

Walter Hower  
**Diskrete Mathematik**  
De Gruyter Studium

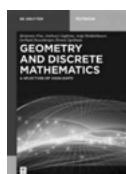
## Weitere empfehlenswerte Titel



*A Primer in Combinatorics*

Alexander Kheyfits, 2021

ISBN 978-3-11-075117-8, e-ISBN 978-3-11-075118-5



*Geometry and Discrete Mathematics*

*A Selection of Highlights*

Benjamin Fine, Anthony Gaglione, Anja Moldenhauer, Gerhard Rosenberger, Dennis Spellman, 2018

ISBN 978-3-11-052145-0, e-ISBN 978-3-11-052150-4



*Maschinelles Lernen*

Ethem Alpaydin, 2019

ISBN 978-3-11-061788-7, e-ISBN 978-3-11-061789-4



*Grundlagen der Informatik*

Heinz-Peter Gumm, Manfred Sommer

*Band 1 Programmierung, Algorithmen und Datenstrukturen*, 2016

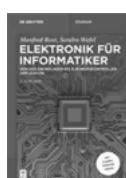
ISBN 978-3-11-044227-4, e-ISBN 978-3-11-044226-7

*Band 2 Rechnerarchitektur, Betriebssysteme, Rechnernetze*, 2017

ISBN 978-3-11-044235-9, e-ISBN 978-3-11-044236-6

*Band 3 Formale Sprachen, Compilerbau, Berechenbarkeit und Komplexität*, 2019

ISBN 978-3-11-044238-0, e-ISBN 978-3-11-044239-7



*Elektronik für Informatiker*

*Von den Grundlagen bis zur Mikrocontroller-Applikation*

Manfred Rost, Sandro Wefel, 2021

ISBN 978-3-11-060882-3, e-ISBN 978-3-11-060906-6

Walter Hower

# Diskrete Mathematik

---

Grundlage der Informatik

**DE GRUYTER**  
OLDENBOURG

## **Autor**

Professor Dr. rer. nat. Walter Hower, Diplom-Informatiker, Studium (Schwerpunkt Künstliche Intelligenz, Nebenfach Wirtschaftswissenschaften) und Promotion (im Schnittfeld Kombinatorische Optimierung / Künstliche Intelligenz) in Informatik; 1996/’97 Senior Research Scientist (Forschunggruppenleiter in einem EU-Projekt) und Honorary Visiting Lecturer (Artificial Intelligence, Knowledge-Based Systems), University College Cork, National University of Ireland, Hobby-Fußballer (Mittel-Stürmer) Kinsale A.F.C.; später, seit Herbst 2002 Professor in Baden-Württemberg, Landes-Lehrpreis 2006; 2009 bundesweit 3. Platz Professor des Jahres Ingenieurwissenschaften/ Informatik (UNICUM Stiftung gGmbH); Vertrauens-Dozent der Gesellschaft für Informatik; Forschungs-Interessen: KI, Kombinatorische Optimierung unter Rand-Bedingungen („constraint satisfaction“), kooperative und nicht-kooperative Spiel-Theorie.

ISBN 978-3-11-069554-0  
e-ISBN (PDF) 978-3-11-069555-7  
e-ISBN (EPUB) 978-3-11-069567-0

**Library of Congress Control Number: 2021942361**

### **Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.dnb.de> abrufbar.

© 2022 Walter de Gruyter GmbH, Berlin/Boston  
Druck und Bindung: CPI books GmbH, Leck  
Coverabbildung: Walter Hower

[www.degruyter.com](http://www.degruyter.com)

Für meine Fans — und die Tapferen, welche es noch werden wollen ☺



# Vorspann zur 2. Auflage

Auf vielfachen Wunsch hin habe ich die Ehre, mein Erst(lings)-Werk neu auflegen zu dürfen. Neben der Verbesserung mancher Details im Hauptteil ergänzte ich im Anhang die zugehörigen Lösungen und fügte weitere Aufgaben (nun gleich mitsamt ihren Auflösungen  $\ddot{\text{S}}$ ) sowie ein sicherlich hilfreiches Sachwort-Register hinzu.

Dank allen Beteiligten — meinen Töchtern für ihre begleitende Ermunterung, meiner Frau für ihren fürsorglichen Hinweis auf mein Arbeitszimmer, meinem Bruder für seine spitzen Kommentare (die mich erst recht nach vorne trieben) und selbstredend dem Verlag für die professionelle Lehrbuch-Umsetzung.<sup>1</sup>

Möge dieser hiermit lesbar gewordene L<sup>A</sup>T<sub>E</sub>Xt (wieder  $\ddot{\text{S}}$ ) Wissen mit Spaß vermitteln.

WHo

---

<sup>1</sup>Nicht zu vergessen: dem Leben allgemein, das es letztlich ja noch gut mit mir meint



# Vorwort zur 1. Auflage

Die Informatik hat die Mathematik zur Technologie gemacht. Auf der einen Seite nutzt sie mathematische Konzepte in unterschiedlichsten Anwendungen, andererseits bereichert sie die Mathematik durch neue Konzepte und Erkenntnisse. Heute gibt es kaum Teilbereiche der Mathematik, deren Methoden im Zusammenhang mit der Informatik in irgendwelchen technischen Anwendungen oder der wissenschaftlichen Forschung nicht angewendet werden. Unter diesen vielen Mathematikkenntnissen gibt es ein paar Grundbereiche, die für die Kerninformatik unumgänglich sind und mit denen jede Informatikerin und jeder Informatiker vertraut sein muss. Gerade diesen zentralen Themen ist das Lehrbuch von Walter Hower gewidmet.

Die Mathematik zu vermitteln bedeutet, die grundlegenden Konzepte und Begriffe zu bilden und ihre Methoden zu präsentieren. Das Lehrbuch fängt mit der Darstellung von Funktionen und Relationen an, fährt fort mit der Mengenlehre und steigert das Thema zum Konzept von Cantor hinsichtlich des Vergleichs unendlicher Größen, der Basis für die Untersuchung der Grenze der Automatisierbarkeit in der Informatik. Das nächste Kapitel, Boolesche Algebra, liefert die Grundlagen der Logik, die für jeden Wissenschaftler unabdingbar sind. Das darauf folgende Kapitel behandelt die korrekte Argumentation in Form von mathematischen Beweisen; hier kommen sowohl der direkte als auch der indirekte Beweis zum Tragen, ebenso die Induktion. Danach folgendes Thema ist den Zähltechniken mit dem Fokus auf der Kombinatorik gewidmet. Das Lehrbuch schließt mit der diskreten Wahrscheinlichkeitstheorie.

Das ganze Buch trägt die klare Unterschrift des Autoren, mindestens für diejenigen, die ihn kennen. Dazu gehören die Präzision und Sinn für das Ganze sowie für das Detail. Die Begeisterung des Verfassers für den zu vermittelnden Stoff kann nicht übersehen werden. Begleitet mit dem entsprechenden Tempo und hoher Prägnanz ist es eine ausgezeichnete Quelle für die Vermittlung der Grundlagen der Mathematik für Informatiker.

Juraj Hromkovič

ETH Zürich



# Inhaltsverzeichnis

<b>0</b>	<b>Einführung</b>	<b>1</b>
<b>1</b>	<b>Grundstock</b>	<b>3</b>
1.1	Basis .....	3
1.2	Funktionen .....	4
1.3	Relationen .....	8
<b>2</b>	<b>Mengen-Lehre</b>	<b>13</b>
2.1	Grundlagen .....	13
2.2	Begriffe .....	15
2.3	Gesetzmäßigkeiten .....	18
2.4	Kardinalität Endlicher Mengen .....	20
2.5	Über-/Abzählbarkeit Unendlicher Mengen .....	25
<b>3</b>	<b>Boolesche Algebra</b>	<b>29</b>
3.1	Begriffe .....	29
3.2	Werte-Tafeln .....	29
3.2.1	Grund-Muster .....	29
3.2.2	Belegungs-Möglichkeiten .....	33
3.3	Gesetzmäßigkeiten .....	33
<b>4</b>	<b>Beweis-Prinzipien</b>	<b>35</b>
4.1	Induktion .....	35
4.1.1	Natürliche Zahlen .....	35
4.1.2	Wort-Längen .....	44
4.2	Direkter Beweis .....	46
4.3	Indirekter Beweis .....	47

<b>5</b>	<b>Zähl-Techniken</b>	<b>49</b>
5.1	Grundlegendes .....	49
5.1.1	Summen-Regel .....	49
5.1.2	Produkt-Regel .....	50
5.1.3	Quotienten-Regel .....	51
5.1.4	Schubfach-Prinzip .....	51
5.2	Ein-/Ausschluss .....	52
5.3	Rekurrenz-Relation .....	55
5.4	Reihenfolgen und Auswählen .....	73
5.4.1	Permutationen .....	73
5.4.2	Kombinationen .....	76
5.5	Stirling- und Bell-Zahlen .....	83
5.5.1	Stirling-Zahlen 1. Art .....	83
5.5.2	Stirling-Zahlen 2. Art .....	86
5.5.3	Bell-Zahlen .....	89
<b>6</b>	<b>Wahrscheinlichkeits-Theorie</b>	<b>93</b>
6.1	Allgemeine Wahrscheinlichkeit .....	93
6.2	Bedingte Wahrscheinlichkeit .....	97
<b>A</b>	<b>Anhang</b>	<b>101</b>
A.1	Übung: Grundstock .....	101
A.2	Übung: Mengen-Lehre .....	103
A.3	Übung: Boolesche Algebra .....	106
A.4	Übung: Beweis-Prinzipien .....	110
A.5	Übung: Zähl-Techniken .....	112
A.6	Übung: Wahrscheinlichkeits-Theorie .....	114
<b>B</b>	<b>Bonus-Track</b> ☺	<b>117</b>
B.1	Übung: Grundstock .....	117
B.2	Übung: Mengen-Lehre .....	119
B.3	Übung: Boolesche Algebra .....	121
B.4	Übung: Beweis-Prinzipien .....	123
B.5	Übung: Zähl-Techniken .....	125
B.6	Übung: Wahrscheinlichkeits-Theorie .....	127

<b>Literaturverzeichnis</b>	<b>129</b>
-----------------------------	------------

<b>Register</b>	<b>131</b>
-----------------	------------



# 0 Einführung

Das vorliegende Buch korrespondierte mal zu meiner gleichnamigen Erst-Semester-Vorlesung, die von 150 englisch-sprachigen Beamer-Folien getragen wurde. Dies bewog mich dazu, auch hier die Terminologie teilweise in Englisch zu fassen — neben dem „Seiten-Effekt“ der einfacheren Erschließung der internationalen Standard-Literatur, aus der ich eine kleine Auswahl am Ende aufgelistet habe, einschließlich eines Werkes in Französisch, für unsere frankophonen Freunde und Freundinnen ☺. (Manchmal unterschlage ich die weibliche Schreib-Form aus Bequemlichkeit und auch im Hinblick auf’s flüssige Lesen; dass die „Ladies“\* mitgemeint sind, ist eine Selbstverständlichkeit.)

Für viele Studierende ist *Diskrete Mathematik* „hartes Brot“; dieses Buch will helfen, den manchmal abstrakten Formalismus gutmütig aufnehmen zu können. Dazu habe ich einen speziellen Präsentations-Stil entwickelt, der den Stoff ☺ hoffentlich schmackhaft darbietet. (Natürlich ist Vieles längst nicht so dramatisch wie hier und da zugespitzt, erst recht nicht für uns Insider; ich adressier’s ja hauptsächlich an Informatik/Math-Interessierte und Studierende in der Eingangs-Phase — ok, auch an Fach-Kolleg\*en, die dieses Büchlein empfehlen mögen. ☺) Somit sollte sich das vorliegende Teil auch „stand-alone“ nutzen lassen, ohne interaktives Erlebnis im Hörsaal oder synchroner Online-Session. Meine Studierenden mögen mir nachsehen, dass ich längst nicht alle Schenkel-Klopfer in den Text einstreuen konnte; trotz vorliegendem Skript-Buch jedoch wird’s in der Vorlesung nicht langweilig. Wie bei manchem Smiley: Da bleibt nicht nur kein Auge trocken (Bemerkung für den „inner circle“). ☺

Der Aufbau hier läuft nicht zwingend entlang einer historischen Schiene oder einer womöglich sonst üblichen Reihenfolge gehorchend; er dient lediglich einem gewissen Pragmatismus. Hier und da wird mit einem erst später präzisierten Begriff vorgegriffen und Menschen-Verstand zugeschaltet (ohne an Genauigkeit verlieren zu wollen); ein hoch-axiomatisch eingefärbtes Werk für die werdende Mathematikerin war nicht geplant. Bei der Themen-Auswahl ließ ich mich vom Bedarf für ein Informatik-Studium leiten. Gerade dort muss peinlichst auf eine saubere Notation geachtet werden — dies einzuüben sollte mit diesem Buch gelingen.

