweder $n_Z = 0_Z$ gilt oder aber n_Z von der Form m'_Z ist... Beim Lösen der Aufgabe $2_Z +_Z 3_Z = ?$ sind wir so “rückwärts” vorgegangen.

5.1.4 Bezeichnungen und Bezeichnetes

Eine grundsätzliche, auch wiederum recht philosophische Frage der Informatik ist die Unterscheidung zwischen einer Bezeichnung und dem, was diese Bezeichnung meint, also bezeichnet. Diese Frage ist eng verwandt mit der Unterscheidung von Syntax und Semantik. In dieser Form ist sie sicher jedem begegnet, der schon einmal etwas programmiert hat. Gibt man seinen ersten kleinen Programmtext in einen Editor ein und übersetzt diesen anschließend, so beschwert sich das Übersetzungsprogramm (der Compiler) gerne mit einem “Syntaxfehler”: Wir haben beispielsweise in einer Zeile ein Semikolon vergessen. Der Compiler kann aber (in der Regel) eben nur feststellen, ob

der Satzbau, den wir in den Editor eingegeben haben, von dem abweicht, was als Satzbau der gewählten Programmiersprache zulässig war. Hingegen bleibt dem Compiler verschlossen, was mit dem Programmtext gemeint war. Die Semantik des Programms liegt einzig in der Verantwortung des Programmierers. Oft genug stellt man fest, dass ein Programmtext zwar syntaktisch korrekt ist, das Programm aber keineswegs das tut, was es soll.

Der oft feine Unterschied zwischen dem Programmtext (als Gegenstand) und dem Programm (das ausgeführt wird) wird bereits bei dem Begriff der “Gleichheit” deutlich: Zwei gleiche Programmtexte gehören sicher zu gleichen Programmen, aber zwei deutlich verschiedene Programmtexte können sehr wohl als Programme dieselbe Funktionalität bieten. In sehr vereinfachter Art und Weise taucht dieses Problem auch schon in Definition 3.1.2 auf: Wenn wir $M_1 = M_2$ schreiben, so meinen wir nicht, dass die verwendeten Mengennamen (als Bezeichner von Mengen) gleich sein müssen, sondern dass die bezeichneten Mengen dieselben Elemente enthalten.

5.1.5 Venn-Diagramme

Wem die bisherigen Beispiele zu abstrakt sind oder auch umgekehrt zu sehr nahelegen, wir würden uns nur mit geometrischen Mengen beschäftigen, dem sei Bild 5.1 zur Betrachtung anempfohlen, das Buchstaben aus drei Zeichensätzen zeigt, nämlich aus dem lateinischen, dem (alt-)griechischen und dem kyrillischen (russischen) Alphabet, das aus dieser Internetquelle stammt. Selbst endliche Mengen (wie Alphabete) können also bereits interessante Beispiele liefern. Je nach Auffassung gehören Y und K zum gemeinsamen Schnitt der Alphabete oder eben nicht (da die kyrillischen Buchstaben üblicherweise etwas anders aussehen).

5.1.6 CSG: Constructive Solid Geometry

Das ist eine Beschreibungssprache für komplexe Oberflächen, im Wesentlichen beruhend auf einfachen Punktmengenoperationen, siehe Bild 5.2. Hier wird der prinzipielle syntaktische Aufbau eines CSG-Ausdrucks mit einem geordneten Baum gezeigt, so wie dies auch sonst im Compilerbau üblich ist. Auch ohne weitere formale Erläuterungen sollte das Beispiel verständlich sein. Nur so viel sei hier verraten: Die Syntax solcher Ausdrücke wird formal durch eine induktive Definition beschrieben oder –gleichwertig– mit Hilfe einer Grammatik. Näheres hierzu erfahren Sie in Veranstaltungen über Formale Sprachen.

Es gibt jedenfalls auch ein sourceforge-Projekt unbboolean für JAVA, das das CSG-Konzept umsetzt. Grundoperationen sind Vereinigung, Durchschnitt und Mengendifferenz. Überlegen Sie sich einmal, wie genau die auf dem Screenshot von Bild 5.3 Figur in Gestalt einer Tasse entstanden ist. Offenbar genügen Vereinigung und Mengendifferenz für die Darstellung einer Tasse aus geeignet vordefinierten Zylindern. Zylinder werden hier als elementare Figuren anderweitig genauer beschrieben.

Informaticup der Gesellschaft für Informatik (GI)

Alljährlich veranstaltet die GI diesen Programmier-Wettbewerb.

Der neue Wettbewerb läuft gerade an: <http://informaticup.gi.de/>

Auch Sie als “junge Studenten” sind herzlich zur Teilnahme eingeladen.

Hinweis zu 2011: Das Siegerteam löste die Aufgabe, ein Konstruktionstool für eine Murmelbahn zu entwickeln, mit Hilfe von CSG. Einen Screenshot der Präsentation der

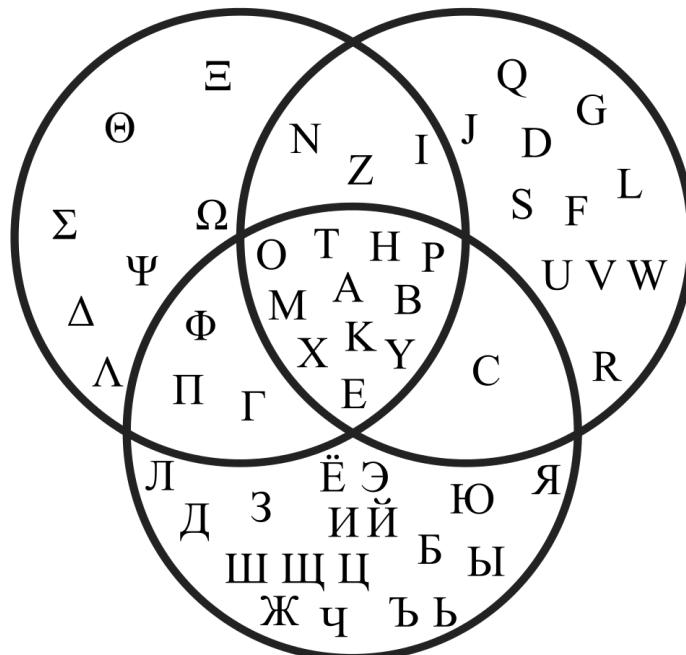


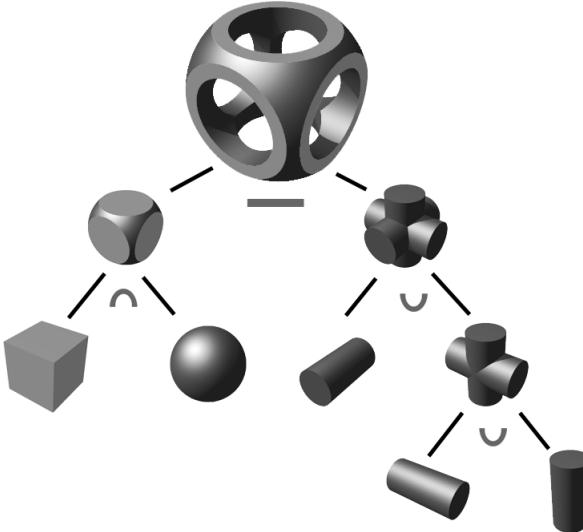
Abbildung 5.1: Es gibt paarweise und sogar insgesamt gemeinsame Buchstaben zwischen dem lateinischen, griechischen und kyrillischen Alphabet, aber auch “private” Zeichen in jedem der Alphabete.

Lösung sehen Sie in Bild 5.4.

5.1.7 Punktmengen und Geometrie

Geometrische Objekte kennen Sie bereits aus dem Schulunterricht. Die dort betrachteten Objekte waren vermutlich deutlich abstrakter als die in Abschnitt 5.1.6 betrachtete Tasse. Darunter werden *geschlossene Polygonzüge* gewesen sein, auch bekannt als *n-Ecke*, wie in Bild 5.5 zu sehen. Formaler ist ein geschlossener Polygonzug gegeben durch eine endliche Menge P von Punkten x_0, \dots, x_{n-1} , $n \geq 3$, in der Ebene.¹ Überdies ist jeder Punkt x_i mit seinen *Punktnachbarn* x_{i+1} bzw. x_{i-1} durch eine *Randlinie* verbunden, wobei wir $x_{-1} = x_{n-1}$ und $x_n = x_0$ ansetzen. Ein Beispiel für ein 8-Eck, also einen geschlossenen Polygonzug mit 8 Punkten, sehen Sie in Bild 5.5. Ist P ein Polygonzug mit $n \geq 4$ Punkten, d.h., $P = \{x_0, \dots, x_{n-1}\}$, so entsteht ein neuer Polygonzug P' durch Löschen eines Punktes $x \in P$, d.h., $P' = P \setminus \{x\}$, denn P' enthält mindestens drei Punkte. Im Bild ist durch eine gestrichelte Linie angedeutet, wie der Polygonzug aussieht, der durch Löschen des Punktes "rechts oben" entsteht. Offensichtlich wird im Bild nicht "nur" der Punkt gelöscht, sondern auch die an diesem Punkt anliegenden beiden Randlinien; dafür ist die gestrichelte Linie eine neue Randlinie von P' . Ein Polygonzug zerlegt die Ebene in drei Punktmengen: (a) den aus den Polygonzugpunkten und den Randlinien bestehenden Polygonzug selbst, geschrieben

¹Sie fragen sich, was eine “endliche Menge” sein soll? Eine sehr gute Frage, wir werden dem im Abschnitt 3.4 genauer nachgehen. Hier genügt erstmal eine sicherlich vorhandene intuitive Vorstellung.

Abbildung 5.2: CSG-Beispiel; Internetquelle

∂P , (b) das durch den Polygonzug abgegrenzte *Innere* des Polygonzugs, kurz P° , sowie (c) die übrigen Punkte, welche das *Äußere* des Polygonzugs bilden. Dieser anschaulich “offenkundige” Sachverhalt ist Spezialfall eines tiefen topologischen Theoremes, dem Jordanschen Kurvensatz. Uns genügt hier allerdings die Anschauung, um weiter zu definieren: Ein Polygonzug $P = \{x_0, \dots, x_{n-1}\}$ ist *konvex*, falls die Verbindungsline $x_i x_j$ für alle Punkte $x_i, x_j \in P$, $i \neq j$, ganz in der Punktmenge $P^\circ \cup \partial P$ liegt. Dieses ist für ein konkretes Punktpaar in Bild 5.5 durch eine gestrichelte Linie gezeigt. Die zwei an einem Punkt eines Polygonzugs anliegenden Linien (die diesen mit seinen beiden Punktnachbarn verbinden) legen zwei Winkel fest: der *Innenwinkel* liegt im Inneren des Polygonzugs, während der *Außenwinkel* im Äußeren des Polygonzugs liegt. Die Summe von Innenwinkel und Außenwinkel (an einem konkreten Punkt) beträgt 360° (Vollkreis). Ist P konvex, so ist jeder Innenwinkel höchstens 180° .

Hinweis: Die meisten der soeben eingeführten Begriffe sollten (anschaulich) klar sein, vermutlich mit Ausnahme des Begriffs der Konvexität. Sollte Ihnen etwas Derartiges beim Durcharbeiten eines mathematisch orientierten Lehrbuchs unterkommen, so sollten Sie kurz innehalten und sich geeignete Beispiele besorgen oder auch einfache Aussagen überlegen. Einfache Fragen sollten Sie dabei leiten. Konkret könnte das in diesem Fall so aussehen:

- Warum ist jedes Dreieck konvex?
- Gibt es ein Viereck, das nicht konvex ist?

Lemma 5.1.1 Ist $P = \{x_0, \dots, x_{n-1}\}$ ein konvexer Polygonzug mit $n \geq 4$ Punkten und $x \in P$, so ist $P' = P \setminus \{x\}$ ein konvexer Polygonzug.

Beweis: Wir hatten schon überlegt, dass P' ein Polygonzug ist. Es bezeichne y, z die beiden Punktnachbarn von x und L die durch die Punkte y, z festgelegte Gerade. L definiert für die Ebene E die Halbebene H_x , die den Punkt x enthält, und in die Halbebene H' , die x nicht enthält, wobei $L = H_x \cap H'$ und $E = H_x \cup H'$. P' liegt gänzlich in H' . Es seien x_i und x_j zwei verschiedene Punkte von P' und damit auch von P . Da P konvex ist, liegt die Verbindungsline

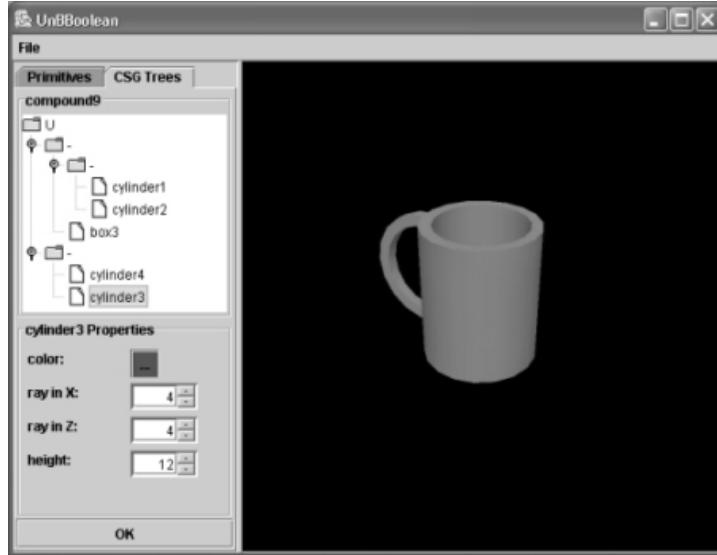


Abbildung 5.3: Unbboolean-Beispiel; Internetquelle

$x_i x_j$ von x_i und x_j in $P^\circ \cup \partial P$. Da x_i und x_j in H' liegen, ist auch die Verbindungsgeradenlinie $x_i x_j$ in H' . Daher liegt $x_i x_j$ in $(P')^\circ \cup \partial P' = (P^\circ \cup \partial P) \cap H'$. \square

Die Begründung aus dem vorigen Beweis legt auch noch eine weitere Kennzeichnung konvexer Polygonzüge nahe, die wir hier ohne Beweis angeben; das wäre aber (wiederum) eine gute Übungsaufgabe für einen Induktionsbeweis.

Lemma 5.1.2 Eine Punktmenge M der Ebene wird durch einen konvexen Polygonzug P berandet genau dann, wenn sie Teilmenge einer Dreiecksfläche ist und sich als Schnitt endlich vieler Halbebenen H_i , $i \in [n]$ für ein n , darstellen lässt, d.h., $M = \bigcap_{i \in [n]} H_i$ und $P = \partial M$.

Hiermit können wir nun zeigen (unter Benutzung von Schulkenntnissen):

Satz 5.1.3 Die Innenwinkelsumme eines konvexen n -Ecks beträgt $(n - 2) \cdot 180^\circ$.

Beweis: Wir führen einen Induktionsbeweis über die Anzahl der Ecken. Für den Induktionsanfang bei $n = 3$ appellieren wir an Ihre Schulkenntnisse: Die Summe der Innenwinkel in einem Dreieck beträgt 180° . Wir nehmen an (Induktionsvoraussetzung), die die Innenwinkelsumme eines konvexen N -Ecks, $N \geq 3$, beträgt $(N - 2) \cdot 180^\circ$. Wir behaupten: Die Innenwinkelsumme eines konvexen $(N + 1)$ -Ecks beträgt $(N - 1) \cdot 180^\circ$. Betrachte daher ein konkav $(N + 1)$ -Eck $P = \{x_0, \dots, x_N\}$. Wegen Lemma 5.1.1 ist $P' = P \setminus \{x_N\}$ ein konvexer Polygonzug. Die Fläche von P – und damit die Innenwinkelsumme – wird zerlegt in die Fläche (bzw. Innenwinkelsumme) von P' und die Fläche (bzw. Innenwinkelsumme) des durch x_0, x_{N-1}, x_N festgelegten Dreiecks. Nach Induktionsvoraussetzung beträgt die Innenwinkelsumme von P' $(N - 2) \cdot 180^\circ$ und nach Induktionsanfang die Innenwinkelsumme des Dreiecks 180° . Daher beträgt die Innenwinkelsumme von P :

$$(N - 2) \cdot 360^\circ + 180^\circ = (N - 1) \cdot 180^\circ.$$

Dies war zu zeigen. Nach dem Prinzip der vollständigen Induktion folgt die Satzbehauptung. \square



Abbildung 5.4: Murmelix-Beispiel; aus dieser Datei

Hinweis: Oft ist es hilfreich, derlei Ergebnisse an bekannten Resultaten zu testen. Beispielsweise dürfte auch noch aus der Schule bekannt sein, dass die Innenwinkelsumme in einem Viereck 360° beträgt.

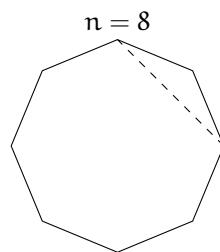


Abbildung 5.5: Ein regelmäßiges Achteck

Der Grundgedanke der Zerlegung einer Polygonfläche in Dreiecke, wie er dem voranstehenden Beweis zugrundeliegt, lässt sich auch auf nicht konvexe Polygone anwenden. Analysieren Sie einmal den voranstehenden Beweis, um eine Klasse von Polygonen zu beschreiben, für die ebenfalls der Innenwinkelsatz gilt, die aber neben den konvexen Polygonen noch weitere Polygone enthält. In dieser allgemeineren Fassung ist er auch in der Vermessungskunde Grundlage für die dort als Triangulation angesprochene Zerlegung von Flächen in Dreiecke, um beliebige durch Linien berandete (Grundstücks-)Flächen vermessen zu können.

5.1.8 Mengenalgebra: Wichtige Aussagen (Zusammenfassung)

Diese Liste von Sätzen soll Ihnen beim Lernen der Rechengesetze helfen. Können Sie die Gesetze auch mit Namen benennen? Wenn nicht, schauen Sie im Abschnitt 3.1 nach.

Satz: $A \cap B \subseteq A \subseteq A \cup B; A \cap B \subseteq B \subseteq A \cup B.$

Satz: $A \cup A = A \cap A = A.$

Satz: $A \cup B = B \cup A; A \cap B = B \cap A.$

Satz: $(A \cup B) \cup C = A \cup (B \cup C); (A \cap B) \cap C = A \cap (B \cap C).$

Satz: $(A \cup B) \cap C = (A \cap C) \cup (B \cap C); (A \cap B) \cup C = (A \cup C) \cap (B \cup C).$

Satz: $\overline{A \cup B} = \overline{A} \cap \overline{B}; \overline{A \cap B} = \overline{A} \cup \overline{B};$

Satz: $(A \cup B = B) \iff A \subseteq B \iff (A \cap B = A).$

Satz: $(A \subseteq B) \implies ((A \cup C \subseteq B \cup C) \wedge (A \cap C \subseteq (B \cap C))).$

5.2 Relationen und gerichtete Graphen

5.2.1 Relationale Datenbanken

Eine *relationale Datenbank* besteht formal aus einer Menge von Tabellen, wobei diese Tabellen im Grunde genommen nichts anderes als in der Regel mehrstellige Relationen sind. Vermutlich ist Ihnen intuitiv durchaus klar, was mehrstellige Relationen sein könnten; die Vorstellung mehrdimensionaler Tabellen genügt hier. Genaueres finden Sie im Abschnitt 4.2.1. Die Zeilen einer solchen Tabelle entsprechen den einzelnen Datensätzen, während die Spalten die sogenannten Attribute der Datensätze darstellen. Schauen wir uns hierzu ein einfaches Beispiel an, in welchem wir die Ihnen bislang geläufige Notation benutzen. Eine Übersetzung in die im Bereich der Datenbanken übliche Sprechweisen sollte Ihnen spätestens dann gelingen, wenn Sie einen entsprechenden Kurs hierzu gehört haben werden.

Professor F. aus T. hat zwei Listen, eine mit Matrikelnummern und zugehörigen Namen und Anschriften und eine andere mit Matrikelnummern und zugehörigen Noten der Prüfung zu DS aus dem vergangenen WS. Er möchte für das nächste WS Korrektoren für DS anwerben. Daher will er als Wunschliste eine Sammlung von Namen und Anschriften (sowie DS-Noten) all derjenigen Studenten erhalten, die beim letzten Mal eine Eins vor dem Komma erzielten.

Wie könnten wir dieses Szenario mit den bislang eingeführten Operationen modellieren? Versuchen wir zunächst, die entsprechenden Grundmengen zu beschreiben.

A: Menge von (möglichen) Anschriften (mit Namen)

M: Menge von (möglichen) Matrikelnummern

N: Menge von Noten, also:

$N = \{1.0, 1.3, 1.7, 2.0, 2.3, 2.7, 3.0, 3.3, 3.7, 4.0, 5.0\}.$

Hieraus müssen wir nun die schon angesprochenen Listen ableiten, indem wir diese als geeignete Relationen beschreiben. Zwei Listen sind ja vorgegeben, nennen wir sie L_1 und L_2 .

L_1 erste Liste mit Matrikelnummern und Anschriften

$$L_1 \subseteq M \times A$$

L_2 zweite Liste mit Matrikelnummern und Noten

$$L_2 \subseteq M \times N$$

K : “interessante Kandidaten”:

$$K = L_2 \cap (M \times \{1.0, 1.3, 1.7\})$$

W : Wunschliste mit den Anschriften der Kandidaten:

$$W = K^- \circ L_1$$

Diese und ähnliche Operationen werden in Abfragesprachen wie SQL effizient implementiert. Beispielsweise würde die Kandidatenauswahl darin mit einer SELECT ... FROM ... WHERE ... Anweisung umgesetzt werden können.

5.2.2 Konkrete Beispiele

Relationen können im Konkreten sehr anschaulich und übersichtlich sein. Es ist daher hilfreich, sich an ihnen die wesentlichen Begriffe klarzumachen, die wir für Relationen kennengelernt haben.

Beispiel: $R = \{(1, 2), (2, 3), (1, 3)\}$ ist eine Relation auf $M = \{1, 2, 3\}$.

- R ist nicht reflexiv, da $(1, 1) \notin R$, ja sogar irreflexiv, da weder $(1, 1)$ noch $(2, 2)$ noch $(3, 3)$ in R liegen.
- R ist nicht symmetrisch, da $(1, 2) \in R$, aber $(2, 1)$ nicht in R liegt. Genauer gilt für jedes Paar $(x, y) \in R$, dass $(y, x) \notin R$ liegt. In relationenalgebraischer Schreibweise bedeutet dies: $R \cap R^- = \emptyset$. Daher ist R auch antisymmetrisch, denn die Prämisse der Implikation “ $(x, y) \in R \wedge (y, x) \in R$ ” ist stets falsch.
- R ist transitiv, denn die in der Prämisse der Bedingung beschriebene Situation “ $(x, y) \in R \wedge (y, z) \in R$ ” ist genau für ein Tripel (x, y, z) erfüllt, nämlich für $(1, 2, 3)$. Tatsächlich gilt dann aber auch die Transitivität, da $(1, 3) \in R$ gilt.
- Da $3 \in M$, aber es kein y gibt mit $(3, y) \in R$, ist R nicht vortotal. Da $1 \in M$, aber es kein x gibt mit $(x, 1) \in R$, ist R nicht nachtotal.
- Da $(1, 2), (1, 3) \in R$, ist R nicht nacheindeutig. Da $(2, 3), (1, 3) \in R$, ist R nicht voreindeutig.

Beispiel: Teilerrelation $|$ auf \mathbb{Z} .

- $|$ ist reflexiv, da a stets Teiler von a ist (selbst für $a = 0$).
- $|$ ist nicht symmetrisch, da $1|2$, aber $2|1$ ist falsch. Da Gegenzahlen wie ± 1 einander teilen, ist $|$ nicht antisymmetrisch. (Das wäre anders, wenn wir die Teilerrelation auf den natürlichen Zahlen betrachteten.)
- $|$ ist transitiv: Ist a ein Teiler von b und b ein Teiler von c , so gilt: a ist ein Teiler von c . Genauer muss man dazu natürlich auf die Definition des Begriffs “Teiler” eingehen: a ist Teiler von b bedeutet, dass es ein $k_{a,b} \in \mathbb{Z}$ gibt mit $a \cdot k_{a,b} = b$. Entsprechend gibt es ein $k_{b,c}$ mit $b \cdot k_{b,c} = c$. Mit $k_{a,c} := k_{a,b} \cdot k_{b,c}$ gilt nun:

$$a \cdot k_{a,c} = a \cdot (k_{a,b} \cdot k_{b,c}) = (a \cdot k_{a,b}) \cdot k_{b,c} = b \cdot k_{b,c} = c.$$

Bei der Gleichungskette haben wir außer den Definitionen der Zahlen nur noch die Assoziativität der Multiplikation ausgenutzt.

- Da $|$ reflexiv, ist $|$ sowohl vor- als auch nachtotal.
- Da Gegenzahlen einander teilen und $|$ reflexiv, ist $|$ weder vor- noch nacheindeutig.

5.2.3 Das Königsberger Brückenproblem

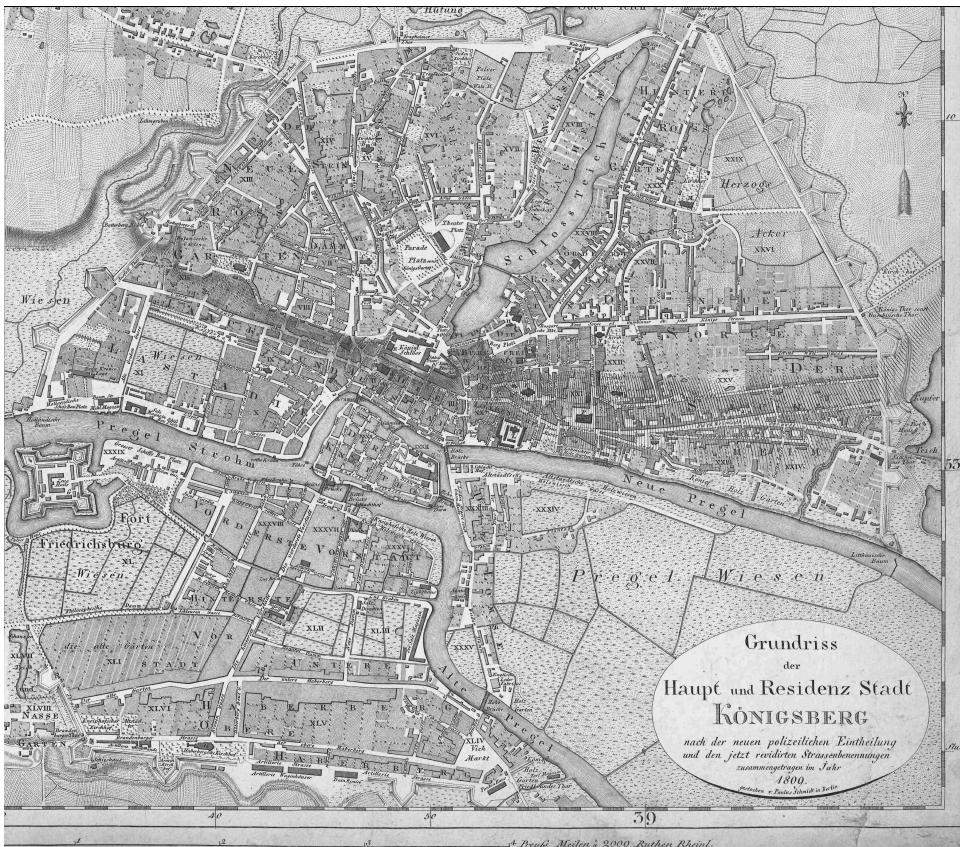


Abbildung 5.6: Karte von Königsberg aus dem Jahre 1809; [hierher](#)

Der bedeutende Mathematiker Leonhard Euler lebte in Königsberg, dem heutigen Kaliningrad. In der Stadt vereinigen sich die Alte und die Neue Pregel wieder zur Pregel, umschließen aber noch die zentrale Stadtinsel, den Kneiphof. Dies ist auf dem Bild 5.6 zu sehen. Die Flüsse Neue Pregel (im Norden) und Alte Pregel (im Süden) fließen aus dem Osten kommend in Richtung Königsberg, vereinigen sich kurz, um noch die Insel Kneiphof zu umschließen. Die (wieder-)vereinigte Pregel fließt dann westwärts weiter Richtung Ostsee (Frisches Haff). Auch die Brücken sind auf der Karte gut zu sehen. Die Grüne Brücke und die Köttelbrücke verbinden den Kneiphof mit der Vorstadt im Süden. Die Kramerbrücke und die Schmied(e)brücke verbinden den Kneiphof mit der Altstadt im Norden. Nach Osten ist der Kneiphof über die Honigbrücke mit den Pregelwiesen bzw. dem dortigen Stadtteil Lomse verbunden. Die Holzbrücke verbindet die Altstadt mit der Lomse, und die Hohebrücke stellt die Verbindung zwischen der

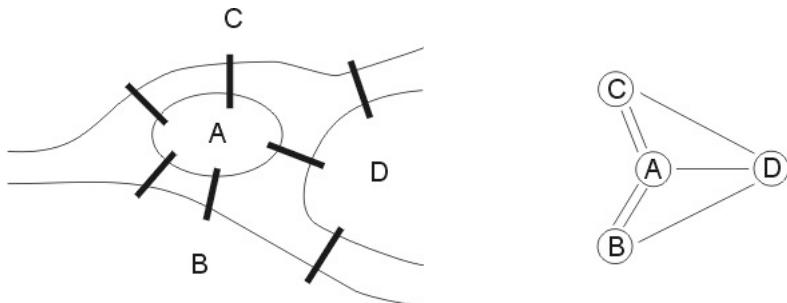


Abbildung 5.7: Schematische Darstellung von Königsberg

Vorstadt (bzw. dem Haberberg) und der Lomse her. Nun haben Sie vermutlich mehr über die Geographie Königsbergs erfahren, als Sie je wissen wollten.

Euler hat sich gefragt, ob es möglich wäre, einen Rundgang durch seine Heimatstadt zu machen und dabei alle sieben Pregelbrücken genau einmal zu überqueren. Wir wollen diese Frage hier (noch) nicht lösen. Neugierige seien auf die Ausarbeitung Das Königsberger Brückenproblem im “Matheprisma” verwiesen. Allgemein möchte ich auch die “Matheprisma” Einführungen für den Übergang von Schule zum Studium empfehlen, die Sie hier finden. Wem diese deutschsprachigen Erklärungen eine zu geringe Herausforderung bieten, der findet im Internet auch eine Kopie von Eulers Originalarbeit (auf Latein).²

Wir wollen an diesem Beispiel zunächst nur aufzeigen, wie man Graphen (gemäß unserer Definition) zur Modellierung dieser Aufgabenstellung benutzen könnte. Ein erster Ansatz wäre eine vereinfachte Darstellung der Karte Königsbergs, wie sie in Bild 5.7 zu sehen ist. Die Namen der Stadtteile und Brücken sind verschwunden, da sie nicht wesentlich zur Lösung der gestellten Aufgabe beitragen. Stattdessen wurden eher symbolische Namen verwendet, wie z.B. A für den Kneiphof. Wichtig ist aber die “Topologie” von Königsberg: Welche Brücken verbinden wie welche Stadtteile. Genau diese Information bleibt in der schematischen Darstellung bewahrt.

Leider ist das eben noch kein Graph, eher ein sogenannter “Multigraph”, da so genannte “Mehrfachkanten” zwischen Knoten gestattet sind. So ein Modell kann man aber einfach durch Einfügen neuer Knoten je Kante in einen paaren ungerichteten Graphen verwandeln, so wie dies in Bild 5.8 zu sehen ist. Dieses Bild ist übrigens direkt mit L^AT_EX erstellt; wer derlei Beispiele einmal anschauen möchte, möge mal hierhin klicken. Dieser paare ungerichtete Graph hat nun 11 Knoten und 14 Kanten.

5.2.4 Graphen als Modellierungswerkzeug

Das Königsberger Brückenproblem zeigt gleich am Anbeginn der Disziplin der Graphentheorie auf, woher die außermathematische Motivation zur systematischen Betrachtung solcher Strukturen stammt: sie stellen ein ideales Werkzeug zur Modellierung unterschiedlichster Alltagssituationen dar. Wie im Hauptteil dargelegt, gibt es sehr enge Verbindungen zu den Relationen, und insofern könnte man natürlich auch sagen, dass Relationen eben diese Modellierungsmächtigkeit zukommt. In diesem Sinne werden sie ja auch im Bereich der Datenbanken eingesetzt, wie in Abschnitt 5.2.1

²Wer die Herausforderung annimmt, dem sei gesagt, dass §2 jener Arbeit die Problemdefinition enthält. Klar wird zudem, dass die Skizze in 5.7 auf die Zeichnung von Euler selbst zurückgeht.

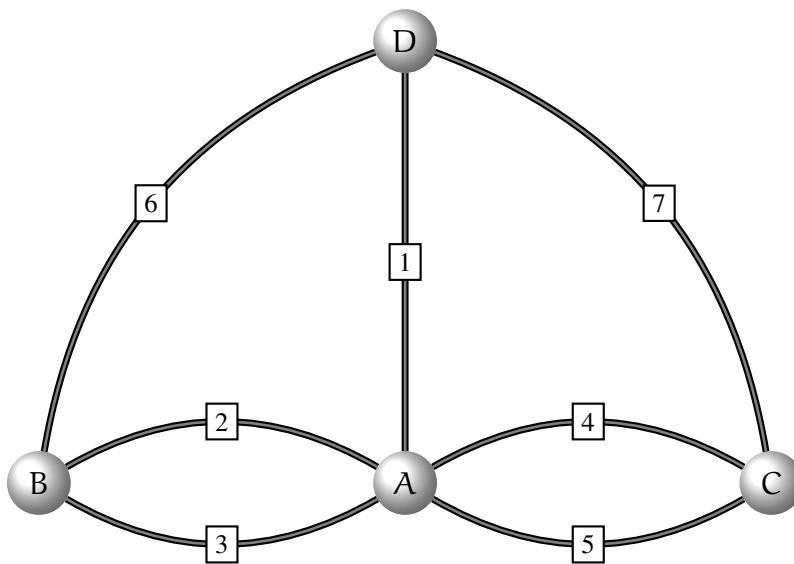


Abbildung 5.8: Das Königsberger Brückenproblem lässt sich als paarer (ungerichteter) Graph modellieren

erläutert. Graphen sind aber aufgrund ihrer graphischen Darstellungsmöglichkeit(en) oft viel intuitiver.

Betrachten wir aber im Folgenden einige Beispiele für Graphen und ihre Darstellungen, so wie sie sozusagen im Alltag auftreten. Johannes Gans hat in dem Stammbaum der Habsburger in Fig. 5.9 versucht, fast alle europäischen Herrscherdynastien auf die Nachkommenschaft Rudolfs von Habsburg zurückzuverfolgen und damit natürlich auch die Vorherrschaft der Habsburger zu legitimieren.³ Diese Darstellung ist vielleicht nicht ganz dem entsprechend, was wir abstrakt mit “Punkten” und “Kanten mit Pfeilen” beschrieben haben, aber es ist klar, dass man es leicht als ausgeschmückte Fassung ansehen kann.

Wie ist solch ein Stammbaum zu lesen? Dazu ist es sinnvoll, die “Knoten” als die zugehörigen Personen zu deuten. Als Adjazenzrelation E “ist Elternteil von” (und gleichzeitig graphische Konvention) gilt, dass die Eltern einer Person p in der Reihe

³Quelle: Arboretum genealogicum annotationibus in arboreis singulis illustratum exhibens omnes fere imperii principes Europae hodie reges linea recta descendentes a Rudolfo I. Imperatore Köln, apvd Ioannem Kinchivm, 1638 (2. Auflage, 1. Auflage: Prag 1635)

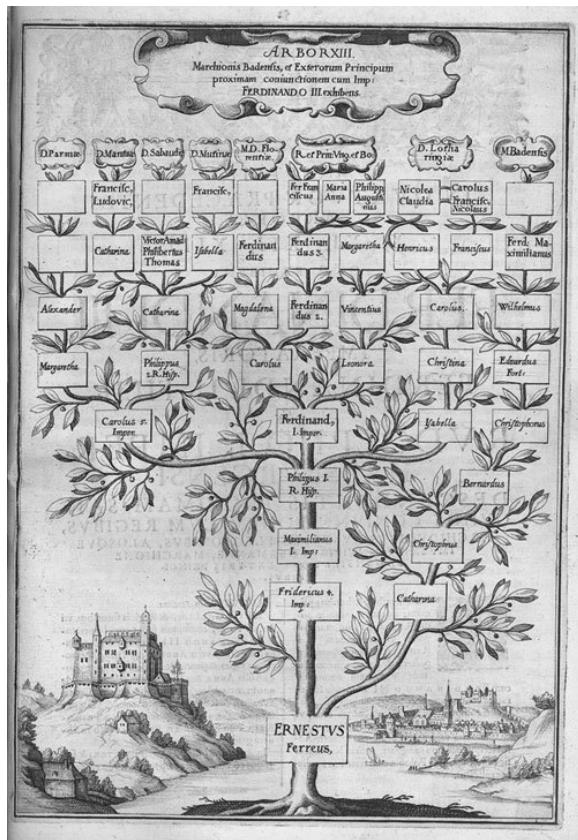


Abbildung 5.9: Ein Stammbaum der Habsburger aus dem 17. Jahrhundert

unterhalb von p angeordnet sind und eine gerichtete Kante von jedem Elternteil nach p zeigt. Jetzt kann man sich einmal überlegen, was es bedeutet, wenn $(p, r) \in E \circ E$ liegt? Das bedeutet nach Definition des Relationenprodukts, dass es eine Person q gibt, die Kind von p ist und Elternteil von r . Mit anderen Worten, p ist ein Großelternteil von r .

Wir können natürlich ganz allgemein für die Menge M aller Menschen die Relation E "ist Elternteil von" betrachten. Wie könnten wir nun andere bekannte Verwandtschaftsbegriffe notieren? Solange wir keinen "Zugriff" auf die Geschlechtsinformation haben, können wir aus $(p, q) \in E$ nicht sogleich Begriffe wie "ist Mutter von" oder "ist Sohn von" ableiten. Ebensowenig kann man Verhältnisse erschließen, die sich durch Heirat ergeben, da eben dieser Status nicht bekannt ist allein aus der Kenntnis von E heraus. Typische Begriffe, die wir nicht erschließen können, sind also "Schwager" oder "Schwägerin". Dennoch kann man schon sehr viel beschreiben:

- “ist Kind von”: p ist Kind von q genau dann, wenn q ein Elternteil von p ist, also $(q, p) \in E$ gilt. Daher lässt sich diese Relation knapp mit E^- beschreiben.
 - “ist Großelternteil von”: Wie oben gesehen, beschreibt dies $E \circ E$.
 - “ist Geschwisterkind von”: p und q sind Geschwister genau dann, wenn sie ein

gemeinsames Elternteil haben. (Achtung: hier genügt ein gemeinsames Elternteil, d.h., der andere Elternteil kann sehr wohl unterschiedlich sein.) Die Relationalgebra gestattet wieder eine knappe Beschreibung durch $E^- \circ E$.

- “ist Kousine oder Cousin von”: Wenn wir uns auf den “ersten Grad” einschränken, so haben p und q diesen Status, wenn sie einen gemeinsamen Großelternteil besitzen. Dies gestattet die Beschreibung durch: $(E \circ E)^- \circ (E \circ E)$.
- “ist Onkel oder Tante von”: p ist Onkel oder Tante von q (ersten Grades), wenn p Bruder (oder Schwester) eines Elternteils von q ist. Also können wir kurz schreiben: $(E^- \circ E) \circ E$; der erste Teil $(E^- \circ E)$ drückt das Geschwisterverhältnis aus, und der zweite die Elternbeziehung. Wie oben angedeutet, schließt dies Begriffe wie “angeheirateter Onkel” nicht mit ein, obwohl dies natürlich umgangssprachlich erfolgt.

Aus unseren bisherigen Überlegungen können wir auch leicht gewisse Erkenntnisse über all diese Verwandtschaftsbegriffe gewinnen. Zum Beispiel gilt: p ist Kousin oder Kousine von q genau dann, wenn p Kind eines Onkels oder einer Tante von q ist. Algebraisch ist nämlich klar (mit den uns bekannten Gesetzen, welchen genau bitte?):

$$(E \circ E)^- \circ (E \circ E) = (E^- \circ E^-) \circ (E \circ E) = E^- \circ ((E^- \circ E) \circ E)$$

5.2.5 Graphenzeichnungen und Intuition

Hier ist allerdings auch eine Warnung angebracht. Ein Graph kann sehr viele “Zeichnungen” (oder mathematisch gesprochen, Einbettungen in der Euklidischen Ebene) besitzen. Der oben angesprochene intuitive Charakter von Graphen ist aber für die meisten Menschen eigentlich der intuitive Charakter der Zeichnungen und daher hängt die Wahrnehmung von Graphen stark von deren konkreter Zeichnung ab. Das hat zu einem eigenen Gebiet innerhalb der Informatik geführt, dem Graphzeichnen. Für Sie als Informatik-Studenten in Trier mag es interessant sein zu erfahren, dass an drei Professuren Arbeiten zu diesem Thema veröffentlicht worden sind (und werden), wie die Zitate [4, 14, 19] der einschlägigen “Graph Drawing” Konferenz belegen. Für viele Anwendungen ist es z.B. interessant, Graphen so zu zeichnen, dass ihre Kanten nur wenige Kreuzungen aufweisen. In diesem Sinne ist Bild 3.6 nicht bestmöglich. Wir können die Knoten (Punkte) auf den drei vertikalen Linien ja sehr wohl vertauschen, da deren Ordnung völlig willkürlich ist.

Will man beispielsweise belegen, dass es gewisse Gruppierungen innerhalb eines sozialen Netzwerks gibt, so kann man diese in örtlicher Nähe zeichnen. Derlei Gruppierungen werden recht viele Verbindungen (Kanten) untereinander aufweisen, aber nur wenige nach außen (zu anderen Gruppierungen). Was nun “viele” oder “wenige” Verbindungen sind, ist oft nicht so klar. Klar sollte aber sein, dass man durch “geschicktes Zeichnen” den Eindruck solcher Gruppierungen unterstützen kann, was auch einen manipulativen Einsatz gestattet.

5.3 Funktionen

5.3.1 Input – Output: Funktionen für Informatiker

Funktionen ordnen Werten aus ihrem Definitionsbereich in eindeutiger Weise Elemente aus ihrem Wertebereich zu. Dieses Verhalten ist Informatikern wohlbekannt: Viele

Programme (oder auch Maschinen) erwarten eine Eingabe (Input), verarbeiten diese und liefern daraufhin (irgendwann) eine Ausgabe (Output). Selbst Phänomene aus der Natur können so modelliert werden, wie das Bild 5.10⁴ zeigt. Neben Programmen werden Ihnen Schaltungen in der Technischen Informatik begegnen. Oft sind die Eingaben sehr eingeschränkt, z.B. mit der Hilfe eines Schalters, der sich in zwei Positionen befinden kann und so den Stromfluss in der Schaltung steuert.

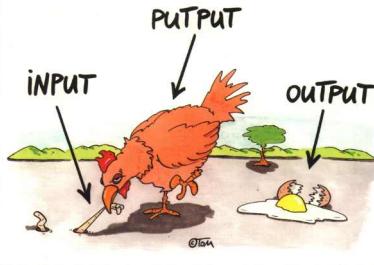


Abbildung 5.10: Das Ein- Ausgabeverhalten der Putput-Maschine.

Eine weitere Anwendung versteckterer doch für Informatiker wichtiger Natur findet sich in der Darstellung von Zahlen im Computer. Tatsächlich ist es nämlich Fiktion anzunehmen, ein Computer könnte problemlos mit den Zahlbereichen umgehen, so wie wir sie auf der Schule kennengelernt haben. Selbst die natürlichen oder die ganzen Zahlen werden intern zumeist als endliche Folgen von Bits dargestellt. Es gibt also eine Abbildung f , die aus der Menge \mathbb{N} der natürlichen Zahlen z.B. auf die Menge aller 32-Bit-Wörter (also Folgen der Länge 32 von einzelnen Bits, die man übrigens auch als Abbildungen von $\{1, 2, \dots, 32\}$ nach $\{0, 1\}$ auffassen kann). Bekanntmaßen gibt es unendlich viele natürliche Zahlen, aber nur endlich viele (wenn auch sehr viele, nämlich 2^{32} viele) verschiedene 32-Bit-Wörter. Daher können längst nicht alle natürlichen Zahlen mit 32-Bit-Wörtern dargestellt werden. In der Praxis wird man sich ein spezielles solches Wort reservieren, das alle Zahlen $\geq 2^{32}$ repräsentiert. Anschaulich (doch abkürzend) könnte man diese Abbildung wie folgt angeben:

$$n \mapsto \begin{cases} 00000000000000000000000000000000, & \text{falls } n = 0 \\ 00000000000000000000000000000001, & \text{falls } n = 1 \\ 0000000000000000000000000000000010, & \text{falls } n = 2 \\ \vdots & \vdots \\ 1111111111111111111111111111111110, & \text{falls } n = 2^{32} - 1 \\ 1111111111111111111111111111111111, & \text{sonst} \end{cases}$$

In der Sprechweise dieses Abschnitts können wir sagen, dass die Funktion, die jeder natürlichen Zahl ihre Zahldarstellung zuordnet, total und (wenn als Wertebereich alle 32-Bit-Zahlen gewählt werden) surjektiv ist, aber eben nicht injektiv. Auch das eigentliche Rechnen muss nun angepasst erfolgen, da Computer eben nur auf der Ebene der Zahldarstellungen rechnen können. So wird in der Technischen Informatik gezeigt, wie aus Halbaddierern Volladdierer aufgebaut werden können, also Schaltungen, die 32-Bit-Zahlen addieren können. Aber auch dabei hat man immer mit einem möglichen “Overflow” zu kämpfen: Selbst wenn zwei Zahlen $< 2^{32}$ zu addieren sind, so kann ihre

⁴Bildnachweis: <http://www.mhaensel.de/images/putput.jpg>

Summe größer als diese Grenze sein, und wir werden notgedrungen entweder einen Fehler signalisieren (z.B. durch die Interpretation von einer Folge aus 32 Einsen als “unendlich”).

5.3.2 Der Graph einer Funktion

Funktionen sind ja bereits aus dem Schulunterricht bekannt. Dort wurden vornehmlich Abbildungen $f : \mathbb{R} \rightarrow \mathbb{R}$ betrachtet, z.B. $x \mapsto x^2$ oder $x \mapsto \sin(x)$. Es wurde auch versucht, diese Abbildungen zu veranschaulichen, indem man die Menge $\{(x, x^2) \mid x \in \mathbb{R}\}$ – um beim ersten Beispiel zu bleiben – in der Euklidischen Ebene $\mathbb{R} \times \mathbb{R}$ als Punkte bzw. Linie eingetragen hat. Diese Darstellung wurde sicher auch als *Graph einer Funktion* angesprochen. Hier ist Vorsicht geboten, denn dieser Begriff eines Graphen ist von dem zu unterscheiden, den wir in den “Diskreten Strukturen” annehmen. In unserer Auffassung ist jedoch $R = \{(x, x^2) \mid x \in \mathbb{R}\}$ nichts anderes als die Relationenschreibweise für die Parabelfunktion.

In der Schule wurde vermutlich auch darauf hingewiesen, dass die Funktion $x \mapsto \sqrt{x}$ “nicht eindeutig” ist. Damit war wohl gemeint, dass die (ja vermutlich bei Ihnen nur für nichtnegative Zahlen definierte) Abbildungsvorschrift zwei Deutungen zulässt, nämlich als positive bzw. negative Wurzel. In unserer Sprechweise liegt das daran, dass die oben eingeführte Relation R nicht voreindeutig ist, weshalb eben die “Wurzelrelation” R^- nicht nacheindeutig und daher keine Funktion ist.

5.3.3 Endliche Folgen und Wörter

Im Bereich der Formalen Sprachen, einem der klassischen Gebiete der Theoretischen Informatik, findet sich eingangs oft folgende Definition:

Definition 5.3.1 Eine endliche, nicht leere Menge heißt Alphabet. Ist Σ ein Alphabet, so heißen seine Elemente auch Buchstaben. Hierauf fußend definiert man Wörter der Länge n über Σ wie folgt induktiv:

- $a \in \Sigma$ ist ein Wort der Länge Eins über Σ .
- Ist w ein Wort der Länge n über Σ und $a \in \Sigma$ ein Buchstabe, so ist wa ein Wort der Länge $n + 1$ über Σ ; das durch Verketten oder Konkatenation der Wörter w und a entstanden ist.

Diese Bildungsvorschrift beschreibt alle Wörter der Länge n über Σ für alle $n \geq 1$. Diese werden auch in der Menge Σ^n aufgesammelt. Schließlich bezeichnet Σ^+ die Menge aller Wörter über Σ beliebiger Länge $n \geq 1$.

Formaler können wir aufschreiben: $\Sigma^+ = \bigcup_{n \in \mathbb{N}, n \geq 1} \Sigma^n$.

Satz 5.3.1 Es sei $n \geq 1$ eine natürliche Zahl und Σ ein Alphabet. Dann gibt es eine Bijektion zwischen Σ^n und $\Sigma^{[n]}$.

Beweis: Wir definieren $f_n : \Sigma^n \rightarrow \Sigma^{[n]}$ induktiv.

$$f_n(w) := \begin{cases} 0 \mapsto w, & \text{falls } n = 1 \\ m \mapsto \begin{cases} f_{n-1}(v)(m), & m < n - 1 \\ a, & m = n \end{cases}, & \text{falls } n > 1, w = va, a \in \Sigma \end{cases}$$

Induktiv kann man beweisen, dass für jede Zahl $n \geq 1$ die Abbildung f_n bijektiv ist. Klar ist dies für $n = 1$.

Sei nun $n > 1$. Wir nehmen nun an, die Aussage gelte für alle $m < n$.

Betrachte eine Folge $h \in \Sigma^{[n]}$. Diese definiert durch $h'(i) := h(i)$ für $i < n - 1$ eine Folge $h' \in \Sigma^{[n-1]}$. Nach Induktionsvoraussetzung gibt es ein Wort w' der Länge $n - 1$ mit $f_{n-1}(w') = h'$. Für das Wort $w := w'a$ der Länge n mit $a = h(n - 1)$ gilt: $f_n(w) = h$. Also ist f_n stets surjektiv.

Betrachte zwei verschiedene Wörter $v = a_1 \cdots a_n$ und $w = b_1 \cdots b_n$ der Länge n über Σ . Gilt $a_n \neq b_n$, so liefert die induktive Definition von f_n , dass die Folgen $h := f_n(v)$ und $g := f_n(w)$ sich unterscheiden, da nämlich $h(n - 1) = a_n \neq b_n = g(n - 1)$. Gilt $a_n = b_n$, so müssen die Wörter $v' := a_1 \cdots a_{n-1}$ und $w' := b_1 \cdots b_{n-1}$ verschieden sein. Nach Induktionsvoraussetzung müssen sich die Folgen $h' := f_{n-1}(v')$ und $g' := f_{n-1}(w')$ unterscheiden, und nach der induktiven Definition von f_n müssen auch $f_n(v)$ und $f_n(w)$ ungleich sein. Also ist f_n stets injektiv. \square

Wir verweisen abschließend auf Abschnitt 4.3.3, in dem endliche Folgen unter einem anderen (verwandten) Blickwinkel betrachtet werden. Dort wird im Übrigen dieselbe Schreibweise M^n für die Menge aller geordneten n -Tupel verwendet wie hier für Wörter der Länge n . Satz 5.3.1 und Satz 4.3.5 drücken aber aus, dass dies dadurch gerechtfertigt ist, dass im Grund dieselben Objekte betrachtet werden.

Als weiterer Ausblick sei erwähnt, dass jede Menge von Wörtern über einem Alphabet Σ auch als Sprache über Σ angesprochen wird. In der Theorie der Formalen Sprachen studiert man vornehmlich Mengen von Sprachen und ihre Eigenschaften, also Teilmengen von 2^{Σ^+} .

Ganz allgemein werden Ihnen induktive Definitionen wie 5.3.1 häufiger in Ihrem Informatik-Studium begegnen.

5.3.4 Induktiv definierte Folgen

Aufgrund des Induktionsaxioms kann man Folgen gut induktiv definieren. Induktiv definierte Folgen sind wie geschaffen für das Praktizieren von Induktionsbeweisen, da diesen dasselbe Schema zugrunde liegt.

Beispiel:

$$f(n) = \begin{cases} 0, & \text{falls } n = 0 \\ 1, & \text{falls } n = 1 \\ f(n-1) + f(n-2), & \text{falls } n > 1 \end{cases}$$

definieren die *Fibonacci-Zahlen*. Mehr dazu finden Sie beispielsweise auch bei einem virtuellen Museumsbesuch.

Der Goldene Schnitt ist die Teilung einer Strecke so, dass die gesamte Strecke X sich zu dem größerem Teilstück der Länge 1 verhält wie das größere Teilstück zum kleineren.

Das Teilverhältnis lässt sich nun einfach ausrechnen. Es gilt:

$$X : 1 = 1 : (X - 1), \quad \text{also: } X^2 - X = 1$$

mit den Lösungen ϕ und $\hat{\phi} = 1 - \phi$, wobei

$$\phi = \frac{1 + \sqrt{5}}{2} \approx 1.6181 \dots$$

die *goldene Schnitzahl* ist.

Eine Möglichkeit zur Konstruktion der goldenen Schnittzahl ϕ bietet das regelmäßige Fünfeck in Gestalt des Pentagramms. Im Pentagramm findet sich ϕ wie folgt: Bildnachweis fehlt. Nach einem Strahlensatz gilt in der Figur 5.11:

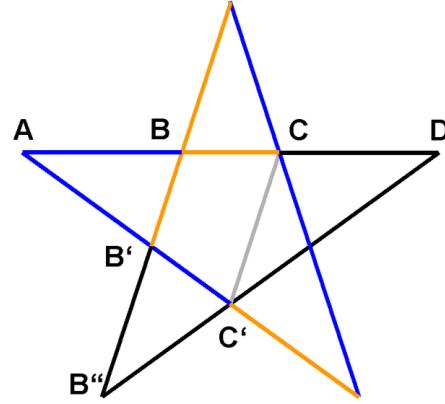


Abbildung 5.11: Ein Hilfs-Pentagramm zur Konstruktion der goldenen Schnittzahl.

$$\frac{\overline{AC}}{\overline{AB}} = \frac{\overline{CC'}}{\overline{BB'}}$$

$$\overline{AB} = \overline{CD} = \overline{CC'} \text{ und } \overline{BC} = \overline{BB'} \rightsquigarrow$$

$$\frac{x}{1} = \frac{\overline{AC}}{\overline{AB}} = \frac{\overline{AB}}{\overline{BC}} = \frac{\overline{AB}}{\overline{AC} - \overline{AB}} = \frac{1}{x-1}$$

Wir diskutieren jetzt noch einige Zusammenhänge zwischen den Fibonacci-Zahlen und dem Goldenen Schnitt.

Satz 5.3.2 (Formel von Binet) $f_n = \frac{\phi^n - (1-\phi)^n}{\sqrt{5}}$, mit $\phi = \frac{1+\sqrt{5}}{2}$ erfüllt $x^2 = x + 1$.

Beweis: Wir führen einen Induktionsbeweis. $n = 0$ und $n = 1$ sind elementar. Für den Induktionsschritt beobachten wir:

$$\phi^2 = 1 + \phi = 1 + \frac{1 + \sqrt{5}}{2}; \quad (1 - \phi)^2 = 1 + (1 - \phi) = 1 + \frac{1 - \sqrt{5}}{2}$$

Also gilt:

$$\begin{aligned} \frac{\phi^{n+2} - (1 - \phi)^{n+2}}{\sqrt{5}} &= \frac{\phi^n(1 + \phi) - (1 - \phi)^n(1 + (1 - \phi))}{\sqrt{5}} \\ &= \frac{\phi^n + \phi^{n+1} - (1 - \phi)^n - (1 - \phi)^{n+1}}{\sqrt{5}} \\ &= f_{n+1} + f_n = f_{n+2} \end{aligned}$$

□

Einen weiteren Zusammenhang zwischen Goldenem Schnitt und Fibonacci-Zahlen bietet folgende Formel:

$$\lim_{n \rightarrow \infty} \frac{f_n}{f_{n-1}} = \phi.$$

Einen formalen Nachweis überlassen wir dem Leser.

5.3.5 Eine Zahlenfolge aus dem Finanzwesen

Nehmen wir einmal an, Sie hätten einen Betrag von 100.000 Euro geerbt und wollen diesen investieren. Die Bank Ihres Vertrauens bietet Ihnen bei zehnjähriger Geldanlage $p\%$ Zinsen, die immer am Jahresende ausgezahlt werden. Die Anlage erfolgt thesaurierend, d.h., auch auf die Zinsen des ersten Jahres gibt es im zweiten Jahr (und in den Folgejahren) ebenfalls Zinsen. Wie hoch ist Ihr so angelegtes Vermögen nach 10 Jahren?

Wir können natürlich sukzessive rechnen, sagen wir konkret für $p = 3$:

- Nach 0 Jahren (also zu Beginn) beträgt das Vermögen $V_0 = 100.000$.
- Nach 1 Jahr gilt: $V_1 = V_0 \cdot (1 + \frac{p}{100}) = 103.000$.
- Nach 2 Jahren haben wir: $V_2 = V_1 \cdot (1 + \frac{p}{100}) = 106.090$.
- Nach 3 Jahren ist: $V_3 = V_2 \cdot (1 + \frac{p}{100}) = 109.182,70$.
- ...

Das ist schon eine langwierige Rechnung, bis wir so auf den Betrag nach 10 Jahren gekommen sind. Können wir die Bildungsvorschrift herausbekommen? Betrachten wir nochmals

$$V_3 = V_2 \cdot q = V_1 \cdot q \cdot q = V_0 \cdot q \cdot q \cdot q$$

mit $q = 1 + \frac{p}{100}$. Die Formel

$$V_n = V_0 \cdot q^n$$

sieht schon deutlich angenehmer aus. Für jedes Zahlenpaar (V_0, p) von Ausgangsvermögen und Zinsfuß erhalten wir so eine Zahlenfolge, deren n -tes Glied das Vermögen nach n Jahren angibt, wobei wir den Zinseszinseffekt in die Formel eingebaut haben.

Wenn Ihnen diese Herleitung zu geschwind erscheint, so ist es natürlich möglich, mit der Aufstellung einer induktiven Vorschrift zu beginnen:

$$V_n = \begin{cases} V_0, & \text{falls } n = 0 \\ V_{n-1} \cdot q, & \text{falls } n > 0 \end{cases}$$

Diese Vorschrift ist eine unmittelbare Umsetzung der vereinbarten Zinszahlungsregel. Die behauptete Formel folgt nun durch einen einfachen Induktionsbeweis.

5.3.6 Zum Multiplizieren langer Zahlen

Wir betrachten das Problem, zwei *sehr* lange natürliche Zahlen auf einem Computer miteinander zu multiplizieren. Worin besteht hier das Problem? Für (relativ) *kurze* natürliche Zahlen gibt es in der Regel Maschinenbefehle, die diese Aufgabe sehr geschwind erledigen. Für längere Zahlen muss man sich eine geeignete Multiplikation selbst programmieren unter Rückgriff auf jene Maschinenbefehle, will man die Aufgabe korrekt erledigen und sich nicht mit Überlauffehlern (overflow errors) zufrieden geben. Weiterhin ist es zumeist so, dass (auf Maschinenebene) die Multiplikation zweier Zahlen erheblich länger dauert als die Addition zweier Zahlen. Daher wollen wir im Folgenden auch nur die Zahl der Multiplikationen (als Maschinenbefehle) berücksichtigen und die Zahl der Additionen vernachlässigen ebenso wie die auftretenden Überträge sowie die Multiplikationen mit Maschinenwortgrößen, die durch "Bitshifts" sehr effizient implementiert werden können.

Es seien also $a = a_n \dots a_1$ und $b = b_n \dots b_1$ zwei (lange) ganze Zahlen, die jeweils aus n Maschinenworten aufgebaut sind. Dabei kann man sich also a_i z.B. als Folge von 32 Bits vorstellen. Die "Schulmethode" wird nun n -mal n Multiplikationen ausführen, z.B. $a_1 \cdot b_1, \dots, a_1 \cdot b_n$ (und daraus die Zahl $a_1 \cdot b$ ermitteln), $a_2 \cdot b_1, \dots, a_2 \cdot b_n$ (und daraus die Zahl $a_2 \cdot b$ ermitteln), $\dots, a_n \cdot b_1, \dots, a_n \cdot b_n$ (und daraus die Zahl $a_n \cdot b$ ermitteln). Aus der Addition der bit-verschobenen Zahlen $a_i \cdot b$ ergibt sich schließlich das erwünschte Ergebnis ab .

Tatsächlich kann man mit deutlich weniger Multiplikationen auskommen. Das wollen wir uns im Folgenden überlegen. Dazu nehmen wir weiter vereinfachend an, dass $n = 2^k$ gilt, also eine Zweierpotenz ist. Die Schulmethode benötigt also $n^2 = (2^k)^2 = 4^k$ Multiplikationen. Unser neues Verfahren wird mit 3^k Multiplikationen auskommen. Wir setzen außerdem g als "Basis" oder "Maschinenwortgröße", d.h.,

$$a = \sum_{i=1}^n g^{i-1} a_i.$$

Nun können wir wie folgt rechnen wegen

$$a = a_n \dots a_{n/2+1} g^{n/2} + a_{n/2} \dots a_1 :$$

$$\begin{aligned} a \cdot b &= (a_n \dots a_{n/2+1} g^{n/2} + a_{n/2} \dots a_1) \cdot (b_n \dots b_{n/2+1} g^{n/2} + b_{n/2} \dots b_1) \\ &= (a_n \dots a_{n/2+1} \cdot b_n \dots b_{n/2+1}) \cdot g^n \\ &\quad + (a_n \dots a_{n/2+1} \cdot b_{n/2} \dots b_1 + a_{n/2} \dots a_1 \cdot b_n \dots b_{n/2+1}) \cdot g^{n/2} \\ &\quad + a_{n/2} \dots a_1 \cdot b_{n/2} \dots b_1 \end{aligned}$$

Wir haben also die Multiplikation von zwei Zahlen der Länge $n = 2^k$ auf vier Multiplikation von zwei Zahlen der Länge $n/2 = 2^{k-1}$ zurückgeführt. Für die Anzahl der benötigten Multiplikationen $M(k)$ können wir also festhalten (da das Verfahren sicher für $n = 1$, also $k = 0$, abbricht, weil nunmehr die elementaren Maschinenbefehle zur Verfügung stehen):

$$M(k) = \begin{cases} 1 & k = 0, \\ 4 \cdot M(k-1) & k > 0. \end{cases}$$

Man überlegt sich leicht (formal per Induktion), dass $M(k) = 4^k$ gilt; wir haben also noch nichts gegenüber der Schulmethode gewonnen.

Der Trick besteht nun darin zu erkennen, dass es genügt, die folgenden drei Hilfsgrößen in der Rekursion zu ermitteln:

$$\begin{aligned} AB_T &= a_{n/2} \dots a_1 \cdot b_{n/2} \dots b_1 \\ AB_H &= a_n \dots a_{n/2+1} \cdot b_n \dots b_{n/2+1} \\ AB_M &= (a_{n/2} \dots a_1 + a_n \dots a_{n/2+1}) \cdot (b_{n/2} \dots b_1 + b_n \dots b_{n/2+1}) \end{aligned}$$

Hierin werden die tiefen, hoch und gemischten Anteile der Multiplikation gespeichert. Diese Information genügt, denn es gilt:

$$(a_n \dots a_{n/2+1} \cdot b_{n/2} \dots b_1 + a_{n/2} \dots a_1 \cdot b_n \dots b_{n/2+1}) = AB_M - AB_T - AB_H.$$

Für die Anzahl $M'(k)$ der benötigten Multiplikationen zweier Zahlen der Länge 2^k ergibt sich für dieses Verfahren:

$$M'(k) = \begin{cases} 1 & k = 0, \\ 3 \cdot M'(k-1) & k > 0. \end{cases}$$

Man überlegt sich leicht (formal per Induktion), dass $M'(k) = 3^k$ gilt; wir haben also deutlich gegenüber der Schulmethode gewonnen.

5.3.7 Nacheindeutigkeit und Vortotalität für Informatiker

Beide Begriffe werden unter diesen Namen kaum in der Praktischen Informatik auftauchen. Dennoch sind sie von großer Wichtigkeit, um viele Konzepte zu verstehen. Wir reißen hier nur drei Bereiche kurz an.

- Beim Entity-Relationship-Modell (kurz ER-Modell) im Bereich der Datenbanken werden den Objekten (Entitäten) gewisse Eigenschaften (Attribute) beigegeben. So könnte eine Entität für Personen als Attribute “Familienname”, “Vorname”, “Anschrift”, “Geburtsdatum”, “Geburtsort”, “Personalausweisnummer”, ... besitzen. Wir können solch eine Entität als mehrstellige Relation begreifen. Wir wollen das hier allerdings nicht vertiefen, da wir ansonsten auf Abschnitt 4.2.1 verweisen müssten. Wir interessieren uns hier mehr für die Frage, welches Attribut (oder auch welche Menge von Attributen gemeinsam) eine Entität eindeutig festlegen. Solche Attribute heißen *Schlüsselattribute*. In unserem Beispiel wäre die Personalausweisnummer solch ein Schlüsselattribut, da jede Personalausweisnummer zweifelsfrei die betroffene Person eindeutig bestimmt (und damit auch alle anderen Attribute). Die Zuordnung Personalausweisnummer \rightarrow Person ist daher eine partielle Funktion. Da unklar ist, ob jede (potentielle) Personalausweisnummer auch einer Person zugeordnet werden kann (insbesondere für die real vorliegende Datenbank), ist die Vortotalität allerdings zweifelhaft. Unklar ist auch, ob überhaupt jede Person in der Datenbank eine Personalausweisnummer besitzt; zum Beispiel ist das bei Kindern ja erst ab einem gewissen Alter Pflicht. Die beschriebene Funktion ist also nicht notwendig nachtotal. Jede Person sollte aber höchstens eine Personalausweisnummer besitzen, d.h., die beschriebene Relation ist voreindeutig.
- Im Bereich der Verschlüsselungstechnik werden Nachrichten (meist aufgefasst als Wörter über dem Binäralphabet $\{0, 1\}$) übersetzt in andere. Die entsprechende Vorschrift $f : \{0, 1\}^+ \rightarrow \{0, 1\}^+$ sollte sicherlich nacheindeutig sein. Da die Nachrichten auch wieder entschlüsselt werden sollen, sollte f auch voreindeutig sein. Ob wirklich alle Binärwörter in die eine oder andere Richtung übersetzt werden müssen, hängt von der Anwendung ab. Jedenfalls wäre das die Frage nach der Vortotalität bzw. Nachtotalität.
- Angenommen, Sie hätten ein Programm geschrieben, das bei Eingabe von n die n -te Fibonacci-Zahl ausrechnen soll (siehe Abschnitt 5.3.4). Wir wollen einmal davon ausgehen, dass es sich funktional verhält in dem Sinne, dass bei derselben Eingabe stets dieselbe Zahlwert ausgegeben wird. Damit ist klar, dass Ihr Programm eine partielle Funktion implementiert. Ob Ihr Programm aber auf allen zulässigen Eingaben tatsächlich hält, ob die von Ihnen implementierte Funktion also total ist, das ist längst nicht so klar. Tatsächlich ist diese Terminierungsfrage nur sehr schwer zu beantworten, und man kann zeigen, dass dies automatisiert sogar unmöglich ist. Dennoch steht außer Frage, dass die Vortotalitätsfrage von größter Bedeutung ist, wann immer Sie eine Implementierung ausführen und testen wollen.

5.3.8 Modellieren mit Mengen, Relationen und Funktionen

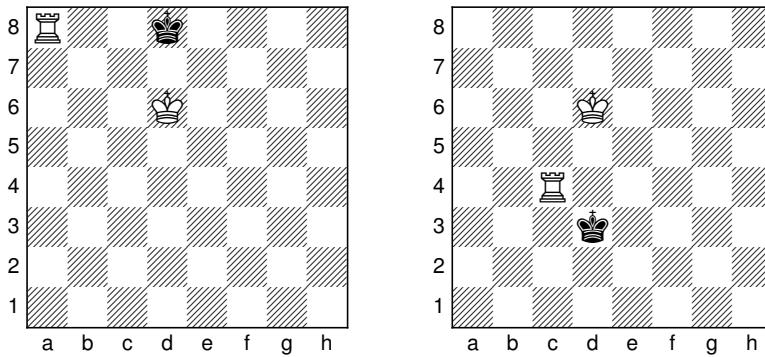


Abbildung 5.12: Zwei gültige Stellungen in einem einfachen Turmendspiel.

Das Modellieren verschiedenster Situationen gehört zum Grundgerüst jedes Informatikers. Dies ist auch notwendig, bevor man irgendein Programm schreiben möchte. So ein (mathematisches) Modell zeigt auch, inwiefern ein Grundverständnis des Gebietes vorhanden ist, in dem das nämliche Programm eingesetzt werden soll.

Wir wollen uns in diesem Sinne im Folgenden mit einfachen Turmendspielen im Schach beschäftigen. Darunter wollen wir Stellungen verstehen, in denen nur noch ein Turm und zwei Könige auf dem Brett sind, wie z.B. in Bild 5.12. Tatsächlich sind hier zahlreiche Modellierungsentscheidungen zu treffen. Wir diskutieren im Folgenden einige wichtige.

- Wie soll das Spielbrett dargestellt werden? Beim üblichen Schachspiel gibt es ein 8x8-Brett mit 64 Feldern. Daher wäre es möglich, dieses durch $[64]$ oder auch durch $[8 \times 8]$ zu modellieren. Den üblichen Positionsschreibweisen folgend, legen wir fest:

$$SB := \{a, b, c, d, e, f, g, h\} \times \{1, 2, 3, 4, 5, 6, 7, 8\}.$$

Ähnlich wie in Abschnitt 5.3.3 schreiben wir die geordneten Paare als (kurze)

	a8	b8	c8	d8	e8	f8	g8	h8
7	a7	b7	c7	d7	e7	f7	g7	h7
6	a6	b6	c6	d6	e6	f6	g6	h6
5	a5	b5	c5	d5	e5	f5	g5	h5
4	a4	b4	c4	d4	e4	f4	g4	h4
3	a3	b3	c3	d3	e3	f3	g3	h3
2	a2	b2	c2	d2	e2	f2	g2	h2
1	a1	b1	c1	d1	e1	f1	g1	h1
	a	b	c	d	e	f	g	h

Wörter. Unsere “Feldnamen” sehen also wie folgt aus:

- Als Nächstes müssen wir Stellungen beschreiben. Dazu müssen wir zunächst verstehen, was das genau in unserem Fall bedeutet. Weiter oben wurde sagt, wir kümmern uns um *einfache Turmendspiele*, was bedeuten sollte, dass ein Turm und zwei Könige auf dem Brett sind. Im üblichen Schachspiel darf jede Figur auf dem Brett nur auf genau einem Feld stehen. Da (spätestens in dieser Spielphase)

Weiβ und Schwarz völlig gleichberechtigt sind, können wir (wie in Bild 5.12) davon ausgehen, dass ein weißer Turm, ein weißer König und ein schwarzer König auf dem Brett sind. Die Menge der Figuren ist also

$$F := \{\kappa, \mathbb{K}, \mathbb{Q}\}$$

Das Setzen einer Figur auf ein Feld können wir als Abbildung $F \rightarrow SB$ auffassen. Allerdings wollen wir verhindern, dass mehrere Figuren auf dasselbe Feld gestellt werden dürfen. Deshalb definieren wir:

$$Pos := \{\pi : F \rightarrow SB \mid \pi \text{ ist injektiv}\}.$$

- Da Schwarz nur noch den König auf dem Feld hat, kann Schwarz nicht mehr gewinnen. Weiβ kann hingegen Schwarz noch mattsetzen. Die linke Seite von Bild 5.12 zeigt so eine Gewinnstellung für Weiβ. Können wir irgendwie formal beschreiben, wie derartige Mattpositionen ausschauen? Der weiße Turm kann ja nur eine Reihe abdecken, sodass die übrigen Fluchtfelder des schwarzen Königs mit dem weißen König blockiert sein müssen. Deshalb muss sich der schwarze König am Rand befinden, und der weiße König muss ihm gegenüber stehen. Wir definieren daher die Relation:

$$opp := opp_o \cup opp_u \cup opp_\ell \cup opp_r \subseteq SB \times SB$$

mit (beispielsweise) $opp_o =$

$$\{(a6, a8), (b6, b8), (c6, c8), (d6, d8), (e6, e8), (f6, f8), (g6, g8), (h6, h8)\}.$$

Die übrigen Teilrelationen von opp kann der Leser sicher selbst definieren. Jetzt können wir genauer sagen: Der schwarze König steht am Rand und gleichzeitig dem weißen König gegenüber in der Stellung $\pi \in Pos$, falls $(\pi(\mathbb{K}), \pi(\mathbb{Q})) \in opp$. Um wirklich ausdrücken zu können, ob eine Mattposition vorliegt, müssen wir noch genauer beschreiben, was es bedeutet, dass eine Figur eine andere bedroht. Das wiederum hängt eng mit der Frage zusammen, wohin bzw. wie Figuren ziehen dürfen.

- Für jede Figur $f \in F$ wollen wir die Relation $Zug_f \subseteq Pos \times Pos$ bestimmen, die angibt, welche Stellung $q \in Pos$ von $p \in Pos$ aus erreicht werden kann, wenn Figur f bewegt wird. Dann genau soll nämlich $(p, q) \in Zug_f$ gelten. Um dies hinschreiben zu können, legen wir zunächst fest, welche Felder erreicht werden könnten, wenn keine weiteren Figuren auf dem Brett stehen. Dazu definieren wir Abbildungen $pot - Zug_f : SB \rightarrow 2^{SB}$ potentieller Züge. Für $f \in \{\mathbb{K}, \mathbb{Q}\}$ gilt:

$$pot - Zug_f(xy) = \{x^-y, x^-y^-, xy^-, x^+y^-, x^+y, x^+y^+, xy^+, x^-y^+\},$$

wobei gilt: $a^+ = b$, $b^+ = c$, $c^+ = d$, $d^+ = e$, $e^+ = f$, $f^+ = g$, $g^+ = h$, $b^- = a$, $c^- = b$, $d^- = c$, $e^- = d$, $f^- = e$, $g^- = f$, $h^- = g$ und entsprechend für die Ziffernbezeichnungen der Zeilen. Ist eine Operation undefiniert, wie beispielsweise a^- , dann bedeutet dies, dass eine a^- enthaltene ‘‘Feldbezeichnung’’ in $pot - Zug_f(ay)$ undefiniert ist und somit $pot - Zug_f(ay)$ weniger Felder enthält als im allgemeinen Fall. Der König kann also potentiell eines seiner Nachbarfelder besuchen. Für den Turm $f = \kappa$ können wir festlegen:

$$pot - Zug_f(xy) = \{uv \in SB \mid u = x \vee v = y\} \setminus \{xy\}$$

Mit diesen Hilfsdefinitionen können wir nun Zug_f genauer festlegen. Beginnen wir mit dem schwarzen König: Dieser kann überall hinziehen, wo er potentiell ziehen dürfte, es sei denn, so ein Feld $xy \in SB$ ist gegenwärtig vom weißen König belegt, oder der weiße König könnte auf nach xy ziehen, oder der weiße Turm könnte nach xy ziehen. Ein Sonderfall ist die Möglichkeit, den weißen Turm zu schlagen, so wie dies auf der rechten Seite von Bild 5.12 gezeigt ist. Da wir (in unserem Modell) ein derartiges Schlagen nicht vorsehen (Woran liegt das formal?), merken wir uns dies an dieser Stelle, da wir weiter unten noch auf das Thema Remispositionen zu sprechen kommen. Wir wollen einen derartigen Zug hier jetzt erstmal nicht erlauben. Somit gilt (formal): $(\pi_1, \pi_2) \in \text{Zug}_\#$ genau dann, wenn

- $\forall f \in F \setminus \{\kappa\} : \pi_1(f) = \pi_2(f)$ (d.h., die übrigen Figuren bleiben unverändert an ihren Plätzen stehen) und
- $\pi_2(\kappa) \in \text{pot} - \text{Zug}_\#(\pi_1(\kappa))$, aber es muss auch gelten:
- $\pi_2(\kappa) \notin \text{pot} - \text{Zug}_\#(\pi_1(\kappa)) \cup \text{pot} - \text{Zug}_\#(\pi_1(\kappa)) \cup \{\pi_1(\kappa), \pi_1(\kappa)\}$ (also darf dem Zug des schwarzen Königs kein weißer Stein “entgegenstehen”).

Ähnlich können wir für den weißen König festlegen: $(\pi_1, \pi_2) \in \text{Zug}_\#$ genau dann, wenn

- $\forall f \in F \setminus \{\kappa\} : \pi_1(f) = \pi_2(f)$ (d.h., die übrigen Figuren bleiben unverändert an ihren Plätzen stehen) und
- $\pi_2(\kappa) \in \text{pot} - \text{Zug}_\#(\pi_1(\kappa))$, aber es muss auch gelten:
- $\pi_2(\kappa) \notin \text{pot} - \text{Zug}_\#(\pi_1(\kappa)) \cup \{\pi_1(\kappa), \pi_1(\kappa)\}$ (also darf dem Zug des weißen Königs kein anderer Stein “entgegenstehen”).

Auf die formale Beschreibung der möglichen Turmnachfolgepositionen Zug_# verzichten wir hier. Das ist sicherlich auch eine gute Übungsaufgabe für Sie. Wir können jetzt noch festlegen, was ein (gültiger) Zug von Weiß bzw. Schwarz sein soll:

- $W - \text{Zug} \subseteq \text{Pos} \times \text{Pos}$ ist festgelegt durch: $W - \text{Zug} = \text{Zug}_\# \cup \text{Zug}_\#$,
- $S - \text{Zug} \subseteq \text{Pos} \times \text{Pos}$ ist festgelegt durch $S - \text{Zug} = \text{Zug}_\#$.

- Die bisherigen Festlegungen gestatten es nun aufzuschreiben, was eine Mattposition und was eine Remisposition sein kann:

- $\pi_1 \in \text{Pos}$ ist Mattposition genau dann, wenn es kein π_2 gibt mit $(\pi_1, \pi_2) \in \text{Zug}_\#$.
- $\pi_1 \in \text{Pos}$ ist Remisposition genau dann, wenn es ein $(\pi_1, \pi_2) \in \text{Zug}_\#$ gibt mit $\pi_2(\kappa) = \pi_1(\kappa)$. Das bedeutet nämlich, dass der weiße Turm nicht durch den weißen König gedeckt wird und somit geschlagen werden könnte. Wenn jetzt (zum Beispiel auf der rechten Seite von Bild 5.12) Schwarz am Zug wäre, könnte eine Position hergestellt werden mit nur noch zwei Königen auf dem Brett, ein sicheres Remis. Offenbar ist es aber hier wichtig, wer am Zuge ist, denn Weiß am Zuge könnte (im Allgemeinen jedenfalls) seinen Turm auch einfach wegziehen und so das Remis verhindern.

Wir haben hierbei auch das Thema Zugwiederholungen außen vor gelassen, da dies erforderte, sich die einmal gemachten Züge zu merken. Das passt nicht in unser Modell.

- Schachspieler werden bemerkt haben, dass die von uns bislang genau genommen Halbzüge beschrieben wurden. Gehen wir nun davon aus, dass ein Turmendspiel immer durch einen (Halb-)Zug von Weiß eröffnet wird, so sehen wir, dass ein (vollständiger) Zug formal wie folgt angegeben werden kann:

$$\text{Zug} := W - \text{Zug} \circ S - \text{Zug},$$

also durch einen weißen Halbzug, gefolgt von einem schwarzen Halbzug. Ein Schachspiel ist nichts Anderes als eine Folge solcher Züge, schließlich gefolgt durch einen weißen Halbzug, der Schwarz mattsetzt oder aber zum Remis führt.

5.4 Zur Größe von Mengen

5.4.1 Indikatorfunktion und Bitvektor

Indikatorfunktionen begegnen wir immer wieder in diesem Skript, angefangen von Beispiel 3.3.17. Sie spielen auch eine wichtige Rolle bei der Implementierung von Mengen und ihren Operationen auf Rechnern. Das wollen wir im Folgenden ausführen.

Eine Teilmenge $A \subseteq M = \{a_1, \dots, a_n\}$ können wir darstellen durch einen Bitvektor $b = (b_1, \dots, b_n)$ mit $b_i = 1$, falls $a_i \in A$, und $b_i = 0$, falls $a_i \notin A$. Offenkundig besteht ein enger Zusammenhang mit der Indikatorfunktion χ_A . Im Grunde genommen wurde nur noch die Nummerierung (Indizierung) der Elemente der Grundmenge M ausgenutzt. Es gilt also: $\chi_A(a_i) = b_i$.

Folgen von Nullen und Einsen sind natürlich wie gemacht zur Verarbeitung in Rechenanlagen. Wie kann man aber nun im Sinne der Mengenalgebra auf Computern rechnen? Wollen wir beispielsweise zwei Mengen A und A' vereinigen, so entspricht das einem “bitweisen Oder” der zugehörigen Bitvektoren b und b' . Gilt also $A \cup = A \cup A'$, so gilt: $\chi_{A \cup} = (b_i \vee b'_i)$. Dafür gibt es in manchen Programmiersprachen einen eigenen Befehl, z.B. in C den einfachen vertikalen Strich. Entsprechend gilt für $A \cap = A \cap A'$: $\chi_{A \cap} = (b_i \wedge b'_i)$. In C schreibt man hierfür `&&`.

Die entsprechenden algebraischen Überlegungen folgen in Abschnitt über Verknüpfungen

Bitvektoren haben wir soeben in Listenschreibweise für Folgen von Elementen aus $\{0, 1\}$ eingeführt. In Abschnitt 5.3.1 haben wir gesehen, dass ihnen (genau) die Binärwörter entsprechen.

Da wir uns in diesem Abschnitt des Haupttexts mit dem Abzählen von Mengen beschäftigen, mag das Folgende interessant erscheinen.

Lemma 5.4.1 *Es gibt $2^{n+1} - 2$ (nicht leere) Binärwörter der Länge höchstens n .*

Da wir das “leere Wort” (das Wort der Länge Null) hier nicht eingeführt haben, zählen wir es auch nicht mit. Die Aufgabe besteht also darin, die Menge

$$\bigcup_{i=1}^n \{0, 1\}^i$$

abzuzählen.

Beweis: Kombiniere: Summenregel, Potenzregel und geometrische Reihe (siehe Aufgabe 6.3.7).

□

Beispiel: Wie viele Folgen der Länge acht über der Menge $\{0, 1\}$ fangen mit Null an oder enden mit 11? Wir lösen diese Frage mit der einfachen allgemeinen Summenregel.

$$A = \{w \in \{0, 1\}^8 \mid \exists x \in \{0, 1\}^7 : w = (0, x)\}$$

$$B = \{w \in \{0, 1\}^8 \mid \exists y \in \{0, 1\}^6 : w = (y, 1, 1)\}$$

$$A \cap B = \{w \in \{0, 1\}^8 \mid \exists z \in \{0, 1\}^5 : w = (0, z, 1, 1)\}$$

$$\leadsto |A \cup B| = |A| + |B| - |A \cap B| = 2^7 + 2^6 - 2^5 = 160.$$

5.4.2 Ein ausführlicheres Beispiel zur Summen- und Produktregel

In einigen (älteren) Programmiersprachen beginnt jeder Variablenname mit einem der 26 Buchstaben des Alphabets.

Anschließend folgen bis zu sieben weitere Zeichen, wovon jeder entweder ein Buchstabe oder eine der Ziffern 0 bis 9 ist.

Wie viele verschiedene Variablennamen gibt es?

Wir können die Menge A der Variablennamen in 8 disjunkte Teilmengen aufteilen: A_i bezeichne all Variablennamen der Länge i , $i = 1, \dots, 8$.

Summenregel $\leadsto |A| = |A_1| + |A_2| + |A_3| + |A_4| + |A_5| + |A_6| + |A_7| + |A_8|$.

Offensichtlich gilt: $|A_1| = 26$.

Die Menge der Buchstaben und Ziffern hat nach der Summenregel 36 Elemente.

Die Produktregel liefert: $|A_i| = 26 \cdot 36^{i-1}$.

Die geometrische Reihe (siehe Aufgabe 6.3.7) liefert im vorigen Beispiel:

$$A = 26 \cdot \left(\sum_{i=0}^7 36^i \right) = 26 \cdot \frac{36^8 - 1}{35} \approx 10^{12}.$$

	2		5		1		9	
8			2		3			6
	3			6			7	
		1				6		
5	4						1	9
		2				7		
	9			3			8	
2			8		4			7
	1		9		7		6	

Ungelöstes Sudoku

4	2	6	5	7	1	3	9	8
8	5	7	2	9	3	1	4	6
1	3	9	4	6	8	2	7	5
9	7	1	3	8	5	6	2	4
5	4	3	7	2	6	8	1	9
6	8	2	1	4	9	7	5	3
7	9	4	6	3	2	5	8	1
2	6	5	8	1	4	9	3	7
3	1	8	9	5	7	4	6	2

Gelöstes Sudoku

Abbildung 5.13: Ein klassisches Sudoku-Rätsel, auch als Beispiel für die Graphikfähigkeiten von L^AT_EX.

5.4.3 Sudoku

Wir wollen uns jetzt mit dem bekannten Sudoku-Spiel beschäftigen. Typischerweise sehen solche Rätsel wie in Bild 5.13 aus. Das ist uns aber für unsere Abzählungsaufgaben zu schwierig. Daher vereinfachen wir das Spiel wie folgt: Wir haben nur noch ein 4×4 -“Spielbrett” zur Verfügung, unterteilt in zweimal zwei 2×2 -Quadrate. Hierin sind nun vier Einsen, vier Zweien, vier Dreien und vier Vieren so einzufügen, dass in jeder Zeile, jeder Spalte und jedem 2×2 -Quadrat genau eine davon steht. Wir wollen uns nun fragen, wie viele derartige “gelöste Sudokus” es überhaupt geben kann. Bild 5.14 zeigt einige solcher Lösungen, die sich immer nur “ein wenig” voneinander unterscheiden.

1	2	3	4
3	4	1	2
2	1	4	3
4	3	2	1

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
3	4	2	1
4	3	1	2
2	1	4	3

1	2	3	4
4	3	2	1
3	4	1	2
2	1	4	3

Abbildung 5.14: Einige gelöste “kleine Sudokus”.

Offensichtlich gibt es $4! = 24$ verschiedene Möglichkeiten, die vier Zahlen auf der obersten Zeile anzugeben. Wir haben uns in Bild 5.14 auf eine Reihenfolge festgelegt: 1 – 2 – 3 – 4. Wenn wir jetzt das erste Feld in der zweiten Reihe belegen wollen, so verbleiben zwei Möglichkeiten: 3 oder 4. Was auch immer wir wählen, das zweite Feld in der zweiten Reihe ist somit festgelegt, damit das 2×2 -Quadrat “links oben” den Regeln gemäß gefüllt ist. Für das dritte Feld der zweiten Reihe gibt es wiederum zwei Möglichkeiten, was dann das letzte Feld der zweiten Reihe festlegt. Somit haben wir insgesamt $24 \times 4 = 96$ Möglichkeiten, die oberen zwei Zeilen zu füllen (falls es überhaupt eine Lösung gibt). Für das erste Feld der dritten Reihe haben wir wieder zwei Freiheitsgrade, ebenso für das zweite Feld der dritten Reihe. Dann ist aber alles andere festgelegt. Das ist sowieso klar für die ersten beiden Felder der letzten Reihe.

Betrachten wir jetzt einmal das dritte Feld der dritten Reihe genauer. Gehen wir davon aus, dass in der ersten Reihe 1 – 2 – 3 – 4 eingetragen wurde. Fixieren wir für eine erste genauere Diskussion auch die zweite Reihe: 3 – 4 – 1 – 2. Es gibt (von dieser Lage aus beurteilt) noch zwei Möglichkeiten, das dritte Feld der dritten Reihe zu füllen; 2 oder 4. Wenn wir nun die (prinzipiellen) Möglichkeiten zum Füllen der ersten beiden Felder der dritten Reihe anschauen: 2 – 1, 2 – 3, 4 – 1, 4 – 3, so sehen wir, dass alle das dritte Feld eindeutig festlegen. Tatsächlich gibt es daher 96 verschiedene Sudoku-Lösungen.