Im grundlegenden ersten Kapitel beginnen wir mit den natürlichen Zahlen, führen Funktionen ein und beleuchten die Welt der Relationen. Im zweiten Kapitel legen wir die Grundlagen der Mengen-Lehre, stellen weiterführende Begriffe vor, präsentieren innenwohnende Gesetzmäßigkeiten und räsonieren über die Größen-Ordnung sowohl endlicher als auch unendlicher Mengen. (Diese Betrachtung der Unendlichkeit bereitet den Boden für ein intuitiveres Verständnis der Unberechenbarkeit in der Theoretischen Informatik.) Das dritte Kapitel behandelt die *Boolesche Algebra*. Begrifflichkeiten und Gesetze werden dargelegt sowie die entsprechenden Werte-Tafeln aufgestellt; interessant zu erwähnen sind die Formeln für die Anzahl möglicher Belegungen und Funktionen. Das

vierte Kapitel beherbergt die gängigsten Beweis-Prinzipien. Dargeboten werden die Induktion sowohl auf natürlichen Zahlen als auch auf Zeichen-Ketten sowie der direkte und der indirekte Beweis. Mit dem fünften Kapitel geht's dann auf die Achterbahn  $\leadsto$  der Zähl-Techniken. Hier finden sich Summen-, Produkt- und Quotienten-Regel ebenso ein wie das Schubfach-Prinzip und der Mechanismus des Ein-/Ausschlusses. Die dort folgende Rekurrenz-Relation lässt sich als Kreativitäts-Werkzeug einsetzen, um bei einer Zähl-Aufgabe auf eine geschlossene Formel hoffen zu dürfen. Es kommen noch Reihenfolge- und Auswahl-Problem-Lösungen an die Reihe, mitsamt Permutations- und Binomial-Koeffizienten. Als Schmankerl biete ich zusätzlich die Stirling-Zahlen erster und zweiter Art, also Zyklus- bzw. Teilmengen-Zahlen, und die Bell-Zahlen an. Das sechste Kapitel mit der allgemeinen und bedingten Wahrscheinlichkeits-Theorie (einschließlich des obligatorischen Ziegen-Problems  $\leadsto$ ) liefert den Show-down.

Es ist ein recht handliches Exemplar geworden; dies sollte Sie/dich dazu verführen, das Buch gerne zu nutzen. Trotz des übersichtlichen Umfangs, vielleicht gerade wegen der Mühe, prägnant und ohne unnötigen Ballast formulieren zu wollen, war es ein kleines Stück Arbeit. Auf diesem Weg dahin haben mich einige mir wohlgesonnene Geister begleitet. Selbstredend sind meine Eltern zu nennen, von denen wenigstens meine Mutter das End-Produkt im wahrsten Sinne des Wortes noch sehen möge.<sup>1</sup> Meine Mathematik-Lehrer/innen (und die -Professoren im Informatik-Studium an der Uni Kaiserslautern) haben natürlich fachlichen Anteil, ohne deren Esprit ich es nicht bis zu diesem Werk gebracht hätte; Robert Kirsch, dem ich dieses Buch ebenfalls widme, hätte es sicher gern noch erlebt. Im privaten Bereich profitiere ich, auch emotional, stark von meiner Familie; meine drei Girlies tragen immer motivierend bei. Nicht ganz unerwähnt lassen möchte ich die professionelle Umgebung, in der man zumindest nicht behindert werden sollte; dieses Umfeld ist mir derzeit vergönnt. Mein Dank gilt auch meinem Fach-Kollegen Juraj Hromkovič, der sich freundlicherweise die Zeit nahm, das Vorwort der Erst-Auflage zu übernehmen. Meine Studierenden, mit denen ich ja schon einiges durchmache<sup>2</sup>  $\leadsto$ , taten ein Übriges: sie wollen die gesprochenen Sätze fixiert haben und dieses Traktat als Souvenir — voilà!

Spätestens zum Ende hin schlägt die Stunde des Verlags. Mein Dank geht an's gesamte Lektorats-Team für die Koordination des Projekts sowie an die Truppe im LATEX-Steinbruch für die damals sehr hilfreiche Herstellung meiner handgezeichneten Vorlagen.

So ist es vollbracht; viel Spaß mit *Diskrete Mathematik — Grundlage der Informatik* !

---

<sup>1</sup>Sollte es für mich 'ne enge Kiste  $\leadsto$  werden, handhabt's einfach wie an folgender Stelle geschildert: **Informatik Spektrum** (Juni-Ausgabe 2008) 31(3):274, oberes Drittel, rechte Spalte, letzter Satz.

<sup>2</sup>Diese Binär-Relation ist weder *symmetrisch* noch *asymmetrisch* und auch nicht *anti-symmetrisch*; siehe das nun folgende Start-Kapitel.

# 1 Grundstock

Wir beginnen ganz harmlos mit den Grundlagen des Gebiets. Fundamental sind sicher die Peano-Axiome zusammen mit der Menge der natürlichen Zahlen; dies ist gleich Gegenstand des ersten Abschnitts. Im zweiten Abschnitt besprechen wir den Funktions-Begriff mitsamt einigen speziellen Ausprägungen. Im dritten Abschnitt widmen wir uns den Relationen; dies schließt das allgemeine  $n$ -stellige Cartesische Produkt ebenso ein wie das Konzept des Verbands mit seiner Partial-Ordnung. Dieses erste Kapitel möge zum mentalen „Booten“<sup>1</sup> reichen.

## 1.1 Basis

Wir führen die *natürlichen Zahlen* ein und beleuchten die fünf Peano-Axiome.

Mit  $\mathcal{N}$  bezeichnen wir die (unendlich große) Menge der Natürlichen Zahlen ;  $\mathcal{N} :=^2 \{0, 1, 2, 3, \dots\}$ . Für Informatiker unerlässlich ist es, als kleinste Zahl die „0“ zu nehmen — weshalb wir der Bequemlichkeit halber erst gar nicht die Bezeichnung  $\mathcal{N}_0$  bemühen. Festgehalten wurde dies bereits von Guiseppe Peano in seinen Axiomen :

1. „0“ ist eine natürliche Zahl.
2. „0“ ist nicht Nachfolger ( $:= n+1$ ) einer natürlichen Zahl ( $n$ ).
3. Jeder natürlichen Zahl  $n$  folgt genau eine Nachfolger-Zahl  $n + 1$ .
4. Verschiedene natürliche Zahlen haben verschiedene Nachfolger-Zahlen.
5. Wenn in einem Teil-Bereich  $T$  („ $\subseteq$ “) der natürlichen Zahlen die „0“ und generell für jede Zahl in  $T$  auch („ $\rightarrow$ “) deren Nachfolger-Zahl in  $T$  enthalten ist, dann („ $\Rightarrow$ “) handelt es sich bei  $T$  um  $\mathcal{N}$ .

Formaler sehen die

Peano-Axiome

so aus:

---

<sup>1</sup>(engl.:) „einen Computer neu starten, wobei alle gespeicherten Anwenderprogramme neu geladen werden“ — DUDEN, Band 5, Das Fremdwörterbuch, 9. Auflage, Seite 147, mittlere Spalte, unten, Dudenverlag, Bibliographisches Institut & F. A. Brockhaus AG, Mannheim, 978-3-411-04059-9, 2007; ebenso: DIE ZEIT, Das Lexikon, Band 2, Seite 314, rechte Spalte, unten, Zeitverlag Gerd Bucerius GmbH & Co. KG, Hamburg / Bibliographisches Institut, Mannheim, 978-3-411-17562-8, 2005

<sup>2</sup>„ $l := r$ “ bedeutet: die linke Seite bekommt ihren Wert von der rechten, „ $l =: r$ “ heißt: die rechte Seite bekommt ihren Wert von der linken; die Wert-Zuweisung geht in Richtung des Doppelpunkts.

1.  $0 \in \mathcal{N}$  ; „ $\in$ “ bedeutet: „(ist) Element von“.
2.  $0 \neq s(n) := n + 1$ ,  $n \in \mathcal{N}$  ;  $s$  := „successor“ ist die Nachfolger-Funktion<sup>3</sup>.
3.  $\forall n \in \mathcal{N} \exists! s(n)$  ;  $\forall$  := „für alle“ (All-Quantor),  $\exists$  := „es gibt“ (Existenz-Q.)<sup>4</sup>.
4.  $n_1 \neq n_2 \implies s(n_1) \neq s(n_2)$  ; die Nachfolger-Funktion ist *injektiv*<sup>5</sup>.
5.  $0 \in T_{[\subseteq \mathcal{N}]}$ ,  $\forall n_{[\in \mathcal{N}]} \in T \implies s(n) \in T \implies T = \mathcal{N}$ ; „Induktions-Axiom“.

Das letztgenannte Axiom stellt das Fundament des Beweis-Prinzips der *Induktion* dar; siehe das generelle Vorgehen beim Induktions-, „Schritt“ in Unter-Abschnitt 4.1.1 (S. 35).

Hier bieten sich jetzt einige Worte zur Un-/Gesichertheit von Axiomen (und auch so-genannten „Hypothesen“) an: Axiome lassen sich i. Allg. nicht beweisen. Sie werden lediglich — aber immerhin — als sinnhaftig angesehen; sie stehen nicht im Widerspruch zum aktuellen mathematischen Weltbild. Genau an dieser Stelle könnte jedoch „der Hund begraben liegen“. Würde man nämlich etwas vorfinden, was sich zu einem Axiom als widersprüchlich erweist, so müsste man sich entscheiden, welche Sicht stimmiger ist. Dies könnte dazu führen, dass das Axiom aufgegeben wird. Würde dies dem o. g. 5. Peano-Axiom passieren, wäre mit Induktions-Beweisen „Hängen im Schacht“.<sup>6</sup>

## 1.2 Funktionen

Kommen wir nun zum zentralen Begriff der *Funktion* mitsamt einigen Spezialisierungen.

$$f : D \rightarrow C$$

Sie weist jedem Eingabe-Element der „Start“-Menge  $D$  (links des Pfeils) genau ein Ausgabe-Element der „Ziel“-Menge  $C$  (rechts des Pfeils) zu — notationell :

$$\forall x \in D \exists! f(x) \in C$$

Da bei einer Funktion das Überführen eines Eingabe-Elements in ein Ausgabe-Element für alle Start-Werte gilt, nennt man manchmal ergänzend eine Funktion *total* .

Für eine *partielle* Funktion muss das o. g. „ $\forall$ “ nicht eingehalten werden. (Sogenannte „Definitions“-Lücken sind also erlaubt.)

Demnach ist natürlich jede (totale) Funktion ebenso eine — wenn auch spezielle — partielle Funktion<sup>7</sup>:  $f \text{ total} \implies f \text{ partiell}$  .

Die Umkehrung gilt selbstredend nicht; d. h.:<sup>8</sup>  $f \text{ partiell} \not\implies f \text{ total}$  .

---

<sup>3</sup> F.: siehe Folge-Abschnitt 1.2

<sup>4</sup> „!“ dahinter (s. o.) bedeutet: „genau 1“

<sup>5</sup> siehe den folgenden Abschnitt 1.2 ab Seite 6

<sup>6</sup> ☺ — Im Jahr 2021 sah's noch verträglich aus.

<sup>7</sup> halt — total definiert — ohne Definitions-Lücken

<sup>8</sup> folgendes Zeichen „ $\not\implies$ “ bedeutet „folg(er)t nicht“

Ähnlich gilt:  $f$  partiell  $\not\Rightarrow f \setminus (\text{„nicht“})$  total, wie in Fußnote 7 beleuchtet; selbstverständlich (wenn auch hier unwichtig):  $f \setminus$  partiell  $\implies f \setminus$  total .

Kommen wir nun zu den Element-Mengen  $D$  und  $C$  :

Die *Definitions-Menge* (engl.: domain, hier  $D$ ) stellt alle Möglichkeiten der Eingabe in die Funktion dar.  
(Für jeden Eingabe-Fall muss der dazugehörige eindeutige Ausgabe-Wert definiert sein.)

Die (potentielle) *Werte-Menge* (engl.: co-domain, hier  $C$ ) bezeichnet die maximal zur Verfügung stehenden Werte für die Funktions-Ausgabe.  
(Es muss nicht jeder potentielle Ziel-Wert durch die Funktion zum Tragen kommen.)

Die *Bild-Menge* (hier  $B$ ; engl.: image, range) repräsentiert schluss-endlich genau diejenigen Werte aus der Co-domain, welche von der jeweiligen Funktion wirklich produziert werden können. (Im Folge-Kapitel führen wir für diesen einfachen mengen-theoretischen Zusammenhang, dass alle Elemente einer Menge [hier  $B$ ] komplett auch einer anderen Menge [hier  $C$ ] angehören, das Schlagwort „[unechte] Teil-Menge“ ein, mit folgendem Zeichen:  $B \subseteq C$ .) Die Bild-Menge  $B$  muss sowohl „korrekt“ als auch „vollständig“ sein<sup>9</sup>: alle gelisteten Werte kommen bei der Funktions-Ausgabe in Frage, und es fehlt auch kein von der Funktion benötigter Wert.

Fokussieren wir ganz allgemein bei einer Funktion  $f$  nur auf eine Teil-Menge<sup>10</sup>  $S$  der Definitions-Menge  $D$ , so nennt man dies eine *Einschränkung* (engl.: restriction) :

$$f|_S^{D \rightarrow C} : S_{[\subseteq D]} \rightarrow C$$

Nach diesem begrifflichen Aufgalopp stellen wir jetzt einige konkrete Funktionen vor :

- inclusion  $i : D \rightarrow C$   
 $i(x) := x$

In  $C$  müssen mindestens die Werte aus  $D$  zur Verfügung stehen, da alle  $D$ -Elemente zur Ausgabe gelangen (können);  $D$  ist in  $C$  „inkludiert“.<sup>11</sup>

- identity  $id : S \rightarrow S$   
 $id(x) := i(x)_{[C = D =: S]} := x$

Die Identitäts-Abbildung ist eine spezielle  $i$ -Funktion, bei der die Definitions-Menge identisch sowohl zur Werte- als auch zur Bild-Menge ist — im Ziel-Bereich also keine unnötige echte „Ober“-Menge (siehe Abschnitt 2.2) vorgehalten wird.

- projection  $\pi_j : \prod_{i=1}^n D_i \rightarrow D_j$   
 $\pi_j(x_1, x_2, x_3, \dots, x_n) := x_j , \quad 1 \leq j \leq n$

<sup>9</sup>ein gängiges Begriffs-Paar in der Informatik

<sup>10</sup>engl.: sub-set

<sup>11</sup> $C$  ist „Ober-Menge“ von  $D$  ( $C \supseteq D$ ),  $D$  ist „Teil-Menge“ von  $C$  ( $D \subseteq C$ ); vgl. Abschnitt 2.2, S. 15.

Die Projektion hat typischerweise eine mehr-gliedrige Eingabe-Struktur<sup>12</sup>, z. B. ein Paar („zwei-stellig“, *binär*), Tripel („drei-stellig“), Quadrupel („vier-stellig“), usw., bis hin zu einem beliebigen „*n*-Tupel“. Nun sind wir beim „Kreuz-Produkt“-Zeichen („Cartesisches Produkt“) für die Definitions-Menge  $D$  angelangt. Für jede der  $n$  Variablen steht eine (Start-)Menge  $D_i$  bereit, aus der das jeweilige  $x_i$  ( $1 \leq i \leq n$ ) beliebig schöpfen darf; insgesamt liegt also ein  $n$ -gliedriger Input vor. Jetzt fehlt uns nur noch eine einzige Zusatz-Information zur Durchführung der Projektion: die Auswahl-Position  $j$  ( $1 \leq j \leq n$ ), auf welche fokussiert wird; diese Nummer wird auch „Index“ genannt. Die eigentliche Operation verläuft völlig schmerzfrei  $\smile$ ; es wird lediglich der Inhalt der Position  $j$  präsentiert:  $x_j$ .

- Auch die folgende „Injektion“ überstehen wir ohne Narkose:  
 $injection$  („1-to-1“), injektive Funktion $_{[D \rightarrow C]}$ ;  
 $x_1 \neq x_2 \implies f_{\text{injektiv}}(x_1) \neq f_{\text{injektiv}}(x_2)$  .

Eine solche Funktion bildet also verschiedene Eingaben auf verschiedene Ausgaben eindeutig ab; daher gilt:<sup>13</sup>  $|D| \leq_{f \text{ injektiv}} |C|$ . (Dass bei einer Injektion  $|D| \not> |C|$ , lehrt uns später das „Schubfach-Prinzip“<sup>14</sup>.)

- Die andere Sichtweise bzgl. der Größen-Ordnung der *Domain* im Vergleich zur *Co-domain* liefert die „Surjektion“:  
 $surjection$  („onto“), surjektive Funktion $_{[D \rightarrow C]}$ ;  
 $\forall y \in C \ \exists x \in D : f(x) = y$  .

Bei einer solchen Funktion wird die Werte-Menge komplett in Anspruch genommen — die *Bild-Menge B* entspricht der *Co-domain C*. Aufgrund der (generellen) Funktions-Eigenschaft gilt hier:  $|D| \geq_{f \text{ surjektiv}} |C|$ , äquivalent zu  $|D| \not< |C|$ .

- Ist die Funktion sowohl injektiv als auch surjektiv, so haben wir eine „Bijektion“:  
 $bijection$  („1-to-1“ correspondence), bijektive Funktion $_{[D \rightarrow C]}$  .

Dies führt zur Gleichheit der Größen-Ordnungen von *Domain* und *Co-domain* :

$$|D| =_{f \text{ bijektiv}} |C| .$$

- Die „Inverse“  $f^{-1}$  (einer Funktion  $f$ ) liefert den Ursprung eines Wertes :  
 $inverse$ , inverse Funktion .

Da sowohl die zugrunde liegende Abbildung  $f$  als auch  $f^{-1}$  selbst jeweils eine totale Funktion ist, wissen wir Folgendes: Zum einen lassen sich nur injektive Funktionen umkehren (sonst liefert die Umkehrung keinen eindeutigen Wert); zum anderen muss auch die inverse Funktion total definiert sein, weshalb die Original-Funktion zusätzlich surjektiv sein muss. Damit haben wir die folgende allgemein-gültige Aussage: Ausschließlich Bijektionen lassen sich invertieren!

<sup>12</sup>bei nur 1 ( $=: n$ ) Eingabe-Parameter nennt man sie „ein-stellig“ (*unär*)

<sup>13</sup>das folgende Zeichen  $|\dots|$  um eine Menge  $S$  bedeutet im Endlichen die Anzahl der Elemente in  $S$

<sup>14</sup>siehe Unter-Abschnitt 5.1.4 ab Seite 51

Gegeben ist also eine bijektive Funktion  $f : X \rightarrow Y$ ; wir schreiben demnach :  
 $f^{-1} : Y \rightarrow X$ ,  $\forall y \in Y \exists! f^{-1}(y) =: x \in X$  mit  $f(x) = y$ .

Da  $f$  und  $f^{-1}$  Bijektionen sind, ist das jeweilige  $x$  natürlich einzigartig;<sup>15</sup>  $x$  hängt von  $y$  und  $f^{-1}$  ab: für jedes  $y$  gibt es ein anderes  $x$ , gemäß der bijektiven Funktion.  
 $(|X| = |Y|)$  Man sagt auch:  $f_{[X \rightarrow Y]}$  ist *invertierbar*:  $\exists$  eine Inverse  $f_{[Y \rightarrow X]}^{-1}$ .

- Funktionen können ineinander geschachtelt sein; dies nennt man „Komposition“ :  
 $composition$ ,  $H_{\text{intereinander-Ausführung}}$  ;  
 $h := g \circ f$ , gesprochen:  $g$  „nach (Ausführung von)“  $f$

Mit der Angabe der Definitions- und Werte-Bereiche sieht das Ganze so aus :

$$f : X \rightarrow Y, \quad g : Y \rightarrow Z; \quad h := g \circ f : X \rightarrow Z$$

Mit Eingabe-Argument ergibt sich dann diese Schachtelung :

$$h(x) := g(f(x)) \in Z$$

Der Input  $x$  wandert in die  $f$ -Funktion, die dort erzeugte Ausgabe  $f(x)$  dient als Eingabe in die  $g$ -Funktion, und der daraus entstehende Output ist das Ergebnis der Komposition. Im Allgemeinen gilt:  $g(f(x)) \neq f(g(x))$ ; Illustration<sup>16</sup>:

$$\begin{aligned} D_f &:= C_f := D_g := C_g := \mathcal{N}; & f(x) &:= x + 1, & g(x) &:= 2^x & ; \\ f(g(1)) &:= f(2^1) = f(2) := 2 + 1 & & & & = 3 & , \\ g(f(1)) &:= g(1 + 1) = g(2) := 2^2 = 4 & & & \neq & & . \end{aligned}$$

- Es gibt selbstverständlich auch eine „inverse Komposition“ :  
 $inverse composition$  ;  
 $h^{-1} := (g \circ f)^{-1}$

Bilden wir zunächst die *Hintereinander-Ausführung*  $h$  der Bijektionen  $g$  und  $f$ :  
 $h := g \circ f$ . Da an dieser Stelle  $g$  nach  $f$  ausgeführt wird und somit  $g$  als Letztes vor der Invertierung berechnet wird, gestaltet sich die Umkehrung der Bijektion  $h$  via Hintereinander-Ausführung der Einzel-Invertierungen in folgender Reihenfolge: erst  $g^{-1}$ , dann  $f^{-1}$ ; also  $f^{-1}$  nach  $g^{-1}$ :

$$h^{-1} := (g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

Durch die Angabe der Definitions- und Werte-Bereiche wird's noch klarer :

$$f : X \rightarrow Y, \quad g : Y \rightarrow Z; \quad h := g \circ f : X \rightarrow Z$$

$$f^{-1} : Y \rightarrow X, \quad g^{-1} : Z \rightarrow Y; \quad h^{-1} := f^{-1} \circ g^{-1} : Z \rightarrow X$$

Mit Eingabe-Argument ergibt sich demnach diese geschachtelte Schreibweise :

$$h^{-1}(z) := f^{-1}(g^{-1}(z)) \in X$$

<sup>15</sup>folgende Notation wäre i. Allg. (für  $|Y| > 1$ ) falsch gewesen:  $\exists! x \in X \quad \forall y \in Y : f(x) = y$

<sup>16</sup>Dass für manche Eingabe-Einzelfälle (wie hier bspw. für  $x := 0$ ) trotzdem „=“ gilt, ist irrelevant.

Abschließend führen wir noch drei Rundungs-Funktionen ein, um aus einer positiven reellen Zahl eine *natürliche* liefert zu bekommen:

- *floor* :  $\lfloor x \rfloor :=$  größte natürliche Zahl  $\leq x$ ,
- *ceiling* :  $\lceil x \rceil :=$  kleinste natürliche Zahl  $\geq x$ ;
- *round* :  $\lfloor x \rfloor :=$  wähle( $\lfloor x \rfloor, \lceil x \rceil$ ), wenn's egal ist.

## 1.3 Relationen

Wir besprechen den Begriff der *Relation* einschließlich einiger Konkretisierungen — wobei wir die typische *Binär*-Relation (Beziehung zwischen 2 Parametern) favorisieren:

$$a R b$$

Hier steht die Relation  $R$  inmitten zweier Eingabe-Werte; daher spricht man von „Infix“-Notation; die folgende Schreibweise nennt man „Präfix“-Notation, da  $R$  davor steht :

$$R(a, b)$$

Jede Komponente eines Paares entspringt ihrer eigenen Definitions-Menge<sup>17</sup>

$$a \in A, \quad b \in B; \quad (a, b) \in A \times B =: C$$

Dies beschreibt die Input-Struktur. Das „ $\times$ “-Zeichen mimt die potentielle Möglichkeit, jedes Element aus den jeweiligen Einzel-Mengen (hier  $A$  bzw.  $B$ ) beliebig auswählen zu können. Dies nennt man das „Kreuz-Produkt“ (oder „Cartesische Produkt“)<sup>18</sup>. Erfüllt das Eingabe-Paar die  $R$ -Eigenschaft, so wird es in diese ( $R$ )-Menge der gültigen Paare aufgenommen; es gilt die Obermengen<sup>19</sup>-Beziehung:  $C \supseteq R$ . Im Endlichen ergibt sich:

$$|C| = |A| \cdot |B| \geq |R|$$

Beispiel<sup>20</sup>

$$A := \{0, 1, 2\}, \quad B := \{1, 3\}; \quad C := \{0, 1, 2\} \times \{1, 3\}, \quad R := <$$

$$0, 1 \in A, \quad 1 \in B; \quad (0, 1), (1, 1) \in A \times B =: C$$

$$0 < 1 : R \ni (0, 1); (1, 1) \notin R \quad [1 \not< 1]$$

$$|R| = |\{(0, 1), (0, 3), (1, 3), (2, 3)\}| = 4 \leq 6 = |C|$$

Diese binäre Struktur lässt sich auf eine beliebige  $n$ -gliedrige Syntax verallgemeinern:<sup>21</sup>

$$C := \prod_{i=1}^n S_i := S_1 \times S_2 \times S_3 \times \dots \times S_n :=$$

<sup>17</sup>Definitions- bzw. Werte-Mengen heißen nicht immer  $D$  bzw.  $C$ ;  $B$  ist nicht immer die Bild-Menge.

<sup>18</sup>initial erwähnt in Abschnitt 1.2 auf Seite 6 als Definitions-Menge (von  $n$ -Tupeln) der Projektion

<sup>19</sup>in Abschnitt 2.2 (ab Seite 15) präzisiert

<sup>20</sup>das hier verwendete Zeichen „ $\ni$ “ steht für „enthält“

<sup>21</sup>„|“ einzeln in einer Menge heißt hier „sodass“ / „wobei“

$$\{(e_1, e_2, e_3, \dots, e_n) \mid e_i \in S_i, 1 \leq i \leq n\},$$

welches man wie folgt lesen kann: „Menge aller  $n$ -Tupel  $(e_1, \dots, e_n)$ , wobei das einzelne  $e_i$  aus der jeweilig dazugehörigen Menge  $S_i$  stammt (dabei läuft  $i$  zwischen 1 und  $n$ )“.<sup>22</sup>

$$|C| = |S_1| \cdot |S_2| \cdot |S_3| \cdot \dots \cdot |S_n| =: \prod_{i:=1}^n |S_i|.$$

Beispiel :  
 $1 \leq i \leq n := 3, S_i := \mathcal{B} := \{0, 1\} \hat{=} \{\text{false}, \text{true}\}$

$$|C| = \prod_{i:=1}^3 |S_i| = |\mathcal{B}|^3 = 2^3 = 8.$$

Beweis :  
 $|C| =$

$$\begin{aligned} &|\{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}| \\ &= 8 = 2^3 = |\mathcal{B}|^3. \end{aligned}$$

Es gilt:

$$|\mathcal{B}^n| = |\mathcal{B}|^n = 2^n.$$

Der Beweis verläuft wie im 5. Beispiel in Unter-Abschnitt 4.1.1 (Seite 43).