Dazu kann man sich noch folgende Überlegungen machen, wieder ausgehend (o.E.) von 1 – 2 – 3 – 4 in der ersten Reihe:

- Auf den dritten und vierten Feldern der zweiten Reihe stehen die Zahlen 1 – 2 oder 2 – 1.
- Wenn wir eine Zeile festlegen (nämlich die dritte oder vierte), in der wir 1 eingetragen im 2×2 -Quadrat links unten, dann ist entweder in der dritten oder in der vierten Spalte klar, ob dort eine 4 bzw. 3 eingetragen werden muss, womit wir zwei Spalten vollständig festgelegt haben.
- Entsprechendes gilt für die Eintragung der 2.

- Keine dieser Festlegungen führt zu Widersprüchen.

5.4.4 Wahrscheinlichkeitsrechnung bei Gleichverteilungen

Eine der wichtigen Anwendungsgebiete der Kombinatorik ist die Wahrscheinlichkeitsrechnung.

Definition 5.4.1 Eine höchstens abzählbare Menge heißt auch (diskreter) Ereignisraum. Die Elemente eines Ereignisraums heißen elementare Ereignisse. Ereignisse sind Teilmengen des Ereignisraums.

Deutung: Ein *Zufallsexperiment* liefert ein Ergebnis, das nicht genau vorherzusagen ist.

Beispiel: Ein *Münzwurf* hat zwei elementare Ereignisse: "Kopf" (liegt oben) oder "Zahl" (liegt oben).

Beispiel: Beim *Würfeln* gibt es sechs elementare Ereignisse.

Beispiel: Unter Vernachlässigung der Zusatzzahl sind elementare Ereignisse des *Lottos* "6 aus 49" alle 6-elementigen Teilmengen der natürlichen Zahlen zwischen 1 und 49.

Der Ereignisraum in den Beispielen (Münzwurf, Würfeln, Lotto) umfasst $2 = |\{\text{Kopf, Zahl}\}|$ bzw. $6 = |\{1, 2, 3, 4, 5, 6\}|$ bzw. $13983816 = \binom{49}{6}$ Elemente.

Beispiel: Der Ereignisraum des Würfels mit zwei Würfeln umfasst $36 = |\{1, \dots, 6\}^2|$ Elemente. Das Ereignis, die Augensumme 7 zu würfeln, ist die Teilmenge:

$$\{(1, 6), (2, 5), (3, 4), (4, 3), (5, 2), (6, 1)\}.$$

Beispiel: Wie viele Elemente enthält das Ereignis, dass der Lotto-Tipp $\{2, 5, 6, 8, 12, 14\}$ genau fünf der gezogenen 6 Zahlen enthält?

Einfachster Fall der Wahrscheinlichkeitsrechnung: Alle elementaren Ereignisse sind gleichwahrscheinlich und der Ereignisraum S ist endlich. Dann gilt für die Wahrscheinlichkeit $P(x)$ eines elementaren Ereignisses $x \in S$: $P(x) = 1/|S|$ (*Gleichverteilung*). Für ein Ereignis $A \subseteq S$ gilt somit:

$$P(A) = \sum_{x \in A} P(x) = \frac{|A|}{|S|}.$$

Es kommt daher essentiell darauf an, die Elemente von A zu zählen.

Das Geburtstagsproblem Wie viele Gäste muss man zu einer Party einladen, damit mit Wahrscheinlichkeit $\geq \frac{1}{2}$ zwei Gäste am selben Tag Geburtstag haben?

Vereinfachende Annahmen: Es gibt 365 Tage im Jahr und alle Tage seien für Geburten gleichwahrscheinlich; zudem sei unsere Gästeauswahl **nicht** z.B. auf Gäste konzentriert, die am 2.1. geboren wurden.

Der Ereignisraum S_k , der sich durch Einladen von k Gästen ergibt, lässt sich durch $\{1, \dots, 365\}^k$ beschreiben, d.h., $|S_k| = 365^k$ nach der Potenzregel. Wir nummerieren die Gäste behelfsweise durch.

Der erste Gast kann an einem beliebigen Tag Geburtstag haben, ohne dass zwei Gäste am selben Tag Geburtstag haben. Der erste Gast "blockiert" aber einen Tag für den zweiten Gast, der nur noch an einem der anderen 364 Tage geboren sein darf, ohne dass zwei Gäste am selben Tag Geburtstag haben.

Schließlich “blockieren” die ersten $k - 1$ Gäste $k - 1$ Tage für den k -ten Gast, der nur noch an einem der nicht-blockierten $365 - (k - 1)$ Tage geboren sein darf, ohne dass zwei Gäste am selben Tag Geburtstag haben.

Für das fragliche Ereignis E_k gilt also: $|E_k| = 365 \cdot 364 \cdots (365 - k + 1)$, Daraus ergibt sich: $P(E_k) = \frac{365 \cdot 364 \cdots (365 - k + 1)}{365^k} \approx 23$ Gäste genügen !

PS: Auf dem Mars mit 669 Tagen müsste man 31 Gäste einladen.

Definition 5.4.2 Zwei Ereignisse A und B heißen unabhängig, gdw.

$$P(A \cap B) = P(A) \cdot P(B).$$

Beispiel: Wir betrachten zwei Münzwürfe.

A bedeute: Der erste Wurf ergibt “Kopf”.

B bedeute: Die beiden Würfe sind verschieden.

C bedeute: Beide Würfe ergeben “Kopf”.

$A \cap B$ heißt: Der erste Wurf ergibt Kopf und der zweite “Zahl”.

$A \cap C$ heißt: Beide Würfe ergeben “Kopf” (also wie C).

$B \cap C$ ist das leere Ereignis.

Daher sind A und B unabhängig, aber nicht A und C oder B und C.

Definition 5.4.3 Eine Zufallsvariable (ZV), auch Zufallsgröße genannt, ist eine Abbildung aus einem Ereignisraum S in die reellen Zahlen.

Beispiel: Eine übliche ZV X_1 für ein Würfelexperiment mit einem Würfel liefert die Augenzahl. Beim Würfeln mit zwei Würfeln ergeben sich mehrere natürliche Möglichkeiten von ZV, z.B.: Minimum X_{\min} / Maximum X_{\max} / Summe der Augenzahlen X_{\sum} .

Es sei S ein Ereignisraum mit Wahrscheinlichkeitsfunktion P und einer ZV X. Die Wahrscheinlichkeit, dass X den Wert r annimmt, ist:

$$P[X = r] = \sum_{e \in X^{-}(r)} P(e).$$

Beispiel: Bestimme $P[X_{\max} = 3]$: $X_{\max}(e) = 3$ für $e \in \{(1,3), (2,3), (3,3), (3,2), (3,1)\}$.
 $\approx P[X_{\max} = 3] = \frac{5}{36}$.

Definition 5.4.4 Der Erwartungswert von X ist gegeben durch:

$$E[X] = \sum_{r \in X(S)} r \cdot P[X = r].$$

Beispiel: $E[X_1] = 3,5$.

Beispiel: $E[X_{\max}] = \frac{1+1+2*3+3*5+4*7+5*9+6*11}{36} = \frac{1+6+15+28+45+66}{36} = \frac{40}{9} \approx 4,44$.

Ein längeres Beispiel: Multiple Choice Bei einer Prüfung mit “Multiple-Choice-Fragen” werden drei Fragen gestellt, wobei für jede der drei Fragen zwei Antworten zur Auswahl vorliegen, von denen jeweils genau eine richtig ist. Die Antworten werden von einem nicht vorbereiteten Prüfling rein zufällig und unabhängig voneinander angekreuzt (Gleichverteilung). Sei Z die Zufallsvariable, welche die Anzahl der richtigen Antworten angibt. Wie viele richtige Antworten liefert ein Prüfling “im Mittel”, wenn er “rein zufällig” seine Antworten wählt?

Wie müssen wir den Wahrscheinlichkeitsraum wählen?

$S = \{r, f\}^3$, wobei r für "richtig" und f für "falsch" stehe.

Ohne Vorkenntnisse gilt: $P(\{x\}) = 1/8$ für $x \in \{r, f\}^3$.

$Z(S) = \{0, 1, 2, 3\}$.

$$P[Z = 0] = P((f, f, f)) = 1/8$$

$$P[Z = 1] = P(\{(r, f, f), (f, r, f), (f, f, r)\}) = 3/8$$

$$P[Z = 2] = P(\{(r, r, f), (f, r, r), (r, f, r)\}) = 3/8$$

$$P[Z = 3] = P((r, r, r)) = 1/8$$

$$E[Z] = \sum_{r \in [3]} r P[Z = r] = \frac{0*1+1*3+2*3+3*1}{8} = 1,5$$

Im Allgemeinen wird man die hier betrachteten Begriffe für sogenannte Wahrscheinlichkeitsverteilungen einführen, die von der Gleichverteilung verschieden sind.

5.5 Quasiordnungen

5.5.1 Ablaufplanung (Scheduling)

Ein schönes Beispiel für die Anwendung der Charakterisierungen von Äquivalenzrelationen liefert die Ablaufplanung (Scheduling). Dabei geht es im Allgemeinen darum, jedem Auftrag eine Maschine zuzuweisen, auf der sie bearbeitet werden kann. In diesem Szenario gibt es zahllose Spielarten. Eine Vereinfachung geht davon aus, dass alle Maschinen gleichartig sind und in dem Sinne auch austauschbar. Außerdem wollen wir davon ausgehen, dass die Bearbeitung eines Auftrags nicht unterbrochen werden darf. Weiterhin könnte bekannt sein, wie viel Zeit ein Auftrag zur Abarbeitung auf einer Maschine benötigt, wann dieser in das System eintritt (also, ab wann er bearbeitet werden könnte) und wann er (unbedingt) beendet sein muss. Unter den Umständen könnte man versuchen, eine Zuordnung der Aufträge auf die Maschinen so zu finden, dass die am längsten laufende Maschine schnellstmöglich fertig ist. Diese an und für sich simpel klingende Problemstellung zählt (bereits) zu den Problemen, für die man keine effizienten Algorithmen kennt (technischer gesprochen: es ist ein NP-hartes Problem; mehr dazu erfahren Sie in Veranstaltungen bzw. Büchern zur Komplexitätstheorie).

Wir wollen nun aber erstmal darangehen, das allgemeine Szenario zu formalisieren. Es ist zunächst einmal eine Menge A von Aufträgen gegeben sowie eine Menge P von p Maschinen (Prozessoren). Die oben angesprochene "Zuordnung" von Aufträgen auf Maschinen ist allgemein zunächst eine Relation $Z \subseteq A \times P$. Welche Eigenschaften hat diese Zuordnung?

- Da Aufgaben nicht unterbrochen werden dürfen, wird einem Auftrag höchstens eine Maschine zugeordnet. Z ist somit nacheindeutig.
- Jedem Auftrag soll eine Maschine zugeordnet werden; Z ist daher vortotal.

Insgesamt zeigt dies, dass Z eine Abbildung ist, wir können also $Z : A \rightarrow P$ notieren. Der Kern von Z ist die Äquivalenzrelation, die dadurch beschrieben werden kann, dass sie diejenigen Aufträge in einer Äquivalenzklasse zusammenfasst, die auf demselben Prozessor abgearbeitet werden sollen. Umgekehrt ist Z gerade die dieser soeben beschriebenen Zerlegung entsprechenden kanonische Abbildung.

Die einfachste Art von Nebenbedingungen ist zweifelsfrei, wenn von allen Aufträgen von vornherein bekannt ist, wann genau sie mit ihrer Arbeit anfangen (sollen) und wann genau sie (unter voller Auslastung eines Prozessors) sie mit ihrer Arbeit fertig sind. Wir können also zwei weitere Abbildungen als gegeben annehmen, $\alpha : A \rightarrow \mathbb{R}$

für die Anfangszeitpunkte und $\omega : A \rightarrow \mathbb{R}$ für die Endzeitpunkte der Aufträge. Das bedeutet natürlich, dass zwei Aufträge nur dann derselben Maschine zugeordnet werden dürfen, wenn ihre “Rechenintervalle” sich nicht überlappen. Formalisiert heißt dies:

$$\forall a_1, a_2 \in A : Z(a_1) = Z(a_2) \implies (a_1 = a_2 \vee |[\alpha(a_1), \omega(a_1)] \cap [\alpha(a_2), \omega(a_2)]| \leq 1).$$

Wir wollen eine Zuordnung Z *zulässig* nennen (bzgl. α und ω), wenn sie diese Bedingung erfüllt. Der einzige mögliche Überlapppunkt zweier Rechenintervalle ist nämlich an ihren Anfangs- bzw. Endzeitpunkten. Hierbei werden die möglicherweise benötigten Zeiten zum Wechseln zwischen verschiedenen Aufgaben vernachlässigt.

Betrachten wir nun die Relation $R \subseteq A \times A$, definiert als

$$R = \{(a_1, a_2) \mid |[\alpha(a_1), \omega(a_1)] \cap [\alpha(a_2), \omega(a_2)]| > 1\}.$$

Diese Relation ist irreflexiv und symmetrisch, kann also als Kantenmenge eines ungerichteten Graphen $G = (A, R)$ aufgefasst werden. Dies gestattet eine Veranschaulichung dafür, was es bedeutet, wenn zwei Aufträge sich ausschließen bezüglich der Abarbeitung auf derselben Maschine.

Lemma 5.5.1 *Eine Prozessorzuordnung $Z : A \rightarrow P$ ist genau dann zulässig, wenn*

$$\forall a \in A : Z(a) \notin Z(N(a)).$$

Hierbei ist $N(a)$ die Menge der Nachbarn von a in $G = (A, R)$ und $Z(N(a))$ demnach die Menge der Prozessoren, die den Nachbarknoten von a zugeordnet sind. Die in dem Lemma ausgesprochene Bedingung kann so gedeutet werden, dass den Knoten von G (durch Z) Farben aus der Farbmenge P so zugeordnet werden, dass keine zwei Nachbarn mit gleicher Farbe benachbart sind. Eine derartige Zuordnung nennt man auch *echte Knotenfärbung* (mit höchstens $|P|$ Farben) von G .

Beweis: Wir zeigen die Implikation von links nach rechts durch Kontraposition. Daher nehmen wir an Z sei keine echte Knotenfärbung. Dann gibt es zwei benachbarte Knoten $a_1, a_2 \in A$ mit $Z(a_1) = Z(a_2)$. Da $a_1 \in N(a_2)$, $|[\alpha(a_1), \omega(a_1)] \cap [\alpha(a_2), \omega(a_2)]| > 1$. Das bedeutet, dass Z nicht zulässig ist.

Die andere Implikationsrichtung zeigt man ebenfalls durch Kontraposition. Wenn Z nicht zulässig ist, so gibt es zwei Aufträge a_1, a_2 , die auf demselben Prozessor abgearbeitet werden, also $Z(a_1) = Z(a_2)$ erfüllen, wobei aber $|[\alpha(a_1), \omega(a_1)] \cap [\alpha(a_2), \omega(a_2)]| \leq 1$ nicht gilt. Daher sind a_1, a_2 in G benachbart und also ist Z keine echte Knotenfärbung. \square

Für allgemeine Graphen ist das Problem festzustellen, ob es eine echte Knotenfärbung mit drei Farben gibt, bereits NP-hart (s.o.). Allerdings sei hier bereits eine Warnung ausgesprochen, derartige Ergebnisse vorschnell zu lesen und so z.B. zu schlussfolgern, dass das Problem, eine zulässige Prozessorzuordnung zu finden, keine effizienten Algorithmen zuließe. Dazu beobachte man, dass die Graphen, die aus dem Prozessorzuordnungsproblem entstanden sind, eben nicht beliebig sind, denn die Kanten entspringen einer Schnittbedingung von Intervallen, und diese Intervalle entsprechen (in gewisser Weise) den Aufträgen. Wer mag, kann sich überlegen, wie man eine zulässige Prozessorzuordnung effizient erhalten kann: Wie würden Sie diese Aufgabe programmieren?

5.5.2 Wie kann man Transitivität algorithmisch testen?

Angenommen, (M, \leq) ist eine Quasiordnung. Um hiermit algorithmisch arbeiten zu können, nehmen wir an, dass man für $a, b \in M$ einen Vergleich $a \stackrel{?}{\leq} b$ in konstanter

Zeit durchführen kann. Es sei nun eine endliche Folge a_1, \dots, a_n von Elementen aus M gegeben, und wir wollen wissen, ob diese Folge sortiert ist bzgl. \leq , d.h., wir wollen überprüfen, ob gilt:

$$\forall 1 \leq i \leq j \leq n : a_i \leq a_j.$$

Naiv könnten wir das durch Vergleich aller Paare lösen, was einen quadratischen Aufwand (gemessen in der Eingabegröße n) bedeutet. Da \leq transitiv ist, können wir den Test wie folgt vereinfachen:

$$\forall 1 \leq i \leq n : a_i \leq a_{i+1}.$$

Natürlich müsste man das erstmal beweisen. Was hätten wir also zu zeigen?

Lemma 5.5.2 $\forall 1 \leq i \leq n : a_i \leq a_{i+1}$ gilt genau dann, wenn $\forall 1 \leq i \leq j \leq n : a_i \leq a_j$.

Beweis: Die Implikation von rechts nach links ist trivial. Für die Richtung von links nach rechts führen wir einen Induktionsbeweis über die Anzahl n der Folgenglieder. Für $n = 1$ oder $n = 2$ gilt die Behauptung wieder trivial. \square

Aus dem Lemma folgt, dass wir den Transitivitätstest mit linearem Zeitaufwand durchführen können. Derlei Überlegungen sind also durchaus von praktischem Interesse. Algebraische Eigenschaften können somit helfen, bessere Programme zu schreiben.

5.5.3 Sortieren

Wir haben im Haupttext ja schon einen Sortieralgorithmus kennengelernt.

Solange $\exists x, y \in N, x \neq y : (x, y) \in \text{Mem} \wedge y \leq x$, **true**:
 $\text{Mem} \leftarrow (\text{Mem} \setminus \{(x, y)\}) \cup \{(y, x)\}.$

Dieser Algorithmus ist in vieler Hinsicht noch sehr abstrakt und unbestimmt, was z.B. die Analyse seiner Laufzeit erschwert (wenn nicht unmöglich macht). Das hat u.a. damit zu tun, dass wir völlig offengelassen haben, wie die Relation Mem implementiert werden sollte. Außerdem ist unklar, aus welcher Grundmenge die zu sortierende Menge N entstammt und wie diese dargestellt ist. Wir wollen beide Aspekte im Folgenden konkretisieren.

- Wir beschränken uns auf das Sortieren einer Menge von `integer`-Zahlen. Diese Art von Zahlen wird standardmäßig von jeder Programmiersprache in einer oder anderen Form angeboten. Es handelt sich hierbei meist um Zahlen, die mit 32 oder 64 Bits dargestellt werden können. Keineswegs ist also die Grundmenge unendlich. Nichtsdestotrotz genügt dies für viele Anwendungen. Überdies wird nun klar, dass wir bei der Zeitanalyse für einfache `integer`-Operationen von einem konstanten Zeitaufwand ausgehen können.
- Da es sich bei Mem um eine lineare Ordnung einer endlichen Menge handelt, können wir (wie im Haupttext angedeutet) davon ausgehen, dass die Elemente von N gemäß der Ordnung Mem im Speicher abgelegt sind. Dies lässt sich am einfachsten durch die Datenstruktur eines *Feldes* oder *Arrays* darstellen. Dazu betrachten wir (formaler) diejenige Bijektion $A : [|N|] \rightarrow N$ mit

$$\forall i, j \in [|N|] : i < j \iff (A[i], A[j]) \in \text{Mem}.$$

```

Data : A: array of n integers
Result : A is sorted
1 notready: boolean; count: integer;
2 notready  $\leftarrow$  true;
3 while notready do
4   notready  $\leftarrow$  false;
5   for count  $\leftarrow$  n - 2 to 0 do
6     if A[count] > A[count + 1] then
7       swap(A[count], A[count + 1]);
8       notready  $\leftarrow$  true;

```

Abbildung 5.15: A first sorting algorithm

In der Formel haben wir schon die übliche Schreibweise mit eckigen Klammern für den Zugriff auf Array-Elemente verwendet. Aufgefasst als Funktion sollten wir eher $A(i)$ schreiben. Im Übrigen bezieht sich die Relation \leq in dem Ausdruck auf den Vergleich von Zahlen in der üblichen Weise; da wir zuvor uns darauf geeinigt hatten, dass die Elemente von N selbst ebenfalls Zahlen sein sollen, kann deren Vergleich problemlos mit demselben Symbol \leq geschrieben werden.

Unser Algorithmus könnte also in der folgenden Weise für unsere nun festgelegten Datenstrukturen angepasst werden.

Solange $\exists i, j \in [N] : i < j \wedge A[i] > A[j]$, tue: Vertausche $A[i]$ und $A[j]$.
--

Das ist natürlich immer noch keine wirkliche Implementierung, aber dieser Pseudocode kommt einem Programmtext schon näher. Versuchen wir also, unsere Darstellung zu verfeinern, siehe Algorithmus 5.15. Hierbei verwenden wir auch gleich die in Lemma 3.5.17 enthaltene Idee, als “Vertauschungskandidaten” nur aufeinander folgende Feldelemente zu betrachten. Außerdem wurde die mit dem Existenzquantor geforderte Suche nach Vertauschungskandidaten mit dem eigentlichen Vertauschen kombiniert. Wenn wir also ein Feld mit n Elementen auf diese Weise sortieren wollen, brauchen wir möglicherweise im schlechtesten Fall n^2 Durchläufe der While-Schleife, die wiederum eine For-Schleife enthält, die $n - 1$ Durchläufe erfordert. Ignorieren wir Konstanten, so erhalten wir insgesamt eine Laufzeit, die kubisch mit der Größe n des Feldes wächst. *Bubblesort* (in Alg. 5.16) verfeinert diesen Sortieralgorithmus weiter, indem klarer begrenzt wird, wie oft die While-Schleife ausgeführt wird. In der üblicheren Lehrbuchform wird allerdings auf die boolesche Variable `notready` verzichtet, die ja auch auf die Laufzeit im schlechtesten Fall keinen Einfluss hat (wohl aber in günstigeren Fällen). Warum ist Algorithmus 5.16 korrekt? Die folgenden beiden Sachverhalte kann man jeweils per Induktion zeigen:

1. Nach Ende des Rumpfes der in Zeile 6 beginnenden For-Schleife (unmittelbar nach Zeile 6) gilt: $A[\text{count}]$ ist kleinstes Element von $\{A[\text{count}], \dots, A[n - 1]\}$.
2. Nach Ende des Rumpfes der in Zeile 6 beginnenden While-Schleife (also unmittelbar nach Zeile 6) gilt: $A[\text{bound}]$ ist kleinstes Element von $\{A[\text{bound}], \dots, A[n - 1]\}$ und die Liste $(A[0], \dots, A[\text{bound}])$ ist sortiert.

```

Data : A: array of n integers
Result : A is sorted
1 notready: boolean; bound, count: integer;
2 notready ← true; bound ← 0;
3 while notready ∧ bound < n do
4   notready ← false;
5   for count ← n - 2 to bound do
6     if A[count] > A[count + 1] then
7       swap(A[count], A[count + 1]);
8       notready ← true;
9   bound ← bound + 1;

```

Abbildung 5.16: A bubblesort variant

Wir führen exemplarisch den zweiten Induktionsbeweis vor. Hierbei setzen wir die Gültigkeit der ersten Aussage voraus.

Induktionsanfang: Betrachte $\text{bound} = 0$. Nach dem Ende der For-Schleife gilt gemäß der ersten Aussage, dass $A[0]$ das kleinste Element der Menge $N = \{A[0], \dots, A[n-1]\}$ enthält. Die Liste $(A[0])$ ist trivialerweise sortiert.

Induktionsvoraussetzung: Wir gehen davon aus, die Behauptung gilt für $\text{bound} = i$, d.h., $A[i]$ ist kleinstes Element von $\{A[i], \dots, A[n-1]\}$ und die Liste $(A[0], \dots, A[i])$ ist sortiert.

Induktionsbehauptung: Zu zeigen haben wir nun, die Behauptung gilt für $\text{bound} = i + 1$, d.h., $A[i + 1]$ ist kleinstes Element von $\{A[i + 1], \dots, A[n - 1]\}$ und die Liste $(A[0], \dots, A[i + 1])$ ist sortiert.

Zum Beweis der Induktionsbehauptung betrachte die Lage für $\text{bound} = i + 1$ unmittelbar nach Zeile 6. Da bei dem letzten (gerade beendeten) Lauf durch den Rumpf der While-Schleife die Werte von $A[0], \dots, A[i]$ nicht verändert und überhaupt nur Tausche benachbarter Feldelemente durchgeführt wurden, gilt (nach Induktionsvoraussetzung) immer noch: $A[i]$ ist kleinstes Element von $\{A[i], \dots, A[n - 1]\}$ und die Liste $(A[0], \dots, A[i])$ ist sortiert. Nach der ersten Aussage gilt außerdem: $A[i + 1]$ ist kleinstes Element von $\{A[i + 1], \dots, A[n - 1]\}$ (was einen Teil der Induktionsbehauptung darstellt). Daher gilt $A[i] \leq A[i + 1]$, und da $(A[0], \dots, A[i])$ bereits sortiert ist, ist auch $(A[0], \dots, A[i + 1])$ sortiert.

Nach dem Prinzip der Induktion gilt die Behauptung für all möglichen Werte von bound (von 0 bis $n - 1$).

Insbesondere folgt für $\text{bound} = n - 1$: Am Schluss des Algorithmus ist die gesamte Liste sortiert.

Man beachte, dass hier Induktion etwas anders angewendet wird als sonst bei uns üblich, da es ja mit $n - 1$ eine obere Grenze für die Werte von bound gibt. Allerdings ist diese Grenze selbst auch wieder variabel, weil wir ja für beliebig (aber endlich) große Mengen N ein korrektes Sortierverfahren angeben wollen.

Machen wir uns abschließend noch etwas mehr Gedanken zur Laufzeit von Algorithmus 5.16. Genauer wollen wir uns fragen, wie oft denn der swap-Befehl höchstens ausgeführt wird. Das ist gleichbedeutend mit der Frage, wie oft der Schleifenrumpf der For-Schleife insgesamt höchstens ausgeführt wird.

- Falls $\text{bound} = 0$, so wird der Rumpf der For-Schleife $(n - 1)$ -mal durchlaufen.

- Falls $\text{bound} = 1$, so wird der Rumpf der For-Schleife $(n - 2)$ -mal durchlaufen.
- Allgemeiner gilt also: Falls $\text{bound} = i$, so wird der Rumpf der For-Schleife $(n - 1 - i)$ -mal durchlaufen. Dies gilt für $i = 0$ bis $i = n - 1$.
- Eine erste Antwort wäre also: $S = \sum_{i=0}^{n-1} (n - 1 - i)$. Eine Indextransformation zeigt: $S = \sum_{i=0}^{n-1} i$. Hierfür kennen wir eine geschlossene Form, nämlich $S = \frac{n(n-1)}{2}$, siehe Übung 6.1.6.
- Dieser Analyse kann man auch entnehmen, dass bei $\text{bound} = n - 1$ die For-Schleife gar nicht durchlaufen wird. Daher kann man auch als Teil der Abbruchbedingung der While-Schleife $\text{bound} < n - 1$ wählen.

Zum Sortieren von Entitäten Wir hatten uns bereits in Abschnitt 5.3.7 kurz mit dem ER-Modell beschäftigt. Noch kürzer: Entitäten (Objekten) sind gewisse Attribute (Eigenschaften) funktional zugeordnet. Man kennt dies auch in Form von Tabellen bei Spreadsheets. Beispielsweise könnten wir für jede Person eine Zeile angelegt haben, und die Spalten entsprechen dann den Attributen. Wenn wir unser Spreadsheetprogramm unsere Personeneinträge nach ihrem Alter sortieren lassen, so bedeutet das im Grunde, dass wir in diesem Moment der Menge der Entitäten (hier: Personen) eine Ordnung aufprägen, die von der Ordnung des entsprechenden Attributs „geerbt“ wurde. Um (mathematisch) einzusehen, dass dies wirklich funktioniert, sind folgende Aussagen hilfreich:

1. Ist M eine Menge, (N, \leq) eine Quasiordnung und ist $f : M \rightarrow N$ eine Abbildung, so definiert (für $a, b \in M$) $a \leq_f b$ gdw. $f(a) \leq f(b)$ eine Quasiordnung auf M .
2. Selbst wenn (N, \leq) eine lineare Ordnung ist, muss (M, \leq_f) keine Halbordnung sein.
3. Ist f injektiv, so gilt hingegen: Ist (N, \leq) Halbordnung, so ist auch (M, \leq_f) Halbordnung.

(Diese Aussagen sollten natürlich bewiesen werden, was nochmal eine gute Übungsaufgabe darstellt.) Die letzte Aussage hebt die Bedeutung von Schlüsselattributen hervor, wie in Abschnitt 5.3.7 erläutert.

Im allereinfachsten Fall lassen sich auch Felder A als Mechanismen begreifen, die der Entität „Zeile“ (z.B. i) ein Attribut zuordnen, nämlich $A[i]$. Diese Sichtweise ist insofern wertvoll, als dass wir bislang unsere Sortieralgorithmen eigentlich unter der Maßgabe analysiert haben, dass A ein Schlüsselattribut bezeichnet. Wir sollten uns also unsere Algorithmen nochmals daraufhin anschauen, was denn passiert, wenn wir $A[i] = A[j]$ für $i \neq j$ zulassen. Das geschieht zum Beispiel (wahrscheinlich) bei der Sortierung der eingangs erwähnten Personentabelle nach dem Alter.

5.6 Ungerichtete Graphen

5.6.1 Algorithmen in Beweisen

In der wissenschaftlichen Literatur werden Algorithmen niemals in der Form von JAVA (o.ä.) Programmen notiert. Bestenfalls finden Sie dort Stücke von Pseudo-Code, so wie

```

Data : G = (V, E): a connected graph
Result : F: set of edges such that (V, F) is a spanning tree of G
1 difference: integer;
2 difference ← |E| − |V|;
3 if difference < 0 then
4   return E;
5 else
6   find edge e in cycle subgraph of G;
7   return ST(V, E \ {e});

```

Abbildung 5.17: A recursive spanning tree algorithm ST

Sie sie auch in diesem Skript hier und dort finden können. Diese geben aber nur den groben Rahmen eines Programms wieder. Viele Details des näheren Programmablaufs oder auch der zu wählenden Datenstrukturen sind oft nicht explizit ausgeführt oder Bestenfalls textuell beschrieben. Als Programmierer kommt Ihnen also die Aufgabe zu, diese Lücken aufzufüllen, wenn Sie die beschriebenen Algorithmen implementieren wollen (oder sollen).

Es ist dabei durchaus üblich, zumindest Details der Algorithmen in den Korrektheits- oder auch Laufzeitanalysebeweisen zu verbergen. Als ein Beispiel hierfür soll uns der Beweis zu Satz 3.6.23 dienen. Dieser Beweis ist ein Induktionsbeweis, der einen rekursiven Algorithmus zur Bestimmung eines Spannbaums in einem vorgelegten Graphen nahelegt, wie in Bild 5.17 in Pseudo-Code angegeben.

Diese Rekursion lässt sich auch leicht in eine Iteration in Form einer While-Schleife verwandeln. Textuell könnte die Beschreibung wie folgt aussehen:

Solange möglich, wähle eine Kante auf einem Kreis im aktuellen Graph und lösche sie.

Übrig bleibt ein Spannbaum der ursprünglichen Eingabe.

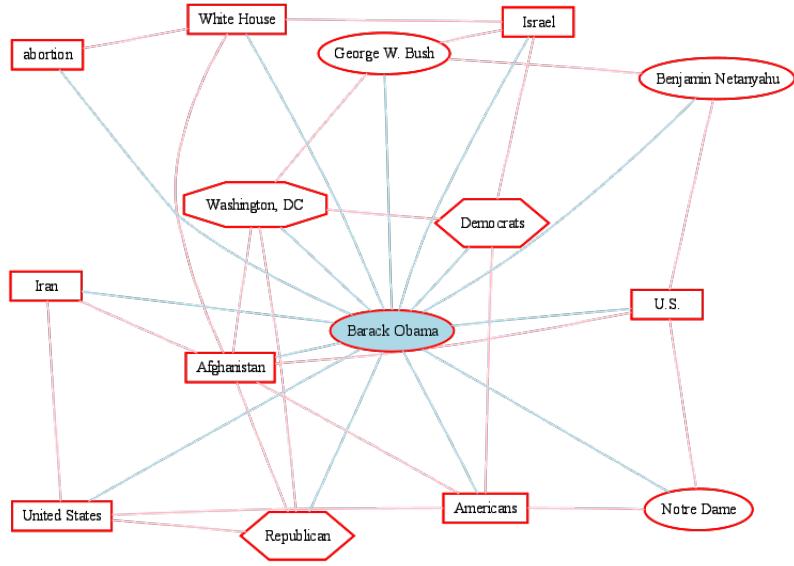
Lernen Sie, Beweise so “algorithmisch” zu lesen, wo möglich. Das wird Ihnen als Informatiker einen einfacheren Zugang zu Beweisen liefern und auch ihre Lektüre für Sie spannender gestalten. Außerdem versetzen Sie sich auf diese Weise in die Lage, wissenschaftliche Arbeiten über Algorithmik lesen zu können.

5.6.2 Modellieren mit Graphen

Graphische Darstellungen finden sich an an verschiedenen Stellen des täglichen Lebens. Sie dienen u.a. dazu, (komplizierte) Sachverhalte zu veranschaulichen.

Soziogramme und ähnliche Darstellungen dienen beispielsweise dazu, die Beziehungen zwischen Menschen oder auch Menschen und gewissen Themen nachzuzeichnen. Die Graphik in Bild 5.18 wurde von dem automatischen Textanalysesystem Textmap erstellt.

Der Klassiker als Beispiel für das Graphzeichnen ist das Londoner U-Bahn-Netz. Warum? Nun, hier wurde es wohl das erste Mal nötig, die geographischen Gegebenheiten zugunsten einer mehr abstrakteren Sichtweise und Darstellung zu vernachlässigen, wenn dies nötig ist. Wichtig ist allein, welche Linie welche Stationen verbindet. Welche Entfernung zwischen den Stationen bestehen, wird Bestenfalls näherungsweise abgebildet.



Copyright 2009, Research Foundation, Stony Brook

Abbildung 5.18: Ein Graph wie aus dem Leben

Schließlich haben wir schon zahlreiche (oft gerichtete) Graph-Darstellungen in diesem Skript gesehen, z.B. Hasse-Diagramme. Aber auch Bild 5.3 zeigt auf der linken Seite einen Graph. Bild 5.20 stellt Inklusionsbeziehungen als Graph dar.

Modellieren — eine wichtige Aufgabe für InformatikerInnen

1. Was sind Gemeinsamkeiten all dieser Bilder?
2. Wo sind die Unterschiede?
3. Wie kann ich das Wesentliche dieser Objekte (mathematisch) beschreiben?
4. Wie kann ich dies demgemäß auf einem Rechner darstellen?
5. Wie sehen also möglicherweise Datenstrukturen und darauf wiederum Operationen / Algorithmen aus?

Definitionsversuche

Ein *Graph* G ist gegeben durch ein Paar von Mengen (V, E) .

V ist die Menge von *Knoten* oder *Punkten* oder *Ecken*.

E ist die Menge von *Kanten*, die die Verbindungen zwischen Punkten ausdrücken soll.

Wie hängen Knoten und Kanten zusammen?

Hierfür gibt es verschiedene Formalisierungsmöglichkeiten, die wir jetzt durchsprechen.

1. Möglichkeit: gerichteter Multigraph

Wir betrachten zwei Abbildungen $\alpha : E \rightarrow V$ und $\omega : E \rightarrow V$.

α liefert zu jeder Kante ihren *Anfangsknoten*.

ω liefert zu jeder Kante ihren *Zielknoten*.

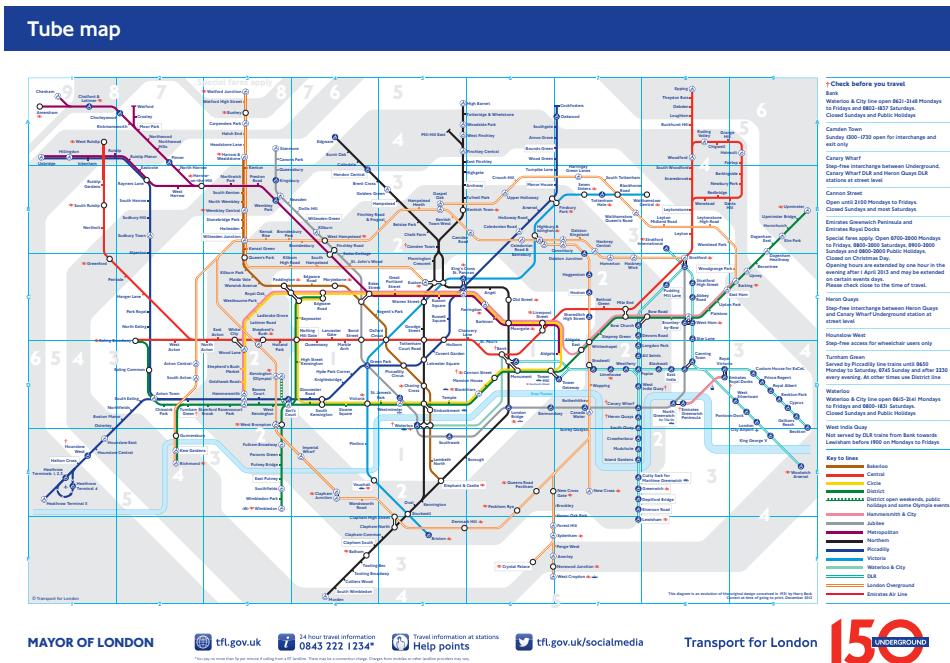


Abbildung 5.19: Londons Unterwelt

Hiermit lassen sich *gerichtete Multigraphen* beschreiben:

Jede Kante e hat nämlich eine Richtung: von $\alpha(e)$ nach $\omega(e)$.

Im Bild drückt man das meist dadurch aus, dass der Verbindungsstrich von $\alpha(e)$ nach $\omega(e)$ eine Pfeilspitze bei $\omega(e)$ erhält.

Solche Kanten mit Richtungsangabe nennt man auch *Bögen*.

Beachte: Zwei verschiedene Kanten können dieselben Anfangs- und Zielknoten besitzen, d.h., zwischen zwei Knoten kann es mehrere unterscheidbare Bögen.

Außerdem kann für eine Kante e gelten: $\alpha(e) = \omega(e)$. Man spricht dann auch von einer *Schlinge*.

Damit könnten die Königsberger sogar Einbahnstraßen bekommen!

2. Möglichkeit: gerichteter Graph

Die *Endknotenabbildung* $\eta : E \rightarrow V \times V, e \mapsto (\alpha(e), \omega(e))$ ist injektiv.

Dies bedeutet: Zwischen je zwei Knoten u, v gibt es höchstens einen Bogen e von u nach v .

Wir schließen also Mehrfachbögen aus.

Hiermit modellieren wir *gerichtete Graphen*.

Alternatives Modell: E ist Binärrelation auf V (wie gehabt).

Wichtige Beobachtung: Jede Binärrelation ist auffassbar als ein gerichteter Graph.

Die Bogenmenge jedes gerichteten Graphen ist eine Binärrelation, die *Bogenrelation*, auch genannt *Adjazenz(relation)*.

Wichtige Darstellung Adjanzenzmatrix: Die Relationenmatrix der Bogenrelation.

Jede $n \times n$ -Matrix mit {0, 1}-Einträgen lässt sich als gerichteter Graph deuten.

3. Möglichkeit: ungerichteter Graph

Es sei $G = (V, E)$ ein gerichteter Graph, also $E \subseteq V \times V$.

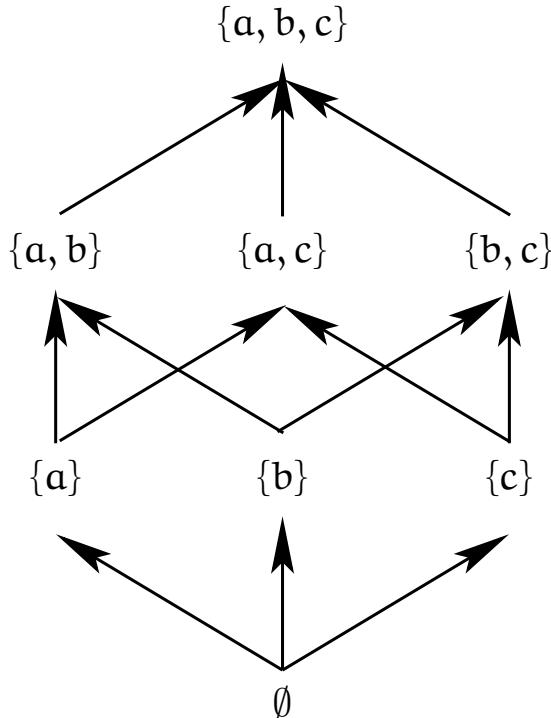


Abbildung 5.20: Wie Mengen zueinander liegen

Ist E symmetrisch, so bedeutet dies:

Gibt es einen Bogen von u nach v , so gibt es auch einen von v nach u .

Graphisch werden wir dann beide Verbindungen identifizieren und die Pfeilspitzen weglassen.

Wir können so einen *ungerichteten Graphen* auch beschreiben durch ein Paar (V, E) , wobei nun $E \subseteq 2^V$ mit $e \in E \implies 1 \leq |e| \leq 2$ gilt.

Schlingen sind hierbei einelementige Knotenmengen.

Diese sind in Anwendungen oft unwichtig. Besitzt ein ungerichteter Graph keine Schlingen, so heißt er *schlicht*.

Frage: Wie sieht die Adjazenzmatrix eines schlichten ungerichteten Graphen aus?

Wir betrachten im Folgenden meist ungerichtete schlichte Graphen (wenn wir nichts anderes vermerken).

Weitere Varianten (oft interessant in Anwendungen):

Wir können Knoten oder Kanten eines Graphen beschriften.

Dies geschieht durch die Einführung von Abbildungen $V \rightarrow B_V$ bzw. $E \rightarrow B_E$, wobei B_V bzw. B_E die Mengen sind, mit deren Elementen die Beschriftung erfolgen soll.

“Beschriften” ist hierbei abstrakt zu verstehen, auch das Verwenden unterschiedlicher Farben (wie beim U-Bahnnetz) ist so eine Beschriftung.

Oft sind auch Zahlenangaben (Kosten, Gewichte, ...) interessant.

Man kann auch ungerichtete Multigraphen einführen.

Dies haben wir bei den Königsberger Brücken getan.

Solche Multigraphen enthalten dann Mehrfachkanten; m.a.W.: Jede höchstens zweiele-

mentige Knotenmenge (Kante) erhält dann eine *Vielfachheit* zugeordnet.

Manchmal kommt es auch auf die Reihenfolge der Bögen bei einem Knoten an (s. Bild 5.3).

5.7 Verknüpfungen

5.7.1 Eine weitere ungewöhnlichere Mengenoperation

Es sei \mathcal{U} ein Universum. Definiere für $A, B \subseteq \mathcal{U}$:

$$A \Delta' B := \begin{cases} \emptyset, & \text{falls } A \cap B = \emptyset \\ \{x \mid x \in A \cup B \wedge x \notin A \cap B\} \end{cases}$$

Klar: $(2^{\mathcal{U}}, \Delta')$ ist ein Gruppoid.

Beispiele:

$$A = \{1, 2\}, B = \{2, 3\}, C = \{3, 4\}$$

$$(A \Delta' B) \Delta' C = \{1, 3\} \Delta' \{3, 4\} = \{1, 4\}$$

$$A \Delta' (B \Delta' C) = \{1, 2\} \Delta' \{2, 4\} = \{1, 4\}$$

$$(A \Delta' C) \Delta' B = \emptyset \Delta' \{2, 3\} = \emptyset$$

$$A \Delta' (C \Delta' B) = \{1, 2\} \Delta' \{2, 4\} = \{1, 4\}$$

Diese Beispiele zeigen:

$(2^{\mathcal{U}}, \Delta')$ ist nicht assoziativ.

Dagegen sind \cup und \cap assoziative Mengen-Verknüpfungen.

5.7.2 Relationen aus Verknüpfungen

Wir wollen jetzt die Gelegenheit nutzen, Begriffe aus vorigen Abschnitten zu wiederholen. Dadurch sollten weitere Zusammenhänge zwischen den Kapiteln klar werden.

Im Folgenden sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. Wir definieren eine Relation \leq_{\circ} auf M wie folgt:

$$a \leq_{\circ} b := (\exists x \in M : a \circ x = b).$$

Als Erstes wollen wir uns fragen, unter welchen Umständen bezüglich \circ gewisse Eigenschaften für die abgeleitete Relation \leq_{\circ} gelten. Wenn Sie diesen Abschnitt als Übung nutzen wollen, so decken Sie am besten die Beweise ab und versuchen Sie, diese alleine zu führen. Machen Sie sich überdies Gedanken darüber, ob es noch andere interessante Dinge über das Verhältnis von \circ und \leq_{\circ} auszusprechen gibt.

Reflexivität

Lemma 5.7.1 Ist $\mathbb{G} = (M, \circ)$ idempotent, so ist \leq_{\circ} reflexiv.

Beweis: Da jedes $a \in M$ idempotent ist, gilt: $a \circ a = a$, also $a \leq_{\circ} a$. □

Lemma 5.7.2 Besitzt $\mathbb{G} = (M, \circ)$ ein neutrales Element $e \in M$, so ist \leq_{\circ} reflexiv.

Beweis: Da $e \in M$ neutrales Element, gilt für jedes $a \in M$: $a \circ e = a$, also $a \leq_{\circ} a$. □

Beachte: Im Grunde genügt die Existenz eines rechtsneutralen Elements.

Transitivität

Lemma 5.7.3 Ist $\mathbb{G} = (M, \circ)$ eine Halbgruppe, so ist \leq_\circ assoziativ.

Beweis: Es seien $a, b, c \in M$ mit $a \leq_\circ b$ und $b \leq_\circ c$. Also gibt es $x \in M$ und $y \in M$ mit $a \circ x = b$ und $b \circ y = c$. Durch Einsetzen und unter Ausnutzen der Assoziativität erhalten wir:

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

Daher existiert zu a, c ein $z \in M$ (nämlich: $z = x \circ y$) mit $a \circ z = c$. Daher gilt $a \leq_\circ c$, was zu zeigen war. \square

Unsere Überlegungen liefern daher:

Lemma 5.7.4 Ist (M, \circ, e) ein Monoid, so ist \leq_\circ eine Quasiordnung auf M .

Beispiele Um weitere Eigenschaften verstehen zu können, betrachten wir im Folgenden einige Beispiele. Hierbei greifen wir auf die soeben erzielten Ergebnisse zurück.

1. Beispiel: Im Monoid $(\mathbb{N}, +, 0)$ bedeutet $a \leq_+ b$: Man kann zu a noch eine nichtnegative Zahl hinzufügen, um auf b zu kommen. Also stimmt \leq_+ mit dem üblichen \leq auf den natürlichen Zahlen überein. Daher ist \leq_+ hier antisymmetrisch und mithin eine Halbordnung.
2. Beispiel: Im Monoid $(\mathbb{Z}, +, 0)$ hingegen bedeutet $a \leq_+ b$: Man kann zu a irgendeine ganze Zahl hinzufügen, um auf b zu kommen. Das kann man aber für alle Paare $a, b \in \mathbb{Z}$. Daher ist \leq_+ hier die Allrelation $\mathbb{Z} \times \mathbb{Z}$. Somit ist \leq_+ hier symmetrisch und daher eine Äquivalenzrelation.
3. Beispiel: Im Monoid $(2^M, \cup, \emptyset)$ bedeutet $A \leq_u B$: Man kann mit A irgendeine Menge X vereinigen, um B zu erhalten. Also sind insbesondere alle Elemente von A in B enthalten. Gilt umgekehrt $A \subseteq B$, so kann man mit A eine Menge X vereinigen, um B zu erhalten, z.B. $X = B$. Daher gilt: $\leq_u = \subseteq$. Wir wissen daher: \leq_u ist antisymmetrisch, also eine Halbordnung.
4. Beispiel: Im Monoid $(2^M, \cap, M)$ bedeutet $A \leq_n B$: Man kann mit A irgendeine Menge X schneiden und erhält B . Wie im vorigen Beispiel überlegt man sich: $\leq_n = \supseteq$. Daraus folgt: \leq_n ist antisymmetrisch, d.h. eine Halbordnung.
5. Beispiel: In der idempotenten Halbgruppe (\mathbb{Z}, \min) bedeutet $a \leq_{\min} b$: Das Minimum von a und einer andern Zahl x ergibt b . Diskutiere hierzu zwei Fälle: Ist $a \geq b$, so kann mit $x = b$ die Gleichung $\min(a, x) = b$ erzwungen werden. Ist $a < b$, so gibt es keine Zahl x mit $\min(a, x) = b$. Daraus folgt: $\leq_{\min} = \leq$. Daher ist \leq_{\min} eine Halbordnung.
6. Beispiel: Es sei X eine nicht-leere Menge. Betrachte das freie Monoid (X^*, \cdot, λ) zu X , mit $X^* = \bigcup_{n \in \mathbb{N}} X^n$. $u \leq_w w$ bedeutet, es gibt ein Element v aus X^* gibt, sodass $u \cdot v = w$. Es geht also darum, u mithilfe von v so zu verlängern, dass sich w ergibt. Wie schon angedeutet, kann man X^* als Menge der Wörter über dem Alphabet X deuten. Dann bedeutet $u \leq_w w$ also, dass u ein Präfix von w ist, oder anders gesagt, dass das Wort w mit u anfängt. Man überlege sich, dass die Antisymmetrie hier gilt: Wenn w mit u anfängt und u mit w beginnt, so muss $u = w$ gelten. Etwas formaler kann man das einsehen, indem zunächst

der Homomorphismus $\ell : (X^*, \cdot, \lambda) \rightarrow (\mathbb{N}, +, 0)$ betrachtet wird, der einem Wort (einer Folge) die Länge zuordnet. Gilt nun $u \cdot x = w$ und $w \cdot y = u$ für gewisse $x, y \in X^*$, so auch $\ell(u \cdot x) = \ell(u) + \ell(x) = \ell(w)$ und $\ell(w) + \ell(y) = \ell(u)$ für nichtnegative ganze Zahlen $\ell(w), \ell(u), \ell(x), \ell(y)$. Das bedeutet mit Beispiel 1, dass $\ell(u) \leq \ell(w)$ und $\ell(w) \leq \ell(u)$ gilt. Das ist nur möglich, wenn $\ell(u) = \ell(w)$ und $\ell(x) = \ell(y) = 0$ gilt. Da λ das einzige Wort der Länge Null ist, muss $x = y = \lambda$ gelten. Also folgt $u = w$.

Man sieht an den Beispielen, dass sowohl Äquivalenzrelationen als auch Halbordnungen bei dieser Konstruktion herauskommen können.

5.7.3 Zum Zählen von Klammern: Die Zahlen von Catalan

Dieser Unterabschnitt bietet einen guten Anschluss an Abschnitt 3.4. Dazu verfeinern wir unsere Term-Definition aus dem Hauptteil wie folgt: Wir definieren die Menge $\mathcal{T}_n(M)$ der Terme (über M) der Größe n induktiv wie folgt:

- Jedes Element a aus M ist ein Term der Größe null.
- Sind s bzw. t Terme der Größe n_s bzw. n_t über M , so ist (st) ein Term der Größe $n = n_s + n_t + 1$ über M .
- Nichts Weiteres sind Terme über M .

Die Größe eines Terms ist also die Anzahl der in ihm vorkommenden Operationen. Beispielsweise enthält $(0(0))$ zwei Operationen. So, wie bei uns Klammern gesetzt werden, ist die Größe auch gleichbedeutend mit der Anzahl der Klammerpaare in einem Term. (Wenn “äußere Klammern” weggelassen werden dürfen, stimmt diese Aussage nicht mehr, daher muss man entsprechende Aussagen in der Literatur auch vorsichtig lesen. Bei uns hingegen gibt es eine natürliche Bijektion zwischen der Menge der Operationenpositionen und der Menge der Klammerpaarpositionen in einem Term.) Wir setzen nun: $C_n = |\mathcal{T}_n(\{0\})|$ und nennen C_n die n -te *Catalansche Zahl*. Aus der Definition ergibt sich unmittelbar die induktive Beschreibung

$$C_{n+1} = \begin{cases} 1, & \text{falls } n = -1 \\ \sum_{k=0}^n C_k C_{n-k}, & \text{sonst} \end{cases}$$

Will man nämlich die möglichen Klammerungen eines Terms mit $n + 1$ Operationen zählen, so kann man zunächst entscheiden, wo der Ort der Operation ist, die zu dem äußeren Klammerpaar gehört; dann stehen k Operationen links von der gewählten Position der “äußeren Operation” und $n - k$ rechts davon, wobei die Extremfälle $k = 0$ bzw. $k = n$ die Möglichkeit beschreiben, dass die äußere Operation ganz links bzw. ganz rechts im Term steht.

Eugène Charles Catalan war ein belgischer Mathematiker. Er hat (laut einem Lehrbuch von Notte) auf den Zusammenhang mit Triangulierungen hingewiesen, wobei Catalan selbst hierbei auf Lamé verweist: Es gibt C_n Triangulierungen eines konvexen $n+2$ -Ecks (siehe Abschnitt 5.1.7). Die Grundüberlegung ist wieder, dass das Einziehen einer Verbindungsline zwischen zwei nicht benachbarten Eckpunkten eines Polygons dieses in zwei Polygone mit $k+2$ bzw. $(n+2-(k+2-1)) = (n+1)-k$ Ecken zerlegt, und jedes kann nun wieder beliebig unterteilt werden, was der induktiven Beschreibung von C_n entspricht.

Eine weitere interessante Beziehung ist:

$$C_{n+1} = \frac{4n+2}{n+2} C_n$$

Dies sieht man kombinatorisch wie folgt ein: $C_{n+1} \cdot (n+2)$ ist die Anzahl der Möglichkeiten, in einem Ausdruck aus $\mathcal{T}_{n+1}(\{0\})$ eine der $n+2$ Nullen zu unterstreichen. Wir zählen also “Terme mit genau einem unterstrichenen Operanden”. Dieser unterstrichene Operand gehört in eindeutiger Weise zu einer Operation (und damit zu einem Klammerpaar). Streichen wir jetzt in Gedanken den unterstrichenen Operanden mit Operation und Klammerpaar, so erhalten wir einen Ausdruck aus $\mathcal{T}_n(\{0\})$. Umgekehrt können wir in einen Ausdruck aus $\mathcal{T}_n(\{0\})$ einen Ausdruck aus $\mathcal{T}_{n+1}(\{0\})$ mit unterstrichener Null machen, indem wir “irgendwo” eben diese unterstrichene Null (mit zugehöriger Operation und Klammerpaar) einfügen. Dazu stelle man sich behelfsweise den Term als Binärbaum mit $n+1$ Blättern und n inneren Knoten vor. Dieser Binärbaum enthält also 2^n Kanten. Jede kann durch Einfügen einer Operation “unterteilt” werden, und der (unterstrichene) Operand ist der linke oder rechte dieser Operation. Das liefert schon einmal $4n$ Möglichkeiten. Darüber hinaus könnte noch eine Operation oberhalb der Wurzel des Binärbaums eingefügt werden, womit die unterstrichene Null zum ersten oder zum letzten Operanden des Terms würde. Auf diese Art und Weise erhalten wir aus jedem Ausdruck aus $\mathcal{T}_n(\{0\})$ $4n+2$ Ausdrücke aus $\mathcal{T}_{n+1}(\{0\})$, bei denen jeweils eine Null unterstrichen ist. Dieses *doppelte Abzählen* liefert einen kombinatorischen Beweis für die Formel.

5.7.4 Das Relationenprodukt als Halbgruppe

Es sei M eine Menge.

$2^{M \times M}$ ist die Menge der Binärrelationen auf M .

Das Relationenprodukt \circ kann als eine Verknüpfung auf $2^{M \times M}$ aufgefasst werden, sodass $(2^{M \times M}, \circ)$ ein Gruppoid bildet.

Δ_M ist neutrales Element dieses Gruppoids.

\emptyset ist absorbierendes Element dieses Gruppoids.

Wir wissen: \circ ist assoziativ.

Die folgenden Mengen beschreiben Untergruppoide:

- 1) Die Menge aller partiellen Funktionen von M in M .
- 2) Die Menge aller totalen Funktionen von M in M .
- 3) Die Menge aller Injektionen von M in M .
- 4) Die Menge aller Bijektionen von M auf M .

5.7.5 Anknüpfungen zu den Formalen Sprachen

Die Konkatenation ist eine der Grundoperationen im Bereich der Formalen Sprachen, die die mathematische Grundlagen des Compilerbaus und für Programmiersprachen insgesamt darstellen.

Beispiel: Sei $M = \{a, b, c\}$. Erinnerung: Listschreibweise von Folgen:

$f := (a, a, b, b, a) \in M^{[5]}$, $g := (b, c, a) \in M^{[3]}$.

$f \cdot g = (a, a, b, b, a) \cdot (b, c, a) = (a, a, b, b, a, b, c, a) \in M^{[8]}$.

Z.B.: $(f \cdot g)(3) = f(3) = b$, da $3 < 5$.

$(f \cdot g)(6) = g(6 - 5) = g(1) = c$, da $6 \geq 5$.

Später und wenn keine Verwechslungsgefahrt besteht, lässt man gerne die Klammern

und Kommata weg und schreibt derlei Folgen kürzer als $f = aabbba$ bzw. $g = bca$, d.h., $f \cdot g = aabbabca$. Die Konkatenation von Folgen ergibt sich also durch Hintereinanderschreiben oder Verketten. Häufig lässt man dann (deshalb) sogar das Operationssymbol \cdot der Konkatenation fort.

Eine nicht-leere, endliche Menge nennt man auch *Alphabet*. Endliche Folgen über A nennt man dann auch *Wörter*. Das einzige Element aus A^0 nennt man auch *das leere Wort*. Das leere Wort ist neutrales Element der Konkatenation. Ist A ein Alphabet, so heißt $L \subseteq A^*$ eine (*formale*) *Sprache* über A . Eine Sprache ist also eine Menge von Wörtern über einem festen Alphabet. Durch das Komplexprodukt der Konkatenation (das man vereinfachend auch wieder \cdot notiert) ist für Sprachen L_1, L_2 über A auch $L_1 \cdot L_2$ definiert. Überdies kann man festhalten: Die Arbeitsweise von Automaten (Formalismen, die mit Wörtern und daher mit Formalen Sprachen umgehen können) lassen sich oft als Homomorphismen begreifen.

5.7.6 Ein erstes Restklassenbeispiel

Auf der Grundmenge $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ betrachte folgende Addition:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Die Einträge ergeben sich auch dadurch, dass man zwei Zahlen “wie üblich” addiert, das Ergebnis durch 6 teilt und dann den dabei gelassenen Rest einträgt. (Daher erklärt sich die Überschrift.) Mühsames Nachrechnen liefert:

$(\mathbb{Z}_6, +)$ ist eine Halbgruppe mit 0 als neutralem Element.

Unterhalbgruppen sind beschrieben durch $\{0\}, \{0, 3\}, \{0, 2, 4\}$.

Für die letzte Menge ergibt sich folgende Verknüpfungstafel:

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

5.8 Hüllen

5.8.1 Der Algorithmus von Floyd/Warshall

Die Idee von Floyd/Warshall (sowie Kleene) Ein Weg $v_0 v_1 \dots v_k$ heißt V' -Weg (für $V' \subseteq V$), wenn $\{v_1, \dots, v_{k-1}\} \subseteq V'$ gilt.

Spezieller: Sei $V = [n]$ (o.E.).

$(u, v) \in E_1^k$ gdw: Es gibt einen $[k]$ -Weg von u nach v der Länge $\leq k + 1$.

Lemma 5.8.1 $E_1^0 = \Delta_V$. Jeder Weg ist ein V -Weg (sogar ein $[n - 1]$ -Weg. Ist $k \geq 1$, so gilt: $E_1^k = E_1^{k-1} \cup \{(u, v) \in V \times V \mid (u, k) \in E_1^{k-1} \wedge (k, v) \in E_1^{k-1}\}$.

Logische Sicht:

x_{ij}^k sei "wahr" gdw. Es gibt einen $[k]$ -Weg von i nach j der Länge höchstens $k + 1$.

Induktiv können wir also ausrechnen:

$$x_{ij}^0 := (i = j) \vee (i, j) \in E \text{ und dann } x_{ij}^k := x_{ij}^{k-1} \vee (x_{ik}^{k-1} \wedge x_{kj}^{k-1}).$$

Das benötigt nur noch etwa $|V|^3$ viele Operationen zur Berechnung der reflexiv-transitiven Hülle von E .

Der Algorithmus von Warshall (Floyd 62 / Kleene 56 / Warshall 62 / Roy 59)

Berechnung der reflexiv-transitiven Hülle R^* von $R \subseteq X \times X$, $X = [n]$.

Dabei sei R als Boolesches $n \times n$ -Array abgespeichert und S enthalte die Lösung:

Gedanken zur Korrektheit:

R kann als Kantenrelation eines gerichteten Graphen gedeutet werden.

R^* drückt Erreichbarkeit aus:

$(u, v) \in R^*$ gdw. es gibt einen (evtl. leeren) Weg von u nach v im Graphen.

Invarianten:

Vor dem k -ten Eintritt in den Schleifenrumpf der äußeren FOR-Schleife zur Hüllberechnung gilt:

(1) Falls $(u, v) \in S$, so gibt es einen Weg von u nach v .

(2) Gibt es einen $[k - 1]$ -Weg der Länge höchstens k von u nach v , so gilt $(u, v) \in S$.

(a) Initialisierung:

Für i von 0 bis $n - 1$:

Für j von 0 bis $n - 1$:

$$S(i, j) \leftarrow R(i, j) \vee (i = j)$$

(b) Hüllberechnung:

Für k von 1 bis $n - 1$:

Für i von 0 bis $n - 1$:

Für j von 0 bis $n - 1$:

$$S(i, j) \leftarrow S(i, j) \vee (S(i, k) \wedge S(k, j))$$

Kapitel 6

Übungen

Es mag sein, dass Sie diese Übungen als ungewohnt abstrakt oder auch “zu mathematisch” empfinden. Wir empfehlen Ihnen dann einmal, das Buch von Mason, Burton und Stacey [31] durchzuarbeiten. Dieses verwenden wir auch als wesentliche Inspiration für unseren Vorkurs, der den Einstieg in den Universitätsalltag erleichtern soll und den Etlichen von Ihnen ja besucht haben.

6.1 Mengenlehre

6.1.1 Mengenangaben

Wir definieren folgende Mengen:

$$\begin{aligned} A &:= \{x \in \mathbb{Z} \mid x^2 = 9\}, \\ B &:= \{x \in \mathbb{N} \mid x \text{ ist gerade}\}, \\ C &:= B \cap \{x \in \mathbb{N} \mid x^2 \text{ ist gerade}\}, \\ D &:= B \cap \{x \in \mathbb{N} \mid x \leq 5\}, \\ E &:= \{x \in \mathbb{N} \mid x^2 - 3x + 2 = 0\}. \end{aligned}$$

Für die folgenden Aufgaben 1.-5. ist es nicht nötig, die Antworten zu beweisen oder zu begründen.

1. Zählen Sie *alle* Elemente der Menge D auf.
2. Zählen Sie *alle* Elemente der Menge E auf.
3. Zählen Sie *alle* Elemente der Menge F := {G | G ⊆ D} auf.
4. Zählen Sie *alle* Elemente der Menge F' := {G | G ⊂ D} auf.
5. Wie viele Elemente hat die Menge H := {G | G ⊆ F}?

Welche der folgenden Aussagen sind korrekt? Nun bitte *mit* Begründung!

6. A = {3}.
7. B ⊆ A.

8. A und D sind disjunkt.
9. F und $\{\emptyset\}$ sind disjunkt.
10. $B \subseteq C$.

Hinweis: Beachten Sie, dass die Mengen F, F' und H ebenfalls wieder Mengen als Elemente haben.

6.1.2 Zermelo-Zahlen

Wir haben in Abschnitt 5.1 die Zermelo-Zahlen eingeführt und deren Addition.

1. Addieren Sie die Zermelo-Zahlen 5_Z und 3_Z und dann die Zahlen 3_Z und 5_Z . Was fällt Ihnen hierbei auf?
2. Versuchen Sie, entsprechend die Multiplikation von Zermelo-Zahlen so zu definieren, dass sie mit der üblichen Multiplikation der natürlichen Zahlen “übereinstimmt”. Sie können hierbei auf die ja bereits eingeführte Addition zurückgreifen.

6.1.3 Mengengleichheit

Es seien a, b, c, d beliebige, nicht notwendigerweise verschiedene Dinge. Untersuchen Sie, unter welchen Umständen gilt:

1. $\{a, b\} = \{c, d\}$ bzw.
2. $\{a, \{a, b\}\} = \{c, \{c, d\}\}$.

6.1.4 Wie Mengen sich zueinander verhalten

Wir betrachten im Folgenden drei Mengen, die ihre Elemente aus dem Universum der wirklichen oder erdachten Personen schöpfen können.

- A = {x | x glaubt, das Innerste anderer Menschen zu kennen.},
- B = {x | x hat große Macht und nutzt diese mit Bedacht.},
- C = {x | x trägt gewöhnlich rote Kleidung.}.

Überlegen Sie: Gibt es Elemente, die ...

1. weder in A noch B noch C liegen?
2. zwar in A, aber weder in B noch in C liegen?
3. zwar in B, aber weder in A noch in C liegen?
4. zwar in C, aber weder in A noch in B liegen?
5. zwar in A und B, aber nicht in C liegen?
6. zwar in A und C, aber nicht in B liegen?
7. zwar in B und C, aber nicht in A liegen?
8. sowohl in A, B und C liegen?

Begründen Sie Ihre Antwort jeweils.

6.1.5 Ein Induktionsbeweis für Ketten gleicher Mengen

Beweisen Sie mit Hilfe der vollständigen Induktion Satz 3.1.8.

6.1.6 Induktionsbeweis einer bekannten geschlossenen Form für eine Reihe

Beweisen Sie durch vollständige Induktion über n die folgende Identität:

$$\sum_{i=0}^n i = \frac{n(n+1)}{2}.$$

6.1.7 Monotoniegesetze

Beweisen Sie Satz 3.1.13. Das bedeutet im Einzelnen das Folgende. Es seien A, B und C Mengen. Dann gilt:

1. Monotoniegesetz der Vereinigung: $(A \subseteq B) \implies (A \cup C \subseteq B \cup C)$;
2. Monotoniegesetz des Durchschnitts: $(A \subseteq B) \implies (A \cap C \subseteq B \cap C)$.

6.1.8 Assoziativgesetze

Beweisen Sie Satz 3.1.16, also: Für alle Mengen A, B, C gilt:

1. Assoziativgesetz der Vereinigung: $(A \cup B) \cup C = A \cup (B \cup C)$;
2. Assoziativgesetz des Durchschnitts: $(A \cap B) \cap C = A \cap (B \cap C)$.

6.1.9 Distributivgesetze

Es seien A, B, C Mengen. Beweisen Sie formal:

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

(Dieser Teil wurde beim Beweis von Satz 3.1.17 ausgelassen.

6.1.10 Allgemeine Distributivität

Wir brauchen zunächst die folgende Definition:

Sei M eine Menge. Für jede natürliche Zahl $n \in \mathbb{N}$ mit $n \geq 1$ und Teilmengen S_1, S_2, \dots, S_n von M sei

$$\bigcap_{i=1}^n S_i := \begin{cases} S_1, & \text{falls } n = 1, \\ \left(\bigcap_{i=1}^{n-1} S_i \right) \cap S_n, & \text{falls } n > 1. \end{cases}$$

Beispielsweise gilt

$$\begin{aligned} \bigcap_{i=1}^5 S_i &= \left(\bigcap_{i=1}^4 S_i \right) \cap S_5 = \left(\left(\bigcap_{i=1}^3 S_i \right) \cap S_4 \right) \cap S_5 = \dots = \\ &(((S_1) \cap S_2) \cap S_3) \cap S_4) \cap S_5 = S_1 \cap S_2 \cap S_3 \cap S_4 \cap S_5. \end{aligned}$$

Beweisen Sie die folgende allgemeine Form eines Distributivgesetzes mit vollständiger Induktion:

Es sei $n \in \mathbb{N}$ eine natürliche Zahl mit $n \geq 1$.

Es seien T und S_1, \dots, S_n Teilmengen von M .

Dann gilt:

$$T \cup \left(\bigcap_{i=1}^n S_i \right) = \bigcap_{i=1}^n (T \cup S_i)$$

In Ihrem Beweis dürfen Sie die Gültigkeit des “normalen Distributivgesetzes” $A \cup (B \cap C) = \dots$ voraussetzen.

Ganz entsprechend sieht man im Übrigen ein, dass ebenso gilt:

$$T \cap \left(\bigcup_{i=1}^n S_i \right) = \bigcup_{i=1}^n (T \cap S_i)$$

6.1.11 Disjunktheit von Mengen

Es seien A_1, \dots, A_n Mengen.

1. A_1, \dots, A_n heißen *disjunkt*, wenn $\bigcap_{i=1}^n A_i = \emptyset$.
2. A_1, \dots, A_n heißen *abschnittsweise disjunkt*, wenn $\forall 1 \leq j, k \leq n : j \neq k \implies \bigcap_{i=j}^k A_i = \emptyset$.
3. A_1, \dots, A_n heißen *paarweise disjunkt*, wenn $\forall 1 \leq j, k \leq n : j \neq k \implies A_j \cap A_k = \emptyset$.
4. A_1, \dots, A_n heißen *geordnet paarweise disjunkt*, wenn $\forall 1 \leq j, k \leq n : j < k \implies A_j \cap A_k = \emptyset$.

Untersuchen Sie, welche Implikationen zwischen diesen Definitionen gelten und welche nicht. Gilt also beispielsweise: Sind A_1, \dots, A_n disjunkt, so sind sie auch paarweise disjunkt?

6.1.12 Rechnen mit der Mengendifferenz

Es seien A, B, C beliebige Mengen. Welche der folgenden Formeln über Mengengleichheit gelten immer?

- Wenn eine Formel immer gilt, so beweisen Sie diesen Umstand. Geben Sie hierbei genau und im Einzelnen die Gesetzmäßigkeiten an, von denen Sie Gebrauch machen.
- Wenn eine Formel nicht allgemeingültig ist, so zeigen Sie das durch ein Gegenbeispiel. Überlegen Sie überdies, ob nicht wenigstens eine Inklusionsrichtung stets gilt.

1. $A \setminus (B \cup C) = (A \setminus B) \cup C$.
2. $A \setminus (B \setminus C) = (A \setminus B) \setminus C$.
3. $A \setminus (B \cup C) = A \cap \overline{B} \cap \overline{C}$.
4. $A \setminus (B \cap C) = (A \setminus B) \cup C$.

6.1.13 Zur binomischen Formel

Aus der Schule sollte die folgende “binomische Formel” bekannt sein:

$$(a + b) \cdot (a - b) = a^2 - b^2.$$

Interpretiert man nun Addition als Vereinigung, Produkt als Durchschnitt und Subtraktion als Mengendifferenz, so ergibt das die folgende Aussage:

Es seien A, B Mengen. Dann gilt: $(A \cup B) \cap (A \setminus B) = (A \cap A) \setminus (B \cap B)$.

1. Überprüfen Sie die Aussage unter Angabe einzelner Schritte für die Zahlenmengen $A = \{1, 2\}$ und $B = \{2, 3\}$.
2. Beweisen Sie die Richtigkeit dieser Formel allgemein.
Verwenden Sie dazu entweder eine “elementweise Argumentation” oder benutzen Sie Ihnen bekannte Rechengesetze der Mengenalgebra.
Begründen bzw. belegen Sie immer jeden einzelnen Schritt.

6.1.14 Zum Mengenprodukt

Beweisen Sie Satz 3.1.24.

6.2 Relationen und gerichtete Graphen

6.2.1 Zum Verstehen von Relationenausdrücken

Beschreiben Sie nacheinander in Worten, was für eine Relation über den ganzen Zahlen mit den folgenden Relationenausdrücken “gemeint” ist:

1. $R_1 = \overline{\Delta_{\mathbb{N}}}$,
2. $R_2 = \overline{\{1\} \times \mathbb{N}}$,
3. $R_3 = \overline{\Delta_{\mathbb{N}} \cap \{1\} \times \mathbb{N}}$,
4. $R_4 = | \cap (\mathbb{N} \times \mathbb{N}) \cap R_3$.

Überlegen Sie überdies, ob oder wie Sie R_3 “einfach” mit R_1 und R_2 ausdrücken können.

6.2.2 Zum Rechnen mit Relationenausdrücken

Betrachten Sie die folgenden Binärrelationen über $A = \{a, b, c, d\}$:

$$\begin{aligned} P &= A \times A \\ Q &= \emptyset \\ R &= \{(a, b), (b, c), (c, d), (d, a)\} \cup \Delta_A \\ S &= \overline{R} \cup \Delta_A \\ T &= \{(a, a), (a, b), (b, a), (b, c), (c, b), (d, d)\} \end{aligned}$$

Bestimmen Sie die folgenden Relationen durch Auflistung ihrer Elemente:

1. \bar{R}
2. $R \circ T$
3. $S \cap \overline{\Delta_A}$
4. T^-
5. $(R \cup T) \circ Q$

6.2.3 Kompakte Kennzeichnungen von Relationen mit dem Relationenprodukt

Kennzeichnen Sie $| \circ |$, $|^- \circ |$ und $P \circ P$ möglichst kompakt!

6.2.4 Monotoniegesetz

Beweisen Sie Satz 3.2.3.

6.2.5 Zerlegungen

Der Begriff der Zerlegung war in Definition 3.2.4 wortreich, aber nicht sehr formall eingeführt worden. Geben Sie hierfür eine saubere(re) mathematische Formulierung an.

6.2.6 Mengensystemgraph

Zeigen Sie den folgenden Sachverhalt: Es sei \mathfrak{M} ein Mengensystem über M und $G = (V, E)$ der zugehörige paare Mengensystemgraph (wobei ausnahmsweise $V = M \cup \mathfrak{M}$ auch unendlich sein darf). Dann gilt: \mathfrak{M} ist eine Zerlegung genau dann, wenn die Relation E vortotal, nachtotal und nacheindeutig ist.

6.2.7 Nacheindeutigkeit und Vortotalität 1

Es sei $R \subseteq A \times B$ eine Relation. Zeigen Sie:

1. R ist nacheindeutig gdw. $R^- \circ R \subseteq \Delta_B$.
2. R ist vortotal gdw. $\Delta_A \subseteq R \circ R^-$.
3. R ist nacheindeutig und vortotal gdw. $R \circ \overline{\Delta_B} = \bar{R}$.

6.2.8 Nacheindeutigkeit und Vortotalität 2

Beweisen Sie Satz 3.2.10.

6.2.9 Abgeschlossenheit der Eigenschaften unter dem Relationenprodukt

Es seien $R, S \subseteq M \times M$. Setze $T = R \circ S$. Untersuchen Sie, welche der folgenden Behauptungen gilt.

1. Sind R und S reflexiv, so ist auch T reflexiv.
2. Sind R und S symmetrisch, so ist auch T symmetrisch.
3. Sind R und S antisymmetrisch, so ist auch T antisymmetrisch.
4. Sind R und S transitiv, so ist auch T transitiv.

6.2.10 Eigenschaften von Relationen

Untersuchen Sie, wie in Abschnitt 5.2.2, die folgenden beiden Relationen auf ihre Eigenschaften:

- $R_1 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 3x\}$
- $R_2 = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x^2 + y^2 = 1\}$

6.2.11 Eine Eigenschaft von Quasiordnungen

Wir werden Relationen auf M , die reflexiv und transitiv sind, später als Quasiordnungen ansprechen und studieren. Daher ist die in Folgenden zu zeigende Eigenschaft wichtig: Ist $R \subseteq M \times M$, so gilt $R \circ R = R$. Überlegen Sie außerdem, ob die Umkehrung immer gilt.

6.3 Funktionen

6.3.1 Urbilder einer Funktion

Zeigen Sie: Für jede (partielle) Funktion $f : A \rightarrow B$ und alle $U, V \subseteq B$ gilt: $f^{-1}(U) \cap f^{-1}(V) = f^{-1}(U \cap V)$.

6.3.2 Der Kern einer Abbildung

Es sei $f : A \rightarrow B$ eine Abbildung. Definiere $x \sim_f y$ gdw. $f(x) = f(y)$. \sim_f ist eine Relation auf A . Diese nennt man auch *Kern* von f . Untersuchen Sie:

1. Gilt $\sim_f = f \circ f^{-1}$ (hier f aufgefasst als Relation)?
2. Ist \sim_f stets reflexiv?
3. Ist \sim_f stets symmetrisch?
4. Ist \sim_f stets antisymmetrisch?
5. Ist \sim_f stets transitiv?

Untersuchen Sie ferner, welche Eigenschaften einer Abbildung für welche Eigenschaften von \sim_f maßgeblich waren und formulieren Sie mögliche Verallgemeinerungen der vorigen Aussagen.

6.3.3 Urbilder einer Abbildung

Es sei $f : A \rightarrow B$ eine Abbildung. Für jedes $b \in B$ ist $f^-(b) = \{a \in A \mid f(a) = b\}$ eine Teilmenge von A . $\mathcal{M}_f = \{f^-(b) \mid b \in f(A)\}$ ist also ein Teilmengensystem von A . Zeigen Sie: Gilt $A \neq \emptyset$, so ist \mathcal{M}_f eine Zerlegung von A .

6.3.4 Eine Kennzeichnung von Injektionen

Beweisen Sie Satz 3.3.6!

6.3.5 Zum Tauschoperator

Beweisen Sie Satz 3.3.8!

6.3.6 Endliche und unendliche Folgen

Wir hatten surjektive Folgen als vollständige Auflistungen kennengelernt. Überlegen Sie, welche der folgenden Aussagen stimmt und begründen Sie Ihre Behauptung.

1. Ist $f : [n] \rightarrow M$ eine endliche surjektive Folge, so ist M endlich.
2. Ist $f : \mathbb{N} \rightarrow M$ eine unendliche surjektive Folge, so ist M unendlich.
3. Es gibt eine endliche Menge M und eine vollständige Auflistung $f : \mathbb{N} \rightarrow M$.

6.3.7 Die geometrische Reihe

Zeigen Sie mit einem Induktionsbeweis: Für Zahlen $a \neq 0$ und $n \in \mathbb{N}$ gilt:

$$\sum_{i=0}^n a^i = \frac{a^{n+1} - 1}{a - 1}.$$

Hinweis: Wir betrachten hier also die Folge $n \mapsto \sum_{i=0}^n a^i$.

6.3.8 Die Fakultätsfunktion

Zeigen Sie die Stirlingsche Formel in der folgenden Fassung (beispielsweise mit vollständiger Induktion).

$$1 < e^{1/(12n+1)} \leq \frac{n!}{\sqrt{2\pi n} \cdot (\frac{n}{e})^n} \leq e^{1/(12n)} < 1 + \frac{1}{11n}$$

6.3.9 Das Cantorsche Abzählungsschema

Sie haben im Haupttext das Cantorsche Abzählungsschema kennen gelernt. Als Tabelle lässt sich dies folgendermaßen darstellen:

	0	1	2	3	4	5	...
0	0	2	5	9	14	20	...
1	1	4	8	13	19	26	...
2	3	7	12	18	25	33	...
3	6	11	17	24	32	41	...
4	10	16	23	31	40	50	...
5	15	22	30	39	49	60	...
:	:	:	:	:	:	:	⋮

Die Tabelle erhält man also wenn man nacheinander, angefangen in der linken oberen Ecke, die Diagonalen von links unten nach rechts oben mit den natürlichen Zahlen ausfüllt. Das Cantorsche Abzählungsschema lässt sich auch folgendermaßen als Cantorsche Paarfunktion darstellen:

$$\langle i, j \rangle = \frac{(i+j)(i+j+1)}{2} + j,$$

d. h., $\langle i, j \rangle$ ist der Eintrag in Zeile i und Spalte j . Genauso gut könnte man die Tabelle auch so ausfüllen, dass man wieder in der oberen Ecke anfängt, dann aber nicht die Diagonalen ausfüllt, sondern die nächste Zeile von links nach rechts füllt bis das erste Feld oberhalb frei ist und dann nach oben läuft und dies wiederholt:

	0	1	2	3	4	5	6	...
0	0	3	8	15	24	35	48	...
1	1	2	7	14	23	34	47	...
2	4	5	6	13	22	33	46	...
3	9	10	11	12	21	32	45	...
4	16	17	18	19	20	31	44	...
5	25	26	27	28	29	30	43	...
6	36	37	38	39	40	41	42	...
:	:	:	:	:	:	:	:	⋮

So befinden sich also, für alle $n \in \mathbb{N}$, in den ersten n Zeilen und n Spalten die ersten n^2 natürlichen Zahlen.

Geben Sie eine Paarfunktion $\widehat{\langle i, j \rangle}$ an (in Form einer Formel, wie wir es auch bei der Cantorschen Paarfunktion gemacht haben), die für Werte i und j den Eintrag der Zeile i und Spalte j der obigen Tabelle liefert.

6.3.10 Indikatorfunktion

Beweisen Sie die Behauptung aus Beispiel 3.3.17:

Die Abbildung $h : 2^M \rightarrow \{0, 1\}^M, A \mapsto \chi_A$ ist eine Bijektion.

6.4 Zur Größe von Mengen

6.4.1 Äquivalenzsatz von Cantor

Laut Bernstein (Mathematische Annalen Band: 61 Erscheinungsjahr: 1905) hat Cantor den folgenden Sachverhalt als Äquivalenzsatz angesprochen; wir formulieren ihn in heutiger Sprechweise:

Sind A und B zwei Mengen, sodass A zu einer Teilmenge von B gleichmächtig ist und B zu einer Teilmenge von A gleichmächtig ist, so gilt, dass A und B gleichmächtig sind.

Hinweis: Vor 100 Jahren sagte man “äquivalent” statt “gleichmächtig”.

1. Beweisen Sie den Äquivalenzsatz. Erklären Sie, wie der Satz von Schröder & Bernstein in den Beweis einfließt.
2. Erläutern Sie, wie man den Satz von Schröder & Bernstein beweisen könnte, wenn man einen davon unabhängigen Beweis für den Äquivalenzsatz besäße.

6.4.2 Surjektiv, injektiv, bijektiv

Im Beweis von Satz 3.4.9 gab es zwei interessante Beweisrichtungen. Wie Sie bemerkt haben werden, haben wir beide Richtungen bewiesen, allerdings mit zwei unterschiedlichen Vorgehensweisen, einmal mit einem Induktionsbeweis und das andere Mal mit Hilfe des Endlichkeitssatzes von Dedekind. Drehen Sie nun diese Vorgehensweisen um, d.h.:

1. Beweisen Sie mit einem Induktionsbeweis, dass in der vorgelegten Situation aus der Injektivität die Surjektivität folgt.
2. Beweisen Sie mit Hilfe des Endlichkeitssatzes von Dedekind, dass in der vorgelegten Situation aus der Surjektivität die Injektivität folgt.

6.4.3 Gleichmächtig oder nicht?

Es seien A und B höchstens abzählbare, nicht leere Mengen. Untersuchen Sie, unter welchen Bedingungen an A und B die Menge B^A der Abbildungen von A nach B und die Menge $(B \cup \{\perp\})^A$ der partiellen Funktionen von A nach B gleichmächtig sind.

6.4.4 Das Löschen eines Elements

Beweisen Sie:

Sei A eine Menge und $a \in A$. Es gilt: A ist endlich $\iff |A \setminus \{a\}| < |A|$.

6.4.5 Eigenschaften von Funktionen auf einer endlichen Menge

Vervollständigen Sie den Beweis von Satz 3.4.9!

6.4.6 Dirichletsches Schubfachprinzip

Wir haben das Dirichletsche Schubfachprinzip für beliebige Mengen (indirekt) mit dem Satz von Schröder & Bernstein bewiesen. Begünden Sie nun “direkt”, warum gilt: Falls man n Gegenstände auf m Fächer ($n > m > 0$) verteilt, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Beweisen Sie sodann die folgende Verallgemeinerung: Sind A und B endliche Mengen und ist $f : A \rightarrow B$ eine Abbildung, so gibt es ein $b' \in B$ mit $|f^{-1}(b')| \geq |A|/|B|$.

6.4.7 Zählen von Relationen

Es sei M eine m -elementige Menge.

1. Wie viele Relationen gibt es auf M ?
2. Wie viele reflexive Relationen gibt es auf M ?
3. Wie viele symmetrische Relationen gibt es auf M ?
4. Wie viele voreinige Relationen gibt es auf M ?

Begründen Sie Ihre „Zählergebnisse“ jeweils mit Sachverhalten aus dem Haupttext.

6.4.8 Binomialkoeffizienten

Es seien $n, k \in \mathbb{N}$ mit $k \leq n$.

1. Beweisen Sie zunächst kombinatorisch die Identität

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

(hierbei sei $k \geq 1$).

2. Beweisen Sie mit Hilfe jener Identität induktiv die bekannte Formel

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

6.4.9 Binomischer Lehrsatz

Der binomische Lehrsatz lautet allgemeiner als möglicherweise von der Schule her geläufig: Für beliebige reelle Zahlen x, y und natürliche Zahlen n gilt:

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

Beweisen Sie diesen Satz mit einem kombinatorischen Argument.

6.4.10 Zählen beim Schach

In Abschnitt 5.3.8 wurden verschiedene Mengen im Zusammenhang mit der Modellierung von einfachen Turmendspielen eingeführt. Wie groß sind Pos, S – Zug, W – Zug und auch Zug? Wie viele Matt- und Remispositionen gibt es? Begründen Sie Ihre einzelnen Überlegungen!

6.4.11 Betrunkene Seemänner

Auf einem Schiff arbeiten 5 Seemänner. Nach der Arbeit sitzen die Männer in geselliger Runde zusammen und gönnen sich eine Menge vom ihrem Rum. Anschließend sind die Seemänner so betrunken, dass sie nicht mehr wissen, welche der 5 Kojen ihre eigene ist. Sie sind nur noch froh, überhaupt eine unbesetzte Koje zum Schlafen zu finden, was auch allen gelingt.

Wie viele Möglichkeiten gibt es, dass kein Seemann in seiner eigenen Koje schläft? Wie wahrscheinlich ist dieser Fall, wenn man davon ausgeht, dass die Seeleute derart betrunken waren, dass sie die Kojen nicht mehr voneinander unterscheiden konnten?

6.4.12 Zählen von Zerlegungen

Wir hatten den Begriff der Zerlegung in Definition 3.2.4 eingeführt. Wie viele Zerlegungen B_n der Menge $[n]$ gibt es nun aber?

Hinweis: Die Konvention $B_0 = 1$ ist sinnvoll, folgt aber nicht aus der obigen kombinatorischen Definition.

1. Geben Sie sämtliche Zerlegungen der Mengen [1], [2] und [3] an.
2. Geben Sie einen kombinatorischen Beweis für die Formel

$$B_{n+1} = \sum_{k=0}^n \binom{n}{k} B_k$$

an (für $n \geq 0$).

6.4.13 Inklusions-Exklusionsprinzip

Beweisen Sie Satz 3.4.31 per Induktion.

6.4.14 Zur Anwendung des Inklusions-Exklusionsprinzips

Bestimmen Sie die Anzahl $s(n, k)$ der Surjektionen von $[n]$ auf $[k]$.

Zusatz: Leiten Sie hieraus eine Summendarstellung für $n!$ ab.

6.4.15 Zum Satz von Ramsey

Es sei $G = (V, E)$ ein ungerichteter Graph.

- Eine Knotenmenge $U \subseteq V$ heißt *unabhängig*, falls kein Knoten aus U Nachbarn eines anderen Knoten aus U ist.
- Eine Knotenmenge $C \subseteq V$ heißt *Clique*, falls jeder Knoten aus C Nachbarn eines jeden anderen Knotens aus C ist.