Wir stellen nun einige allgemeine Typisierungen binärer *Relationen* (engl.-sprachig) vor:

- reflexive

$a R a$   
 Beispiel:  $R := \text{„so erfolgreich wie“}$

- irreflexive:

$a \not R a$

Bsp.:  $R := \text{„stellt sich blöder an als“}$

- converse:

$b R^{-1} a \iff a R b$

Bsp.:  $R := \text{„ist die Hälfte von“}; R^{-1} = \text{„ist das Doppelte von“}$

- complement

$a \bar{R} b \iff a R b$

Bsp.:  $R := \text{„=“}; \bar{R} = \text{„≠“}$

- composition

$a (R_2 \circ R_1) c \iff a R_1 b \text{ und}^{23} b R_2 c$

Bsp.:  $R_1 := \text{„Doppelte“}, R_2 := \text{„Dreifache“}; R_2 \circ R_1 = \text{„Sechsfache“}$

<sup>22</sup>Jedes Element hat seine genaue Auftritts-Position im Tupel; siehe auch noch vorherige Fußnote 18.

<sup>23</sup>beide Fälle müssen zugleich zutreffen

- symmetric  $a R b \implies b R a$   
Bsp.:  $R :=$  „sitzt neben“
- asymmetric:  $a R b \implies b \not R a$   
Bsp.:  $R :=$  „liegt unter“
- anti-symmetric:  $a R b \text{ und } b R a \implies a = b$   
Bsp.:  $R := , \geq$
- transitive:  $a R b \text{ und } b R c \implies a R c$   
Bsp.:  $R := , >$
- intransitive  $a R b \text{ und } b R c \implies a \not R c$   
Bsp.:  $R :=$  „steht in der Tabelle genau einen Platz über“
- union  $a (R_1 \cup R_2) b \iff a R_1 b \text{ oder}^{24} a R_2 b$   
Bsp.:  $R_1 :=$  „benachrichtigt“,  $R_2 :=$  „besucht“;  $R_1 \cup R_2 =$  „kontaktiert“
- intersection  $a (R_1 \cap R_2) b \iff a R_1 b \text{ und } a R_2 b$   
Bsp.:  $R_1 := , \geq$ ;  $R_2 := , \neq$ ;  $R_1 \cap R_2 = , >$
- difference  $a (R_1 - R_2) b \iff a R_1 b \text{ und } a \not R_2 b$   
Bsp.:  $R_1 := , \geq$ ;  $R_2 := , \neq$ ;  $R_1 - R_2 = , =$
- symmetric difference:  $a (R_1 \oplus R_2) b \iff a R_1 b \text{ eXklusiv-}OdeR^{25} a R_2 b$   
Bsp.:  $R_1 := , \geq$ ;  $R_2 := , \neq$ ;  $R_1 \oplus R_2 = , \leq$
- pre-order (Vor-Ordnung) : sowohl reflexive als auch transitive Relation  
Bsp.:  $R := , \geq$
- equivalence relation symmetrische Vor-Ordnung  
Bsp.:  $R :=$  „gleichbedeutend mit“
- partial order/ing  $\leq^{26}$  (auf einer Menge  $S$ ): anti-symmetrische Vor-Ordnung  
Bsp.:  $R_{[\leq]} := , \supseteq^{27}$ .

Auf dieser Begriffs-Basis setzen wir nun folgende Konzepte auf :

- partially ordered set, poSet( $S, \leq$ ): Menge  $S$  mit Partial-Ordnung  $\leq$   
Bsp.:  $S :=$  Menge aller Teilmengen von  $\mathcal{B}^{28}$   $\{\{\}, \{0\}, \{1\}, \{0, 1\}\}$ ;  $R_{[\leq]} := , \supseteq$
- comparable: 2 Elemente  $a, b \in poSet$  sind vergleichbar  $\iff a \leq b \text{ oder } b \leq a$   
Bsp.:  $S := \{\{\}, \{0\}, \{1\}, \mathcal{B}\} =: 2^{\mathcal{B}}$ ,  $R_{[\leq]} := , \supseteq$  (s. o.),  $a := \{0\}$ ,  $b := \mathcal{B}$ ;  $b \leq a$
- incomparable:  $a, b \in S$  sind unvergleichbar  $\iff a \text{ und } b \text{ sind nicht vergleichbar}$   
Bsp.:  $S$ ,  $R_{[\leq]}$  und  $a$  definiert wie vorhin,  $b := \{1\}$ ;  $a \not\leq b$  und  $b \not\leq a$

<sup>24</sup>einschließlich beide Fälle zugleich

<sup>25</sup>genau einer der zwei Fälle, nicht beide zugleich (jedoch auch nicht keiner)

<sup>26</sup>nur als Symbol für o. g. Partial-Ordnung zu verstehen – nicht als üblicher Operator „kleiner-gleich“

<sup>27</sup>Ober-Menge: in Abschnitt 2.2 (ab Seite 15) präzisiert

<sup>28</sup> $\mathcal{B}$  findet sich im Bsp. auf S. 9; „ $\{\}$ “ und die Menge aller Teilmengen: siehe Folge-Kapitel, ab S. 13

- totally<sup>29</sup> ordered set, toS : poSet mit ausschließlich vergleichbaren Element-Paaren  
Bsp.:  $R_{[\leq]} := „\geq“$  (wie eben),  $S := \{\{\}, \{0\}, \mathcal{B}\}; \forall a, b \in S: a \leq b$  oder  $b \leq a$
- chain („Kette“): Teil-Menge einer toS  
Bsp.:  $S$  wie soeben definiert;  $T := \{\{0\}, \mathcal{B}\} \subseteq^{30} S$
- well-ordered set  $S$ :  $\text{poSet}(S, \leq), \forall T_{[\neq \{\}] \subseteq S} \exists$  minimales Element<sup>31</sup>  $m$   
Bsp.:  $S := \{1, 2\}, R_{[\leq]} := „\geq“.$   $T_1 := \{1\}, m_1 = 1; T_2 := \{2\}, T_3 := S: m_{2/3} = 2$
- upper bound (für  $T_{[\subseteq S]}$ )  $b_u$ :  $\forall c \in T: c \leq b_u [ \in \text{poSet}(S, \leq) ]$   
Bsp.:  $S := 2^{\mathcal{B}}$  (s. o.),  $R_{[\leq]} := „\subseteq“, T := \{\{\}, \{0\}\}; b_u := \mathcal{B}: \{\}, \{0\} \leq b_u$
- least upper bound  $\text{lub}(T_S)_{[\in S]}$ :  $\forall b_u$ : upper bound  $\text{lub}(T_S) \leq b_u [ \in \text{poSet}(S, \leq) ]$   
Bsp.:  $S, R_{[\leq]}, T$  wie soeben definiert;  $\text{lub}(T_S) = \{0\}: \{\}, \{0\} \leq \text{lub}(T_S) \leq \forall b_u$
- lower bound (für  $T_{[\subseteq S]}$ )  $b_l$ :  $\forall c \in T: b_l [ \in \text{poSet}(S, \leq) ] \leq c$   
Bsp.:  $S$  und  $R_{[\leq]}$  wie gerade definiert,  $T := \{\{0\}, \mathcal{B}\}; b_l := \{\}: b_l \leq \{0\}, \mathcal{B}$
- greatest lower bound  $\text{glb}(T_S)_{[\in S]}$ :  $\forall b_l$ :  $b_l [ \in \text{poSet}(S, \leq) ] \leq$  lower bound  $\text{glb}(T_S)$   
Bsp.:  $S, R_{[\leq]}, T$  wie frisch definiert;  $\text{glb}(T_S) = \{0\}: \forall b_l \leq \text{glb}(T_S) \leq \{0\}, \mathcal{B}$
- lattice (Verband)  $L$ :  $\text{poSet}(L, \leq), \forall (x, y) \in L^2 : \exists \text{lub}(\{x, y\}), \exists \text{glb}(\{x, y\})$   
Bsp.:  $R_{[\leq]} := „\subseteq“; V := \{1, \dots, n\}, L := 2^V :=$  Menge aller Teilmengen von  $V$ .  
$$\text{lub}(\{S_1, S_2\}) = S_1 \cup S_2, \text{ glb}(\{S_1, S_2\}) = S_1 \cap S_2.$$
<sup>32</sup>

In Abbildung 1.1 sehen wir den Teilmengen-Verband für  $n := 4$ . Jeder Strich dort repräsentiert eine Relation zwischen zwei Mengen: von einer Ebene zur nächst höheren echte Teil-, von einer Ebene zur nächst niedrigeren echte Ober-Menge; weitere echte Teil-/Ober-Mengen-Beziehungen ergeben sich via Transitivität, welche jeder Vor-Ordnung (siehe Seite 10) innenwohnt. Diese „transitive Hülle“ einer Relation bzgl. einer Menge  $M$  erhält man konstruktiv, indem man im Bild einfach von  $M$  aus die Ebenen entlang der Striche in gleichbleibender Richtung auf allen Wegen durchläuft. Die vorhin genannten *lub* und *glb* lassen sich ebenfalls im Bild konstruieren. Ausgehend von den beiden gegebenen Mengen  $S_1$  und  $S_2$  geht man zur ersten „gemeinsamen“ Menge: zur Bildung des *lub* nach oben zur kleinsten Menge, welche alle Elemente aus den beiden Eingangs-Mengen umfasst, zur Bildung des *glb* nach unten zur größten Menge, deren Elemente in beiden Eingangs-Mengen enthalten sind — wie in den folgenden drei Beispielen illustriert:

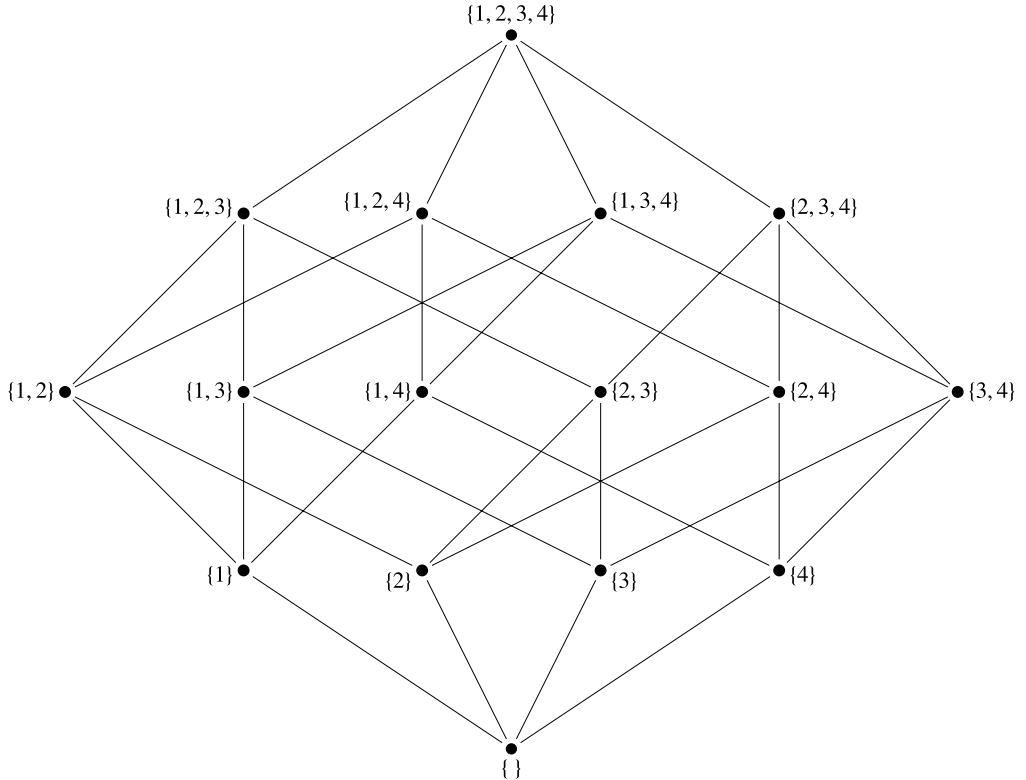
---

<sup>29</sup>bzw. „linearly“: alle Elemente lassen sich „auf einer Linie“ anordnen und miteinander vergleichen

<sup>30</sup>Teil-Menge: in Abschnitt 2.2 (ab Seite 15) präzisiert

<sup>31</sup>Es (evtl. nicht einzigartig) gibt kein „kleineres“ in Bezug auf die jeweils vorliegende  $\leq$ -Relation, im Sinne „erstes“ Element; hab' bewusst die abstrakte  $R$ -Platzhalter-Notation „ $\leq$ “ auf „ $\geq$ “ definiert, um die Feinheit dass „ $\leq$ “ nur als Stellvertreter-Symbol steht, in einem Aufwasch mitzudemonstrieren.

<sup>32</sup>„ $\cup$ “ (Mengen-„Vereinigung“) und „ $\cap$ “ (-„Schnitt“) werden in Abschnitt 2.2 (ab Seite 16) präzisiert.