Beweisen Sie:

1. Ist $e \in E$, so gibt es ein $x \in V \setminus U$, sodass e mit x inzidiert.
2. Zu jeder natürlichen Zahl k gibt es eine natürliche Zahl $n(k)$, sodass für jeden Graphen $G = (V, E)$ mit wenigstens $n(k)$ Knoten gilt: G enthält eine unabhängige Menge der Größe k oder G enthält eine Clique der Größe k .

(Lesen Sie zur Vorbereitung Abschnitt 4.4.5.)

6.5 Quasiordnungen

6.5.1 Quasiordnungen aus Quasiordnungen

Beweisen Sie die Folgerungen 3.5.2 und 3.5.3.

6.5.2 Äquivalenzrelationen und das Relationenprodukt

Beweisen Sie: Sind R und S Äquivalenzrelationen auf der Menge M , so sind die folgenden drei Aussagen äquivalent:

1. $R \circ S$ ist eine Äquivalenzrelation;
2. $S \circ R$ ist eine Äquivalenzrelation;
3. $R \circ S = S \circ R$.

6.5.3 Wie viele Äquivalenzrelationen gibt es?

Bestimmen Sie sämtliche Äquivalenzrelationen auf der Menge $M = \{0, 1, 2\}$.

6.5.4 Restklassen

In Beispiel 3.5.8 wurde die Relation $R_m = \{(a, b) \in \mathbb{Z}^2 : m \mid (a - b)\}$ eingeführt. Zeigen Sie, dass es sich hierbei (für beliebige $m \in \mathbb{N} \setminus \{0\}$) um eine Äquivalenzrelation handelt.

6.5.5 Eine Eigenschaft von Äquivalenzklassen

Beweisen Sie Lemma 3.5.9.

6.5.6 Äquivalenzrelationen und Zerlegungen

Zeigen Sie: Ist R Äquivalenzrelation, so gilt $R = (\sim_{Z_R})$.

6.5.7 Quasiordnungen auf den komplexen Zahlen

Betrachten Sie über der Menge \mathbb{C} der komplexen Zahlen die Relation $y \prec z \iff |y| \leq |z|$.

Sollten Ihnen die komplexen Zahlen nicht vertraut sein, für unsere Betrachtungen genügt es, diese Menge mit der Euklidischen Ebene \mathbb{R}^2 gleichzusetzen. Dann ist für $x = (x_1, x_2) \in \mathbb{R}^2$ $|x|$ die Länge des Vektors x , also $|x| = \sqrt{x_1^2 + x_2^2}$.

Zeigen Sie:

1. \prec ist eine Quasiordnung auf \mathbb{C} .
2. \prec ist weder symmetrisch noch antisymmetrisch.
3. Wie sehen die Äquivalenzklassen von der \prec zugeordneten Äquivalenzrelation \sim_\prec auf \mathbb{C} aus?

6.5.8 Zur Existenz von größten Elementen und Suprema

Betrachten Sie die im Folgenden angegebenen Halbordnungen und diskutieren Sie die Existenz von größten Elementen und von Suprema von Teilmengen der Grundmenge.

Beispiel: Teilmengenhalbordnung von $\{a, b, c\}$. (Grundmenge der HO ist also $2^{\{a, b, c\}}$.)

Beispiel: $0 \prec 2 \prec 4 \prec \dots \prec 1 \prec 3 \prec 5 \prec \dots$ auf \mathbb{N} .

6.5.9 Quasiordnungen und Inverse

Es sei $R \subseteq M \times M$ eine Binärrelation. Zeigen Sie:

1. R ist reflexiv gdw. R^- ist reflexiv.
2. R ist transitiv gdw. R^- ist transitiv.
3. R ist Quasiordnung gdw. R^- ist Quasiordnung.
4. R ist symmetrisch gdw. R^- ist symmetrisch.
5. R ist Äquivalenzrelation gdw. R^- ist Äquivalenzrelation.
6. R ist antisymmetrisch gdw. R^- ist antisymmetrisch.
7. R ist Halbordnung gdw. R^- ist Halbordnung.
8. R ist lineare Ordnung gdw. R^- ist lineare Ordnung.

6.5.10 Vergleichbarkeit

Es sei M eine Menge und $V \subseteq M \times M$ die zu einer Halbordnung $R \subseteq M \times M$ gehörende Vergleichbarkeitsrelation. Zeigen Sie: Ist V transitiv, so ist V eine Äquivalenzrelation.

6.5.11 Sortieren

Beweisen Sie Lemma 3.5.16 mit Induktion über m .

6.6 Ungerichtete Graphen

6.6.1 Zwillinge

Es sei $G = (V, E)$ ein ungerichteter Graph. Zu $v \in V$ bezeichnet $N(v)$ die Menge der Nachbarn von v , d.h.,

$$N(v) = \{u \in V \mid uv \in E\}.$$

Setze (wie üblich) $N[v] = N(v) \cup \{v\}$.

Zeigen Sie, dass es sich bei den im Folgenden definierten Relationen jeweils um Äquivalenzrelationen handelt:

falscher Zwilling $FZ \subseteq V \times V$ mit $(u, v) \in FZ \iff N(u) = N(v)$.

wahrer Zwilling $WZ \subseteq V \times V$ mit $(u, v) \in WZ \iff N[u] = N[v]$.

Zwilling $Z = FZ \cup WZ$.

Zusatz: Überlegen Sie, ob die Vereinigung zweier Äquivalenzrelationen über der selben Grundmenge stets wieder eine Äquivalenzrelation liefert.

6.6.2 Isomorphie: Ein Beweis

Zeigen Sie Satz 3.6.6.

6.6.3 Isomorphie: Beispiele

In Beispiel 3.6.7 sind viele kleine Graphen aufgelistet. Überprüfen Sie, ob dies alle paarweise nicht-isomorphen Graphen mit höchstens vier Knoten sind.

6.6.4 Vom Nutzen der Isomorphie

Isomorphe Graphen sollen “gleiche Eigenschaften” haben.

Beweisen Sie die folgenden Aussagen.

Es seien $G = (V, E)$ und $G' = (V', E')$ Graphen und $\phi : V \rightarrow V'$ ein Isomorphismus von G auf G' .

1. ϕ^{-1} ist ein Isomorphismus von G' auf G .
2. $\phi_E : E \rightarrow E'$, $xy \mapsto \phi(x)\phi(y)$ ist eine Bijektion.
3. $\forall v \in V : d(v) = d(\phi(v))$.

6.6.5 Eine Kennzeichnung von Pfaden

Beweisen Sie: Ein zusammenhängender Graph $G = (V, E)$ der Ordnung mindestens zwei ist ein Pfad gdw. G besitzt zwei Knoten vom Grad eins und $|V| - 2$ Knoten vom Grad zwei.

6.6.6 Knoten- und Kantenanzahlen in Bäumen

Beweisen Sie Lemma 3.6.9, indem Sie (nur) auf die induktive Definition von Bäumen zurückgreifen.

6.6.7 Eine weitere Baumkennzeichnung

Beweisen Sie Satz 3.6.22.

6.6.8 Ein Spannbaumalgorithmus

In Abschnitt 5.6.1 ist ein rekursiver Spannbaumalgorithmus in Pseudo-Code angegeben und eine iterative Variante (nur) textuell. Geben Sie die iterative Variante als Pseudo-Code an.

6.6.9 Cayley-Formel

Vervollständigen Sie den Beweis von Satz 3.6.24.

6.7 Verknüpfungen

6.7.1 Absorbierende Elemente

Beweisen Sie Lemma 3.7.2.

6.7.2 Komplexprodukt

Die Implikation als Verknüpfung auf der Menge $M = \{0, 1\}$ ist wie folgt gegeben:

\implies	0	1
0	1	1
1	0	1

Geben Sie die Verknüpfungstafel für das Komplexprodukt $\implies \kappa$ von \implies an.
Beweisen Sie als Nächstes Satz 3.7.3.

6.7.3 Produktgruppoide

Im Haupttext wurden die Verknüpfungstafeln für Konjunktion \wedge und Disjunktion \vee auf der Menge $M = \{0, 1\}$ angegeben, die die Gruppoide \mathbb{G}_\wedge und \mathbb{G}_\vee beschreiben. Geben Sie die Verknüpfungstafel für das Produktgruppoide $\mathbb{G}_\wedge \times \mathbb{G}_\vee$ an.

Beweisen Sie als Nächstes Satz 3.7.4. Untersuchen Sie außerdem die Frage: Wie übertragen sich neutrale und absorbierende Elemente?

6.7.4 Komplementbildung als Homomorphismus

Es sei \mathcal{U} ein Universum. Dann sind $(2^\mathcal{U}, \cup)$ und $(2^\mathcal{U}, \cap)$ Gruppoide. Betrachte $h : 2^\mathcal{U} \rightarrow 2^\mathcal{U}, A \mapsto \overline{A}$.

Zeigen Sie: In diesem Sinne ist die Komplementbildung ein Homomorphismus.

6.7.5 Isomorphie als Äquivalenzrelation

Es sei M eine nicht-leere Menge und $\mathbb{G}(M)$ die Menge aller Gruppoide mit Grundmenge M . Für G_1, G_2 schreiben wir:

$$G_1 \cong G_2 \iff \exists f : M \rightarrow M : f \text{ ist Isomorphismus von } G_1 \text{ auf } G_2$$

Zeigen Sie: \cong ist Äquivalenzrelation auf $\mathbb{G}(M)$,

6.7.6 Äquivalenzrelationen liefern Homomorphismen

Beweisen Sie Lemma 3.7.26.

6.7.7 Quasiordnungen aus Homomorphismen

Es sei (H, \circ) eine Halbgruppe. Sei \mathcal{H} die Menge aller Halbgruppenhomomorphismen der Form $h : H \rightarrow H$. Definiere auf H die Relation \leq_\circ wie folgt:

$$a \leq_\circ b : \iff \exists h \in \mathcal{H} : h(b) = a.$$

1. Zeigen Sie. (H, \leq_\circ) ist eine Quasiordnung. Welche Eigenschaften von Homomorphismen bzw. von \mathcal{H} haben Sie benutzt?
2. Geben Sie eine Halbgruppe (H_1, \circ_1) an, sodass (H_1, \leq_{\circ_1}) eine Halbordnung ist.
3. Geben Sie eine Halbgruppe (H_2, \circ_2) an, sodass (H_2, \leq_{\circ_2}) eine Äquivalenzrelation ist.
4. Geben Sie eine Halbgruppe (H_3, \circ_3) an, sodass (H_3, \leq_{\circ_3}) weder eine Halbordnung noch eine Äquivalenzrelation ist.

6.7.8 Assoziativität

Überprüfen Sie, ob die folgenden Verknüpfungen assoziativ sind. Sei $M = \{1, 2, 3, 4\}$.

\circ_1	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

\circ_2	1	2	3	4
1	1	1	1	1
2	1	2	3	4
3	1	3	1	4
4	1	4	1	2

6.7.9 Konkatenation

Beweisen Sie Lemma 3.7.13.

6.7.10 Potenzen von Relationen

Beweisen Sie Satz 3.7.15.

6.7.11 Kommutativität

Beweisen Sie die Sätze 3.7.16 und 3.7.17.

6.7.12 Idempotente Elemente

Es sei $G = (M, \circ)$ ein Gruppoid. Ein Element $a \in M$ heißt *idempotent*, falls $a \circ a = a$ gilt. Viele bekannte Gruppoide wie $(\mathbb{Z}, +)$ oder (\mathbb{Z}, \cdot) besitzen idempotente Elemente. Zeigen Sie:

1. Jedes Monoid besitzt idempotente Elemente.
2. Jede endliche Halbgruppe besitzt idempotente Elemente.
3. Es gibt Halbgruppen ohne idempotente Elemente.

6.7.13 Idempotente Untermonoide

Es sei M eine nicht-leere Menge. Bekanntermaßen ist $\mathbb{M} := (2^{M \times M}, \circ, \Delta_M)$ ein Monoid, wobei \circ das Relationenprodukt bezeichnet.

1. Zeigen Sie: $D_M := \{R \subseteq M \times M \mid R \subseteq \Delta_M\}$ beschreibt ein Untermonoid \mathbb{D}_M von \mathbb{M} .
2. Zeigen Sie: \mathbb{D}_M ist idempotent.
3. Wie viele Elemente enthält D_M , wenn M endlich ist und m Elemente besitzt?
4. Geben Sie ein “möglichst einfaches” zu \mathbb{D}_M isomorphes Monoid an.

6.7.14 Funktionengrupoide

Es seien $\mathbb{G} = (M, \circ)$ ein Gruppoid und N eine beliebige Menge. Im Haupttext wurde das Funktionengrupoide $\mathbb{G}^N := (M^N, \circ_N)$ eingeführt. Beweisen Sie:

- Ist \mathbb{G} assoziativ, so ist auch \mathbb{G}^N assoziativ.
- Ist \mathbb{G} kommutativ, so ist auch \mathbb{G}^N kommutativ.
- Ist \mathbb{G} idempotent, so ist auch \mathbb{G}^N idempotent.
- Besitzt \mathbb{G} ein neutrales Element, so auch \mathbb{G}^N .
- Besitzt \mathbb{G} ein absorbierendes Element, so auch \mathbb{G}^N .

6.7.15 Eigenschaften von Verknüpfungen und gewissen zugehörigen Relationen

Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid.

- Wir definieren die *Erreichbarkeitsrelation* $R_{\mathbb{G}}$ auf M wie folgt:

$$(a, c) \in R_{\mathbb{G}} : \iff \exists b \in M : a \circ b = c.$$

Zeigen Sie: Ist \mathbb{G} eine Halbgruppe, dann ist $R_{\mathbb{G}}$ transitiv.

- Für jedes $c \in M$ definiere die Relation $Ziel_{\mathbb{G}, c}$ folgendermaßen:

$$(a, b) \in Ziel_{\mathbb{G}, c} : \iff a \circ b = c.$$

Zeigen Sie: Ist \mathbb{G} kommutativ, dann ist $Ziel_{\mathbb{G}, c}$ symmetrisch. Hier gilt auch eine Umkehrung in folgendem Sinne: Ist $Ziel_{\mathbb{G}, c}$ symmetrisch für jedes $c \in M$, so ist \mathbb{G} kommutativ.

- Definiere die Relation $Zurück_{\mathbb{G}}$ auf M wie folgt:

$$(a, b) \in Zurück_{\mathbb{G}} : \iff a \circ b = b.$$

Zeigen Sie: \mathbb{G} ist idempotent genau dann, wenn $Zurück_{\mathbb{G}}$ reflexiv ist.

6.7.16 Halbverbände aus Halbordnungen

Beweisen Sie Satz 3.7.22.

6.8 Hullen

6.8.1 Abgeschlossene Intervalle

Wir versuchen folgende Verallgemeinerung der Definition aus dem Haupttext: Zu $A \subseteq \mathbb{R}$ setze: $H(A) := [\inf A, \sup A]$. Zeigen Sie:

1. Auf jedem Universum $U_{a,b} := [a, b]$, $a \leq b$ ist H ein Hullenoperator.
2. Diskutieren Sie die definitorischen Probleme dieses Operators auf dem Universum $U = \mathbb{R}$. Ist H hier auch ein Hullenoperator?

6.8.2 Konvexe Mengen

Im Haupttext findet sich folgende Definition:

Sei $U = \mathbb{R} \times \mathbb{R}$ (Ebene). Zu $A \subseteq \mathbb{R} \times \mathbb{R}$ sei:

$$\text{conv}(A) := \left\{ \left(\sum_{i=1}^n \alpha_i x_i, \sum_{i=1}^n \alpha_i y_i \right) \mid n \in \mathbb{N}, \sum_{i=1}^n \alpha_i = 1, \forall 1 \leq i \leq n : (x_i, y_i) \in A \wedge \alpha_i \geq 0 \right\}.$$

Die abgeschlossenen Mengen sind hier die *konvexen Mengen*.

1. Beweisen Sie: $\text{conv} : 2^{\mathbb{R} \times \mathbb{R}} \rightarrow 2^{\mathbb{R} \times \mathbb{R}}$ ist ein Hüllenoperator.
2. Zeigen Sie: Eine Menge $A \subseteq \mathbb{R} \times \mathbb{R}$ ist konvex genau dann, wenn mit $x, y \in A$ auch die gesamte Verbindungsstrecke \overline{xy} in A liegt.
3. Zeigen Sie: Eine Menge $A \subseteq \mathbb{R} \times \mathbb{R}$ ist konvex genau dann, wenn sie sich als Schnitt beliebig vieler Halbebene ergibt. Hierbei ist eine *Halbebene* durch eine Gerade g und ein Vorzeichen \pm gegeben, und $H_{g,+}$ bzw. $H_{g,-}$ versammelt alle Punkte, die auf und oberhalb bzw. auf und unterhalb von g liegen.
4. Welche der drei Kennzeichnungen konvexer Mengen ist besonders für einen direkten Nachweis dafür geeignet, dass das Mengensystem der konvexen Mengen ein abgeschlossenes System bildet?

6.8.3 Oberhalbmengen

Zeigen Sie: Ist (U, \leq) eine Quasiordnung, so bildet $O_{\leq} : 2^U \rightarrow 2^U$ einen Hüllenoperator.

Betrachten wir nun konkreter die Quasiordnung $(2^{\{0,1,2\}}, \subseteq)$.

1. Bestimmen Sie die Menge \mathcal{O} aller zugehörigen Oberhalbmengen.
2. Ist die Abbildung $h : 2^{\{0,1,2\}} \rightarrow \mathcal{O}, A \mapsto O_{\leq}(A)$ bijektiv?
3. Wir wissen aus Satz 3.8.2, dass \mathcal{O} gegen Schnittbildung abgeschlossen ist. Bestätigen Sie diesen Sachverhalt anhand von drei Beispielen.
4. Ist h ein Homomorphismus zwischen den Halbverbänden $(2^{\{0,1,2\}}, \cup)$ und (\mathcal{O}, \cap) ?

6.8.4 Hüllen und abgeschlossene Systeme

Beweisen Sie Satz 3.8.6.

6.8.5 Hüllen und Halbordnungen

Sei U eine Menge und sei (U, \leq_1) eine lineare Ordnung. Für beliebige $A \subseteq U$ definieren wir

$$H_1(A) := \{x \mid x \in U, \text{ es gibt } y, z \in A \text{ mit } y \leq_1 x \text{ und } x \leq_1 z\}.$$

1. Beweisen Sie, falls $A \subseteq U$, dann ist $(H_1(A), \leq_1)$ eine lineare Ordnung.
2. Beweisen Sie, dass H_1 ein Hüllenoperator ist.

Sei nun (U, \leq_2) eine Quasiordnung. Für beliebige $A \subseteq U$ definieren wir

$$H_2(A) := \{x \mid x \in U, \text{ es gibt } y \in A \text{ mit } y \leq_2 x\}.$$

3. Beweisen Sie, falls $A \subseteq U$, dann ist $(H_2(A), \leq_2)$ eine Quasiordnung.
4. Beweisen Sie, dass H_2 ein Hüllenoperator ist.

6.8.6 Hüllen und Gruppoide

Sei $n \in \mathbb{N}$. Wir betrachten folgende Gruppoide: $\mathbb{G}_1 := (\mathbb{N}, \cdot)$, $\mathbb{G}_2 := (\mathbb{N}, +)$ und $\mathbb{G}_3 := (2^{[n]}, \cup)$. Die Verknüpfungen \cdot , $+$ und \cup entsprechen der Multiplikation und der Addition auf natürlichen Zahlen, sowie der Mengenvereinigung. Geben Sie die vom Erzeugendensystem A erzeugten Gruppoide an:

1. $\langle A \rangle_{\mathbb{G}_1}$ mit $A = \{3\}$.
2. $\langle A \rangle_{\mathbb{G}_2}$ mit $A = \{1\}$.
3. $\langle A \rangle_{\mathbb{G}_3}$ mit $A = \{\emptyset, \{0\}, \{1\}, \{2\}, \dots, \{n-1\}\}$.

Begründen Sie ihre Antworten möglichst ausführlich.

6.8.7 Zur Implementierung des Relationenprodukts

Ist M eine endliche Menge, so lässt sich jede Teilmenge R von $M \times M$ als Bitvektor implementieren. Ist $|M| = m$, so gibt es daher eine natürliche Bijektion $h : 2^{M \times M} \rightarrow \{0, 1\}^{[m] \times [m]}$. Geben Sie eine derartige Bijektion formal an und definieren Sie eine Verknüpfung \cdot auf $\{0, 1\}^{[m] \times [m]}$ derart, dass $h; (2^{M \times M}, \circ) \rightarrow (\{0, 1\}^{[m] \times [m]}, \cdot)$ ein Halbgruppenisomorphismus ist. Hierbei ist \circ das Relationenprodukt.

Hinweis: \cdot entspricht dem Matrixprodukt.

6.8.8 Äquivalenzhüllen: Charakterisierung

Beweisen Sie Satz 3.8.15.

6.8.9 Äquivalenzhüllen

Zeigen Sie, dass für jede Menge M die Menge der Äquivalenzrelationen auf M ein abgeschlossenes System bildet.

Betrachten wir konkreter die Menge $M = \{0, 1, 2\}$. $R_1 = \{(0, 1)\}$, $R_2 = \{(0, 1), (1, 2)\}$ und $R_3 = \{(0, 1), (1, 1)\}$ sind drei Relationen auf M . Beschreiben Sie jeweils die von R_i , $i = 1, 2, 3$, erzeugten Äquivalenzrelationen.

Kapitel 7

Ausgewählte Lösungen

Hier finden Sie Lösungsvorschläge zu einigen, wenn auch nicht allen Aufgaben aus Kapitel 6. Stets gibt es allerdings hier Lösungshinweise. Die Lösungsvorschläge sind insofern nicht als Musterlösungen anzusehen, als dass es in der Regel durchaus mehrere als richtig anzuerkennende Lösungswege gibt. Sollte also Ihre Lösung von der hier gegebenen abweichen, bedeutet das nicht unbedingt, dass Ihre Lösung falsch sein muss. Achten Sie aber immer darauf, dass jeder Schritt in Ihrer Lösung ausreichend begründet wurde, so wie wir es hier auch versuchen.

7.1 Mengenlehre

7.1.1 Mengenangaben

Wir möchten hier nicht zuviel verraten, aber zwei kleine Hinweise wollen wir doch geben. F enthält die meisten Elemente, und genau eine der Ja-Nein-Fragen ist mit Nein zu beantworten.

7.1.2 Zermelo-Zahlen

Diese Aufgabe sollten Sie mit den vorherigen Beispielen selbst lösen können.

7.1.3 Mengengleichheit

Es seien a, b, c, d beliebige, nicht notwendigerweise verschiedene Dinge.

1. Wann gilt: $\{a, b\} = \{c, d\}$?

Nach Definition der Mengengleichheit muss jedes x aus $\{a, b\}$ in $\{c, d\}$ vorkommen. Daher gilt (i) $a = c$ oder (ii) $a = d$. Wir unterscheiden nun zwei Fälle:

- Ist $a = b$, so fallen (i) und (ii) zusammen, und es gilt: $\{a, b\} = \{c, d\} \iff a = b = c = d$.
- Ist $a \neq b$, so muss auch b in $\{c, d\}$ vorkommen. Im augenblicklichen Fall bedeutet das für (i): $b = d$ und für (ii) $b = c$. Wäre nämlich (z.B.) im Fall (i) $b = c$, so würde $a = c = b$ folgen, im Widerspruch zur Annahme, dass $a \neq b$ gilt.

Wir können also zusammenfassen: Wenn $\{a, b\} = \{c, d\}$, so gilt ($a = c$ und $b = d$) oder ($a = d$ und $b = c$). In dieser Formulierung haben wir den Fall $a = b$ eingeschlossen, in dem ja alle vier soeben aufgeführten einzelnen Gleichheiten gelten. Gilt umgekehrt ($a = c$ und $b = d$) oder ($a = d$ und $b = c$), so folgt $\{a, b\} = \{c, d\}$, wie man durch nochmaliges Betrachten der obigen Fälle einsieht.

2. Wann gilt: $\{a, \{a, b\}\} = \{c, \{c, d\}\}$?

Sollte $a = \{c, d\}$ sein, dann ist gewiss $c = \{a, b\}$ unmöglich.

Es gilt also: $a = c$ und $\{a, b\} = \{c, d\}$.

Nach den Betrachtungen unter 1. folgt daraus $b = d$.

Zusammengefasst heißt das: Wenn $\{a, \{a, b\}\} = \{c, \{c, d\}\}$, so gilt $a = c$ und $b = d$. Gilt umgekehrt $a = c$ und $b = d$, so ist gemäß 1. $\{a, b\} = \{c, d\}$, und trivialerweise gilt (auch noch) $a = c$, weshalb $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ folgt.

Wir haben also für beide Aufgabenteile eine Kennzeichnung gefunden. Fassen wir diese nochmals zusammen:

1. $\{a, b\} = \{c, d\}$ gilt genau dann, wenn ($a = c$ und $b = d$) oder ($a = d$ und $b = c$).
2. $\{a, \{a, b\}\} = \{c, \{c, d\}\}$ gilt genau dann, wenn $a = c$ und $b = d$.

7.1.4 Wie Mengen sich zueinander verhalten

Die Lösung der Aufgabe hängt von der Person ab, die sie lösen soll. Wichtig ist es jedoch, zunächst die jeweilige Frage an und für sich zu verstehen. Deshalb übersetzen wir sie zuerst in alltäglicheres Deutsch, bevor wir eine mögliche Antwort geben.

1. Gibt es eine wirkliche oder erdachte Person, die das Innerste anderer Menschen nicht zu kennen glaubt, die keine große Macht besitzt oder diese unbedacht einsetzt, und die gewöhnlich keine rote Kleidung trägt?

Die Meisten werden hier mit ja antworten und können dann auch gleich sich selbst als Beispiel vorschlagen.

2. Gibt es eine wirkliche oder erdachte Person, die zwar das Innerste anderer Menschen zu kennen glaubt, die aber keine große Macht besitzt oder diese unbedacht einsetzt, und die gewöhnlich keine rote Kleidung trägt?

Hier sind durchaus verschiedene Antworten möglich. Entweder fallen einem konkrete Beispiele solcher Personen aus dem persönlichen Umfeld ein (das ist dann meist keine besonders angenehme Sache), oder man steht auf dem Standpunkt, nur Personen mit großer Macht können überhaupt derartige Einsichten in das Innenleben anderer Menschen erhalten.

3. Gibt es eine wirkliche oder erdachte Person, die große Macht besitzt und diese mit Bedacht nutzt, aber nicht meint, das Innerste anderer Menschen zu kennen, und auch gewöhnlich keine rote Kleidung trägt?

Bei dieser Antwort kann es darauf ankommen, wie "groß" die "große Macht" sein muss. Wenn dieser Begriff nicht allzu mächtig gedeutet wird, so könnte es durchaus sein, dass man aus seinem persönlichen Umfeld Menschen kennt, die in Verantwortung stehen, aber ihre Machtposition nicht ausnutzen und nicht meinen, das Innerste anderer Menschen zu kennen (und auch gewöhnlich keine rote Kleidung tragen).

Wenn die “große Macht” allumfassender gedeutet wird, mag schwer vorzustellen sein, wie ein quasi allmächtiges und gutmütiges Wesen nicht auch das Innerste anderer Menschen erkennen könnte, ganz abgesehen von der Kleiderfrage.

4. Gibt es eine wirkliche oder erdachte Person, die gewöhnlich rote Kleidung trägt, aber die das Innerste anderer Menschen nicht zu kennen glaubt und die auch keine große Macht besitzt oder diese unbedacht einsetzt?

Wahrscheinlich kann jeder hier rasch ein Beispiel finden, sofern er überhaupt einen Menschen kennt, der gewöhnlich rote Kleidung trägt. In jedem Fall könnte man sich so einen Menschen vorstellen, eine derartige erdachte Person gibt es also in jedem Fall.

5. Gibt es eine wirkliche oder erdachte Person, die das Innerste anderer Menschen zu kennen glaubt, die große Macht besitzt und diese mit Bedacht nutzt, aber gewöhnlich keine rote Kleidung trägt?

Diese Frage kann essentiell religiösen Charakters sein. Atheisten könnten die Existenz so einer Person bestreiten, während Christen zum Beispiel hier Jesus oder Gott selbst anführen könnten.

6. Gibt es eine wirkliche oder erdachte Person, die das Innerste anderer Menschen zu kennen glaubt, gewöhnlich rote Kleidung trägt, aber keine große Macht besitzt oder diese unbedacht einsetzt?

Mitglieder der spanischen Inquisition in der frühen Neuzeit scheinen diese Attribute zu erfüllen.

7. Gibt es eine wirkliche oder erdachte Person, die gewöhnlich rote Kleidung trägt und große Macht besitzt, die sie mit Bedacht einsetzt, aber nicht glaubt, das Innerste anderer Menschen zu kennen?

Wenn wir mal an “erdachte Personen” denken, so könnte einem hier “Spider-man” einfallen.

8. Gibt es eine wirkliche oder erdachte Person, die gewöhnlich rote Kleidung trägt und große Macht besitzt, die sie mit Bedacht einsetzt, und glaubt, das Innerste anderer Menschen zu kennen?

Das kommt nun darauf an, ob man noch an den Weihnachtsmann glaubt, insbesondere in der amerikanischen Santa-Claus-Variante (“naughty or nice”). Eine erdachte Person mit diesen Attributen scheint es jedenfalls zu geben.

7.1.5 Ein Induktionsbeweis für Ketten gleicher Mengen

Wir müssen also die folgende Aussage per Induktion beweisen:

Es sei $n \in \mathbb{N}$ mit $n \geq 2$. Es seien A_1, \dots, A_n Mengen.

Gilt für alle i von $i = 1$ bis $n - 1$ die Gleichheit $A_i = A_{i+1}$, so folgt $A_1 = A_n$.

Der folgende Beweis stimmt fast wortwörtlich mit dem von Satz 3.1.7 überein. Ganz allgemein folgen Induktionsbeweise oft einem starren Schema. Deshalb besteht auch kein Grund, vor diesen Beweisen einen allzu großen Respekt zu entwickeln. Man muss lediglich einmal das Schema verinnerlicht haben.

Beweis: IA: Die Aussage gilt für die kleinste infrage kommende natürliche Zahl $n = 2$ in trivialer Weise. Wir können ja $A_1 = A_2$ voraussetzen, woraus $A_1 = A_n$ wegen $n = 2$ sofort folgt.

IS: Wir müssen zeigen, dass aus der IV die IB folgt. Formulieren wir diese explizit.

IV: Die Aussage gilt für $n = N \geq 2$. Also: Sind A_1, \dots, A_N Mengen, sodass für alle $i \in \{1, \dots, N-1\}$ die Gleichheit $A_i = A_{i+1}$ gilt, so folgt $A_1 = A_N$.

IB: Die Aussage gilt für $n = N + 1$. Also ist zu zeigen: Sind A_1, \dots, A_{N+1} Mengen, sodass für alle $i \in \{1, \dots, N\}$ die Gleichheit $A_i = A_{i+1}$ gilt, so folgt $A_1 = A_{N+1}$.

Zum Beweis der IB betrachten wir also $N + 1$ viele beliebige Mengen A_1, \dots, A_{N+1} , sodass für alle $i \in \{1, \dots, N\}$ die Gleichheit $A_i = A_{i+1}$ gilt. Daraus folgt unmittelbar für die N vielen Mengen A_1, \dots, A_N Mengen, dass für alle $i \in \{1, \dots, N-1\}$ die Gleichheit $A_i = A_{i+1}$ gültig ist. Mit der IV können wir folgern: $A_1 = A_N$. Ferner gilt ja $A_N = A_{N+1}$. Mit Satz 3.1.6.2 folgt daraus $A_1 = A_{N+1}$, was zu zeigen war.

Nach dem Prinzip der mathematischen Induktion folgt die behauptete Aussage. \square

7.1.6 Induktionsbeweis einer bekannten geschlossenen Form für eine Reihe

IA für $n = 0$:

$$\sum_{i=0}^n i = \sum_{i=0}^0 = 0 = \frac{0(0+1)}{2} = \frac{n(n+1)}{2}.$$

IV: Die Behauptung gelte für $n = m$, also kann vorausgesetzt werden:

$$\sum_{i=0}^m i = \frac{m(m+1)}{2}.$$

IB: Die Behauptung gilt für $n = m + 1$, wir müssen also zeigen:

$$\sum_{i=0}^{m+1} i = \frac{(m+1)(m+2)}{2}.$$

Dazu betrachten wir folgende Gleichheitskette:

$$\begin{aligned} \sum_{i=0}^{m+1} i &= \left(\sum_{i=0}^m i \right) + (m+1) \\ &\stackrel{\text{IV}}{=} \frac{m(m+1)}{2} + \frac{2(m+1)}{2} \\ &= \frac{(m+1)(m+2)}{2}. \end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die behauptete Aussage.

7.1.7 Monotoniegesetze

1. Wir zeigen die Monotonie der Vereinigung: $(A \subseteq B) \implies (A \cup C \subseteq B \cup C)$. Betrachte dazu ein bel. $x \in A \cup C$. Wir unterscheiden zwei Fälle:

- (a) Falls $x \in A$, so gilt nach Voraussetzung $x \in B$ und (mit Satz 3.1.9) $x \in B \cup C$.
- (b) Falls $x \in C$, so folgt (mit Satz 3.1.9) $x \in B \cup C$.

2. Wir zeigen die Monotonie des Durchschnitts: $(A \subseteq B) \implies (A \cap C \subseteq B \cap C)$.

Betrachte dazu ein bel. $x \in A \cap C$.

Nach Def. des Durchschnitts gilt sowohl $x \in A$ als auch $x \in C$.

Wegen $(A \subseteq B)$ gilt daher sowohl $x \in B$ als auch $x \in C$.

Nach Def. des Durchschnitts bedeutet dies: $x \in B \cap C$. \square

7.1.8 Assoziativgesetze

Wir beschränken uns auf den Beweis von $(A \cup B) \cup C \supseteq A \cup (B \cup C)$.

Die anderen drei zu beweisenden Inklusionen (siehe Satz 3.1.3) zeigt man ähnlich und sollten daher keine Schwierigkeiten bereiten.

Sei also $x \in A \cup (B \cup C)$ beliebig. Nach der Definition der Vereinigung ergeben sich zwei mögliche Fälle:

Fall 1.: $x \in A$. Dann gilt $x \in A \cup B$ wegen Satz 3.1.9, und somit aus demselben Grund $x \in (A \cup B) \cup C$.

Fall 2.: $x \in B \cup C$ zerfällt in zwei Unterfälle: $x \in B$ und $x \in C$.

Fall 2a: Falls $x \in B$, so $x \in A \cup B$ wegen Satz 3.1.9, und aus demselben Grund folgt $x \in (A \cup B) \cup C$.

Fall 2b: Falls $x \in C$, so folgt sogar unmittelbar aus Satz 3.1.9, dass $x \in (A \cup B) \cup C$.

\square

7.1.9 Distributivgesetze

Vollziehen Sie den Beweis von Satz 3.1.17 nach, soweit er aufgeschrieben wurde. Bedenken Sie, dass Sie zwei Beweisrichtungen führen müssen.

7.1.10 Allgemeine Distributivität

Induktionsanfang: $T \cup \left(\bigcap_{i=1}^1 S_i \right) = T \cup S_1 = \bigcap_{i=1}^1 (T \cup S_i)$.

Induktionsannahme: $T \cup \left(\bigcap_{i=1}^n S_i \right) = \bigcap_{i=1}^n (T \cup S_i)$.

Induktionsbehauptung: $T \cup \left(\bigcap_{i=1}^{n+1} S_i \right) = \bigcap_{i=1}^{n+1} (T \cup S_i)$.

Beweis der IB:

$$\begin{aligned}
 T \cup \left(\bigcap_{i=1}^{n+1} S_i \right) &= && \text{Def. } \bigcap \\
 T \cup \left(\left(\bigcap_{i=1}^n S_i \right) \cap S_{n+1} \right) &= && \text{Distributivgesetz} \\
 \left(T \cup \left(\bigcap_{i=1}^n S_i \right) \right) \cap (T \cup S_{n+1}) &= && \text{Induktionsannahme} \\
 \left(\bigcap_{i=1}^n (T \cup S_i) \right) \cap (T \cup S_{n+1}) &= && \text{Def. } \bigcap \\
 \bigcap_{i=1}^{n+1} (T \cup S_i).
 \end{aligned}$$

\square

Das andere allgemeine Distributivgesetz sieht man völlig analog ein.

7.1.11 Disjunktheit von Mengen

Hier sind lediglich die Definitionen sauber zu lesen und zu verarbeiten. Möglicherweise sind aber auch Fallunterscheidungen bezüglich der Anzahl n der beteiligten Mengen notwendig. Beispielsweise sind für $n = 2$ alle Begriffe äquivalent. Beachten Sie bei Ihrer Argumentation, welche Eigenschaften des Durchschnitts verwendet werden. Beispielsweise werden Sie zum Nachweis der Äquivalenz von “paarweise disjunkt” und “geordnet paarweise disjunkt” das Kommutativgesetz des Durchschnitts benötigen.

7.1.12 Rechnen mit der Mengendifferenz

Wir möchten hier nur drei Hinweise geben:

- Bei der Frage, ob derlei Identitäten gelten, sind Venn-Diagramme oft hilfreich.
- Ebenso hilfreich ist die Betrachtung von “Extremfällen”: Was geschieht, wenn eine oder zwei der Mengen leer sind oder das gesamte Universum umfassen?
- Zum Aufspüren von Gegenbeispielen ist meist die Betrachtung sehr kleiner Universen ausreichend. Konkret: Da bei der Aufgabenstellung drei Mengen im Spiel sind, genügen mit Sicherheit achtelementige Universen zur Konstruktion möglicher Gegenbeispiele.

7.1.13 Zur binomischen Formel

Es geht um die folgende Behauptung:

Es seien A, B Mengen. Dann gilt: $(A \cup B) \cap (A \setminus B) = (A \cap A) \setminus (B \cap B)$.

Wir wollen an diesem Beispiel klarmachen, dass es sehr wohl unterschiedliche Lösungswege geben kann, insbesondere, wenn es um Beweisführungen geht. Hier gibt es zunächst auch nur das Kriterium “richtig” bzw. “falsch”, aber Sie werden u.a. an der Länge der Beweisgänge sehen, dass es oft auch so etwas wie “Eleganz” gibt, oder dass man über die eigentliche Aussage hinausgehende Dinge anhand von Beweisen verdeutlich kann.

1. Schrittweises Lösen des Beispiels:

$$\begin{aligned} (\{1, 2\} \cup \{2, 3\}) \cap (\{1, 2\} \setminus \{2, 3\}) &= (\{1, 2\} \cap \{1, 2\}) \setminus (\{2, 3\} \cap \{2, 3\}) \\ \{1, 2, 3\} \cap \{1\} &= \{1, 2\} \setminus \{2, 3\} \\ \{1\} &= \{1\}. \end{aligned}$$

2. Per “Gleichungsumformung”:

$$\begin{array}{ll} (A \cup B) \cap (A \setminus B) = (A \cap A) \setminus (B \cap B) & \text{Idempotenzgesetz} \\ (A \cup B) \cap (A \setminus B) = A \setminus B & \text{Def. von Mengendiff.} \\ (A \cup B) \cap (A \cap \bar{B}) = A \cap \bar{B} & \text{Distributivgesetz} \\ (A \cap (A \cap \bar{B})) \cup (B \cap (A \cap \bar{B})) = A \cap \bar{B} & \text{Kommutativität von } \cap \\ (A \cap (A \cap \bar{B})) \cup (B \cap (\bar{B} \cap A)) = A \cap \bar{B} & \text{Assoziativität von } \cap \\ ((A \cap A) \cap \bar{B}) \cup ((B \cap \bar{B}) \cap A) = A \cap \bar{B} & \text{Idempotenz, } B \cap \bar{B} = \emptyset \\ (A \cap \bar{B}) \cup (\emptyset \cap A) = A \cap \bar{B} & \emptyset \text{ absorbierendes Element von } \cap \\ (A \cap \bar{B}) \cup \emptyset = A \cap \bar{B} & \emptyset \text{ neutrales Element von } \cup \\ A \cap \bar{B} = A \cap \bar{B}. & \end{array}$$

Per “elementweise Argumentation”:

$$\begin{aligned}\subseteq: & \text{Sei } x \in (A \cup B) \cap (A \setminus B) \\ \Rightarrow & x \in (A \setminus B) \\ \Rightarrow & x \in (A \cap A) \setminus (B \cap B).\end{aligned}$$

(Beim letzten Schritt wurden das Idempotenzgesetz für \cap angewendet.)

$$\begin{aligned}\supseteq: & \text{Sei } x \in (A \cap A) \setminus (B \cap B) \\ \Rightarrow & x \in A \setminus B \\ \Rightarrow & x \in A \setminus B \text{ und } x \in A \\ \Rightarrow & x \in A \setminus B \text{ und } (x \in A \text{ oder } x \in B) \\ \Rightarrow & x \in A \setminus B \text{ und } x \in (A \cup B) \\ \Rightarrow & x \in (A \cup B) \text{ und } x \in A \setminus B \\ \Rightarrow & x \in (A \cup B) \cap (A \setminus B).\end{aligned}$$

(Beim ersten Schritt wurden das Idempotenzgesetz für \cap angewendet.)

Es gibt aber auch noch die folgende elegante Lösung.

Nach Definition der Mengendifferenz und mit den Monotoniegesetzen gilt:

$$A \setminus B \subseteq A \subseteq A \cup B, \text{ also } A \setminus B \subseteq A \cup B.$$

Mit dem Charakterisierungssatz 3.1.12 ist das äquivalent zu: $(A \setminus B) \cap (A \cup B) = A \setminus B$.

Wegen des Idempotenzgesetzes gilt: $(A \cap A) \setminus (B \cap B) = A \setminus B$.

Daraus folgt sofort die Behauptung.

Es ist lehrreich, die obige algebraische Lösung mit einer “algebraischen Begründung” für die entsprechende binomische Formal auf der Ebene der Zahlen zu vergleichen. Da z.B. das Idempotenzgesetz dort nicht gilt, ist tatsächlich eine andere Argumentation nötig.

$$\begin{aligned}(a + b) \cdot (a - b) &= (a \cdot (a - b)) + (b \cdot (a - b)) && \text{Distributivgesetz} \\ &= (a \cdot a - a \cdot b) + (b \cdot a - b \cdot b) && \text{Distributivgesetz} \\ &= (a \cdot a + (-a \cdot b + b \cdot a)) - b \cdot b && \text{Assoziativgesetz zweimal} \\ &= (a \cdot a + (-a \cdot b + a \cdot b)) - b \cdot b && \text{Kommutativgesetz} \\ &= a \cdot a - b \cdot b && x - x = 0\end{aligned}$$

7.1.14 Zum Mengenprodukt

“Elementweise Argumentation” sollte als Hinweis genügen.

7.2 Relationen und gerichtete Graphen

7.2.1 Zum Verstehen von Relationenausdrücken

Beschreiben Sie nacheinander in Worten, was für eine Relation über den ganzen Zahlen mit den folgenden Relationenausdrücken “gemeint” ist:

1. $R_1 = \overline{\Delta_{\mathbb{N}}}$ ist die Ungleichheitsrelation auf \mathbb{N} ;
2. $R_2 = \overline{\{1\} \times \mathbb{N}}$ beinhaltet alle geordneten Paare natürlicher Zahlen, deren erste Komponente von Eins verschieden ist;

3. $R_3 = \overline{\Delta_N} \cup \{1\} \times \overline{N}$ ist (nach de Morgan – und das beantwortet auch schon die Zusatzaufgabe –) die Menge aller ungleichen geordneten Paare natürlicher Zahlen, deren erste Komponente von Eins verschieden ist;
4. $R_4 = | \cap R_3$: Ein Paar (n, m) liegt genau dann in R_4 , wenn $m \neq 1$ ein echter Teiler von n ist, was zur Folge hat, dass die Zahl in der zweiten Komponente keine Primzahl sein kann.

7.2.2 Zum Rechnen mit Relationenausdrücken

1. $\bar{R} = \{(a, c), (a, d), (b, a), (b, d), (c, a), (c, b), (d, b), (d, c)\}$
2. $R \circ T = \{(a, a), (a, c), (b, b), (c, d), (d, a), (d, b), (a, b), (b, a), (b, c), (c, b), (d, d)\}$
3. $S \cap \overline{\Delta_A} = \overline{\{(a, b), (b, c), (c, d), (d, a)\}} \cap \overline{\Delta_A} = \{(a, c), (a, d), (b, a), (b, d), (c, a), (c, b), (d, b), (d, c)\}$
4. $T^- = T$.
5. $(R \cup T) \circ Q = \emptyset$

7.2.3 Kompakte Kennzeichnungen von Relationen

Es gilt: $|\circ| = |$ (wie man leicht zeigen kann).

Betrachte $(a, b) \in |^- \circ |$. Es gibt also eine Zahl c mit: c teilt a und b teilt c . Also gilt: b teilt a . Gilt umgekehrt b teilt a , so gibt es ein c (z.B. $c = a$), sodass c teilt a und b teilt $c = a$, also $(a, b) \in |^- \circ |$. Daher gilt: $|- \circ | = |^-$. Betrachte $(a, b) \in P \circ P$, d.h., es gibt eine Zahl c mit $(a, c) \in P$ und $(b, c) \in P$. Also ist die Summe $a + c$ gerade und ebenso die Summe $c + b$. Ist c gerade, so bedeutet das, dass a und b gerade sind, also auch $a + b$. Ist c ungerade, so muss sowohl a als auch b ungerade sein, also ist $a + b$ gerade. Daher gilt $P \circ P \subseteq |^-$. Gilt umgekehrt $(a, b) \in |^-$, so ist $a + b$ gerade. Das bedeutet, dass entweder a und b beide gerade oder beide ungerade sind. Im ersten Fall zeigt irgendeine gerade Zahl c , dass $(a, c) \in P$ und $(c, b) \in P$ gilt, also $(a, b) \in P \circ P$. Im zweiten Fall wähle irgendeine ungerade Zahl c , sodass $(a, c) \in P$ und $(c, b) \in P$ gilt, mithin $(a, b) \in P \circ P$.

7.2.4 Monotoniegesetz

Hinweis: elementweise Argumentation

7.2.5 Zerlegungen

Es sei M eine Menge, $M \neq \emptyset$. Eine *Zerlegung* von M ist ein Mengensystem $Z \subseteq 2^M$ mit:

1. $M = \bigcup_{A \in Z} A$.
2. $\emptyset \notin Z$.
3. $\forall A, B \in Z : A \cap B \neq \emptyset \implies A = B$.

7.2.6 Mengensystemgraph

Sei zunächst \mathfrak{M} eine Zerlegung. Da jedes $a \in M$ in einer Menge $M_a \in \mathfrak{M}$ vorkommen soll, ist E vortotal. Gäbe es Mengen $M, N \in \mathfrak{M}$ mit $(a, M), (a, N) \in E$, so wäre $a \in M \cap N$, also muss aufgrund der Disjunktionsforderung für Mengen in einer Zerlegung $M = N$ gelten. Da $\emptyset \notin \mathfrak{M}$, enthält jede Menge $M \in \mathfrak{M}$ mindestens ein Element aus M , weshalb es auch mindestens ein $a \in M$ gibt mit $(a, M) \in E$, d.h., E ist nachtotal.

Ist umgekehrt E vortotal, nachtotal und nacheindeutig, so bedeutet das insbesondere (Vortotalität), dass jedes $a \in M$ in einer Menge $M_a \in \mathfrak{M}$ vorkommt. Da E nachtotal ist, ist $\emptyset \notin \mathfrak{M}$. Gäbe es zwei verschiedene Mengen $M, N \in \mathfrak{M}$ mit $M \cap N \neq \emptyset$, so gäbe es ein $a \in M$ mit $(a, N), (a, M) \in E$, d.h., E wäre nicht nacheindeutig.

7.2.7 Nacheindeutigkeit und Vortotalität 1

1. R ist nacheindeutig gdw. $R^- \circ R \subseteq \Delta_B$.
2. R ist vortotal gdw. $\Delta_A \subseteq R \circ R^-$.
3. R ist nacheindeutig und vortotal gdw. $R \circ \overline{\Delta_B} = \overline{R}$.

Angenommen, R ist nacheindeutig. Dann wähle $b_1, b_2 \in B$ mit $(b_1, b_2) \in R^- \circ R$. Also gibt es ein $a \in A$ mit $(b_1, a) \in R^-$ und $(a, b_2) \in R$. Da $(b_1, a) \in R^-$ gleichwertig ist mit $(a, b_1) \in R$, folgt aus der Nacheindeutigkeit von R , dass $b_1 = b_2$ gilt, d.h., $(b_1, b_2) \in \Delta_B$.

Gilt umgekehrt $R^- \circ R \subseteq \Delta_B$, so betrachte $(a, b_1) \in R$ und $(a, b_2) \in R$. Also gilt: $(b_1, a) \in R^-$, und somit $(b_1, b_2) \in R^- \circ R$. Da $R^- \circ R \subseteq \Delta_B$, folgt $(b_1, b_2) \in \Delta_B$, also $b_1 = b_2$. Daher ist R nacheindeutig.

Sei nun R vortotal. Betrachte $a \in A$. Da R vortotal, gibt es ein $b \in B$ mit $(a, b) \in R$ und somit auch $(b, a) \in R^-$. Daher gilt: $(a, a) \in R \circ R^-$. Da a beliebig, folgt $\Delta_A \subseteq R \circ R^-$.

Gilt umgekehrt $\Delta_A \subseteq R \circ R^-$, so muss es zu jedem $a \in A$ ein Brückenelement $b \in B$ geben, sodass $(a, b) \in R$ und somit $(b, a) \in R^-$. Also ist R vortotal.

Die dritte Behauptung zeigt man am einfachsten, indem man (wie soeben schon getan) zwei weitere Kennzeichnungen der Nacheindeutigkeit und der Vortotalität nachweist; dies wollen wir dem Leser überlassen.

- R ist nacheindeutig gdw. $R \circ \overline{\Delta_B} \subseteq \overline{R}$.
- R ist vortotal gdw. $R \circ \overline{\Delta_B} \supseteq \overline{R}$.

7.2.8 Nacheindeutigkeit und Vortotalität 2

Natürlich kann man einen elementweisen Beweis führen. Wir wollen hier als Alternative einen relationalen algebraischen Beweis angeben.

Es seien M_1, M_2, M_3 Mengen und $R \subseteq M_1 \times M_2$ sowie $S \subseteq M_2 \times M_3$. Betrachte $T := R \circ S$.

Seien zunächst R und S nacheindeutig.

Da R und S nacheindeutig, gilt mit Abschnitt 6.2.7 (der vorigen Übung): $R^- \circ R \subseteq \Delta_{M_2}$ und $S^- \circ S \subseteq \Delta_{M_3}$. Der “Einschub” von Δ_{M_2} ändert nichts, sodass gilt:

$$\Delta_{M_3} \supseteq S^- \circ \Delta_{M_2} \circ S \supseteq^{(1)} S^- \circ R^- \circ R \circ S =^{(2)} (R \circ S)^- \circ (R \circ S)$$

Bei $\supseteq^{(1)}$ wurde das Monotoniegesetz angewendet (Satz 3.2.3), bei $=^{(2)}$ Satz 3.2.6. Implizit wurde außerdem das Assoziativgesetz des Relationenproduktes angewendet (sonst hätten wir keine Klammern weglassen dürfen). Aus der angegebenen Inklusionskette folgt, dass $(R \circ S)^- \circ (R \circ S) \subseteq \Delta_{M_3}$, woraus wegen Abschnitt 6.2.7 die Nacheindeutigkeit von $R \circ S$ folgt.

Sind nun R und S vortotal, so kann man ganz entsprechend argumentieren.

7.2.9 Abgeschlossenheit der Eigenschaften unter dem Relationenprodukt

noch zu tun

Mit R und S ist $R \circ S$ nicht notwendig transitiv:

$R = \{(1, 2), (3, 4)\}, S = \{(2, 3), (4, 5)\} \rightsquigarrow R \circ S = \{(1, 3), (3, 5)\}$, aber $(1, 5) \notin R \circ S$.

7.2.10 Eigenschaften von Relationen

Die ausführlich vorgerechneten Beispiele in Abschnitt 5.2.2 sollten als Hinweise genügen.

7.2.11 Eine Eigenschaft von Quasiordnungen

Wegen Satz 3.2.18 gilt $R \circ R \subseteq R$ genau dann, wenn R transitiv. Ist R reflexiv, so gilt (ebenfalls mit Satz 3.2.18): $\Delta_M \subseteq R$. Also ist: $R = R \circ \Delta_M \subseteq R \circ R$. Die erste Gleichheit gilt mit Satz 3.2.4 (Δ_M als neutrales Element), die zweite mit Satz 3.2.3 (Monotoniegesetz). Mit $M = \{1, 2\}$ gilt für $R = \{(1, 1)\}$: $R \circ R = R$, aber R ist nicht reflexiv.

7.3 Funktionen

7.3.1 Urbilder einer Funktion

Natürlich kann man den Sachverhalt elementweise nachrechnen.

Wir gehen in der folgenden Lösung einen anderen Weg, den der Verallgemeinerung. Hierbei ist es notwendig, auf die Relationenschreibweise überzugehen. Wir behaupten jetzt (allgemeiner):

$$T \circ (R \cap S) = (T \circ R) \cap (T \circ S)$$

falls T nacheindeutig. T entspricht nun der partiellen Funktion $f : A \rightarrow B$, also $f(a) = b$ genau dann, wenn $(a, b) \in T$. Also gilt: $a \in f^-(U) \iff \exists b \in U : (a, b) \in T$. Wenn nun $R = \{(b, b) \mid b \in U\} = \Delta_U$, so gilt: $a \in f^-(U) \iff (a, b) \in T \circ R$. Entsprechend kann man $S = \{(b, b) \mid b \in V\} = \Delta_V$ setzen, um einzusehen, dass wir im Folgenden tatsächlich eine Verallgemeinerung der eigentlichen Behauptung betrachten.

Wegen Satz 3.2.7 gilt die Inklusion \subseteq sowieso. Aufgrund der Monotonie des Relationenprodukts und mit der Kennzeichnung der Nacheindeutigkeit in Abschnitt 6.2.7 gilt:

$$T \circ (R \cap S) \supseteq (T \cap (T \circ S \circ R^-)) \circ (R \cap (T^- \circ T \circ S)).$$

Diese scheinbare Aufblähung der Formel hat ihren Sinn, da wir jetzt die Dedekind-Formel (siehe Abschnitt 4.2.2) anwenden können. Diese zeigt, dass die rechte Seite Obermenge von $(T \circ R) \cap (T \circ S)$ ist, was zu zeigen war.

7.3.2 Der Kern einer Abbildung

Warum gilt $\sim_f = f \circ f^-$ für $f : A \rightarrow B$? Klar, $\sim_f, f \circ f^- \subseteq A \times A$. Betrachte also $a, a' \in A$. Wenn $a \sim_f a'$, so $f(a) = f(a')$. Es gibt also ein $b \in B$ mit $(a, b) \in f$ und $(a', b) \in f$, also $(b, a') \in f^-$ (hier wird f als Relation begriffen). Daher gilt $(a, a') \in f \circ f^-$. Gilt umgekehrt $(a, a') \in f \circ f^-$, so gibt es ein $b \in B$ mit $(a, b) \in f$ und $(b, a') \in f^-$. Also gilt $f(a) = b = f(a')$, d.h., $a \sim_f a'$.

Wir geben nur als weiteren Hinweis: Der Kern einer Abbildung ist immer eine reflexive, symmetrische und transitive Relation, also eine Äquivalenzrelation, wie wir dies später nennen werden.

Wenn man alle Elemente von A , für die f nicht definiert ist, als äquivalent zueinander ansieht, so ist der Kern auch für jede Funktion eine Äquivalenzrelation. Auf die Nacheindeutigkeit kann man insofern nicht verzichten, als dass die Schreibweise $f(x)$ sonst nicht sinnvoll wäre.

7.3.3 Urbilder einer Abbildung

Wir müssen nachweisen:

- $\emptyset \notin \mathcal{M}_f$: Da $b \in f(A)$ gewählt wird, ist dies gewährleistet, insbesondere da $A \neq \emptyset$.
- Für $X, Y \in \mathcal{M}_f$ mit $X \cap Y \neq \emptyset$ gilt $X = Y$. Jedenfalls gibt es $b_X \in f(A)$ und $b_Y \in f(A)$ mit $X = f^-(b_X)$ und $Y = f^-(b_Y)$. Gäbe es ein $a \in X \cap Y$, so würde also sowohl $f(a) = b_X$ als auch $f(a) = b_Y$ gelten, was (da f Funktion) nur geht, wenn $b_X = b_Y$ gilt. Also folgt $X = Y$.
- $A = \bigcup_{b \in f(A)} f^-(b)$. Da f linkstotal, folgt dies unmittelbar.

7.3.4 Eine Kennzeichnung von Injektionen

Wir verweisen auf das Buch [33].

7.3.5 Zum Tauschoperator

Überprüfen Sie im Einzelnen die Eigenschaften der Totalität bzw. der Eindeutigkeit.

7.3.6 Endliche und unendliche Folgen

1. Ist $f : [n] \rightarrow M$ eine endliche surjektive Folge, so ist M endlich.

Diese Aussage stimmt. Wir müssen zum Nachweis eine Abbildung $g : M \rightarrow [n]$ erstellen; dass wir hier dieselbe natürliche Zahl zum Beschreiben des endlichen Abschnitts der natürlichen Zahlen nehmen können wie im Definitionsbereich von f , ist eine glückliche Fügung, aber keineswegs notwendig für den Beweis. Da f surjektiv, kommt jedes Element m von M als Bild (unter f) wenigstens einer Zahl $< n$ vor. Wähle nun willkürlich eine dieser Zahlen aus und nenne sie

$g(m)$. Mit Aufgabe 6.3.3 kann nicht für zwei verschiedene m, m' gelten, dass $g(m) = g(m')$. Daher ist g nacheindeutig und somit M endlich.

2. Ist $f : \mathbb{N} \rightarrow M$ eine unendliche surjektive Folge, so ist M unendlich.

Diese Aussage ist falsch, da die folgende richtig ist.

3. Es gibt eine endliche Menge M und eine vollständige Auflistung $f : \mathbb{N} \rightarrow M$.

Betrachte nämlich $M = \{1\}$ und die Abbildung $f : \mathbb{N} \rightarrow M, n \mapsto 1$.

7.3.7 Die geometrische Reihe

Beweis: per Induktion: IA $n = 0 \checkmark$. Zum Induktionsschritt betrachte $n > 0$:

$$\sum_{i=0}^n a^i = \left(\sum_{i=0}^{n-1} a^i \right) + a^n = \frac{a^n - 1}{a - 1} + \frac{a^{n+1} - a^n}{a - 1} = \frac{a^{n+1} - 1}{a - 1}.$$

□

7.3.8 Die Fakultätsfunktion

Den betreffenden Induktionsbeweis sollten Sie ohne weitere Einhilfe hinbekommen.

7.3.9 Das Cantorsche Abzählungsschema

	0	1	2	...	k	...
0	0	3	8	⋮	$(k^2 + 2k)$	⋮
1	1	2	7	⋮	⋮	⋮
2	4	5	6	⋮	$(k^2 + k + 2)$	⋮
⋮	⋮	⋮	⋮	⋮	$(k^2 + k + 1)$	⋮
k	(k^2)	$(k^2 + 1)$	$(k^2 + 2)$...	$(k^2 + k)$	⋮
⋮	⋮	⋮	⋮	⋮	⋮	⋮

$$\widehat{\langle i, j \rangle} = \begin{cases} i^2 + j, & \text{falls } j \leq i, \\ j^2 + 2j - i, & \text{falls } i < j. \end{cases}$$

7.3.10 Indikatorfunktion

Das elementare Nachrechnen der Eigenschaften sollte Ihnen gelingen.

7.4 Zur Größe von Mengen

7.4.1 Äquivalenzsatz von Cantor

1. Beweisen Sie den Äquivalenzsatz. Erklären Sie, wie der Satz von Schröder & Bernstein in den Beweis einfließt.

Am einfachsten könnte man wohl wie folgt argumentieren: Angenommen, $A' \subseteq A$ ist gleichmächtig zu B und $B' \subseteq B$ ist gleichmächtig zu A . Aus $A' \subseteq A$ folgt: $|A'| \leq |A|$. Wegen $|B| = |A'|$ und der Transitivität von \leq bei Kardinalitäten folgt $|B| \leq |A|$. Ganz entsprechend sieht man: $|A| \leq |B|$. Daraus folgt nun wiederum nach dem Satz von Schröder & Bernstein, dass A und B gleichmächtig sind.

2. Erläutern Sie, wie man den Satz von Schröder & Bernstein beweisen könnte, wenn man einen davon unabhängigen Beweis für den Äquivalenzsatz besäße.

Angenommen, $f : A \rightarrow B$ und $g : B \rightarrow A$ sind injektiv. Dann sind $f' : A \rightarrow f(A)$, $x \mapsto f(x)$ und $g' : B \rightarrow g(B)$, $y \mapsto g(y)$ Bijektionen. Also gibt es eine Teilmenge von B , nämlich $f(A)$, die zu A gleichmächtig ist, und es gibt eine Teilmenge von A , nämlich $g(B)$, die zu B gleichmächtig ist. Nach dem Äquivalenzsatz gilt daher, dass $|A| = |B|$ wahr ist, es mithin eine Bijektion zwischen A und B geben muss.

7.4.2 Surjektiv, injektiv, bijektiv

Der Induktionsbeweis ist müßig aber eher Standard. Wir geben daher nur das (elegantere) Argument mit dem Endlichkeitssatz von Dedekind an.

Es sei $f : A \rightarrow A$ surjektiv, also $f(A) = A$. Wäre f nicht injektiv, so gäbe es $a, a' \in A$ mit $f(a) = f(a')$. Betrachte $A' = A \setminus \{a'\}$. Sei f' die Restriktion von f auf A' . Wegen Satz 3.4.2 gilt: $|f'(A')| \leq |A'|$. Andererseits gilt $f(A) = f(A') = f'(A')$ und $A' \subsetneq A$, und mithin (mit Satz 3.4.1):

$$|A| = |f(A)| = |f'(A')| \leq |A'| \leq |A|.$$

A' ist also eine zu A gleichmächtige echte Teilmenge von A , was der vorausgesetzten Endlichkeit von A nach Satz 3.4.6 widerspricht.

7.4.3 Gleichmächtig oder nicht?

Wenn A und B beide endlich sind, so ist die fragliche Gleichmächtigkeit nicht gegeben. Ist B abzählbar unendlich, aber A endlich, so sind B^A und $(B \cup \{\perp\})^A$ gleichmächtig, und zwar sind beide abzählbar unendlich. Ist B endlich, aber A abzählbar unendlich, so muss man zwischen $|B| = 1$ und $|B| > 1$ unterscheiden. Hat B die Mächtigkeit Eins, so hat B^A ebenfalls die Mächtigkeit Eins, während $(B \cup \{\perp\})^A$ offenbar zu 2^A gleichmächtig ist und, da $A \neq \emptyset$, ist die betreffende Mächtigkeit somit größer als Eins. Hat B eine Mächtigkeit größer als Eins, so ist B^A und $(B \cup \{\perp\})^A$ gleichmächtig. Da $B^A \subseteq (B \cup \{\perp\})^A$, genügt es nach dem Satz von Schröder & Bernstein, eine Injektion $f : (B \cup \{\perp\})^A \rightarrow B^A$ anzugeben. Da A abzählbar unendlich, wollen wir dazu jetzt von $A = \mathbb{N}$ ausgehen (damit wir die arithmetischen Operationen auf den natürlichen Zahlen nutzen können) und zwei verschiedene $b_1, b_2 \in B$ fixieren. Setze

$$(f(g))(n) := \begin{cases} g(n/2), & \text{falls } n \text{ gerade und } g(n/2) \notin \{\perp\} \\ b_1, & \text{falls } n \text{ gerade und } g(n/2) \in \{\perp\} \\ b_1, & \text{falls } n \text{ ungerade und } g((n+1)/2) = b_1 \\ b_2, & \text{falls } n \text{ ungerade und } g((n+1)/2) = \perp \end{cases}$$

Man kann zeigen, dass f injektiv ist. Außerdem sieht man, wie die Unendlichkeit von \mathbb{N} benutzt wird, um den “Speicherbereich” durch “Aufspreizen” zu verdoppeln.

7.4.4 Das Löschen eines Elements

Setze $A' := A \setminus \{a\}$. Da $A' \subseteq A$, gilt nach Satz 3.4.1 $|A'| \leq |A|$. Wäre $|A'| = |A|$, so wäre A nach Satz 3.4.6 unendlich. Gilt nun $|A'| < |A|$, so nehmen wir für einen Widerspruchsbeweis an, A wäre unendlich. Nach Satz 3.4.6 gibt es also eine Teilmenge A'' von A mit $|A''| = |A|$.

(a) Falls $a \notin A''$, muss $A'' \subseteq A'$ gelten. Nach Satz 3.4.1 folgt aus $A'' \subseteq A' \subseteq A$: $|A''| \leq |A'| \leq |A|$ und damit $|A''| = |A'| = |A|$, im Widerspruch zu $|A'| < |A|$.

(b) Also liegt $a' \in A''$, aber $A'' \setminus \{a'\} \subseteq A'$ muss immer noch gelten. Da $A \neq A''$, muss es ein Element $a'' \in A''$ geben mit $a'' \notin A'$. Daher gibt es eine Bijektion von A'' auf $A''' := (A'' \setminus \{a''\}) \cup \{a'\}$. Es gilt deshalb: $|A'''| = |A|$ und $A''' \subseteq A'$, woraus wir wie im Fall (a) einen Widerspruch erhalten.

Dieser Sachverhalt zeigt übrigens auch, dass die Umkehrung von Lemma 3.4.5 stimmt.

7.4.5 Eigenschaften von Funktionen auf einer endlichen Menge

Was ist denn überhaupt noch zu zeigen? Im Haupttext wurde bewiesen:

Ist A endlich, so ist jede Surjektion $f : A \rightarrow A$ auch Injektion.

Daraus folgt, dass jede Surjektion $f : A \rightarrow A$ auch Bijektion ist. Laut Definition ist jedenfalls jede Bijektion sowohl Injektion als auch Surjektion. Zu zeigen bliebe also:

Ist A endlich, so ist jede Injektion $f : A \rightarrow A$ auch Surjektion.

Dies ergibt sich sofort aus dem Schubfachprinzip aus folgender Überlegung: Ist $f : A \rightarrow A$ eine Injektion, die keine Surjektion ist, so gibt es ein $a' \in A \setminus f(A)$. Wir können f also auch als Injektion $A \rightarrow A'$ auffassen mit $A' = A \setminus \{a'\}$. Das ist aber unmöglich, da $|A'| < |A|$, siehe Aufgabe 6.4.4.

7.4.6 Dirichletsches Schubfachprinzip

Falls man n Gegenstände auf m Fächer ($n > m > 0$) verteilt, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Begründung: Falls das Prinzip nicht stimmt, dann landet in jedem Schubfach höchstens ein Gegenstand. Damit gibt es höchstens soviele Gegenstände wie Schubfächer.

↪ Widerspruch zur Annahme, dass es mehr Gegenstände als Schubfächer gibt.

Für die allgemeinere Aussage beachte, dass $A = \bigcup_{b \in B} f^-(b)$, da f total. Aus Folgerung 3.4.32 ergibt sich: $|A| \leq \sum_{b \in B} |f^-(b)|$. Wähle nun $b_0 \in B$ mit $|f^-(b_0)|$ maximal. Dann gilt $|A| \geq |B| \cdot |f^-(b_0)|$, woraus die Behauptung folgt.

7.4.7 Zählen von Relationen

Es sei M eine m -elementige Menge.

1. $2^{M \times M}$ ist die Menge aller Relationen auf M .

$$|2^{M \times M}| = 2^{|M \times M|} = 2^{|M| \cdot |M|} = 2^{m^2}$$

nach der Potenzmengenregel und der Produktregel.

2. Es gibt eine offensichtliche Bijektion zwischen den Relationen auf M und den Relationen zwischen M und $[m - 1]$. O.E. sei $M = [m]$; die konkreten Elemente von M sind für die Zählaufgabe irrelevant. Setze zunächst

$$f((x, y)) := \begin{cases} (x, y), & \text{falls } y < x \\ (x, y - 1), & \text{falls } y > x \end{cases}$$

$f : [m] \times [m] \rightarrow [m] \times [m - 1]$ ist eine partielle Funktion. Sie bildet (men- genwertig interpretiert) die reflexive Relation $R \subseteq [m] \times [m]$ auf die Relation $f(R) \subseteq [m] \times [m - 1]$ ab. Umgekehrt kann jede Relation $R' \subseteq [m] \times [m - 1]$ auf $f^{-1}(R') \cup \Delta_{[m]}$ abgebildet werden. Dies beschreibt eine Bijektion von der Menge der reflexiven Relationen auf M auf die Menge der Relationen zwischen $[m]$ und $[m - 1]$. Ähnlich wie in Aufgabenteil 1 rechnet man mit Potenzmengenregel und Produktregel nach, dass es $2^{m(m-1)}$ viele Relationen zwischen $[m]$ und $[m - 1]$ gibt und daher genauso viele reflexive Relationen auf M .

3. Hier ist zu beachten, dass die Symmetrie die Anzahl der Möglichkeiten erheblich einschränkt. Die 0 kann mit m Elementen in Relation gesetzt werden, die 1 dann nur noch mit $m - 1$ Elementen usf. Die Details seien diesmal dem Leser überlassen.
4. Im Haupttext hatten wir als Trick zum Zählen von partiellen Funktionen kennengelernt, diese Aufgabe auf das Zählen von Abbildungen zurückzuführen, indem ein “undefined”-Symbol \perp ausdrücklich in den Wertebereich aufgenommen wird. Die Menge der nacheindeutigen Relationen und die der voreindeutigen Relationen lassen sich mit der Inversionsabbildung bijektiv aufeinander abbilden. Daher funktioniert der besagte Trick auch hier und liefert sofort $(m + 1)^m$ als Lösung dieser Zählaufgabe.

7.4.8 Binomialkoeffizienten

1. Betrachte $\{(A, a) \mid A \subseteq [n], |A| = k, a \in A\}$. Nach der Produktregel hat diese Menge $\binom{n}{k} \cdot k$ viele Elemente. Genauer haben wir zunächst $\binom{n}{k}$ viele Möglichkeiten, A auszuwählen, und dann nochmal $|A| = k$ viele, a zu bestimmen. Wir könnten aber auch andersherum vorgehen: Es gibt offenbar n Möglichkeiten, als Erstes a zu wählen, was dann aber nur noch $\binom{n-1}{k-1}$ Wahlmöglichkeiten für $A \setminus \{a\}$ aus $[n] \setminus \{a\}$ übrig lässt. Daher gilt die behauptete Identität.

Hinweis: Diese Idee, dieselbe Menge auf zwei unterschiedliche Weisen abzuzählen, ist zum kombinatorischen Nachweis von Gleichheiten häufig anzutreffen und hat auch einen eigenen treffenden Namen: *Doppeltes Abzählen*.

2. Für $k = 0$ gilt offenbar: $\binom{n}{k} = \binom{n}{0} = 1 = \frac{n!}{0!(n-0)!}$. Nach dieser Beobachtung führen wir einen Induktionsbeweis über $n + k$. Der Induktionsanfang (für $n + k = 0$, also $n = k = 0$) folgt aus der Beobachtung. Angenommen (Induktionsvoraussetzung), die Behauptung gilt für alle $n + k < N + K$. Wegen der Beobachtung können wir $K > 0$ voraussetzen. Daher liefert die vorher gezeigte Identität:

$$\binom{N}{K} = \frac{N}{K} \cdot \binom{N-1}{K-1}$$

Da $(N-1)+(K-1) < N+K$, lässt sich die Induktionsvoraussetzung anwenden, d.h.:

$$\binom{N}{K} = \frac{N}{K} \cdot \frac{(N-1)!}{(K-1)! \cdot (N-1-(K-1))!} = \frac{N!}{K! \cdot (N-K)!}$$

Die letzte Gleichheit gilt aufgrund der Definition der Fakultätsfunktion. Das zeigt die Induktionsbehauptung. Nach dem Prinzip der vollständigen Induktion folgt die Gültigkeit der Formel allgemein.

7.4.9 Binomischer Lehrsatz

Fixiere reelle Zahlen x, y und eine natürliche Zahl $n > 0$ (für $n = 0$ gilt die Behauptung sowieso). Betrachte also

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

Nach Anwendung von Assoziativ- bzw. Kommutativgesetzen findet sich beim Ausmultiplizieren der Term $x^{n-k}y^k$ dadurch, dass wir genau bei k der n vielen Faktoren y ausgewählt haben. Es gibt genau (nach der Definition des Binomialkoeffizienten) $\binom{n}{k}$ viele Möglichkeiten, k aus der Menge der n Faktoren (und damit k -mal y) auszuwählen, was den Koeffizienten $\binom{n}{k}$ beim Term $x^{n-k}y^k$ in der Summe erklärt.

7.4.10 Zählen beim Schach

[Pos] kann man durch Produktregel und Funktionenregel ausrechnen. Die Zugmengen erfordern mehr Überlegungen. Die Anzahl der Mattstellungen wurde im Haupttext schon fast "vorgerechnet". Der Leser sollte hier aber noch die verschiedenen Behauptungen in Abschnitt 5.3.8 nachprüfen. Die Remisstellungen kann man wie folgt zählen: Zunächst einmal gibt es 64 Möglichkeiten für die Positionierung des schwarzen Königs. Dann muss man anschließend den weißen Turm so stellen, dass er überhaupt geschlagen werden könnte, und schließlich muss der weiße König so aufgestellt werden, dass er nicht den Turm deckt.

7.4.11 Betrunkene Seemänner

Hinweis: Diese und ähnliche Aufgaben zur Kombinatorik finden Sie auch im folgenden Blog. Das klingt auf den ersten Blick verlockend, aber hier (insbesondere bei Blogs) ist Vorsicht geboten: Konkret ist die dort angebotene Lösung der Seemannsaufgabe einfach falsch.

Schauen wir uns das Problem allgemeiner an: Wir haben n betrunkene Seeleute und n Kojen. Wir fragen, wie viele Möglichkeiten es gibt, dass sich die Seeleute so in die Kojen legen, dass niemand in seiner eigenen Koje schläft. Das ist offenbar dieselbe Frage, wie nach der Anzahl von bijektiven Abbildungen $f : [n] \rightarrow [n]$ ohne Fixpunkt zu fragen, also ohne $i \in [n]$ mit $f(i) = i$. Es bezeichne D_n diese Anzahl (fixpunktfreie Permutationen heißen auch Derangements).

Für Derangements $f : [n] \rightarrow [n]$ gibt es offenbar $n - 1$ mögliche Werte für $f(0)$. Betrachte $f(0) = i \neq 0$. Falls $f(i) = 0$, so verbleiben noch D_{n-2} viele Möglichkeiten, Derangements mit $f(0) = i$ und $f(i) = 0$ zu erstellen. Andernfalls ($f(i) \neq 0$) definiert f ein Derangement von $n - 1$ Objekten $\{1, \dots, n - 1\}$. Daher gilt für $n \geq 3$:

$$D_n = (n-1)(D_{n-1} + D_{n-2}).$$

Mit den Startwerten $D_1 = 0$, $D_2 = 1$ erhalten wir: $D_3 = 2(1 + 0) = 2$, $D_4 = 3(2 + 1) = 9$ und schließlich $D_5 = 4(9 + 2) = 44$ als unseren gesuchten Wert. Nach Satz 3.4.28 gibt es $5! = 120$ Möglichkeiten, die fünf Seeleute auf 5 Kojen zu verteilen. Daher liegt die Wahrscheinlichkeit (immerhin) bei $44/120 = 36\frac{2}{3}\%$ für das perfekte Schlaf-Chaos.

Derangements sind ein beliebtes Thema in der Kombinatorik. Diese konkrete Aufgabe ließe sich auch unter Verwendung des Inklusions-Exklusionsprinzips lösen. Versuchen Sie sich an einem derartigen Alternativbeweis! Als kleiner Hinweis mag dienen: Betrachten Sie

$$F_i := \{f : [n] \rightarrow [n] \mid f \text{ ist bijektiv und } f(i) = i\}$$

Offenbar gilt:

$$D_n = n! - \left| \bigcup_{i \in [n]} F_i \right|.$$

In der Vereinigung aller F_i stecken nämlich alle Bijektionen $f : [n] \rightarrow [n]$, die irgendeinen Fixpunkt haben. Aber natürlich gibt es Bijektionen mit mehr als einem Fixpunkt, und diese kommen in mehreren Mengen F_i vor, sodass die Vereinigungsbildung nicht (paarweise) disjunkt ist. Daher muss hier das Inklusions-Exklusionsprinzip benutzt werden. Es mag daher lehrreich sein, so eine allgemeine (geschlossene) Formel für D_n aufzustellen und dann per Induktion zu beweisen, dass diese Formel dasselbe liefert wie die vorher für D_n aufgestellte induktive Formel.

Wenn Sie noch weiter Ihre Analysis-Kenntnisse prüfen wollen, so können Sie auch beweisen, dass

$$\lim_{n \rightarrow \infty} \frac{D_n}{n!} = \frac{1}{e} \approx 0,3679$$

gilt, unser zuvor bestimmter Bruch $D_5/5!$ also schon eine recht gute Annäherung an den Kehrwert der Eulerschen Zahl e ergeben hatte.

7.4.12 Zählen von Zerlegungen

Die Angabe sämtlicher Zerlegungen von [1], [2] und [3] sollte gelingen. Für die induktive Formel überlege man Folgendes: Betrachte $[n+1]$. Die Zahl n muss in irgendeiner Menge M in jeder Zerlegung von $[n+1]$ stecken. Genauer lässt sich M schreiben als $M = N \cup \{n\}$, wobei $N \subseteq [n]$. N kann beliebig alle Teilmengen von $[n]$ durchlaufen. Hat N nun k Elemente, so gilt es, die verbleibende $(n-k)$ -elementige Menge weiter zu zerlegen bzw. die betreffenden Möglichkeiten zu zählen. Da auf diese Weise keine Zerlegungen doppelt gezählt werden und auch alle Zerlegungen von $[n+1]$ erreicht werden, folgt die Gültigkeit der Formel. (Versuchen Sie, die soeben mehr in Worten gegebene Begründung formaler auszugestalten. Erklären Sie, wo beispielsweise die Summenregel angewendet wurde.)

Die Zahlenfolge B_n ist auch als Bellsche Zahlen bekannt.

7.4.13 Inklusions-Exklusionsprinzip

Hierzu wurde im Haupttext schon genügend verraten.

7.4.14 Zur Anwendung des Inklusions-Exklusionsprinzips

Für $I \subseteq [k]$ sei $A_{n,I}$ die Menge der Abbildungen von $[n]$ nach $[k] \setminus I$. Offensichtlich gilt: $A_{n,I} = \bigcap_{i \in I} A_{n,\{i\}}$. Wir wollen zählen, wie viele Funktionen $[n] \rightarrow [k]$ es gibt, die nicht in einer der Mengen $A_{n,\{i\}}$ liegen für ein $i \in [k]$. Das sind nämlich gerade die gesuchten Surjektionen. Das Inklusions-Exklusionsprinzip liefert:

$$s(n, k) = \sum_{I \subseteq [k]} (-1)^{|I|} |A_{n,I}|.$$

Nach der Funktionenregel gilt: $|A_{n,I}| = (k - |I|)^n$. Daraus ergibt sich:

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

Zum Zusatz: Wir wissen wegen Satz 3.4.9 und Satz 3.4.28, dass es $n!$ viele Surjektionen $[n] \rightarrow [n]$ gibt. Andererseits gibt es $s(n, n)$ viele. Also ergibt sich:

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

7.4.15 Zum Satz von Ramsey

Die erste Behauptung hat nichts mit dem Satz von Ramsey zu tun, sie sagt (in Worten) aus, dass das Komplement einer unabhängigen Menge eine Knotenüberdeckung ist. Man zeigt sie durch einen einfachen Widerspruchsbeweis: Wenn es eine Kante e gäbe, von welcher keine der beiden Endknoten im Komplement von U liegt, so müssten also beide Endknoten u, v in U liegen; u und v (aus U) wären also durch eine Kante verbunden, im Widerspruch zur Tatsache, dass U unabhängig ist.

Für die zweite Behauptung wählt man $n(k) = R(k, k)$. Ist nun $G_1 = (V, E_1)$ ein ungerichteter Graph mit wenigstens $n(k)$ vielen Knoten, so setze $E_2 = V \times V \setminus (\Delta_V \cup E_1)$. Im vollständigen Graphen $G = (V, E)$ gibt es nun entweder den Fall, dass $E_1 = \emptyset$ oder $E_2 = \emptyset$ (dann gilt die Behauptung, weil $n(k) \geq k$), oder der Satz von Ramsey liefert die Behauptung direkt. (Wer sich – nicht zu unrecht – über den Fall $k = 1$ Gedanken macht: Diesen sollte man extra behandeln.)

7.5 Quasiordnungen

7.5.1 Quasiordnungen aus Quasiordnungen

Wir zeigen nur den Beweis zu Folgerung 3.5.2.

Beweis: Wegen Satz 3.5.1 bleibt noch die Symmetrie nachzuweisen. Betrachte beliebiges Paar $((a_1, a_2), (b_1, b_2)) \in R$. Nach Konstruktion gilt: $(a_1, b_1) \in R_1$ und $(a_2, b_2) \in R_2$. Da R_1 und R_2 symmetrisch, gilt mithin: $(b_1, a_1) \in R_1$ und $(b_2, a_2) \in R_2$. Das bedeutet, dass $((b_1, b_2), (a_1, a_2)) \in R$. Also ist R symmetrisch und somit Äquivalenzrelation. \square

Der andere eingeforderte Beweis verläuft ganz entsprechend.

7.5.2 Äquivalenzrelationen und das Relationenprodukt

Einen hübschen algebraischen Beweis finden Sie in [33, Satz 4.12].

7.5.3 Wie viele Äquivalenzrelationen gibt es?

Hier ist es gut, sich an die Kennzeichnung von Äquivalenzrelationen über Zerlegungen zu erinnern und daher die Frage zu betrachten, wie viele Zerlegungen der Menge $M = \{0, 1, 2\}$ es gibt. Zerlegungen sind Mengensysteme. Systematisch erscheint dabei die Vorgehensweise, nach der Anzahl der Mengen in den Zerlegungen vorzugehen.

- Es gibt genau eine Zerlegung, die ein Element enthält, nämlich $\{\{0, 1, 2\}\}$.
- Es gibt drei Zerlegungen, die zwei Elemente enthalten, z.B.: $\{\{0\}, \{1, 2\}\}$.
- Es gibt genau eine Zerlegung, die drei Elemente enthält, nämlich $\{\{0\}, \{1\}, \{2\}\}$.

Da es keine weiteren Zerlegungen von M gibt, besitzt M genau fünf Zerlegungen und mithin fünf Äquivalenzrelationen. Alternativ kann man natürlich auch über Fallunterscheidungen argumentieren, etwa wie folgt:

- Betrachte das Element 0.
- Fall 1: 0 ist zu keinem anderen Element äquivalent. Dann sind entweder 1 und 2 äquivalent oder nicht; es ergeben sich somit zwei mögliche Äquivalenzrelationen für diesen Fall. Diese entsprechen den Zerlegungen $\{\{0\}, \{1, 2\}\}$ und $\{\{0\}, \{1\}, \{2\}\}$.
- Fall 2: 0 und 1 sind äquivalent. Nun könnte 2 in derselben Äquivalenzklasse liegen oder nicht. Wir erhalten hier zwei weitere mögliche Äquivalenzrelationen. Diese entsprechen den Zerlegungen $\{\{0, 1, 2\}\}$ und $\{\{0, 1\}, \{2\}\}$.
- Fall 3: 0 und 1 sind nicht äquivalent. Nun könnte 2 mit 0 äquivalent sein oder mit 1 oder weder mit 0 noch mit 1. Dies entspricht den Zerlegungen $\{\{0, 2\}, \{1\}\}$, $\{\{0\}, \{1, 2\}\}$, $\{\{0\}, \{1\}, \{2\}\}$. Die letzten beiden Zerlegungen wurden schon in Fall 1 betrachtet. Es ergibt sich daher nur eine weitere Äquivalenzrelation in diesem Fall.

Vergleichen Sie diese Vorgehensweisen auch mit den allgemeineren Überlegungen in Aufgabe 6.5.3!

7.5.4 Restklassen

Betrachte die Relation $R_m = \{(a, b) \in \mathbb{Z}^2 : m \mid (a - b)\}$. Hierbei gilt: $m \mid c$ gdw. $\exists k \in \mathbb{Z} : c = m \cdot k$.

Mit $k = 0$ gilt offenbar $m \mid 0$ für alle m . Daher ist R_m reflexiv.

Gilt $(a, b) \in R_m$, also $m \mid (a - b)$, so gibt es ein $k \in \mathbb{Z}$ mit $(a - b) = m \cdot k$. Daher gilt: $(b - a) = m \cdot (-k)$, d.h., $(b, a) \in R_m$. Daher ist R_m symmetrisch. Auch die Transitivität sieht man recht leicht:

Gilt $(a, b) \in R_m$ und $(b, c) \in R_m$, so heißt das: $(a - b) = m \cdot k$ und $(b - c) = m \cdot k'$ für geeignete $k, k' \in \mathbb{Z}$. Daher gilt:

$$(a - c) = ((a - b) + (b - c)) = m \cdot k + m \cdot k' = m \cdot (k + k').$$

Deshalb gilt: $(a, c) \in R_m$.

7.5.5 Eine Eigenschaft von Äquivalenzklassen

Betrachte $x, y \in M$ mit $\{x, y\} \subseteq [b]_R$.

Nach Def. bedeutet das: $\{(x, b), (y, b)\} \subseteq R$.

Da R symmetrisch, gilt auch: $(b, y) \in R$.

Da R transitiv, folgt aus $\{(x, b), (b, y)\} \subseteq R$: $(x, y) \in R$.

Da R symmetrisch, folgt weiter: $(y, x) \in R$. \square

7.5.6 Äquivalenzrelationen und Zerlegungen

Es sei $R \subseteq M \times M$ eine Äquivalenzrelation. Gilt $(x, y) \in R$, so liegen x und y in derselben Äquivalenzklasse. Also gilt: $[x]_R = [y]_R$ für die entsprechende induzierte Zerlegung Z_R . Damit ist aber auch (per Def.) $x \sim_{Z_R} y$. Die umgekehrte Richtung sieht man ähnlich.

7.5.7 Quasiordnungen auf den komplexen Zahlen

1. Sei $x \in \mathbb{C}$ bel. Aus $|x| = |x|$ folgt sofort $x \prec x$ (Reflexivität). Gilt $x \prec y$ und $y \prec z$, so heißt das: $|x| \leq |y|$ und $|y| \leq |z|$. Das “normale Kleiner-Gleich” auf reellen Zahlen ist transitiv, d.h., $|x| \leq |z|$ folgt, und damit $x \prec z$, was zu zeigen war (Transitivität). Daher ist \prec reflexiv und transitiv, mithin eine Quasiordnung.
2. Da $|-1| = |1| = 1$ gilt $-1 \prec 1$ und $1 \prec -1$, aber sicher nicht $1 = -1$, also ist \prec nicht antisymmetrisch. $0 \prec 1$ während eben $1 \prec 0$ nicht gilt, d.h., \prec ist nicht symmetrisch.
3. $x \prec y$ und $y \prec x$ bedeutet, dass x und y gleichen Betrag haben, also (in der üblichen Ebenendarstellung der komplexen Zahlen) gleichen Abstand zum Ursprung des Koordinatensystems.

7.5.8 Zur Existenz von größten Elementen und Suprema

Folgende Hinweise mögen genügen:

- Die Suprema existieren im ersten Beispiel immer und ergeben sich durch Vereinigung der beteiligten Mengen. Z.B. gilt: $\sup(\{\{a\}, \{a, b\}\}) = \{a, b\}$. Größte Elemente existieren hingegen “nur selten”. Beispielsweise hat $\{\{a\}, \{a, b\}\}$ als größtes Element $\{a, b\}$, aber $\{\{a\}, \{b\}\}$ hat kein größtes Element. Können Sie genau beschreiben, wann solche größten Elemente existieren?
- Im zweiten Beispiel existieren Suprema für alle Teilmengen der Grundmenge bis auf \mathbb{N} (die Grundmenge) selbst. Größte Elemente gibt es zudem nicht für die Menge der geraden Zahlen (deren Supremum 1 ist).

7.5.9 Quasiordnungen und Inverse

Wir werden vornehmlich Satz 3.2.18 anwenden, um möglichst algebraische Beweise zu führen.