**Abb. 1.1:** Teilmengen-Verband einer 4-elementigen Menge mit allen  $2^4$  unechten Teil-Mengen

1.  $S_1 := \{1\}$ ,  $S_2 := \{3, 4\}$ ;  $\text{lub}(\{S_1, S_2\}) = \{1, 3, 4\}$ ,  $\text{glb}(\{S_1, S_2\}) = \{\}$ :  
 $\text{lub}$ : von  $\{1\}$  kann man über  $\{1, 3\}$  oder  $\{1, 4\}$  nach  $\{1, 3, 4\}$  gelangen,  
von  $\{3, 4\}$  in einem Schritt direkt nach  $\{1, 3, 4\}$ , aber nicht eher;  
 $\text{glb}$ : von  $\{1\}$  kommt man in einem Schritt direkt zur  $\{\}$ ,  
von  $\{3, 4\}$  über  $\{3\}$  oder  $\{4\}$  zur  $\{\}$ , nicht eher.
2.  $S_1 := \{1, 2\}$ ,  $S_2 := \{2, 3\}$ ;  $\text{lub}(\{S_1, S_2\}) = \{1, 2, 3\}$ ,  $\text{glb}(\{S_1, S_2\}) = \{2\}$ :  
 $\text{lub}$ : von  $\{1, 2\}$  kommt man in einem Schritt direkt nach  $\{1, 2, 3\}$ ,  
von  $\{2, 3\}$  ebenfalls, eben nicht eher;  
 $\text{glb}$ : von  $\{1, 2\}$  geht's in einem Schritt zu  $\{2\}$ , von  $\{2, 3\}$  ebenfalls, nicht eher.
3.  $S_1 := \{1\}$ ,  $S_2 := \{1, 2\}$ ;  $\text{lub}(\{S_1, S_2\}) =_{[S_2 \supseteq S_1]} S_2$ ,  $\text{glb}(\{S_1, S_2\}) =_{[S_1 \subseteq S_2]} S_1$ :  
 $\text{lub}$ : von  $\{1\}$  geht's in einem Schritt zu  $\{1, 2\}$ , in  $\{1, 2\}$  ist man bereits dort;  
 $\text{glb}$ : in  $\{1\}$  ist man schon da, von  $\{1, 2\}$  geht's in einem Schritt nach  $\{1\}$ .  
In diesem letzten Beispiel sieht man sehr schön den Rückgriff auch auf die andere Eigenschaft der Vor-Ordnung (neben der Transitivität, siehe Seite 10), nämlich die Reflexivität: eine Menge ist sich selbst Ober- bzw. Teil-Menge.

Mag's etwas abstrakt dahergekommen sein — aber so ist der Tisch ordentlich gedeckt.

# 2 Mengen-Lehre

Hier legen wir die Basis einer vernünftigen Mengen-Lehre, führen die für uns wichtigsten Begriffe ein und listen die gängisten Gesetzmäßigkeiten auf. Sodann definieren wir die Größen-Ordnung einer Menge und beleuchten Gemeinsamkeiten von und Unterschiede zwischen endlichen und unendlichen Mengen. Die am Ende des Kapitels diskutierte Unendlichkeit bereitet die *Unberechenbarkeit* in der Theoretischen Informatik vor. Letztlich schrecken wir auch nicht vor der *Verallgemeinerten Kontinuums-Hypothese* zurück.

## 2.1 Grundlagen

Eine *Standard-Menge*  $S$  ist eine Ansammlung einzigartiger Elemente, ohne Kopien. Manchmal jedoch braucht man die Funktionalität des Mehrfach-Vorhandenseins von Elementen; eine solche Struktur nennt man im Englischen *multi-set* (Kopien erlaubt).<sup>1</sup> Dann interessiert man sich auch für die Anzahl des Auftretens der jeweiligen Elemente: diese bezeichnet man als die entsprechende *Multiplizität*<sup>2</sup>. Die spezielle Menge mit genau einem Element nennt man englisch-sprachig *singleton*.

Wir führen nun eine Bezeichnung für die „Mächtigkeit“ einer Menge  $S$  ein — deren Kardinal-Zahl, knackiger *Kardinalität* genannt:  $|S|$ . Sie bezeichnet im Endlichen die Anzahl („#“) der Elemente und im Unendlichen deren sogenannte Größen-Ordnung. Die kleinste Menge, die leere Menge  $\{ \} =: \emptyset$ , hat selbstverständlich die kleinste Kardinalität:

$$|\emptyset| = 0$$

Eine Menge heißt *abzählbar unendlich*, wenn es eine Bijektion mit  $\mathbb{N}$  gibt. (Am Ende dieses Abschnittes sehen wir, dass dies nur die erste Stufe der Unendlichkeit darstellt.) Eine Menge  $S_c$  ist *abzählbar*<sup>3</sup>, wenn es nicht darüber hinaus geht ( $|S_c| \leq |\mathbb{N}|$ ) :

- $0 \leq |S_c| \leq i_{[\in \mathbb{N}]} < |\mathbb{N}| : S_c$  endlich ;
- $0 \leq i_{[\in \mathbb{N}]} < |S_c| = |\mathbb{N}| : S_c$  unendlich .

Kommen wir nun zu etwas ganz Fundamentalem im Bereich Mengen und Funktionen :

$$|A| = |B| \iff \exists \text{ Bijektion } f : A \rightarrow B$$

Im Endlichen ist es klar: Wenn die Anzahl der Elemente in den Mengen verschieden ist, hat nicht jedes Element aus der größeren Menge eine/n exklusive/n Partner/in in der

<sup>1</sup>Im Unter-Abschnitt 5.4.1 (ab Seite 75) wird jedes Objekt, ungeachtet seiner „Identität“, gezählt.

<sup>2</sup>in einer nicht-leeren Standard-Menge für jedes Element immer 1

<sup>3</sup>englisch: countable

kleineren;<sup>4</sup> es gibt keine Bijektion. Hat aber jede Menge die gleiche Elemente-Anzahl, so käme auf jedes Element ein Partner<sup>5</sup>-Element; es gibt eine Bijektion, mindestens<sup>6</sup> 1.

Im Unendlichen geht's wilder zu: Hier schafft man in bestimmten Konstellationen eine Bijektion, selbst wenn eine Menge auf den ersten naiven Blick weniger Elemente zu haben scheint als die andere, wie dies ja bei einer echten (hier unendlich großen) Teilmenge<sup>7</sup> (ihrer Obermenge<sup>8</sup>) zunächst aussieht — Beispiel:

Sei  $E_{[\subset \mathcal{N}]} :=$  Menge der geraden<sup>9</sup> natürlichen Zahlen; dann gilt folgender Sachverhalt:

$$|E| = |\mathcal{N}|$$

Die bijektive Funktion  $f$  könnte so aussehen:

$$f : E \rightarrow \mathcal{N}$$

$$f(0) := 0$$

$$f(2) := 1$$

$$f(4) := 2$$

$$\vdots$$

$$f(e) := e/2$$

Gehen wir auf die beiden Merkmale *Injektivität* und *Surjektivität* ein: Verschiedene gerade Zahlen bekommen unterschiedliche natürliche Zahlen injektiv zugeordnet. Es wird kein  $n$  vergessen; jede natürliche Zahl wird von einer geraden Zahl als Funktionswert surjektiv erreicht. Wir sehen: beide Mengen (echte Teil- und Ober-Menge) sind gleich-, „mächtig“<sup>10</sup> — sie haben die gleiche Größen-Ordnung.<sup>11</sup>

Dass der Vergleich der jeweiligen Kardinalität zweier unendlich großer Mengen auch ganz anders ausgehen kann, zeigt folgender Passus:

Eine ganz wichtige Menge ist die *Menge aller Teilmengen*<sup>12</sup> einer (Grund-)Menge  $S$  — „power set“<sup>13</sup>  $\mathcal{P}(S) := \{s \mid s \subseteq S\}$  — in manchen Werken mit  $2^S$  bezeichnet, u. a. aus folgendem Grund: Gegeben  $|S|$ ; dann gilt für endliche Mengen folgende Behauptung<sup>14</sup>:

$$|\mathcal{P}(S)| = |2^S| = 2^{|S|}$$

Folgende weiterführende Tatsache, welche sowohl für endliche als auch für unendliche Mengen gilt, hat fundamentale Bedeutung für unser Ende („des Kapitels“)

$$|\mathcal{P}(S)| > |S| \quad [\geq 0]$$

<sup>4</sup>Das ist wie im richtigen Leben, was für solche Fälle dann sogenannte „work-arounds“ bereithält.

<sup>5</sup>der/die Leser/in möge natürlich die gewünschte Form des Geschlechts für sich personalisieren

<sup>6</sup>dass Abwechslung „geboten werden könnte, wird im Kapitel 5 auf den Seiten 74 und 87 gezeigt

<sup>7</sup>Teilmengen werden im Folge-Abschnitt 2.2 präzisiert; Symbole:  $\subset$  für „echte“,  $\subseteq$  für „unechte“ T.

<sup>8</sup>welche stets alle Elemente ihrer Teilmenge enthält — wird im Folge-Abschnitt 2.2 sauber eingeführt

<sup>9</sup>englisch: *even*

<sup>10</sup>ähnlich ließe sich zeigen, dass auch die Kardinalität der Menge der Brüche der von  $\mathcal{N}$  entspricht

<sup>11</sup>Im Unendlichen spricht man deshalb (wegen „ $\subset$ “ bzw. „ $\subseteq$ “) nicht von „Anzahl“ (von Elementen).

<sup>12</sup>siehe obige Fußnote 7, mit der Ausprägung „unechte ( $\subseteq$ ) Teil-Menge“

<sup>13</sup>Potenz-Menge

<sup>14</sup>siehe Unter-Abschnitte 4.1.1 (Seite 43, „5.“, Abschluss) und 5.4.2 (S. 81, spez. Binomial-Theorem)

Im Endlichen ist dies leicht einzusehen: Jedes vorhandene Element aus  $S$  lässt sich jeweils in ein „singleton“ in  $\mathcal{P}(S)$  stecken, dazu kommt mindestens noch die leere Menge (die kein Element enthält), welche immer Teilmenge jeder beliebigen Menge  $S$  (auch sich selbst gegenüber) und damit ein weiteres Element von  $\mathcal{P}(S)$  ist.

Im Unendlichen bedeutet die „ $>$ “-Aussage, dass es eine<sup>15</sup> „höhere“ Unendlichkeit geben muss als die der Menge ( $S := \mathbb{N}$  der Natürlichen Zahlen). Genau hier liegt die Quelle der *Unberechenbarkeit* in der Theoretischen Informatik — die leichter zu verstehen ist, wenn man, wie im laufenden Kapitel, frühzeitig die Basis legt. Im Gegensatz zu nur abzählbar unendlich großen Mengen (wie  $\mathbb{N}$  und die eben definierte Menge  $E$ ), welche bijektiv aufeinander abbildbar sind, ist die angedeutete — unendlich große — „power set“  $\mathcal{P}(\mathbb{N})$  ein Beispiel für eine sogenannte „über-abzählbare“ Menge: Die nur abzählbar unendlich vielen natürlichen Zahlen reichen nicht aus, um jedem Element aus der Menge aller Teilmengen von  $\mathbb{N}$  ein Element aus  $\mathbb{N}$  bijektiv zuzuordnen; diese beiden Mengen sind unterschiedlich mächtig, haben also verschiedene Größen-Ordnungen. Dazu später mehr im Abschnitt 2.5 (auf Seite 27).

## 2.2 Begriffe

Wir beginnen sinnigerweise mit dem bereits angesprochenen Konzept der *Teilmenge* :

$$A \subseteq B : \quad \forall x \in A \implies x \in B$$

Für deren Kardinalitäten gilt ganz offensichtlich:  $|A| \leq |B|$ .  
Da  $A$  und  $B$  identisch sein können, sprechen wir auch von *unechter* Teil-Menge.

Wenn dieser Spezial-Fall ausgeschlossen ist, nennt man die Mengen-Inklusion *echt* :

$$A \subset B : \quad A \subseteq B \text{ und } A \neq B \iff A \subseteq B \text{ und } \exists x \in B, x \notin A.$$

Im Endlichen hat die echte Teilmenge weniger Elemente als die „übergeordnete“ Menge:  $|A| < |B|$ . Im Unendlichen kann sie gleich-mächtig sein — siehe Abschnitt 2.1, Seite 14.

Die gegenläufige Beziehung heißt *Obermenge* :

$$A \supseteq B : \quad \forall x \in B \implies x \in A$$

Für deren Kardinalitäten gilt ganz offensichtlich:  $|A| \geq |B|$ .  
Da  $A$  und  $B$  identisch sein können, sprechen wir auch von *unechter* Ober-Menge.

Wenn dieser Spezial-Fall ausgeschlossen ist, handelt es sich um eine *echte* Obermenge:

$$A \supset B : \quad A \supseteq B \text{ und } A \neq B \iff A \supseteq B \text{ und } \exists x \in A, x \notin B.$$

Im Endlichen hat die echte Ober-Menge natürlich mehr Elemente als die echte Teil-Menge:  $|A| > |B|$ . Im Unendlichen kann sie gleich-mächtig sein, wie vorhin geschildert.