1. R reflexiv gdw. $\Delta_M \subseteq R$ gdw. $\Delta_M = \Delta_M^- \subseteq R^-$ gdw. R^- reflexiv.
2. R transitiv gdw. $R \circ R \subseteq R$ gdw. $(R \circ R)^- \subseteq R^-$ gdw. (Satz 3.2.6) $R^- \circ R^- \subseteq R^-$ gdw. R^- transitiv.

3. Die Aussage über Quasiordnungen ergibt sich unmittelbar aus den beiden vorigen Punkten.
4. R symmetrisch gdw. $R^- = R$ gdw. R^- symmetrisch.
5. Die Aussage über Äquivalenzrelationen ergibt sich unmittelbar aus den beiden vorigen Punkten.
6. R antisymmetrisch gdw. $R \cap R^- \subseteq \Delta_M$ gdw. $R^- \cap R \subseteq \Delta_M$ gdw. R^- antisymmetrisch.
7. Die Aussage über Halbordnungen folgt aus dem bislang Gesagten.
8. Für die Aussage zu linearen Ordnungen überlegen wir uns noch: $x, y \in M$ sind bzgl. R vergleichbar gdw. $(x, y) \in R \vee (y, x) \in R$, also gdw. $(y, x) \in R^- \vee (x, y) \in R^-$ gdw. x, y sind bzgl. R^- vergleichbar. Also sind alle Elemente von M untereinander bzgl. R vergleichbar gdw. alle Elemente von M sind untereinander bzgl. R^- vergleichbar. Daraus ergibt sich die gewünschte Aussage wegen der bereits gezeigten Aussage zu Halbordnungen.

7.5.10 Vergleichbarkeit

Offenbar ist (nur) noch die Reflexivität und die Symmetrie von V zu zeigen. Die Reflexivität von V folgt aus der Reflexivität von R , bedeutet doch $(a, a) \in V$, dass $(a, a) \in R \vee (a, a) \in R$ gilt.

Gilt nun $(a, b) \in V$, so heißt das: $(a, b) \in R \vee (b, a) \in R$. Aufgrund der Kommutativität der Disjunktion folgt daraus: $(b, a) \in R \vee (a, b) \in R$, was wiederum gleichbedeutend mit $(b, a) \in V$ ist.

7.5.11 Sortieren

Für den Induktionsschritt sind folgende Überlegungen nötig:

- Paare $(x, y) \in N \times N$, für die nach dem m -ten Schleifendurchlauf gilt, dass $(x, y) \in \text{Mem}_m$ und $x \leq y$, erfüllen diese Bedingung auch noch nach dem $(m+1)$ -ten Schleifendurchlauf.
- Bei der Ausführung des Schleifenrumpfes wird wenigstens ein Paar $(x_{m+1}, y_{m+1}) \in N \times N$ „neu sortiert“.

Formalisiere man die Überlegungen wohl am einfachsten, indem man zum Einen mit Mem_m die Speicherrelation nach dem m -ten Schleifendurchlauf bezeichnet und sodann die Folge S_m von Relationen betrachtet mit

$$S_m := \{(x, y) \in N \times N \mid (x, y) \in \text{Mem}_m \wedge x \leq y\}.$$

Die Behauptungen bedeuten nun, dass für alle $m \in \mathbb{N}$ gilt:

- $S_m \subseteq S_{m+1}$ sowie
- $\exists (x_{m+1}, y_{m+1}) \in S_{m+1} \setminus S_m$.

Nach diesen Vorüberlegungen sollte die eigentliche Induktion sehr einfach sein. Sie können hieran aber auch erkennen, dass eine gute und vollständige Formalisierung sehr wertvoll ist für einen Beweis. Gerade bei solchen Korrektheitsüberlegungen ist sonst oft nicht klar, was denn eigentlich bewiesen werden muss.

7.6 Ungerichtete Graphen

7.6.1 Zwillinge

falscher Zwilling $FZ \subseteq V \times V$ mit $(u, v) \in FZ \iff N(u) = N(v)$.

Rechnen wir die Eigenschaften nach:

- $\forall v \in V : N(v) = N(v)$, also $\forall v \in V : (v, v) \in FZ$. FZ ist daher reflexiv.
- $\forall u, v \in V : N(u) = N(v) \implies N(v) = N(u)$. Also gilt: $\forall u, v \in V : (u, v) \in FZ \implies (v, u) \in FZ$. FZ ist daher symmetrisch.
- $\forall u, v, w \in V : (N(u) = N(v) \wedge N(v) = N(w)) \implies N(u) = N(w)$. Hieraus folgt die Transitivität.

Beachten Sie, wie sich die bekannten Eigenschaften der Gleichheitsrelation übertragen auf die Eigenschaften von FZ .

Eine andere Sichtweise / Lösungsmöglichkeit besteht auf den Rückgriff auf Aufgabe 6.3.2. Dazu definiere die Abbildung $f : V \rightarrow 2^V, v \mapsto N(v)$ und beobachte, dass FZ der Kern dieser Abbildung ist.

wahrer Zwilling $WZ \subseteq V \times V$ mit $(u, v) \in WZ \iff N[u] = N[v]$.

Diese Aufgabe kann man genauso wie den vorigen Aufgabenteil angehen.

Zwilling $Z = FZ \cup WZ$.

Hier ist ein genaues Betrachten einzelner Fälle vonnöten.

Die Zusatzüberlegung sollte Ihnen zeigen, dass im letzten Aufgabenteil wirklich eine Einzelüberlegung Not tut. Betrachten wir z.B. die Menge \mathbb{Z} mit den beiden Äquivalenzrelationen

- $(x, y) \in R_2 \iff x$ lässt beim Teilen durch 2 denselben Rest wie y sowie
- $(x, y) \in R_3 \iff x$ lässt beim Teilen durch 3 denselben Rest wie y .

Offenbar gilt: $(2, 0) \in R_2$ und $(0, 3) \in R_3$ und mithin $\{(2, 0), (0, 3)\} \subseteq R_2 \cup R_3$, aber $(2, 3) \notin R_2 \cup R_3$, d.h., $R_2 \cup R_3$ ist nicht transitiv und daher keine Äquivalenzrelation.

7.6.2 Isomorphie: Ein Beweis

Wir zeigen im Folgenden nur die wesentlichen Ideen für den erforderlichen Nachweis.

- Reflexivität: Die Identität ist ein Graphisomorphismus.
- Symmetrie: Ist ϕ ein Graphisomorphismus, so auch ϕ^{-1} .
- Transitivität: Sind $\phi_1 : V_1 \rightarrow V_2$ und $\phi_2 : V_2 \rightarrow V_3$ Graphisomorphismen zwischen den Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ bzw. G_2 und $G_3 = (V_3, E_3)$, so ist auch $\phi_1 \circ \phi_2$ ein Graphisomorphismus zwischen den Graphen G_1 und G_3 .

7.6.3 Isomorphie: Beispiele

Zum Einen kann man beobachten, dass alle in Abb. 3.8 dargestellten Graphen zusammenhängend sind. Natürlich gibt es unzusammenhängende Graphen mit 2,3 oder 4 Knoten. Tatsächlich sind alle zusammenhängenden Graphen mit höchstens 3 Knoten gelistet, aber längst nicht alle mit 4 Knoten. So lassen sich in den Kreis C_4 noch Diagonalen einzeichnen.

7.6.4 Vom Nutzen der Isomorphie

Beweis: (1) ist unmittelbar klar.

(2) Da ϕ Isomorphismus, ist das Bild $\phi_E(e)$ einer Kante $e \in E$ eine Kante in E' .

Betrachte $e' = x'y' \in E'$. Da ϕ bijektiv, gibt es hierzu eindeutig $x, y \in V$ mit $x' = \phi(x)$ und $y' = \phi(y)$. Da ϕ Isomorphismus und $x'y' = \phi(x)\phi(y)$, folgt $xy \in E$. Daher ist ϕ_E eine Surjektion.

Betrachte eine Kante $e' = x'y' \in E'$ mit $\phi_E(e_1) = \phi_E(e_2) = e'$. Es sei $e_1 = xy$ und demzufolge $e' = \phi(x)\phi(y)$, o.E. mit $\phi(x) = x'$ und $\phi(y) = y'$. Für gewisse Knoten $u, v \in E$ muss aber auch gelten: $uv = e_2$, also (o.E.) $\phi(u) = x'$ und $\phi(v) = y'$, da $\phi_E(e_2) = e'$. Damit wäre aber (da wir keine Mehrfachkanten haben) $u = x$ und $v = y$. Also gilt $e_1 = e_2$, d.h., ϕ_E ist injektiv.

(3) Betrachte einen Knoten $v \in V$ und sein Bild $\phi(v) \in V'$.

Jede Kante $vw \in E$ wird durch ϕ_E auf die Kante $\phi(v)\phi(w)$ abgebildet.

Da ϕ_E injektiv ist, gilt:

$$d(v) = |\{vw \mid vw \in E\}| = |\{\phi(v)\phi(w) \mid vw \in E\}| \leq |\{\phi(v)x \mid \phi(v)x \in E'\}| = d(\phi(v)). (*)$$

Betrachte eine Kante $\phi(v)x \in E'$.

Da ϕ Isomorphismus, gilt: $\phi_E^{-1}(\phi(v)x) = \phi^{-1}(\phi(v))\phi^{-1}(x) = v\phi^{-1}(x) \in E$.

Also gilt: $\phi^{-1}(x) \in N(v)$, und mithin $\phi(v)x \in \{\phi(v)\phi(w) \mid vw \in E\}$.

Daher ist die einzige Ungleichung in (*) tatsächlich eine Gleichheit. \square

7.6.5 Eine Kennzeichnung von Pfaden

Der Beweis geht ähnlich zu dem von Satz 3.6.15. Da Pfade die Eigenschaften besitzen, bleibt Folgendes zu tun für einen vorgelegten Graphen $G = (V, E)$ mit den besagten Eigenschaften: Es ist also (induktiv) eine geeignete Bijektion $|\mathbb{N}_0| \rightarrow V$ anzugeben, die sich dann als Graphisomorphismus von $P_{|\mathbb{N}_0|}$ auf G erweist.

7.6.6 Knoten- und Kantenzahlen in Bäumen

Am einfachsten ist es, die Eigenschaften in die induktive Definition von Bäumen hinzuschreiben, um die Beweisführung einzusehen.

Anker: Für jeden Knoten v gilt: $(\{v\}, \emptyset)$ ist ein Baum mit 1 Knoten und 0 Kanten.

Induktionsschritt: Ist (V, E) ein Baum mit n Knoten und $n - 1$ Kanten und $v \notin V$ ein neuer Knoten sowie $u \in V$ beliebig, so ist $(V \cup \{v\}, E \cup \{uv\})$ ein Baum mit $n + 1$ Knoten und n Kanten.

7.6.7 Eine weitere Baumkennzeichnung

Zu zeigen ist für einen zusammenhängenden Graphen G der Ordnung n :
 G ist ein Baum gdw. G hat Größe $n - 1$.

Beweis: Ein Baum mit n Knoten hat $n - 1$ Kanten (Lemma 3.6.9). Warum ist nun jeder zusammenhängende Graph mit $n - 1$ Kanten ein Baum? Wäre dem nicht so, gäbe es ein Gegenbeispiel. Wähle ein Gegenbeispiel G mit einer kleinstmöglichen Ordnung n . Wie man leicht überprüft, muss $n > 1$ gelten. Daher hat G keine Knoten vom Grad Null. Wären alle Knoten von G vom Grad mindestens Zwei, so hätte G wegen Satz 3.6.3 mindestens n Kanten. Daher besitzt G wenigstens einen Knoten v vom Grad Eins. Entfernt man diesen samt der anliegenden Kante, erhält man einen zusammenhängenden Graphen G' der Ordnung $n - 1$ mit $n - 2$ Kanten. Nach der Wahl des Gegenbeispiels ist G' ein Baum. Nun entsteht G aber aus G' durch Einführen eines neuen Knotens und durch Verbinden desselben mit genau einem Knoten aus G . Das entspricht genau der induktiven Definition von Bäumen, d.h., G muss auch ein Baum sein, im Widerspruch zur Annahme. \square

7.6.8 Ein Spannbaumalgorithmus

Eine mögliche Lösung sehen Sie in Bild 7.1.

```

Data :  $G = (V, E)$ : a connected graph
Result :  $F$ : set of edges such that  $(V, F)$  is a spanning tree of  $G$ 
1 while  $|E| - |V| \geq 0$  do
2   |   find edge  $e$  in cycle subgraph of  $(V, E)$ ;
3   |    $E \leftarrow E \setminus \{e\}$ ;
4 return  $E$ ;

```

Abbildung 7.1: An iterative spanning tree algorithm STiter

7.6.9 Cayley-Formel

Das sollte Ihnen eigentlich mit Ihrem bisherigen Wissen und den gegebenen Hinweisen gelingen. Für den Sachverhalt gibt es vier sehr verschiedene schöne Beweise, die sich im BUCH von Aigner und Ziegler finden [2].

7.7 Verknüpfungen

7.7.1 Absorbierende Elemente

Im Haupttext finden Sie den entscheidenden Hinweis.

7.7.2 Komplexprodukt

Die Verknüpfungstafel für das Komplexprodukt sieht wie folgt aus:

\Rightarrow	κ	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$
\emptyset	\emptyset	\emptyset	\emptyset	\emptyset	\emptyset
$\{0\}$	\emptyset	$\{1\}$	$\{1\}$	$\{1\}$	$\{1\}$
$\{1\}$	\emptyset	$\{0\}$	$\{1\}$	$\{0, 1\}$	$\{0, 1\}$
$\{0, 1\}$	\emptyset	$\{0, 1\}$	$\{1\}$	$\{0, 1\}$	$\{0, 1\}$

Zum Beweis von Satz 3.7.3: Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid. Es wurde definiert:

$$M_1 \circ_K M_2 := \{x_1 \circ x_2 \mid x_1 \in M_1, x_2 \in M_2\} \quad \text{für } M_1, M_2 \subseteq M.$$

- Wir müssen zeigen, dass aus \circ_K eine Abbildung ist, die zwei Teilmengen M_1 und M_2 von M eine Teilmenge von M zuordnet (Abgeschlossenheit). Sind M_1 und M_2 beide nicht leer, so betrachte $(x_1, x_2) \in M_1 \times M_2$ beliebig. Da \mathbb{G} Gruppoid, gilt: $x_1 \circ x_2 \in M$. Daher folgt $M_1 \circ_K M_2 \subseteq M$. Sind M_1 oder M_2 die leere Menge, so ist $M_1 \circ_K M_2$ ebenfalls die leere Menge.
- Aus dem letzten Satz folgt auch, dass \emptyset stets absorbierendes Element ist. Wir haben also gezeigt:
 $2^{\mathbb{G}} := (2^M, \circ_K)$ ist ein Gruppoid mit absorbierendem Element \emptyset .
- Ist $e \in M$ neutrales Element von \mathbb{G} , so gilt für alle $A \subseteq M$:

$$\begin{aligned} A \circ_K \{e\} &= \{a \circ e \mid a \in A\} \\ &= \{a \mid a \in A\} \\ &= A \\ &= \{e \circ a \mid a \in A\} \\ &= \{e\} \circ_K A \end{aligned}$$

Also ist $\{e\}$ das neutrale Element von $2^{\mathbb{G}}$.

Ist umgekehrt E neutrales Element von $2^{\mathbb{G}}$, so muss insbesondere $E \circ_K \{a\} = \{a\} \circ_K E = \{a\}$ für jedes $a \in M$ gelten. Also ist nach Definition:

$$E \circ_K \{a\} = \{e \circ a \mid e \in E\} = \{a\}$$

Daraus folgt, dass für jedes $e \in E$ gilt: $e \circ a = a$. Entsprechend sieht man, dass für jedes $e \in E$ gilt: $a \circ e = a$. Jedes $e \in E$ ist also neutrales Element von \mathbb{G} . Wegen Lemma 3.7.1 muss $|E| = 1$ gelten, also folgt $E = \{e\}$ und e ist das neutrale Element von \mathbb{G} .

7.7.3 Produktgruppoide

Vollziehen Sie die Definition genau nach (wie bei der vorigen Musterlösung zu Komplexprodukten vorgestellt). Dies sollte als Hinweis genügen.

7.7.4 Komplementbildung als Homomorphismus

Es seien $A, B \in 2^{\mathcal{U}}$ beliebig, also $A, B \subseteq \mathcal{U}$.

Dann gilt:

$$\begin{aligned} h(A \cup B) &\stackrel{\text{Def.}}{=} \overline{A \cup B} \\ &\stackrel{\text{De M.}}{=} \overline{A} \cap \overline{B} \\ &\stackrel{\text{Def.}}{=} h(A) \cap h(B) \end{aligned}$$

7.7.5 Isomorphie als Äquivalenzrelation

Wir müssen zeigen: \cong ist Äquivalenzrelation auf $\mathbb{G}(M)$,

- Reflexivität: Die Identität ist ein Isomorphismus.
- Symmetrie: Folgt aus Satz 3.7.9.
- Transitivität: Folgt aus Satz 3.7.10.

7.7.6 Äquivalenzrelationen liefern Homomorphismen

Das Nachrechnen der Eigenschaften sollte Ihnen gelingen. Beachten Sie, wo überall “Kerne” und “Homomorphismen” bereits diskutiert wurden.

7.7.7 Quasiordnungen aus Homomorphismen

Wir wollen hier nur insofern helfen, als dass wir verraten, dass die Identität stets zu \mathcal{H} gehört und dass wir überdies wissen (woher genau?), dass die Komposition zweier Homomorphismen wieder ein Homomorphismus ist. Das sollte zur Bearbeitung des ersten Aufgabenteils als Hinweise genügen. Für die anderen Aufgabenteils sollte das Durchrechnen kleiner Beispiele helfen.

7.7.8 Assoziativität

Die erste Verknüpfung \circ_1 ist assoziativ, wie man leicht, wenn auch mühsam, durch Überprüfen aller $4 \times 4 \times 4 = 64$ Tripel feststellt.

Mit demselben Verfahren kann man herausbekommen, dass die zweite Verknüpfung \circ_2 nicht assoziativ ist. Allerdings gibt es nur wenige “nichtassoziatives Tripel”, z.B.:

$$(4 \circ_2 4) \circ_2 3 = 2 \circ_2 3 = 3, \quad \text{aber } 4 \circ_2 (4 \circ_2 3) = 4 \circ_2 1 = 1,$$

während z.B.

$$(3 \circ_2 4) \circ_2 3 = 3 \circ_2 3 = 1, \quad \text{aber } 3 \circ_2 (4 \circ_2 3) = 1 \circ_2 3 = 1,$$

$$(4 \circ_2 3) \circ_2 4 = 1 \circ_2 3 = 1, \quad \text{aber } 4 \circ_2 (3 \circ_2 4) = 4 \circ_2 3 = 1.$$

Das letzte Tripel ist übrigens fälschlicherweise in [32, Seite 126] als nichtassoziatives Tripel vermerkt.

7.7.9 Konkatenation

Aus der Definition ergibt sich, dass die Konkatenation zweier endlicher Folgen, konkret einer Folge $f : [n] \rightarrow M$ mit einer Folge $g : [m] \rightarrow M$ wieder eine endliche Folge, nämlich $h : [n+m] \rightarrow M$, liefert. Damit ist die Gruppoid-Eigenschaft nachgewiesen. Die Assoziativität ist etwas mühsamer, doch elementar nachzurechnen.

7.7.10 Potenzen von Relationen

Hierzu wurde im Haupttext genug verraten.

7.7.11 Kommutativität

Das geht sehr ähnlich zur Assoziativität.

7.7.12 Idempotente Elemente

1. Jedes neutrale Element ist idempotent.
2. Wähle ein beliebiges Element a und berechne die Folge

$$a, a^2, a^3, \dots$$

Da M endlich ist, gibt es zwei kleinste Zahlen i, j mit $i < j$ und $a^i = a^j$. Da $j - i \geq 1$, gibt es eine Zahl $k \geq 1$ mit $i \leq k(j-i) < j$. Nun gilt für jede Zahl ℓ mit $i \leq \ell < j$, dass $(a^\ell) \circ a^{j-i} = a^\ell$ gilt, denn $a^\ell \circ a^{j-i} = a^{\ell-i} \circ a^i \circ a^{j-i} = a^{\ell-i} \circ a^j = a^{\ell-i} \circ a^i = a^\ell$ wegen der Assoziativität von \circ . Induktiv folgt hieraus leicht, dass für jede Zahl $r \geq 1$ gilt: $a^\ell \circ a^{r(j-i)} = a^\ell$. Daher gilt insbesondere: $a^{k(j-i)} \circ a^{r(j-i)} = a^{k(j-i)}$. Wählt man nun $r = k$, so sieht man, dass $a^{k(j-i)}$ idempotent ist.

3. Betrachte $(\{n \in \mathbb{N} \mid n \geq 1\}, +)$.

7.7.13 Idempotente Untermonoide

Die ersten beiden Punkte sind leicht nachzuweisen, weshalb wir keine weiteren Hinweise geben. Der dritte Punkt wird über den vierten quasi mit erledigt. Als isomorphe Struktur kann nämlich $(2^M, \cap, M)$ dienen mit der Zuordnung einer Teilmenge $X \subseteq \Delta_M$ auf $\{x \mid (x, x) \in X\}$. Offenbar gilt nun für Teilmengen $A, B \subseteq M$:

$$\{(a, a) \mid a \in A\} \circ \{(b, b) \mid b \in B\} = \{(c, c) \mid c \in A \cap B\},$$

was die Homomorphieeigenschaft zeigt. Die Bijektivität ist leicht nachzurechnen. Daraus gilt: $|D_M| = |2^M| = 2^{|M|}$.

7.7.14 Funktionengruppoide

Exemplarisch wollen wir hier die Kommutativität und das neutrale Element diskutieren. Die übrigen Teile kann man ganz entsprechend zeigen.

Zur Kommutativität: Es seien $f, g \in M^N$. Sei $n \in N$ beliebig. Nun gilt für $h := f \circ_N g$ und $h' := g \circ_N f$:

$$\begin{aligned} h(n) &= (f \circ_N g)(n) \\ &= f(n) \circ g(n) \\ &\stackrel{(*)}{=} g(n) \circ f(n) \\ &= (g \circ_N f)(n) \\ &= h'(n) \end{aligned}$$

Bei $(*)$ wurde die Kommutativität von G , also von \circ , benutzt. Da n beliebig, folgt: $h = h'$, also, $f \circ_N g = g \circ_N f$. Also ist G^N kommutativ.

Sei nun $e \in M$ das neutrale Element von G . Betrachte die konstante Funktion $f_e : N \rightarrow M, n \mapsto e$ für n beliebig. Nun gilt:

$$(f \circ_N f_e)(n) = f(n) \circ f_e(n) = f(n) \circ e = f(n) = e \circ f(n) = f_e(n) \circ f(n) = (f_e \circ_N f)(n)$$

für beliebige $f : N \rightarrow M$, da e neutrales Element. Also ist f_e neutrales Element in G^N .

7.7.15 Eigenschaften von Verknüpfungen und gewissen zugehörigen Relationen

Es sei $\mathbb{G} = (M, \circ)$ ein Gruppoid.

- Die Erreichbarkeitsrelation $R_{\mathbb{G}}$ auf M bedeutet:

$$(a, c) \in R_{\mathbb{G}} : \iff \exists b \in M : a \circ b = c.$$

Ist \mathbb{G} eine Halbgruppe, so ist \circ assoziativ. Betrachten wir nun drei (nicht notwendig verschiedene) beliebige Elemente x, y, z aus M , für die $\{(x, y), (y, z)\} \subseteq R_{\mathbb{G}}$ gilt. Nach Def. gibt es also $x', y' \in M$ mit: $x \circ x' = y$ und $y \circ y' = z$. Mithin gilt:

$$z = y \circ y' = (x \circ x') \circ y' = x \circ (x' \circ y')$$

Die letzte Gleichheit gilt wegen der Assoziativität von \circ . Nach Definition ist daher $(x, z) \in R_{\mathbb{G}}$. Also ist $R_{\mathbb{G}}$ transitiv.

- Dieser Teil der Übung ist leicht und daher dem Leser überlassen.
- Dieser Übungsteil ist sogar noch leichter. Vergessen Sie aber nicht, beide Implikationsrichtungen zu zeigen.

7.7.16 Halbverbände aus Halbordnungen

Als Hinweise sollten genügen:

- Schauen Sie nochmal den Beweis zu Satz 3.7.20 an. Dann sollte klar werden, wie Eigenschaften von Verknüpfungen und von Relationen zusammenpassen.
- Beobachten Sie, wo genau Sie Bedingung (*) verwenden.

7.8 Hüllen

7.8.1 Abgeschlossene Intervalle

Der erste Teil sollte elementar durch Nachvollziehen der Definition einzusehen sein. Daraus folgt auch insbesondere die Behauptung aus dem Haupttext (für das Einheitsintervall $U_{0,1}$). Für den zweiten Teil beachte, dass die Infima und Suprema nicht existieren müssen. Während also im ersten Teil die abgeschlossenen Mengen von H gerade den abgeschlossenen Intervallen entsprechen, würde das jetzt nicht mehr der Fall sein. So wäre $H(\mathbb{N}) = [0, \sup \emptyset] = [0, \infty]$ keine sinnvolle Festlegung (auch wenn sie den Definitionen folgt), denn damit wäre $H(\mathbb{N})$ keine Teilmenge von \mathbb{R} . In diesem Sinne wäre H dann kein Hüllenoperator mehr. Wenn wir aber $H(\mathbb{N})$ als $[0, \infty)$ festlegen (und entsprechend $H(\mathbb{Z}) = (-\infty, \infty) = \mathbb{R}$, um nur ein weiteres Beispiel anzugeben), so würde H einen Hüllenoperator darstellen.

7.8.2 Konvexe Mengen

Sollten Sie hier Schwierigkeiten bekommen: Im Internet finden Sie sicherlich Anregungen, denn konvexe Mengen sind eine bekannte Klasse von Mengen.

7.8.3 Oberhalbmengen

Hier dürfte ein genaues Nachrechnen der Eigenschaften der Hüllenoperatoren keine Schwierigkeiten bereiten. Beachten Sie dabei, wie die Eigenschaften der Quasiordnung hierbei eingehen.

Für das konkrete Beispiel beachte:

- $O_{\subseteq}(\emptyset) = 2^{\{0, 1, 2\}}$;
- $O_{\subseteq}(\{0\}) = \{\{0\}, \{0, 1\}, \{0, 2\}, \{0, 1, 2\}\}$;
- $O_{\subseteq}(\{0, 1\}) = \{\{0, 1\}, \{0, 1, 2\}\}$;
- $O_{\subseteq}(\{1, 2\}) = \{\{1, 2\}, \{0, 1, 2\}\}$.

Diese Beispiele sollten genügen, um Sie für die Aufgabe auf die richtige Fährte zu führen. So gilt:

$$\{\{0, 1, 2\}\} = O_{\subseteq}(\{0, 1, 2\}) = O_{\subseteq}(\{0, 1\} \cup \{1, 2\}) = O_{\subseteq}(\{0, 1\}) \cap O_{\subseteq}(\{1, 2\})$$

7.8.4 Hüllen und abgeschlossene Systeme

Am Ende dieses Skripts sollte Ihnen das ohne Hilfe gelingen. Denken Sie daran, beide Richtungen zu beweisen.

7.8.5 Hüllen und Halbordnungen

1. Falls \leq_1 reflexiv, transitiv und antisymmetrisch bezüglich U und alle Elemente in U vergleichbar sind bezüglich \leq_1 sind, dann ist \leq_1 auch bezüglich jeder Teilmenge von $A \subseteq U$ reflexiv, transitiv und antisymmetrisch und alle Elemente in A vergleichbar bezüglich \leq_1 . Da $H_1(A) \subseteq U$, ist $(H_1(A), \leq_1)$ eine lineare Ordnung.
Monotonie: Sei $A \subseteq B$ und $x \in H_1(A) \Rightarrow$ es gibt $y, z \in A$ mit $y \leq_1 x \leq_1 z \Rightarrow$ es gibt $y, z \in B$ mit $y \leq_1 x \leq_1 z \Rightarrow x \in H_1(B)$.
Idempotenz: Zu zeigen ist $H_1(A) = H_1(H_1(A))$. $H_1(A) \subseteq H_1(H_1(A))$ folgt aus Extensivität und Monotonie.
Sei $x \in H_1(H_1(A)) \Rightarrow$ es gibt $y, z \in H_1(A)$ mit $y \leq_1 x \leq_1 z \Rightarrow$ es gibt $y_1, y_2, z_1, z_2 \in A$ mit $y_1 \leq_1 y \leq_1 y_2$ und $z_1 \leq_1 z \leq_1 z_2 \Rightarrow$ da $y_1 \leq_1 y \leq_1 x$ gilt $y_1 \leq_1 x$ und da $x \leq_1 z \leq_1 z_2$ gilt $x \leq_1 z_2 \Rightarrow y_1 \leq_1 x \leq_1 z_2$ mit $y_1, z_2 \in A \Rightarrow x \in H_1(A)$. Also gilt $H_1(H_1(A)) \subseteq H_1(A)$.
3. Analog zu a).
4. *Extensivität:* Sei $x \in A$. Da \leq_2 reflexiv, gilt $x \leq_2$, also $x \in H_2(A)$ und somit $A \subseteq H_2(A)$.
Monotonie: Sei $A \subseteq B$ und $x \in H_2(A) \Rightarrow$ es gibt $y \in A$ mit $y \leq_2 x \Rightarrow$ es gibt $y \in B$ mit $y \leq_2 x \Rightarrow x \in H_2(B)$.
Idempotenz: Zu zeigen ist $H_2(A) = H_2(H_2(A))$. $H_2(A) \subseteq H_2(H_2(A))$ folgt aus Extensivität und Monotonie.
Sei $x \in H_2(H_2(A)) \Rightarrow$ es gibt $y \in H_2(A)$ mit $y \leq_2 x \Rightarrow$ es gibt $y' \in A$ mit $y' \leq_2 y \Rightarrow$ da $y' \leq_2 y$ und $y \leq_2 x$ gilt $y' \leq_2 x$ mit $y' \in H_2(A) \Rightarrow x \in H_2(A)$. Also gilt $H_2(H_2(A)) \subseteq H_2(A)$.

7.8.6 Hullen und Gruppoide

1. Sei $A = \{3\}$, dann ist $E^0(A) = \{3\}$, $E^1(A) = (E^0 \circ E)(A) = \{3, 3^2\}$, $E^2(A) = (E^1 \circ E)(A) = \{3, 3^2, 3^3, 3^4\}$, Also gilt, nach Satz 7, $\langle A \rangle_{G_1} = \bigcup_{i=1}^{\infty} E^i(A) = \{3^i \mid i \geq 1\}$.
2. Sei $A = \{1\}$, dann ist $E^0(A) = \{1\}$, $E^1(A) = \{1, 2\}$, $E^2(A) = \{1, 2, 3, 4\}$, $E^3(A) = \{1, 2, 3, 4, 5, 6, 7, 8\}$, Also gilt, nach Satz 7, $\langle A \rangle_{G_2} = \bigcup_{i=1}^{\infty} E^i(A) = \mathbb{N} \setminus \{0\}$.
3. Sei $A = \{\emptyset, \{0\}, \{1\}, \{2\}, \dots, \{n-1\}\}$, dann ist $E^0(A) = \{\emptyset, \{0\}, \{1\}, \{2\}, \dots, \{n-1\}\}$, $E^1(A) = \{B \mid B \subseteq 2^{[n]}, |B| \leq 2\}$, $E^2(A) = \{B \mid B \subseteq 2^{[n]}, |B| \leq 4\}$, Also gilt, nach Satz 7, $\langle A \rangle_{G_3} = \bigcup_{i=1}^{\infty} E^i(A) = 2^{[n]}$.

7.8.7 Zur Implementierung des Relationenprodukts

Sind $X, Y \in \{0, 1\}^{[m] \times [m]}$, so definiere die Abbildung $Z : [m] \times [m] \rightarrow \{0, 1\}$ durch

$$Z(i, j) := \max\{\min(X(i, k), Y(k, j)) \mid k \in [m]\}$$

für alle $i, j \in [m]$. Setze nun $X \cdot Y := Z$ (Matrixprodukt). Definiere ferner $(h(R))(i, j) = 1$ gdw. $(\phi(i), \phi(j)) \in R$, wobei $\phi : [m] \rightarrow M$ eine beliebige aber feste Bijektion ist. Zu zeigen bleibt:

- h ist eine Bijektion.
- h ist ein Gruppoide-Homomorphismus.

Die Assoziativität des Matrixproduktes folgt aus einem bekannten Satz (welchem genau?).

7.8.8 Äquivalenzhüllen: Charakterisierung

Beweis: Da $\langle R \rangle_{Eq}$ symmetrisch ist und R umfasst, ist $R \cup R^- \subseteq \langle R \rangle_{Eq}$. Da $\langle R \rangle_{Eq}$ überdies Quasiordnung, gilt $(R \cup R^-)^* \subseteq \langle R \rangle_{Eq}$.

Wir zeigen die umgekehrte Inklusion, indem wir nachweisen, dass die Quasiordnung $(R \cup R^-)^*$ symmetrisch ist, denn $\langle R \rangle_{Eq}$ ist ja Teilmenge jeder R enthaltenen Äquivalenzrelation.

Betrachte $(x, y) \in \langle R \rangle_{Eq}$. Wegen Satz 3.8.14 gibt es ein k mit $(x, y) \in (R \cup R^-)^k$. $k = 0$ ist trivial.

Also gibt es $k - 1$ Brückenelemente x_1, \dots, x_{k-1} mit $(x_i, x_{i+1}) \in (R \cup R^-)$ (für $i = 0, \dots, k - 1$) mit $x = x_0$ und $y = x_k$). Da R symmetrisch, gilt mithin: $(x_{i+1}, x_i) \in (R \cup R^-)$ für $i \in [k]$.

Da $(R \cup R^-)^*$ transitiv, folgt $(y, x) \in \langle R \rangle_{Eq}$. \square

7.8.9 Äquivalenzhüllen

Für die allgemeine Aussage dürfen Sie natürlich Lemma 3.8.8 verwenden. Für die speziellere Aussage betrachten Sie nochmals die Übung 6.5.3. Dort waren ja alle Äquivalenzrelationen beschrieben worden, die als Ergebnis der Hüllberechnung in Frage kommen.

Kapitel 8

Ergänzende algebraische Gedanken

8.1 Boolesche Algebra

Dieser Abschnitt will eine Brücke schlagen zwischen der Einführung in die Logik und der Mengenalgebra und allgemeiner den algebraischen Überlegungen, wie wir sie bislang hier kennengelernt haben. Wir orientieren uns hier an [33], auch wenn wir die ein oder andere Verkürzung in Kauf nehmen. Im Gegensatz zu den früheren Abschnitten gibt es keine (gesonderten) Übungsaufgaben. Jedoch lassen sich (wie oft in mathematische Texte) Übungsaufgaben leicht selbst erzeugen, indem man beispielsweise zunächst selbst versucht, gewisse Beweise zu führen, bevor man die Ausführungen im Skript liest.

Auch wenn die Darstellung hier abstrakter ist als im Kapitel über Mengenlehre, sollte es Ihnen nicht allzu schwer fallen, dieses Kapitel eigenständig durchzuarbeiten. Eine Motivation mag der Hinweis geben, dass der Umfang dieses Kapitels (und von Kapitel 3.1) im Wesentlichen dem eines für den Oberstufenunterricht in Mathematik entworfenen “Themenheftes” [30] entspricht.

8.1.1 Definition und Beispiele

Wir werden in der folgenden grundlegenden Definition auf Aspekte von Syntax und Semantik getrennt eingehen, um die Zusammenhänge mit den andernorts kurz besprochenen allgemeinen Algebren herauszustreichen.

Definition 8.1.1 Eine Boolesche Algebra ist beschrieben durch ein 6-Tupel $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$:

Hierbei ist:

B die Grundmenge,

$\oplus, \otimes : B \times B \rightarrow B$ sind zweistellige Verknüpfungen auf B ,

$\kappa : B \rightarrow B$ ist eine einstellige Operation auf B , und

$0, 1 \in B$ sind Konstanten (nullstellige Operationen).

Wir fordern als Eigenschaften:

- $0 \neq 1$;

- Kommutativgesetze: (1) $\forall a, b \in B : a \oplus b = b \oplus a$, (2) $\forall a, b \in B : a \otimes b = b \otimes a$;
- Distributivgesetze: (1) $\forall a, b, c \in B : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ und
(2) $\forall a, b, c \in B : a \oplus (b \otimes c) = (a \oplus b) \otimes (a \oplus c)$;
- Neutralitätsgesetze: (1) 0 ist rechtsneutrales Element bzgl. \oplus , d.h.: $a \oplus 0 = a$ und (2) 1 ist rechtsneutrales Element bzgl. \otimes , d.h.: $a \otimes 1 = a$;
- Komplementgesetze: (1) $\kappa(a)$ ist das Komplement von a , d.h.: (1) $a \oplus \kappa(a) = 1$ und (2) $a \otimes \kappa(a) = 0$.

0 heißt auch Nullelement, 1 Einselement von B .

Das Dualitätsprinzip Eine Eigenschaft P Boolescher Algebren kann naturgemäß mit Hilfe der Operationen $\oplus, \otimes, \kappa, 0, 1$ ausgedrückt werden.

Eigenschaft P' heißt *dual* zu P , falls sie aus P durch gleichzeitiges und durchgängiges Vertauschen aller \oplus und \otimes -Operatoren sowie aller Konstanten 0 und 1 entsteht. Aus der Symmetrie der Definition ergibt sich unmittelbar das *Dualitätsprinzip*:

- Mit der Eigenschaft P gilt auch stets die duale Eigenschaft P' .

Morphismen Wir hatten zuvor den Begriff des Morphismus, also der strukturerhaltenden Abbildung, kennengelernt. Was bedeutet dies für Boolesche Algebren?

Definition 8.1.2 $B = (B, \oplus, \otimes, \kappa, 0, 1)$ und $B' = (B', \oplus', \otimes', \kappa', 0', 1')$ seien Boolesche Algebren. $h : B \rightarrow B'$ heißt B.A.-Morphismus gdw.

1. $\forall a, b \in B : h(a \oplus b) = h(a) \oplus' h(b)$;
2. $\forall a, b \in B : h(a \otimes b) = h(a) \otimes' h(b)$;
3. $\forall a \in B : h(\kappa(a)) = \kappa'(h(a))$; sowie
4. $h(0) = 0'$ und $h(1) = 1'$.

Ein bijektiver B.A.-Morphismus heißt auch B.A.-Isomorphismus.

Lemma 8.1.1 Für B.A.-Morphismen genügt der Nachweis von (1), (2) und (4).

Beweis: (3) folgt aus der Eindeutigkeit des Komplements in B' . □

Hinweis: (2) lässt sich oft “dual” zu (1) zeigen. Weiß man jedoch (3), kann man aber immer auf den Nachweis von entweder (1) oder (2) verzichten aufgrund der de Morganschen Gesetze.

Wie in Satz 3.7.9 kann man zeigen:

Lemma 8.1.2 Die Umkehrung eines B.A.-Isomorphismus ist ein B.A.-Isomorphismus.

Das Dualitätsprinzip kann man nun auch wie folgt deuten:

Satz 8.1.3 Der Komplementoperator κ kann als Isomorphismus aufgefasst werden.

Beweis: Betrachte B.A. $B = (B, \oplus, \otimes, \kappa, 0, 1)$. $B' = (B, \otimes, \oplus, \kappa, 1, 0)$ heißt auch *duale Boolesche Algebra*. $\kappa : B \rightarrow B$ ist offenbar bijektiv. Die Morphismuseigenschaften ergeben sich aus den Gesetzen von De Morgan. □

Schaltalgebra $(\{0, 1\}, \vee, \wedge, \neg, 0, 1)$ ist eine Boolesche Algebra. In der Schreibweise $(\{0, 1\}, +, \cdot, \neg, 0, 1)$ heißt sie auch *Schaltalgebra*.

Satz 8.1.4 Die Schaltalgebra ist (bis auf Isomorphie) die kleinste Boolesche Algebra.

Beweis: Die Eigenschaften einer Booleschen Algebra sind für die Schaltalgebra aus der Logik-Vorlesung bekannt.¹ Da $0 \neq 1$ stets zwei verschiedene Elemente mit definierten Eigenschaften sind, folgt die Minimalität und Eindeutigkeit. \square

Potenzmengenalgebren Aus Abschnitt 3.1 wissen wir:

Satz 8.1.5 Für jede Menge $M \neq \emptyset$ bildet $(2^M, \cup, \cap, \neg, \emptyset, M)$ eine Boolesche Algebra, die so genannte Potenzmengenalgebra (über M). (Das Komplement ist bezüglich M zu verstehen.)

Zum Beweis erinnere man: die Sätze 3.1.15, 3.1.17 sowie Lemmata 3.1.10, 3.1.11 und 3.1.20.

Lemma 8.1.6 Die Potenzmengenalgebra einer einelementigen Menge ist isomorph zur Schaltalgebra.

Teileralgebra als etwas ungewöhnlicheres Beispiel:

Betrachte $T(n) := \{k \in \mathbb{N} \mid k|n\}$, also die Menge der Teiler von n .

$\text{kgV}(a, b)$: das kleinste gemeinsame Vielfache von a und b

$\text{ggT}(a, b)$: der größte gemeinsame Teiler von a und b

Definiere für $a \in T(n)$: $u_n(a) := n/a$.

Problem: Ist, für $n \geq 2$, $T(n) = (T(n), \text{ggT}, \text{kgV}, u_n, n, 1)$ stets eine Boolesche Algebra?

Wenn $T(n)$ B.A., so nennen wir sie *Teileralgebra*.

Beobachte: Die betrachtete Schaltalgebra ist zu $T(2)$ isomorph:

$\text{ggT}(1, 1) = \text{ggT}(1, 2) = \text{ggT}(2, 1) = 1, \text{ggT}(2, 2) = 2$.

$\text{kgV}(1, 1) = 1, \text{kgV}(1, 2) = \text{kgV}(2, 1) = \text{kgV}(2, 2) = 2$.

Wir überprüfen die geforderten Eigenschaften.

$0 \neq 1$: Da $n \geq 2$, gilt $1 \neq n$. Dies ist stets erfüllt.

Kommutativgesetze: (1) $\forall a, b \in T(n) : \text{ggT}(a, b) = \text{ggT}(b, a)$, (2) $\forall a, b \in B : \text{kgV}(a, b) = \text{kgV}(b, a)$.

Nach Def. von kgV und ggT kommt es offenbar nicht auf die Reihenfolge der Argumente an. Die Kommutativität gilt also immer.

Neutralitätsgesetze: (1) $\forall a|n : \text{ggT}(a, n) = a$. (2) $\forall a|n : \text{kgV}(a, 1) = a$. Auch dies gilt immer.

Distributivgesetze: (1) $\forall a, b, c \in T(n) : \text{kgV}(a, \text{ggT}(b, c)) = \text{ggT}(\text{kgV}(a, b), \text{kgV}(a, c))$.

Betrachte Zahl t mit $t| \text{kgV}(a, \text{ggT}(b, c))$.

t lässt sich schreiben als $t = pq$ mit $p|a$ und $q| \text{ggT}(b, c)$.

Wegen $p|a$ gilt: $p| \text{kgV}(a, x)$ für jedes x , und somit $p| \text{ggT}(\text{kgV}(a, b), \text{kgV}(a, c))$.

$q| \text{ggT}(b, c) \rightsquigarrow (q|b) \wedge (q|c) \rightsquigarrow (q| \text{kgV}(a, b)) \wedge (q| \text{kgV}(a, c)) \rightsquigarrow$

$t| \text{ggT}(\text{kgV}(a, b), \text{kgV}(a, c))$ mit $t = pq$; insbesondere $t = \text{kgV}(a, \text{ggT}(b, c))$.

¹Wir verweisen auch auf die Einführung von Verknüpfungstafeln anhand Boolescher Operationen in Abschnitt 3.7.1.

Umgekehrt: Betrachte Zahl t mit $t \mid ggT(kgV(a, b), kgV(a, c))$.

Dann gilt: $t \mid kgV(a, b)$ und $t \mid kgV(a, c)$.

t lässt sich schreiben als $t = pq$ mit $p \mid a$ und $q \mid b$.

t lässt sich schreiben als $t = p'q'$ mit $p' \mid a$ und $q' \mid c$.

Mit $p'' = kgV(p, p')$ haben wir eine weitere Darstellung $t = p''q''$ mit $p'' \mid a$.

Aus der Aufteilung der Primfaktoren von t ergibt sich sofort: $q'' = ggT(q, q')$.

Es gilt: $q'' \mid ggT(b, c)$, denn $((q \mid b) \wedge (q' \mid c)) \implies (ggT(q, q') \mid ggT(b, c))$.

Aus $p'' \mid a$ und $q'' \mid ggT(b, c)$ folgt für $t = p''q''$: $t \mid kgV(a, ggT(b, c))$.

(2) $\forall a, b, c \in T(n) : ggT(a, kgV(b, c)) = kgV(ggT(a, b), ggT(a, c))$.

Der Beweis folgt ganz analog.

Also gelten die Distributivgesetze immer.

Komplementgesetze: (1) $ggT(a, u_n(a)) = ggT(a, n/a) = 1$.

Das gilt nur für jedes $a \mid n$, falls es keine Quadratzahl größer 1 gibt, die n teilt. (Dann jedoch ist es klar.) (2) sieht man entsprechend.

Alles zusammen genommen zeigen unsere Überlegungen:

Satz 8.1.7 $T(n)$ ist eine Boolesche Algebra genau dann, wenn es keine Zahl größer 1 gibt, deren Quadrat n teilt.

Boolesche Algebren aus Booleschen Algebren : Funktionenalgebren. Erinnern Sie hierzu die in Abschnitt 3.7.1 betrachteten Funktionengruppoide. In gewissem Sinne ist das im Folgende Eingeführte spezieller. (Begründen Sie diese Aussage.)

Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra.

$B_n := B^{B^n}$ bezeichne die n -stelligen Booleschen Funktionen.

Definiere für $f, g \in B_n$ folgende Operationen:

$$(f \star g)(x_1, \dots, x_n) := f(x_1, \dots, x_n) \oplus g(x_1, \dots, x_n)$$

$$(f \odot g)(x_1, \dots, x_n) := f(x_1, \dots, x_n) \otimes g(x_1, \dots, x_n)$$

$$(\Gamma(f))(x_1, \dots, x_n) := \kappa(f(x_1, \dots, x_n))$$

0 und 1 sollen der Einfachheit halber auch die n -stelligen Funktionen bezeichnen, die konstant 0 bzw. 1 liefern. Mit Blick auf den folgenden Satz heißtt

$$\mathcal{B}_n = (B_n, \star, \odot, \Gamma, 0, 1)$$

die *Funktionenalgebra* zu \mathcal{B} .

Satz 8.1.8 Für $n \in \mathbb{N}$ ist $\mathcal{B}_n = (B_n, \star, \odot, \Gamma, 0, 1)$ eine Boolesche Algebra. Diese ist für $n = 0$ zu \mathcal{B} isomorph.

Was wäre also noch zu zeigen?

Ausdruck-Algebra Die Menge WAA_n der wohlgeformten aussagenlogischen Ausdrücke (w.a.A.) über n aussagenlogischen Variablen $X_n = \{x_1, \dots, x_n\}$ ist wie folgt induktiv definiert:

- Die Wahrheitswerte 0 und 1 sind w.a.A.
- Ist x_i eine aussagenlogische Variable, so ist x_i ein w.a.A.
- Ist p ein w.a.A., so auch $\neg p$.
- Sind p, q w.a.A., so auch $(p \wedge q), (p \vee q), (p \implies q), (p \iff q)$.

- Nichts anderes sind w.a.A.

Eine *Belegung* β eines w.a.A. $\alpha \in WAA_n$ ist eine Abbildung $\{x_1, \dots, x_n\} \rightarrow \{0, 1\}$. Der Wahrheitswert $\beta(\alpha)$ ergibt sich entlang der induktiven Definition der w.a.A. wie folgt:

- $\beta(0) = 0, \beta(1) = 1$.
- Für eine aussagenlogische Variable x_i ist $\beta(x_i)$ explizit gegeben.
- Ist p ein w.a.A., so ist $\beta(\neg p) := \neg(\beta(p))$.
- Sind p, q w.a.A., so ist $\beta((p \wedge q)) := \beta(p) \wedge \beta(q), \beta((p \vee q)) := \beta(p) \vee \beta(q), \beta((p \Rightarrow q)) := \beta(p) \Rightarrow \beta(q), \beta((p \Leftrightarrow q)) := \beta(p) \Leftrightarrow \beta(q)$.

Zwei w.a.A. α, α' heißen *äquivalent*, falls $\beta(\alpha) = \beta(\alpha')$. Als Kern von β handelt es sich hierbei um eine Äquivalenzrelation. Es sei A_n die Menge aller Äquivalenzklassen von w.a.A. mit Variablenmenge $X_n = \{x_1, \dots, x_n\}$.

Die Äquivalenzklasse von α werde $[\alpha]$ notiert.

Definiere: $[\alpha] \sqcup [\alpha'] := [(\alpha) \vee (\alpha')], [\alpha] \sqcap [\alpha'] := [(\alpha) \wedge (\alpha')], C_n([\alpha]) := [\neg \alpha]$.

Satz 8.1.9 Für jedes $n \in \mathbb{N}$ ist $\mathcal{A}_n = (A_n, \sqcup, \sqcap, C_n, [0], [1])$ eine Boolesche Algebra. Diese ist für $n = 0$ zur Schaltalgebra isomorph.

8.1.2 Rechengesetze in Booleschen Algebren

Distributivgesetze Boolesche Algebren sind für uns die ersten algebraischen Strukturen, in denen zwei zweistellige Operationen auftreten. Daher sind (erst) hierfür Distributivgesetze sinnvoll zu fordern. Sie kennen diese allerdings von den Rechengesetzen über Zahlen, wie sie aus der Schule bekannt sind, und auch die Rechenregeln für Mengen enthielten derartige Gesetze.

Satz 8.1.10 In einer Booleschen Algebra gelten neben den genannten noch weitere Distributivgesetze: (1a) $\forall a, b, c \in B : (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$ und (2a) $\forall a, b, c \in B : (b \otimes c) \oplus a = (b \oplus a) \otimes (c \oplus a)$

Beweis: Insgesamt dreimalige Anwendung des Kommutativgesetzes (für \otimes) und einmalige Anwendung des Distributivgesetzes (1) liefert:

$$(b \oplus c) \otimes a = a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c) = (b \otimes a) \oplus (c \otimes a).$$

Aussage (2a) folgt mit dem Dualitätsprinzip. \square

Mit Induktion kann (leicht?) folgende Verallgemeinerung bewiesen:

Satz 8.1.11 In einer Booleschen Algebra gilt:

$$(a \oplus (b_1 \otimes b_2 \otimes \dots \otimes b_\ell)) = (a \oplus b_1) \otimes (a \oplus b_2) \otimes \dots \otimes (a \oplus b_\ell)$$

sowie die duale Aussage.

Neutrale Elemente Da \otimes und \oplus kommutative zweistellige Verknüpfungen sind, können wir mit Lemma 3.7.1 schlussfolgern:

Satz 8.1.12 (1) Das Nullelement ist eindeutig bestimmt und ist auch ein linksneutrales Element bzgl. \oplus . (2) Das Einselement ist eindeutig bestimmt und ist auch ein linksneutrales Element bzgl. \otimes . \square

Idempotenz

Satz 8.1.13 In jeder Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ sind sowohl \oplus als auch \otimes idempotent.

Beweis: Aufgrund des Dualitätsprinzips brauchen wir die Aussage nur für eine der Operationen zu zeigen.

$$\begin{aligned}
 x \otimes x &= (x \otimes x) \oplus 0 && \text{Neutralitätsgesetz} \\
 &= (x \otimes x) \oplus (x \otimes \kappa(x)) && \text{Komplementgesetz} \\
 &= x \otimes (x \oplus \kappa(x)) && \text{Distributivgesetz} \\
 &= x \otimes 1 && \text{Komplementgesetz} \\
 &= x && \text{Neutralitätsgesetz}
 \end{aligned}$$

□

Dominanz

Satz 8.1.14 In jeder Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gelten zwei Dominanzgesetze: $a \oplus 1 = 1$ und $a \otimes 0 = 0$.

Beweis: Aufgrund des Dualitätsprinzips brauchen wir die Aussage nur für eine der Operationen zu zeigen.

$$\begin{aligned}
 a \oplus 1 &= (a \oplus 1) \otimes 1 && \text{Neutralitätsgesetz} \\
 &= (a \oplus 1) \otimes (a \oplus \kappa(a)) && \text{Komplementgesetz} \\
 &= a \oplus (1 \otimes \kappa(a)) && \text{Distributivgesetz} \\
 &= a \oplus \kappa(a) && \text{Neutralitätsgesetz} \\
 &= 1 && \text{Komplementgesetz}
 \end{aligned}$$

□

Absorption

Satz 8.1.15 In jeder Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gelten zwei Verschmelzungsgesetze (Absorptionsgesetze): $a \oplus (a \otimes b) = a$ und $a \otimes (a \oplus b) = a$.

Beweis: Aufgrund des Dualitätsprinzips brauchen wir die Aussage nur für eine der Operationen zu zeigen.

$$\begin{aligned}
 a \oplus (a \otimes b) &= (a \otimes 1) \oplus (a \otimes b) && \text{Neutralitätsgesetz} \\
 &= a \otimes (1 \oplus b) && \text{Distributivgesetz} \\
 &= a \otimes (b \oplus 1) && \text{Kommutativgesetz} \\
 &= a \otimes 1 && \text{Dominanzgesetz} \\
 &= a && \text{Neutralitätsgesetz}
 \end{aligned}$$

□

Zur Vereinfachung von Gleichungen

Satz 8.1.16 In jeder Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ kann man aus $b \oplus a = c \oplus a$ und aus $b \oplus \kappa(a) = c \oplus \kappa(a)$ auf $b = c$ schließen.

Hinweis: Natürlich gibt es auch eine duale Vereinfachungsregel. Wie lautet sie?

Beweis: Zunächst eine Vorüberlegung. Es sei $x \in B$ beliebig.

$$\begin{aligned}
 (x \oplus a) \otimes (x \oplus \kappa(a)) &= x \oplus (a \otimes \kappa(a)) && \text{Distributivgesetz} \\
 &= x \oplus 0 && \text{Komplementgesetz} \\
 &= x && \text{Neutralitätsgesetz}
 \end{aligned}$$

Nach Voraussetzung gilt $b \oplus a = c \oplus a$ und $b \oplus \kappa(a) = c \oplus \kappa(a)$.

Damit gilt auch: $(b \oplus a) \otimes (b \oplus \kappa(a)) = (c \oplus a) \otimes (c \oplus \kappa(a))$.

Nach der Vorüberlegung ist die linke Seite der Gleichung gleich b und die rechte gleich c . Dies liefert die Behauptung. \square

Abgeleitete Monoide

Satz 8.1.17 Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Dann bilden $\mathcal{B}_+ = (B, \oplus, 0)$ und $\mathcal{B}_* = (B, \otimes, 1)$ kommutative Monoide.

Beweis: Zu zeigen bleibt das Assoziativitätsgesetz.

Beweisgedanke: Wir zeigen zunächst zwei Hilfsaussagen:

- (1) $\forall a, b, c \in B : ((a \oplus b) \oplus c) \otimes a = (a \oplus (b \oplus c)) \otimes a$ und
- (2) $\forall a, b, c \in B : ((a \oplus b) \oplus c) \otimes \kappa(a) = (a \oplus (b \oplus c)) \otimes \kappa(a)$.

Aus der Vereinfachungsregel folgt dann die Behauptung. \square

Wir beweisen jetzt die zwei Hilfsaussagen.

Hilfsaussage (1) zum Assoziativitätsgesetz:

$$\begin{aligned}
 ((a \oplus b) \oplus c) \otimes a &= a \otimes ((a \oplus b) \oplus c) && \text{Kommutativgesetz} \\
 &= (a \otimes (a \oplus b)) \oplus (a \otimes c) && \text{Distributivgesetz} \\
 &= a \oplus (a \otimes c) && \text{Absorptionsgesetz} \\
 &= a && \text{Absorptionsgesetz} \\
 &= a \otimes (a \oplus (b \otimes c)) && \text{Absorptionsgesetz} \\
 &= (a \oplus (b \otimes c)) \otimes a && \text{Kommutativgesetz}
 \end{aligned}$$

Hilfsaussage (2) zum Assoziativitätsgesetz:

$$\begin{aligned}
 ((a \oplus b) \oplus c) \otimes \kappa(a) &= \kappa(a) \otimes ((a \oplus b) \oplus c) && \text{Kommutativgesetz} \\
 &= (\kappa(a) \otimes (a \oplus b)) \oplus (\kappa(a) \otimes c) && \text{Distributivgesetz} \\
 &= ((\kappa(a) \otimes a) \oplus (\kappa(a) \otimes b)) \oplus (\kappa(a) \otimes c) && \text{Distributivgesetz} \\
 &= (0 \oplus (\kappa(a) \otimes b)) \oplus (\kappa(a) \otimes c) && \text{Komplementgesetz} \\
 &= (\kappa(a) \otimes b) \oplus (\kappa(a) \otimes c) && \text{Komplementgesetz} \\
 &= \kappa(a) \otimes (b \oplus c) && \text{Distributivgesetz} \\
 &= 0 \oplus (\kappa(a) \otimes (b \oplus c)) && \text{Neutralitätsgesetz} \\
 &= (\kappa(a) \otimes a) \oplus (\kappa(a) \otimes (b \oplus c)) && \text{Komplementgesetz} \\
 &= \kappa(a) \otimes (a \oplus (b \oplus c)) && \text{Distributivgesetz} \\
 &= (a \oplus (b \oplus c)) \otimes \kappa(a) && \text{Kommutativgesetz}
 \end{aligned}$$

Anmerkungen zum Komplement

Satz 8.1.18 (Eindeutigkeit des Komplements) In einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: Aus $a \oplus b = 1$ und $a \otimes b = 0$ folgt $b = \kappa(a)$.

Beweis: Aus $a \oplus b = 1$ folgt durch Multiplikation von $\kappa(a)$ von links (linke Seite):

$$\kappa(a) \otimes (a \oplus b) = (\kappa(a) \otimes a) \oplus (\kappa(a) \otimes b) = 0 \oplus (\kappa(a) \otimes b) = \kappa(a) \otimes b.$$

Die rechte Seite ergibt: $\kappa(a) \otimes 1 = \kappa(a)$.

Aus $\kappa(a) \oplus a = 1$ folgt durch Multiplikation von b von rechts (linke Seite):

$$(\kappa(a) \oplus a) \otimes b = (\kappa(a) \otimes b) \oplus (a \otimes b) = (\kappa(a) \otimes b) \oplus 0 = \kappa(a) \otimes b.$$

Die rechte Seite ergibt: $1 \otimes b = b$.

Das ergibt zusammen: $\kappa(a) \otimes b = \kappa(a) = b$. \square

Hinweis: Überlegen Sie genau: Welche Rechengesetze wurden im Beweis angewendet?

Satz 8.1.19 (*Regeln von De Morgan*) In einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: $\kappa(a \oplus b) = \kappa(a) \otimes \kappa(b)$ und dual: $\kappa(a \otimes b) = \kappa(a) \oplus \kappa(b)$.

Beweis: Wir benutzen den Satz von der Eindeutigkeit des Komplements im Beweis.

$$\begin{aligned} (a \oplus b) \otimes (\kappa(a) \otimes \kappa(b)) &= (a \otimes (\kappa(a) \otimes \kappa(b))) \oplus (b \otimes (\kappa(a) \otimes \kappa(b))) \\ &= (a \otimes (\kappa(a) \otimes \kappa(b))) \oplus (b \otimes (\kappa(b) \otimes \kappa(a))) \\ &= ((a \otimes \kappa(a) \otimes \kappa(b))) \oplus ((b \otimes \kappa(b)) \otimes \kappa(a)) \\ &= 0 \oplus 0 = 0 \\ (a \oplus b) \oplus (\kappa(a) \otimes \kappa(b)) &= (a \oplus b \oplus \kappa(a)) \otimes (a \oplus b \oplus \kappa(b)) \\ &= 1 \otimes 1 = 1 \end{aligned}$$

□

Lemma 8.1.20 (*Komplementarität der neutralen Elemente*) $\kappa(0) = 1$ und $\kappa(1) = 0$.

Beweis: Neutralitätsgesetze liefern: $0 \oplus 1 = 1$ und $0 \otimes 1 = 0$; Komplementgesetze ergeben $0 \oplus \kappa(0) = 1$ und $0 \otimes \kappa(0) = 0$, woraus mit der Eindeutigkeit des Komplements die eine Behauptung folgt; die andere folgt dual. □

Satz 8.1.21 (*Gesetz vom doppelten Komplement*) In einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: $\kappa(\kappa(a)) = a$.

Beweis: Aus dem Komplementgesetz (einmal für a und dann für $\kappa(a)$) und dem Kommutativitätsgesetz folgt: $\kappa(a) \oplus a = 1$ und $\kappa(a) \otimes \kappa(\kappa(a)) = 1$ sowie $\kappa(a) \otimes a = 0$ und $\kappa(a) \otimes \kappa(\kappa(a)) = 0$, woraus mit der Eindeutigkeit des Komplements die Behauptung folgt. □

8.1.3 Halbordnungen auf Booleschen Algebren

Wegen Satz 3.7.20 können wir festlegen:

Definition 8.1.3 Auf einer B.A. $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ kann durch $a \leq b$ gdw. $a \oplus b = b$ eine Halbordnung auf B definiert werden (die von B.A. induzierte Halbordnung).

Die Betrachtung der dualen Booleschen Algebra liefert sofort eine weitere Halbordnung \geq auf B . Also: $x \geq y$ gdw. $x \otimes y = y$. Im Folgenden betrachten wir $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ bzw. dual $\mathcal{B}_d = (B, \otimes, \oplus, \kappa, 1, 0)$ mit den Halbordnungen \leq bzw. \geq auf B .

Satz 8.1.22 $\forall x, y \in B : (x \leq y) \iff (y \geq x)$.

Beweis: Es gelte $x \leq y$, d.h.: $x \oplus y = y$. Absorptionsgesetz $\sim x \otimes (x \oplus y) = x$, also $x \otimes y = x$ wegen $x \leq y$. Also folgt $y \geq x$ aus $x \leq y$. Das Dualitätsprinzip liefert die Umkehrung. □

Folgerung 8.1.23 $\forall x, y \in B : (x \leq y) \iff (\kappa(y) \leq \kappa(x))$.

Satz 8.1.24 In der von einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ induzierten Halbordnung \leq gibt es stets ein kleinstes und ein größtes Element, nämlich 0 und 1 .

Beweis: Dies folgt sofort aus $0 \oplus x = x$ (Neutralitätsgesetz) und $x \oplus 1 = 1$ (Dominanzgesetz). \square

Beispiel: Für die Potenzmengenalgebra ist \subseteq die induzierte Halbordnung (bzw. dual dazu \supseteq). Kleinstes Element von \subseteq ist \emptyset , größtes Element das Universum.

Satz 8.1.25 In der von einer Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ induzierten Halbordnung \leq gilt: $x \leq y$ gdw. $x \otimes \kappa(y) = 0$ gdw. $\kappa(x) \oplus y = 1$.

Beweis: $x \leq y$ heißt nach Def. $x \oplus y = y$. Komplementieren der beiden Seiten liefert mit dem De Morganschen Gesetz: $\kappa(x) \otimes \kappa(y) = \kappa(y)$. Multiplikation von links mit x liefert: $x \otimes (\kappa(x) \otimes \kappa(y)) = x \otimes \kappa(y)$. Das Assoziativitätsgesetz zusammen mit dem Komplementgesetz ergibt: $0 = x \otimes \kappa(y)$, woraus nach De Morgan $\kappa(x) \oplus y = 1$ folgt.

Die Umkehrung folgt aus $0 = x \otimes \kappa(y)$ durch Addition von y : $y = 0 \oplus y$ (linke Seite) sowie für die rechte:

$$(x \otimes \kappa(y)) \oplus y = (x \oplus y) \otimes (\kappa(y) \oplus y) = (x \oplus y) \otimes 1 = x \oplus y.$$

Prüfen Sie: Welche Gesetze wurden verwendet? \square

Interpretation des Satzes in der Mengenlehre für $A, B \subseteq M$:
 $\overline{A} \subseteq B$ gdw. $\overline{A} \cap (M \setminus B) = \emptyset$ gdw. $(M \setminus A) \cup B = M$.

Satz 8.1.26 Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Dann gelten die folgenden Regeln:

1. $\forall x, y \in B : (x \otimes y \leq x \wedge x \leq x \oplus y)$;
2. $\forall x, y \in B : (x \otimes y \leq y \wedge y \leq x \oplus y)$;
3. Für $x, y \in B$ gilt: Aus $x \leq y$ und $x \leq \kappa(y)$ folgt: $x = 0$.

Beweis: ad 1.: $\kappa(x \otimes y) \oplus x = (\kappa(x) \oplus \kappa(y)) \oplus x = (\kappa(x) \oplus x) \oplus \kappa(y) = 1 \oplus \kappa(y) = 1$.

$x \oplus (x \oplus y) = (x \oplus x) \oplus y = x \oplus y$, also $x \leq x \oplus y$.

ad 2.: Beachte Kommutativgesetze

ad 3.: $x = x \otimes \kappa(y) = (x \otimes y) \otimes \kappa(y) = 0$. \square

Atome und Hyperatome

Definition 8.1.4 Ein Element a in einer B.A. $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$, das nicht kleinstes Element ist, heißt irreduzibel oder unzerlegbar, falls aus $a = x \oplus y$ folgt $a = x$ oder $a = y$. Mit der induzierten Halbordnung \leq können wir definieren: $p \in B$, $p \neq 0$, heißt Atom gdw. $\forall a \in B : 0 \leq a \leq p \Rightarrow (a = 0 \vee a = p)$. Atome in der dualen B.A. heißen auch Hyperatome.

Im Hasse-Diagramm einer B.A. sind die Atome genau die direkten Nachfolger des Nullelements.

Primzahlen sind Hyperatome in der Teileralgebra.

Satz 8.1.27 Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Dann ist p Atom gdw. p irreduzibel ist.

Beweis: (1) Es sei p ein Atom und betrachte $p = x \oplus y$. Per def. gilt: $x \leq x \oplus y$. Da $x \oplus y$ Atom, gilt $x = p$ oder $x = 0$. Falls nun $x = 0$, so $y = p$. Daher gilt: $x = p$ oder $y = p$, d.h., $p = x \oplus y$ ist unzerlegbar.

(2) Ist p unzerlegbar, so ist zum einen $p \neq 0$. Angenommen, p wäre kein Atom. Dann gäbe es ein q mit $0 < q < p$ (hierbei: $<:= \leq \cap \neq$). Damit gilt: $p = q \oplus p = (q \oplus p) \otimes 1 = (q \oplus p) \otimes (q \oplus \kappa(q)) = q \oplus (p \otimes \kappa(q))$. Da p irreduzibel und da $p \neq q$, folgt $p = p \otimes \kappa(q)$, also $p \leq \kappa(q)$. Da \leq transitiv, folgt $q \leq \kappa(q)$, also $q = q \otimes \kappa(q) = 0$, Widerspruch! \square

Lemma 8.1.28 Sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Ist $a \in B$ Atom und $x \in B$ beliebig, so gilt: $a \otimes x = 0$ oder $a \otimes x = a$.

Satz 8.1.29 Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Ist $a \in B$ Atom und $x \in B$ beliebig, so gilt: $a \otimes x = 0$ gdw. $a \otimes \kappa(x) = a$.

Beweis: Angenommen, $a \otimes \kappa(x) = a$, also $a \leq \kappa(x)$. Wäre $a \otimes x \neq 0$, so folgt mit Lemma 8.1.28 $a \otimes x = a$, da a Atom; also $a \leq x$. Eigenschaft 3 aus Satz 8.1.26 liefert $a = 0$ im Widerspruch dazu, dass a Atom.

Angenommen, $a \otimes x = 0$, also $a \leq \kappa(x)$. Gölte außerdem $a \otimes \kappa(x) \neq a$, also wegen $a \otimes \kappa(x) \leq a$ (nach Eigenschaft 1 aus Satz 8.1.26) $a \otimes \kappa(x) = 0$, da a Atom, so hätten wir $a \leq x$. Eigenschaft 3 aus Satz 8.1.26 liefert $a = 0$ im Widerspruch dazu, dass a Atom. \square

Satz 8.1.30 Es sei $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ eine Boolesche Algebra. Ist $a \in B$ Atom und $x \in B$ beliebig, so gilt: Entweder $a \leq x$ oder $a \leq \kappa(x)$, aber nicht beides zugleich.

Beweis: Gölte beides zugleich, zu folgte $a = 0$ mit Eigenschaft 3 aus Satz 8.1.26, im Widerspruch zur Atom-Eigenschaft von a . Gilt nicht $a \leq x$, so gilt nicht $a \otimes \kappa(x) = 0$, also gilt mit Satz 8.1.29 $a \otimes \kappa(x) \neq a$. Da a Atom und mit Eigenschaft 1 aus Satz 8.1.26 $a \otimes \kappa(x) \leq a$, folgt $a \otimes \kappa(x) = 0$, also $a \leq \kappa(x)$. \square

Darstellungssatz

Satz 8.1.31 In einer endlichen Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: $x \in B$ lässt sich schreiben als: $x = a_1 \oplus \dots \oplus a_k$, wobei $\{a_1, \dots, a_k\}$ die Menge der Atome a ist, für die $a \leq x$ gilt. Diese Darstellung ist sogar eindeutig.

Beweis: Es bezeichne $\sigma_x = a_1 \oplus \dots \oplus a_k$. Wir zeigen $x \leq \sigma_x$ und $\sigma_x \leq x$, woraus die Behauptung aufgrund der Antisymmetrie von \leq folgt. Mit Satz 8.1.11 können wir schreiben:

$$\begin{aligned} x \otimes \sigma_x &= x \otimes (a_1 \oplus \dots \oplus a_k) \\ &= (x \otimes a_1) \oplus (x \otimes a_2) \oplus \dots \oplus (x \otimes a_k) \\ &= a_1 \oplus a_2 \oplus \dots \oplus a_k \\ &= \sigma_x \end{aligned}$$

Also gilt: $\sigma_x \leq x$.

$$x \otimes \kappa(\sigma_x) = x \otimes \kappa(a_1) \otimes \kappa(a_2) \otimes \dots \otimes \kappa(a_k)$$

Gölte $x \otimes \kappa(\sigma_x) \neq 0$, so gäbe es ein Atom $a \in B$ mit $a \leq x \otimes \kappa(\sigma_x)$, da \mathcal{B} endlich (Beweis? Am einfachsten über Irrduzibilitätseigenschaft!). Das bedeutet: $a = a \otimes x \otimes \kappa(\sigma_x)$. Annahme: $a = a \otimes x$, also $a \leq x$. Dann wäre $a = a_j$ für einer der Summanden.

Also gölte dann: $a = a_j = a_j \otimes x \otimes \kappa(\sigma_x) = a_j \otimes x \otimes \kappa(a_j) \otimes \kappa(\sigma_x) = 0$, denn $\kappa(a_j)$ steckt ja ausgeschrieben in der Produktdarstellung von $\kappa(\sigma_x)$. Dies steht im Widerspruch zu a Atom. Mit dem vorigen Satz gilt, da Annahme $a \leq x$ falsch: $a \leq \kappa(x)$, also $a \otimes \kappa(x) = a$. Dies führt ebenfalls zu einem Widerspruch: $a = a \otimes x \otimes \kappa(\sigma_x) = a \otimes \kappa(x) \otimes x \otimes \kappa(\sigma_x) = 0$, also kann es solch ein Atom a nicht geben, d.h., $x \otimes \kappa(\sigma_x) = 0$, also $x \leq \sigma_x$. Zur Eindeutigkeit: Angenommen, x könne man durch zwei Atom-Summen σ und $\sigma' = a_1 \oplus \dots \oplus a_k$ darstellen. Dann gäbe es in einer der beiden Summen, z.B. σ ein Atom $a \leq x = \sigma'$, das in der anderen, σ' , nicht vorkäme. Daher gilt:

$$a = a \otimes \sigma' = (a \otimes a_1) \oplus \dots \oplus (a \otimes a_k), \quad k \geq 2$$

Mit Lemma 8.1.28 haben wir $a \otimes a_j = 0$ für alle j , denn sonst wäre ja a in der Atom-Summe σ' enthalten. Daher ist die rechte Seite eine Summe von Nullen, also $a = 0$ im Widerspruch dazu, dass a Atom ist. \square

Aus dem Idempotenzgesetz folgt mit ein wenig Kombinatorik (Bit-Vektoren !):

Folgerung 8.1.32 *Besitzt eine Boolesche Algebra n Atome, so hat sie genau 2^n Elemente.*

Mit der Auffassung von κ als B.A.-Isomorphismus folgt sofort.

Folgerung 8.1.33 *In einer endlichen Booleschen Algebra $\mathcal{B} = (B, \oplus, \otimes, \kappa, 0, 1)$ gilt: $x \in B$ lässt sich (bis auf die Reihenfolge sogar in eindeutiger Weise) schreiben als: $x = a_1 \otimes \dots \otimes a_k$, wobei $\{a_1, \dots, a_k\}$ die Menge der Hyperatome a ist, für die $a \geq x$ gilt.*

Ferner sind die Hyper-Atome von \mathcal{B} gerade die Komplemente der Atome von \mathcal{B} . Daher hat \mathcal{B} genauso viele Atome wie Hyperatome, sagen wir n Stück. Damit gilt dann $|B| = 2^n$.

Hyper-Atome heißen daher auch *Atomkomplemente*.

Im Sinne von Abschnitt 3.8 können wir aussprechen:

Folgerung 8.1.34 *Eine endliche Boolesche Algebra ist das Erzeugnis ihrer Atome (bzw. Hyper-Atome).*

Daher übernimmt die Menge der Atome die Rolle einer Basis (wie sie aus der Linearen Algebra bekannt sein sollte). Insbesondere gilt:

Folgerung 8.1.35 *Ein B.A.-Morphismus von einer endlichen B.A. in eine andere B.A. ist schon eindeutig durch die Angabe seiner Werte bei den Atomen (oder auch bei den Hyper-Atomen) festgelegt.*

Wir hatten im Abschnitt 3.7.1 den Begriff des Funktionengruppoids kennengelernt. Diesem Konzept folgend, sollten wir “eigentlich” versuchen, B^M zu einer B.A. zu machen für eine beliebige Menge M , nicht “nur” für $M = B^n$. Aufgrund der Wichtigkeit für die Anwendungen beschränken wir uns im Folgenden aber auf den genannten Spezialfall. Der Leser sei ermuntert, das allgemeinere Konzept zu studieren und zu schauen, inwiefern oder auch in welcher Weise die folgenden Aussagen für den allgemeineren Fall Gültigkeit besitzen.

Satz 8.1.36 *Für $n \in \mathbb{N}$ ist $\mathcal{B}_n = (B_n, \star, \odot, \Gamma, 0, 1)$ eine Boolesche Algebra. Diese ist für $n = 0$ zu \mathcal{B} isomorph.*

Am bekanntesten ist die Funktionenalgebra zur Schaltalgebra \mathbf{B} : Dies liefert die n -stellige Boolesche Schaltfunktionen B_n . \leq entspricht hier dem positionsweisen Vergleich der Funktionswerte. Atome sind hier genau die Funktionen, deren Funktionswert nur für genau ein Argument 1 (w) ist uns sonst immer 0. So gibt es in B_2 daher beispielsweise genau vier Atome. Wer schon etwas zur Schaltalgebra im Rahmen der Technischen Informatik oder auch im Rahmen einer Einführung in die Logik gehört hat, dem wird die Wichtigkeit der Booleschen Schaltfunktionen, die genau für ein Argument 1 bzw. 0 liefern, bewusst sein. Genau diese daher wohl geläufigen Darstellungssätze werden wir im Folgenden verallgemeinern.

Satz 8.1.37 $\forall n : A_n$ und B_n sind isomorph.

Beweis: Da die Mengen A_n durch äquivalente w.a.A. bestimmt sind und diese Äquivalenz wiederum durch die Gleichheit der Werte definiert ist, die sich beim Einsetzen gleicher Variablenbelegungen ergeben, ist klar, dass jeder w.a.A. $\alpha \in A_n$ eine n -stellige Boolesche Schaltfunktion beschreibt.

Umgekehrt lässt sich jede Boolesche Schaltfunktion als Summe von Atomen in der Funktionenalgebra ausdrücken. Ein Atom lässt sich durch einen Ausdruck der Form $\ell_1 \wedge \dots \wedge \ell_n$ beschreiben mit $\ell_i = x_i$ oder $\ell_i = \bar{x}_i$: genau für eine Variablenbelegung wird der Ausdruck wahr.

Man mache sich klar, dass hierdurch tatsächlich ein Isomorphismus beschrieben wird. \square

Bezeichnungen: Die ℓ_i nennt man auch *Literale*; ein Produkt (also eine Konjunktion) von Literalen heißt auch *Minterm*; taucht in einem Minterm jede Variable genau einmal vor, spricht man auch von einem *vollständigen Minterm*.

Folgerung 8.1.38 Jeder Boolesche Ausdruck ist äquivalent zu einer Summe vollständiger Minterme.

Eine Konjunktion von Literalen heißt auch manchmal *Konjunktionsterm*, und ein Ausdruck, der eine Disjunktion von Konjunktionstermen ist, heißt in *disjunktiver Normalform (DNF)*.

Folgerung 8.1.39 Zu jedem w.a.A. existiert ein äquivalenter in disjunktiver Normalform.

Eine Summe (Disjunktion) von Literalen heißt auch *Maxterm* oder *Disjunktionsterm* oder *Klausel*; taucht in einem Maxterm jede Variable genau einmal vor, spricht man auch von einem *vollständigen Maxterm*; ein Ausdruck, der eine Konjunktion von Disjunktionstermen ist, heißt in *konjunktiver Normalform (KNF)*.

Folgerung 8.1.40 Zu jedem w.a.A. existiert ein äquivalenter in konjunktiver Normalform.

Folgerung 8.1.41 Jeder Boolesche Ausdruck ist äquivalent zu einer Summe vollständiger Minterme, und diese Darstellung ist kanonisch in dem Sinne, dass sie bis auf Anwenden des Kommutativitätsgesetzes bei Summe und Produkt eindeutig ist, sobald man z.B. positive Literale stets vor negativen sortiert.

Eine entsprechende Aussage gilt für die Darstellung durch Produkte vollständiger Maxterme.

Beide kanonische Darstellungen gestatten sodann einen einfachen Äquivalenz-Test für Boolesche Ausdrücke.

Kapitel 9

Schrifttum

Die Literatur zu dem Thema ist vielschichtig. Wir empfehlen jedem Leser, wenigstens eines der im Verlauf dieses Skripts besprochenen Bücher als ergänzende Begleitlektüre auszuwählen.

Wir werden im Folgenden noch ein paar weitere Bücher kurz besprechen. Die Geschmäcker sind bekanntlich verschieden, und das gilt auch für die Darstellung von mathematischen Inhalten. Das werden Sie spüren, wenn Sie sich auf eines der Bücher näher einlassen. Die Besprechung erhebt keinerlei Anspruch auf Vollständigkeit, ja angesichts des Reichtums der Bücher zu diesem Thema hat sie wohl auch einen gewissen zufälligen Charakter, da sie doch die Werke hervorhebt, die dem Autor gerade zu Gebote standen.

- Manchen von Ihnen mögen Bücher entgegenkommen, die den Stoff dieser Veranstaltung ausführlicher und mit (viel) mehr Beispielen dargestellt wissen wollen. Beispiele für einen derartigen Schreibstil bieten die Bücher von Dean [9], Haggarty [21] Ross und Wright [36] oder auch von Townsend [40]. Die beiden erstgenannten Bücher decken aber ähnlich wie das (aber auch dünne) Buch von Hower [24] nur Teileaspekte dieser Vorlesung ab.
- Einen gänzlich anderen Blick auf den Stoff dieses Skripts, der Veranstaltung “Einführung in die Logik” und sogar der ersten Hälfte von “Automaten und Formale Sprachen” bietet das Buch von Kastens und Kleine Büning [27], da alles aus der (Anwendungs-)Perspektive der Modellierung betrachtet wird.
- Andere Bücher mit verwandtem Titel enthalten doch deutlich mehr und auch weiteren Stoff, wie das Buch von Aigner [1], das zweibändige Werk von Dierkert, Kufleitner und Rosenberger [13, 12] oder auch das Buch von Struckmann und Wätjen [39]. Diese Bücher können aber oft mit Gewinn für und im Hinblick auf andere Veranstaltungen gelesen werden und lassen entsprechende Querverbindungen erkennen, z.B. zur Kryptologie oder zur (Linearen) Algebra. Ähnliches gilt (sogar) für das knappe Taschenbuch von Berendt [5].

Literaturverzeichnis

- [1] AIGNER, M.: *Diskrete Mathematik*. 5. Auflage. vieweg studium, Wiesbaden, 2004
- [2] AIGNER, M. ; ZIEGLER, G. M.: *Das BUCH der Beweise*. Springer, 2010
- [3] BEAUDRY, M. ; DUBÉ, D. ; DUBÉ, M. ; LATENDRESSE, M. ; TESSON, P.: Conservative groupoids recognize only regular languages. In: *Information and Computation* 239 (2014), S. 13–28
- [4] BEKOS, M. A. ; KAUFMANN, M. ; KRUG, R. ; NÄHER, S. ; ROSELLI, V.: Slanted Orthogonal Drawings. In: WISMATH, S. (Hrsg.) ; WOLFF, A. (Hrsg.): *Graph Drawing — 21st International Symposium, GD Bd. 8242*, Springer, 2013 (LNCS), S. 424–435
- [5] BERENDT, G.: *Mathematische Grundlagen für Informatiker; Band 1: Diskrete Mathematik*. BI Wissenschaftsverlag Mannheim / Wien / Zürich, 1989
- [6] CANTOR, G.: *Grundlagen einer allgemeinen Mannigfaltigkeitslehre*. Leipzig: Teubner, 1883
- [7] CANTOR, G.: Beiträge zur Begründung der transfiniten Mengenlehre. In: *Mathematische Annalen* 46 (1895), November, Nr. 4, S. 481–512
- [8] CIOABA, S. M. ; MURTY, M. R.: *trim: Text and Readings in Mathematics*. Bd. 55: *A First Course in Graph Theory and Combinatorics*. Hindustan Book Agency, 2009
- [9] DEAN, N.: *Diskrete Mathematik*. Pearson Studium, 2003
- [10] DEDEKIND, R.: *Was sind und was sollen die Zahlen?* 1. Auflage. Braunschweig, 1888
- [11] DENECKE, K.: *Algebra und Diskrete Mathematik für Informatiker*. Teubner Stuttgart · Leipzig · Wiesbaden, 2003
- [12] DIEKERT, V. ; KUFLEITNER, M. ; ROSENBERGER, G.: *Diskrete algebraische Methoden: Arithmetik, Kryptographie, Automaten und Gruppen*. Walter de Gruyter, 2013
- [13] DIEKERT, V. ; KUFLEITNER, M. ; ROSENBERGER, G.: *Elemente der Diskreten Mathematik: Zahlen und Zählen, Graphen und Verbände*. Walter de Gruyter, 2013

- [14] DUJMOVIĆ, V. ; FERNAU, H. ; KAUFMANN, M.: Fixed parameter algorithms for one-sided crossing minimization revisited. In: LIOTTA, G. (Hrsg.): *Graph Drawing, 11th International Symposium GD 2003* Bd. 2912, Springer, 2004 (LNCS), S. 332–344
- [15] ENGELKING, R.: *Sigma Series in Pure Mathematics*. Bd. 6: *General Topology*. Berlin: Heldermann, 1989
- [16] FREGE, G.: Über Sinn und Bedeutung. In: *Zeitschrift für Philosophie und philosophische Kritik* (1892), S. 25–50
- [17] FRINK, O.: A Proof of the Maximal Chain Theorem. In: *American Journal of Mathematics* (1952), S. 676–678
- [18] GILLMAN, L.: Two classical surprises concerning the axiom of choice and the continuum hypothesis. In: *American Mathematical Monthly* 109 (2002), S. 544–553
- [19] GÖRG, C. ; BIRKE, P. ; POHL, M. ; DIEHL, S.: Dynamic Graph Drawing of Sequences of Orthogonal and Hierarchical Graphs. In: PACH, J. (Hrsg.): *Graph Drawing, 12th International Symposium, GD* Bd. 3383, Springer, 2004 (LNCS), S. 228–238
- [20] GRAHAM, R. ; KNUTH, D. E. ; PATASHNIK, O.: *Concrete Mathematics*. 3. edition. Reading, MA: Addison-Wesley, 1989
- [21] HAGGARTY, R.: *Diskrete Mathematik für Informatiker*. Pearson Studium, 2004
- [22] HARTOGS, F. M.: Über das Problem der Wohlordnung. In: *Math. Ann.* (1915)
- [23] HINKIS, A.: *Proofs of the Cantor-Bernstein Theorem: A Mathematical Excursion*. Springer, 2013
- [24] HOWER, W.: *Diskrete Mathematik; Grundlage der Informatik*. Oldenbourg, 2010
- [25] IHRINGER, T.: *Allgemeine Algebra*. Stuttgart: Teubner, 1988
- [26] IHRINGER, T.: *Diskrete Mathematik*. Stuttgart: Teubner, 1994
- [27] KASTENS, U. ; BÜNING, H. K.: *Modellierung; Grundlagen und formale Methoden*. Hanser, 2005
- [28] KURATOWSKI, C.: Sur la notion d'ensemble fini. In: *Fundamenta Mathematicae* 1 (1920), S. 129–131
- [29] KURATOWSKI, K.: Sur l'opération $\bar{\wedge}$ de l'Analysis Situs. In: *Fundamenta Mathematicae* 3 (1922), S. 182–199
- [30] LESKY, P. ; ULSHÖFER, K. ; CHRISTMANN, N.: *Boolesche Algebra*. Ernst Klett Verlag, Stuttgart, 1976
- [31] MASON, J. ; BURTON, L. ; STACEY, K.: *Mathematisch denken; Mathematik ist keine Hexerei*. 4. Auflage. Oldenbourg Verlag, 2006
- [32] MATOUŠEK, J.: *Thirty-three Miniatures: Mathematical and Algorithmic Applications of Linear Algebra*. American Mathematical Society, AMS, 2010 (Student Mathematical Library)

- [33] MEINEL, C. ; MUNDHENK, M.: *Mathematische Grundlagen der Informatik; Mathematisches Denken und Beweisen; Eine Einführung*. 2. Auflage. Teubner, 2002
- [34] PETERSEN, J.: Die Theorie der regulären graphs. In: *Acta Mathematica* 15 (1891), Nr. 1, S. 193–220. <http://dx.doi.org/10.1007/BF02392606>. – DOI 10.1007/BF02392606. – ISSN 0001–5962
- [35] RINOW, W.: *Hochschulbücher für Mathematik*. Bd. 79: *Lehrbuch der Topologie*. Berlin: Deutscher Verlag der Wissenschaften, 1975
- [36] ROSS, K. A. ; WRIGHT, C. R. B.: *Discrete Mathematics*. 3. edition. Prentice Hall, Eaglewood Cliffs, 1992
- [37] SCHMIDT, G. ; STRÖHLEIN, T.: *Relationen und Graphen*. Springer-Verlag, 1989 (Mathematik für Informatiker)
- [38] SCHÖNING, U.: *Logik für Informatiker*. 4. Auflage. Spektrum Verlag, 1995
- [39] STRUCKMANN, W. ; WÄTJEN, D.: *Mathematik für Informatiker – Grundlagen und Anwendungen*. 1. Auflage. Spektrum Akademischer Verlag, Heidelberg, 2007
- [40] TOWNSEND, M.: *Discrete Mathematics: Applied Combinatorics and Graph Theory*. The Benjamin / Cummings Publishing Company, 1987
- [41] TURAU, V.: *Algorithmische Graphentheorie*. 3. Auflage. Oldenbourg Verlag München, 2009
- [42] VOLKMANN, L.: *Graphen und Digraphen; eine Einführung in die Graphentheorie*. Springer-Verlag, 1991
- [43] WAGNER, K.: *Graphentheorie*. Bibliographisches Institut Mannheim / Wien / Zürich, B.I.-Wissenschaftsverlag, 1970