---

<sup>15</sup>es gibt gar unendlich viele (Unendlichkeiten) — wie am Schluss dieses Kapitels illustriert

Kommen wir nun zur

*Mengen-Gleichheit*

$$A = B \iff A \subseteq B \text{ und } A \supseteq B \iff A \subseteq B \text{ und } B \subseteq A .$$

Demnach gilt  $\forall x : x \in A$  genau dann wenn („gdw“)<sup>16</sup>  $x \in B$ .

Als Nächstes beschreiben wir den *Mengen-Schnitt* (die *Schnitt-Menge*) :

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\} .$$

Ähnlich charakterisieren wir die *Mengen-Vereinigung* (*Vereinigungs-Menge*) :

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\} .$$

Für deren Kardinalität im Endlichen gilt

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

Die Differenz korrigiert das Zählen der Elemente im Schnitt, da diese sonst zweimal gezählt würden. (Das o. g. „oder“ schließt den Fall der Doppel-Zugehörigkeit mit ein.) Sind  $A$  und  $B$  schnitt-frei und haben damit kein gemeinsames Element, so ergibt sich für diesen Spezial-Fall

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

Holen wir etwas weiter aus und betrachten das „Universum“ aller Möglichkeiten. Ist eine Menge  $A (\subseteq U)$  gegeben, so interessieren wir uns jetzt für alle Elemente aus  $U$  „ohne“ („\“)  $A$ , welche also in  $A$  nicht vorkommen; man nennt diese Menge das *Komplement*<sup>17</sup>:

$$\bar{A} := U \setminus A := \{x \in U_{[\supseteq A]} \mid x \notin A\} =: A^c .$$

(Wir kommen gleich noch offiziell auf die Operation „\“ zurück.)

Da sich  $A$  und  $A^c$  gegenseitig zu  $U$  ergänzen ( $A \cup A^c = U$ ) und definitionsgemäß keine gemeinsamen Elemente haben, ergibt sich im Endlichen bzgl. deren Kardinalitäten :

$$|A| + |A^c| = |U| \iff |A^c| = |U| - |A| .$$

Nun zum benutzten „\“, dem Zeichen für die *Mengen-Differenz* (*Differenz-Menge*) :

$$A \setminus B := \{x \in A \mid x \notin B\} = A \cap B^c .$$

Für deren Kardinalität im Endlichen gilt

$$|A \setminus B| = |A| - |A \cap B| .$$

---

<sup>16</sup>englisch: if and only if („iff“) [„if“:  $x \in A \Leftarrow x \in B$ ; „only if“:  $x \notin A \Leftarrow x \notin B$ :  $x \in A \Rightarrow x \in B$ ]

<sup>17</sup>(von  $A$ ) englisch: complement

Ist wie vorhin beim Universum die Menge vor dem „\“ eine Ober-Menge der hinteren, so ergibt sich im Spezial-Fall

$$A \supseteq B : |A \setminus B|_{[\subseteq A]} =_{[U := A_{(\supseteq B)}]} |A| - |B| [= |B^c|] ,$$

auch weil  $B$  identisch ist mit dem Mengen-Schnitt mit  $A$ .

Ein ganz interessantes Konzept ist die *Symmetrische Differenz* :

$$A \oplus B := (A \cup B) \setminus (A \cap B) .$$

Es sind diejenigen Elemente dabei, welche nur in einer der beiden Grund-Mengen sind, jedoch nicht in beiden zugleich, also nicht im Schnitt.

Da beim Zählen der Anzahl der Elemente in der Vereinigung die Schnitt-Elemente bereits  $1 \times$  subtrahiert wurden (damit sie nicht doppelt berücksichtigt werden), wird der Schnitt ein zweites Mal herausgenommen, damit er überhaupt nicht mehr auftaucht. Für die Kardinalität im Endlichen gilt folglich :

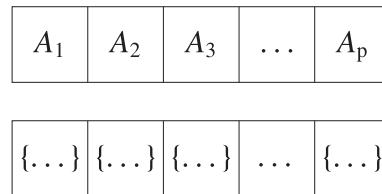
$$|A \oplus B| = |A| + |B| - 2 \cdot |A \cap B| .$$

Fokussieren wir nun auf verschiedene schnitt-freie Mengen; diese nennt man *disjunkt* :

$$\nexists x \in A \cap B_{[\neq A]} [= \emptyset] .$$

Eine sogenannte *Mengen-Familie* ist eine systematische Aufsammlung von Mengen, die in gewissem Zusammenhang zueinander gesehen werden können. Lässt sich nun eine Grund-Menge  $S$  vollständig als Mengen-Familie  $P_S$  von  $p$  nicht-leeren Teil-Mengen  $A_i$  darstellen, welche alle gegenseitig disjunkt sind, also in beliebigen Schnitt-Paar-Kombinationen keine gemeinsamen Elemente haben, aber vereinigt die Grund-Menge  $S$  bilden, so liegt eine  *$p$ -gliedrige Partition* vor, siehe Abbildung 2.1:

$$P_S := \{A_1, A_2, A_3, \dots, A_p\} , \quad p := |P_S| ;$$



**Abb. 2.1:**  $p$ -gliedrige Partition

$$\forall_{[1 \leq i \neq j \leq p]} : A_i \cap A_j = \emptyset , \quad \bigcup_{i:=1}^p A_i = S .$$

Da keine Schnitt-Elemente zu betrachten sind, gilt für die Kardinalität im Endlichen :

$$|S| = |\bigcup_{i:=1}^p A_i| = \sum_{i:=1}^p |A_i| .$$

## 2.3 Gesetzmäßigkeiten

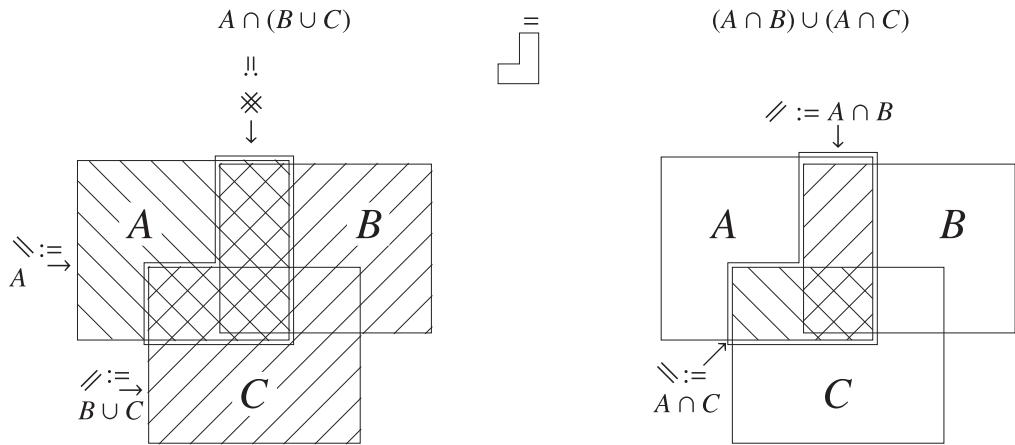
Wir lernen nun die 10 bekanntesten Gesetze endlicher Mengen englisch-sprachig kennen.

- complement<sup>18</sup>:  $A \cap A^c = \emptyset$  ;  $A \cup A^c = U$
- double complement:  $(A^c)^c = A$
- commutativity:  $A \cap B = B \cap A$  ;  $A \cup B = B \cup A$
- associativity:  $(A \cap B) \cap C = A \cap (B \cap C)$  ;  $(A \cup B) \cup C = A \cup (B \cup C)$
- dominance:  $\emptyset \cap A = \emptyset$  ;  $U \cup A = U$
- identity:  $U \cap A = A$  ;  $\emptyset \cup A = A$
- idempotence:  $A \cap A = A$  ;  $A \cup A = A$
- absorption:  $A \cap (A \cup B) = A$  ;  $A \cup (A \cap B) = A$

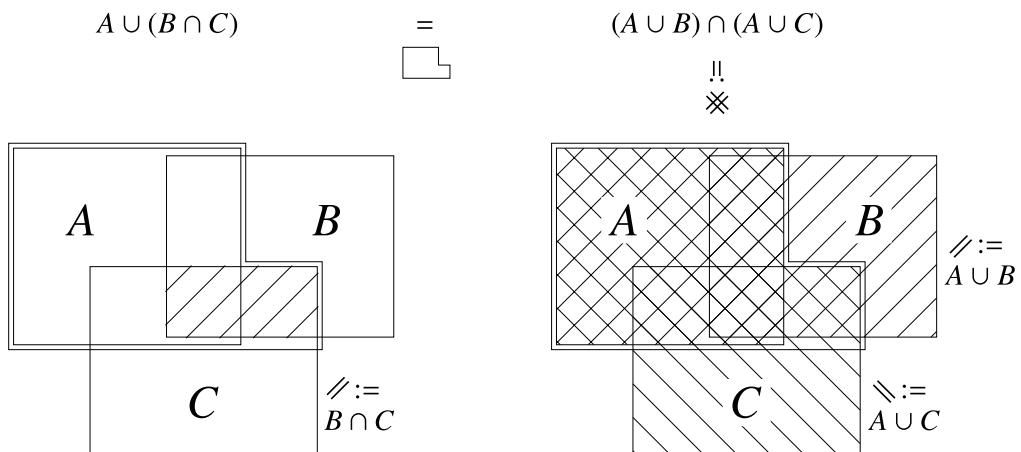
---

<sup>18</sup> „completion“: (o. g.)  $A^c$  ergänzt  $A$  zu  $U$

- distributivity:  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ;  $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$



**Abb. 2.2:** Mengen-Schnitt mit Vereinigungs-Menge



**Abb. 2.3:** Mengen-Vereinigung mit Schnitt-Menge

Abbildung 2.2 zeigt wie sich der Mengen-Schnitt mit einer Vereinigungs-Menge verhält, während Abbildung 2.3 es umgekehrt hält.

- De Morgan  $(\bigcap_{i=1}^n S_i)^c = \bigcup_{i=1}^n (S_i^c)$  ;  $(\bigcup_{i=1}^n S_i)^c = \bigcap_{i=1}^n (S_i^c)$ .

Abbildung 2.4 illustriert die Äquivalenz des Schnitt-Komplements mit der Vereinigung der Einzel-Komplemente und Abbildung 2.5 umgekehrt diejenige zwischen Vereinigungs-Komplement und Schnitt über die Einzel-Komplemente.

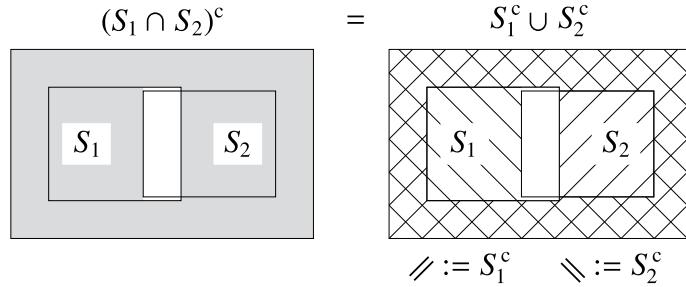


Abb. 2.4: Schnitt-Komplement

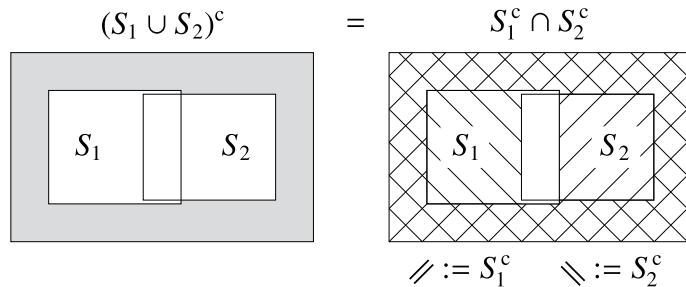


Abb. 2.5: Vereinigungs-Komplement

## 2.4 Kardinalität Endlicher Mengen

Wir beleuchten die hilfreiche Methode des Zählens von Elementen über eine Partition.

- $U := A [ \supset B_{\neq \{ \}} ] , P_U := \{A \setminus B, B\}$

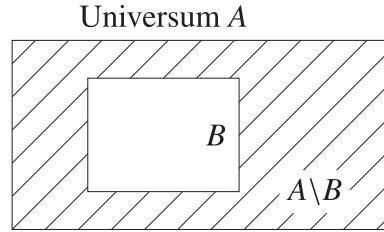
Bild 2.6 zeigt die Zählung der Elemente einer solchen Differenz-Menge.

$$|A| = |A \setminus B| + |B| \iff |A \setminus B| = |A| - |B|$$

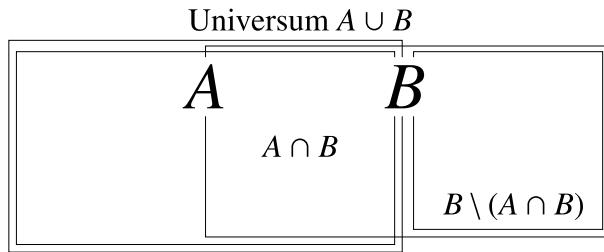
- $U := A \cup B , P_U := \{A, B \setminus (A \cap B)\}$

Bild 2.7 zeigt die Zählung für die Vereinigung unterschiedlicher Mengen.

$$\begin{aligned} |A \cup B| &= |A| + |B \setminus (A \cap B)| &=_{[B \supset A \cap B]} \\ &|A| + |B| - |A \cap B| \end{aligned}$$



**Abb. 2.6:** Differenzmengen-Kardinalität zwischen echter Ober- zu echter Teil-Menge



**Abb. 2.7:** Vereinigung mit Differenz-Menge

- $U := A \cup B, P_U := \{A \oplus B, A \cap B\}$

Bild 2.8 will auf diverse Arten die Kardinalität für's *XOR* zeigen.  $\smile$

$$\begin{aligned}
 |A \cup B| &= |A \oplus B| + |A \cap B| \iff \\
 |A \oplus B| &= |A \cup B| - |A \cap B| \\
 &= |A| + |B| - |A \cap B| - |A \cap B| \\
 &= |A| + |B| - 2 \cdot |A \cap B| \\
 &= (|A| - |A \cap B|) + (|B| - |B \cap A|) \\
 &= |A \setminus B| + |B \setminus A|
 \end{aligned}$$

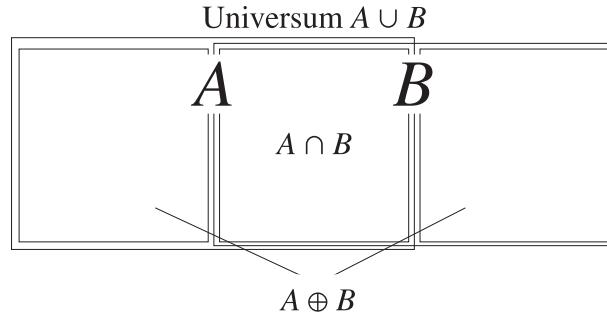
- $U := A \cup B, A \subset B$  oder  $A \supset B ; |U| = \max\{|A|, |B|\} :$

a)  $A \subset B =: U, P_U := \{B \setminus A, A\}$

$$|U| = |B \setminus A| + |A| =_{[B \supset A]} |B| - |A| + |A| = |B| = \max\{|A|, |B|\}$$

b)  $B \subset A =: U, P_U := \{A \setminus B, B\}$

$$|U| = |A \setminus B| + |B| =_{[A \supset B]} |A| - |B| + |B| = |A| = \max\{|A|, |B|\}$$

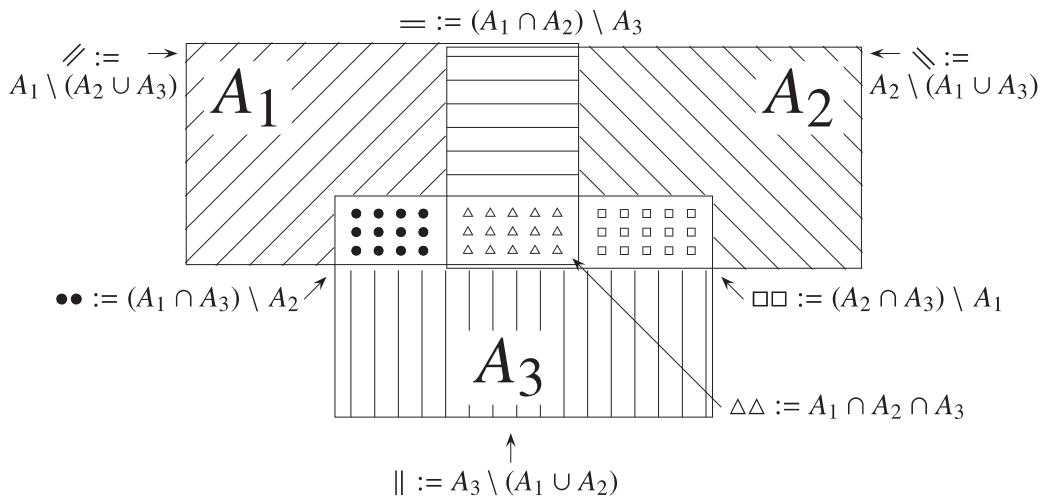


**Abb. 2.8:**  $|XOR|$

- $U := A_1 \cup A_2 \cup A_3, P_U := \{ //, \\ \backslash, \|, =, \bullet\bullet, \square\square, \triangle\triangle \}$

$$= \{A_1 \setminus (A_2 \cup A_3), A_2 \setminus (A_1 \cup A_3), A_3 \setminus (A_1 \cup A_2), (A_1 \cap A_2) \setminus A_3, (A_1 \cap A_3) \setminus A_2, (A_2 \cap A_3) \setminus A_1, A_1 \cap A_2 \cap A_3\}$$

Bild 2.9 bereitet die Formel für die Kardinalität der Vereinigung dreier Mengen vor.



**Abb. 2.9:** Mehrfach-Vereinigung

$$|A_1 \cup A_2 \cup A_3| =$$

$$\begin{aligned}
& |A_1| - |A_1 \cap (A_2 \cup A_3)| + |A_2| - |A_2 \cap (A_1 \cup A_3)| + |A_3| - |A_3 \cap (A_1 \cup A_2)| + \\
& |A_1 \cap A_2| - |(A_1 \cap A_2) \cap A_3| + |A_1 \cap A_3| - |(A_1 \cap A_3) \cap A_2| + |A_2 \cap A_3| - |(A_2 \cap A_3) \cap A_1| + |A_1 \cap A_2 \cap A_3| \\
= & |A_1| - |(A_1 \cap A_2) \cup (A_1 \cap A_3)| + \\
& |A_2| - |(A_2 \cap A_1) \cup (A_2 \cap A_3)| + \\
& |A_3| - |(A_3 \cap A_1) \cup (A_3 \cap A_2)| + \\
& |A_1 \cap A_2| - |A_1 \cap A_2 \cap A_3| + \\
& |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3| + \\
& |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3| + \\
& |A_1 \cap A_2 \cap A_3| \\
= & |A_1| - (|A_1 \cap A_2| + |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3|) + \\
& |A_2| - (|A_1 \cap A_2| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|) + \\
& |A_3| - (|A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|) + \\
& |A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3| + \\
& |A_1 \cap A_2 \cap A_3| - 3 \cdot |A_1 \cap A_2 \cap A_3| \\
= & |A_1| + |A_2| + |A_3| \\
& - 2 \cdot (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\
& + 1 \cdot (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\
& + 3 \cdot |A_1 \cap A_2 \cap A_3| \\
& - 3 \cdot |A_1 \cap A_2 \cap A_3| \\
& + |A_1 \cap A_2 \cap A_3| \\
= & |A_1| + |A_2| + |A_3| \\
& - (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) \\
& + |A_1 \cap A_2 \cap A_3|
\end{aligned}.$$

Welch ein Wahnsinn! Unsere ganze Hoffnung liegt jetzt in der nicht nur optischen Regelmäßigkeit des Ergebnisses: Man startet bei den Kardinalitäten der Einzel-Mengen, subtrahiert die Kardinalitäten der Paar-Schnitte<sup>a</sup> und addiert abschließend die Kardinalität des Schnitts dreier Mengen. Dieses „Ein-/Ausschluss“-Prinzip — also anfangs die Elemente aller Mengen aufzunehmen, danach manche wegzunehmen, dann wieder welche „einzuschließen“ usw.<sup>b</sup> — lässt sich sogar verallgemeinern zur Berechnung der Anzahl der Elemente in der Vereinigung beliebig vieler Mengen<sup>c</sup>; es ist Gegenstand des Abschnitts 5.2, der eine derartige Zähl-Formel in ihrer allgemeinsten Form präsentiert. Damit sind wir in der Lage, ohne mühsame Zwischen-Rechnung gleich nach dem hier geschilderten Prinzip strukturiert vorzugehen.

---

<sup>a</sup>bei der  $\cup$  nur zweier Mengen wird die Schnittmenge auch einmal abgezogen

<sup>b</sup>ab vier Mengen würde man dann alle „4er“-Schnitte „ausschließen“ ...

<sup>c</sup>ob disjunkt oder nicht — wie man oben schön sieht

- $U := A_1 \cup A_2 \cup A_3, P_U := \{A_1 \setminus A_2, A_2 \setminus A_1, A_1 \cap A_2, A_3 \setminus (A_1 \cup A_2)\}$

Fertigen Sie zuerst eine Skizze<sup>19</sup> und visualisieren sich diese Partition!

$$\begin{aligned}
 |A_1 \cup A_2 \cup A_3| &= |A_1 \setminus A_2| + |A_2 \setminus A_1| + |A_1 \cap A_2| + |A_3 \setminus (A_1 \cup A_2)| \\
 &= |A_1| - |A_1 \cap A_2| + \\
 &\quad |A_2| - |A_2 \cap A_1| + \\
 &\quad |A_1 \cap A_2| + \\
 &\quad |A_3| - |A_3 \cap (A_1 \cup A_2)| \\
 &= |A_1| + |A_2| + |A_3| \\
 &\quad - |A_1 \cap A_2| \\
 &\quad - |(A_3 \cap A_1) \cup (A_3 \cap A_2)| \\
 &= |A_1| + |A_2| + |A_3| \\
 &\quad - |A_1 \cap A_2| \\
 &\quad - (|A_1 \cap A_3| + |A_2 \cap A_3| - |A_1 \cap A_2 \cap A_3|) \\
 &= |A_1| + |A_2| + |A_3| \\
 &\quad - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| \\
 &\quad + |A_1 \cap A_2 \cap A_3|
 \end{aligned} .$$

---

<sup>19</sup>bitte nicht in's Buch hinein ☺ — obwohl, bei 'nem eigenen Unikat ... hätt' doch auch etwas ...

## 2.5 Über-/Abzählbarkeit Unendlicher Mengen

Wir kommen nun mit diesem Abschnitt zum Höhepunkt der ersten Hälfte dieses Buches. Lassen wir ihn gleich mit etwas beginnen, was es im Endlichen nicht gibt: jede unendliche Menge (engl.: *set*) hat eine (unendlich große) echte *Teil-Menge* gleicher Kardinalität :

$$S \text{ unendlich} \iff \exists T \subset S \text{ mit } |T| = |S| .$$

Schauen wir uns noch an, wieweit wir kommen bei der umgekehrten Blickrichtung: die o. g. unendlich große (*Teil-)Menge*  $T$  hat eine echte Ober-Menge  $S$  identischer Kardinalität — klingt irgendwie nach Ende der Fahnenstange, was die Größen-Ordnung unendlicher Mengen angeht. Aber es geht weiter; es gibt ein Leben „danach“ :)

Wir konstruieren die unendlich vielen diskreten Zahlen mengen-theoretisch und stellen dabei jeder Zahl jeweils eine „gleichwertige“ Menge gegenüber — womit wir bei den *Ordinal-Zahlen* („*Ordinalen*“) angelangt wären:

$$\begin{aligned} 0 &:= \emptyset [= \{\}] ; 0. \text{ (endliche) } \text{Ordinal-Zahl} &=: \omega_0 \hat{=} |\{\}| \\ \alpha+1 &=: \alpha^+ [\hat{=} s(\alpha) := \text{Nachfolger}(\alpha)] &:= \alpha \cup \{\alpha\}; \alpha \text{ } \text{Ordinal} \\ 1 &= 0 + 1 &:= \emptyset \cup \{\emptyset\} &= \{\emptyset\} &= \{0\} &\hat{=} |\{0\}| \\ 2 &= 1 + 1 &:= \{\emptyset\} \cup \{\{\emptyset\}\} &= \{\emptyset, \{\emptyset\}\} &= \{0, 1\} &\hat{=} |\{0, 1\}| \\ 3 &= 2 + 1 &:= \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} &= \{0, 1, 2\} &&\hat{=} |\{0, 1, 2\}| \\ &\vdots &&&& \\ \omega &= \{0, 1, 2, \dots\} &=: \mathcal{N}; 1. \text{ unendl. } \text{Ordinal-Z.} &=: \omega_1 [\hat{=} |\mathcal{N}|]; \\ \text{allgemein: } \alpha &&&\hat{=}&&|\alpha|. \end{aligned}$$

Wir sehen:  $\alpha_1 < \alpha_2 \iff \alpha_1 \in \alpha_2 \iff_{\text{hier}} \alpha_1 \subset \alpha_2$ .

[Ist dies ein Ausstieg aus dem Mengen-Paradoxon von Bertrand Arthur William Russell? Schließlich ließe sich die soeben aufgestellte Äquivalenz zur Not wie folgt zurechtbiegen:

$$\alpha \not< \alpha \iff \alpha \notin \alpha \quad \therefore \quad .$$

Wir gelangen jetzt zur *Grenz-Ordinalzahl* (englisch: *limit ordinal* — *lol* :); sie hat keinen direkten Vorgänger :

$$\beta \text{ lol} \iff \exists \alpha \text{ mit } \beta = s(\alpha) .$$

Wir kennen schon zwei:  $\omega_0$  und  $\omega_1$ , einmal die einzige endliche sowie die erste unendliche (Grenz-Ordinalzahl). Wir setzen nun munter eins drauf — eben immer weiter:

$$\omega_1 + 1 := \omega_1 \cup \{\omega_1\} = \{\omega_1, \{\omega_1\}\}$$

⋮

$$\begin{aligned}
\omega_1 + k &= \{0, 1, 2, 3, \dots, \omega_1, \omega_1 + 1, \dots, \omega_1 + k - 1\} \\
\omega_2 &= \omega_1 \cup \{\omega_1 + n \mid n \in \omega\} && \text{2. unendliche lol} \\
&\vdots \\
\omega_i &= \omega_{i-1} \cup \{\omega_{i-1} + n \mid n \in \omega\} && \text{i. unendliche lol} \\
&\vdots
\end{aligned}$$

(Das wird echt gebraucht, bspw. als Basis für die *Transfinite Induktion*, einem Beweis<sup>20</sup>-Mechanismus zur Fixpunkt-Semantik in PROLOG, einer vor allem in Europa und Japan geschätzten Programmier-Sprache im Bereich *Intellektik / Künstliche Intelligenz*.)

Wir erzielen so nahezu spielerisch unendlich viele Unendlichkeits-Stufen. Dies schaffen wir ebenso durch die fortwährende Konstruktion der jeweiligen Menge aller (bisherigen) Teilmengen über der Grund-Menge  $\mathcal{N}$  – wie wir nachher auf Seite 27 sehen werden. Ist die Kardinalität einer Menge  $M$  größer als  $|\mathcal{N}|$ , so nennt man  $M$  im Hinblick auf ihre Größen-Ordnung *über-abzählbar*.

Die Addition zweier Ordinale, bei der mindestens eine Zahl unendlich groß ist, ist nicht kommutativ: Beim Ritt durch die Unendlichkeit kommt es also bei einem geplanten Pferde-Wechsel auf die Reihenfolge des Zureitens der Schlacht-Rösser an. ☺ Beispiel :

$$\begin{aligned}
1 + \omega : \quad 1 < \omega &\implies 1 \subset \omega &\implies 1 \cup \omega &= \omega ; \\
\omega + 1 : \quad 1 < \omega < \omega + 1 &:= \omega \cup \{\omega\} &= \{\omega, \{\omega\}\} &\neq \omega .
\end{aligned}$$

Somit gilt:  $1 + \omega \neq \omega + 1$  .

Schon beim Versuch einer Bijektion zwischen der Menge der Brüche und der Menge der natürlichen Zahlen müssen wir beim Durchlaufen der in beiden Dimensionen (Zeilen und Spalten)<sup>21</sup> unendlich großen Matrix höllisch aufpassen: Blieben wir z. B. stur in einer der unendlich langen Zeilen, kämen wir nie zu allen Brüchen; wir müssen sie in geschickter Weise diagonal traversieren, was hier nicht Gegenstand der Diskussion sein möge, und erhalten dadurch tatsächlich eine Bijektion, welche die Möglichkeit der Gleich-Mächtigkeit einer Obermenge zu ihrer unendlich großen echten Teilmenge zeigt.<sup>22</sup>

Entwickeln wir die bedeutsame Bemerkung hinsichtlich verschiedener Mächtigkeiten zweier ganz spezieller unendlich großer Mengen nun „im Großen“; wie in Abschnitt 2.1 (ab Seite 14) geschildert: Jede noch so beliebig große Menge ist von geringerer Größen-Ordnung als ihre Potenz-Menge

$$\begin{aligned}
S_1 &:= \omega_1 \\
\omega_1 &\hat{=} |S_1| < |\mathcal{P}(S_1)| \\
S_2 &:= \mathcal{P}(S_1)
\end{aligned}$$

<sup>20</sup>via Fall-Unterscheidung bzgl. Nachfolger- und Grenz-Ordinalzahl

<sup>21</sup>für die jeweilige Bildung der Zähler und Nenner

<sup>22</sup>wie auf Seite 14 in Fußnote 10 bereits erwähnt

$$\begin{aligned}
\omega_2 &\stackrel{\triangle}{=} |S_2| < |\mathcal{P}(S_2)| \\
S_3 &:= \mathcal{P}(S_2) \\
\omega_3 &\stackrel{\triangle}{=} |S_3| < |\mathcal{P}(S_3)| \\
&\vdots \\
S_i &:= \mathcal{P}(S_{i-1}) & [= \{s \mid s \subseteq S_{i-1}\}] & , \quad i > 1 \\
\omega_i &\stackrel{\triangle}{=} |S_i| < |\mathcal{P}(S_i)| & & , \quad i \geq 0 \\
&\vdots \\
\end{aligned} .$$

Die Potenz-Menge bezeichnet bekanntlich die Menge aller Teilmengen. Wird sie, wie hier, über eine unendlich große Grundmenge  $S_{i-1}$  konstruiert, schlägt ihre ganze Kraft durch; für  $i > 1$  sattelt  $\mathcal{P}(S_{i-1})$ , im Vergleich zu  $S_{i-1}$ , genau eine höhere Unendlichkeits-Stufe — womit wir eine weitere Art der Konstruktion der  $\omega_i$  [ $\stackrel{\triangle}{=} |\mathcal{P}(\omega_{i-1})|$ ] vorliegen haben. Wir gehen aus von der sogenannten *Verallgemeinerten Kontinuums-Hypothese*<sup>23</sup>:

$$\omega_{i-1} <_{[i>0]} \omega_{i-1} \cup \{\omega_{i-1} + n \mid n \in \omega\} = \omega_i \stackrel{\triangle}{=}_{[i>1]} |\mathcal{P}(\omega_{i-1})|;$$

anders ausgedrückt:

$$\omega_{i+1} \stackrel{\triangle}{=}_{[i \geq 1]} |\mathcal{P}^i(\mathcal{N})|,$$

der Kardinalität der  $i$ -fachen Ausführung der Potenzmengen-Konstruktion ausgehend von der „kleinsten“ unendlichen Menge  $\mathcal{N}$  (welche die erste Unendlichkeits-Stufe bildet).

Die zu Kapitel-Anfang (Abschnitt 2.1, S. 15) angerissene Bedeutung der Existenz verschiedener Größen-Ordnungen für die Theoretische Informatik<sup>24</sup> lässt sich nun wie folgt beleuchten: Sei  $\Sigma^*$  die unendliche Menge aller möglichen „Wörter“ (Zeichenketten) über einem (nicht-leeren endlichen) Alphabet  $\Sigma$ , dann bedeutet  $\mathcal{P}(\Sigma^*)$  die noch größere Menge aller möglichen Teilmengen, „Sprachen“ genannt. Setzt man „Wörter“ mit „Algorithmen“ und „Sprachen“ mit „Problemen“ gleich, so gibt es mehr Problem-Stellungen als Lösungs-Verfahren. Es existieren also Probleme, welche durch keinen Algorithmus berechnet/gelöst werden können; mathematisch ausgedrückt: Eine Surjektion aus der Menge der Algorithmen in die Menge der Sprachen ist unmöglich<sup>25</sup>, da die zu wenigen Algorithmen, aufgrund der Definition einer Funktion, gar nicht alle (über-abzählbar vielen) Sprachen abdecken können.<sup>26</sup> Zunächst kann man jedem Element aus  $\Sigma^*$  (also einem Wort, einem Algorithmus) ein Element aus der Menge der Natürlichen Zahlen bijektiv zuordnen.  $\mathcal{P}(\mathcal{N})$  entspricht somit  $\mathcal{P}(\Sigma^*)$ , der Menge der Probleme, die — wie dargestellt — eine höhere Kardinalität hat als die Menge der Algorithmen. Damit haben wir nun eine solide Basis für die *Unberechenbarkeit*  $\supset$  in der Theoretischen Informatik.

<sup>23</sup>engl.: Generalized Continuum Hypothesis; die „einfache“ Cantor-CH:  $|\mathcal{N}| < |\mathcal{R}| \stackrel{\triangle}{=} \omega_2 \stackrel{\triangle}{=} |\mathcal{P}(\mathcal{N})|$

<sup>24</sup>in den Bereichen Sprach- und Berechenbarkeits-Theorie („Unentscheidbarkeit“)

<sup>25</sup> $\Rightarrow \exists$  Bijektion  $\Sigma^* \rightarrow \mathcal{P}(\Sigma^*) \iff |\Sigma^*| \neq_{[<]} |\mathcal{P}(\Sigma^*)|$

<sup>26</sup>In meiner Theorie-Vorlesung *Formale Grundlagen* biete ich noch weitere Betrachtungsweisen an.



# 3 Boolesche Algebra

In diesem Kapitel führen wir zunächst mit einigen Grund-Begriffen in die Aussagen-Logik ein. Via Werte-Tafeln definieren wir sodann die Bildung zusammengesetzter Aussagen, auch Schalt-Logik genannt. Abschließend beleuchten wir noch einige Gesetzmäßigkeiten („Äquivalenzen“).

## 3.1 Begriffe

Sei  $\mathcal{B} := \{0, 1\}$  die Boolesche Menge mit den zwei Werten 0 und 1, welche als die beiden „Wahrheits“-Werte *false* („f“) bzw. *true* („t“) interpretiert werden. Diese booleschen Konstanten werden als „Atome“ bezeichnet, als „atomare“ Formeln oder besser „atomistische“<sup>1</sup>. Eine aussagen-logische Variable stellt ein sogenanntes (0-stelliges) „Prädikat“ (ohne Eingabe-Parameter) dar, welches mit *f* oder *t* belegt werden kann. Unter Einsatz von „Konnektoren“ werden schließlich zusammengesetzte Ausdrücke („wohl-geformte Formeln“) gebildet, im Folgenden beispielsweise mit den booleschen Variablen *p*, *q*, *r*.

## 3.2 Werte-Tafeln

Wir stellen logische Operatoren vor und legen die große Zahl möglicher Belegungen dar.

### 3.2.1 Grund-Muster

- NOT                      Negation                       $\neg$                       (Bild 3.1)

$\mathbf{p}$	$\neg\mathbf{p}$
0	1
1	0

*Abb. 3.1: NOT*

- AND                      Konjunktion                       $\wedge$                       (Bild 3.2)

Der Konnektor  $\wedge$  steht hier inmitten zweier boolescher Variablen, weshalb man auch von Infix-Notation spricht. Vor allem bei längeren gleichförmigen Ausdrücken

<sup>1</sup>im Englischen (auch nicht „atomal“ sondern) „atomic“

<b>p</b>	<b>q</b>	<b>p <math>\wedge</math> q</b>
0	0	0
0	1	0
1	0	0
1	1	1

Abb. 3.2: AND

bietet sich jedoch die Präfix-Schreibweise an, bei der man das Verbindungs-Zeichen vor die Variablen platziert :

$$\begin{aligned}
 p \wedge q &=: \wedge(p, q) & ; \\
 p_1 \wedge p_2 \wedge p_3 \wedge \dots \wedge p_n &= \wedge(p_1, p_2, p_3, \dots, p_n) & =: \bigwedge_{i:=1}^n p_i & . \\
 \bullet \text{ NAND } (\neg \text{AND}) & \quad \text{Sheffer-Strich} & | & \quad (\text{Bild 3.3})
 \end{aligned}$$

<b>p</b>	<b>q</b>	<b><math>\neg(p \wedge q)</math></b>
0	0	1
0	1	1
1	0	1
1	1	0

Abb. 3.3: NAND

$$\bullet \text{ OR } (\text{Inklusiv-ODER}) \quad \text{Disjunktion} \quad \vee \quad (\text{Bild 3.4})$$

<b>p</b>	<b>q</b>	<b>p <math>\vee</math> q</b>
0	0	0
0	1	1
1	0	1
1	1	1

Abb. 3.4: OR

$$\begin{aligned}
 p \vee q &=: \vee(p, q) & ; \\
 p_1 \vee p_2 \vee p_3 \vee \dots \vee p_n &= \vee(p_1, p_2, p_3, \dots, p_n) & =: \bigvee_{i:=1}^n p_i & .
 \end{aligned}$$

• NOR              ( $\neg$  OR)              Peirce-Pfeil               $\downarrow$               (Bild 3.5)

$p$	$q$	$\neg(p \vee q)$
0	0	1
0	1	0
1	0	0
1	1	0

Abb. 3.5: NOR

• XOR              Exklusiv-ODER               $\oplus$               (Bild 3.6)

$p$	$q$	$p \oplus q$
0	0	0
0	1	1
1	0	1
1	1	0

Abb. 3.6: XOR

• implication              Konditional               $\rightarrow$               (Bild 3.7)

$p$	$q$	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

Abb. 3.7: Implikation

Hierzu existieren viele Sprechweisen; die gängigsten scheinen diese zu sein :

- $p$  impliziert  $q$
- wenn  $p$  dann  $q$
- $q$  wann immer  $p$
- $q$  folgt aus  $p$
- $q$  wenn  $p$
- $p$  nur wenn  $q$
- $q$  notwendig für  $p$
- $p$  hinreichend für  $q$

Der Teil vor dem Pfeil heißt im Englischen „antecedent“, der hintere „consequent“. Desweiteren gibt es interessante logische Entsprechungen, welche beweis-technisch von Bedeutung sind; zudem lernen wir die dazugehörigen Fach-Ausdrücke kennen:

$$p \rightarrow q \iff \neg p \vee q \iff \neg q \rightarrow \neg p .$$

Die letzte Form nennt man „contrapositive“ und ist nicht identisch mit dieser :

$$q \rightarrow p \iff \neg p \rightarrow \neg q .$$

In Bezug auf „ $p \rightarrow q$ “ heißt der erste Ausdruck „converse“ und der letzte „inverse“.

- equivalence Bi-Konditional  $\leftrightarrow$  (Bild 3.8)

<b><math>p</math></b>	<b><math>q</math></b>	<b><math>p \leftrightarrow q</math></b>
0	0	1
0	1	0
1	0	0
1	1	1

**Abb. 3.8:** Äquivalenz

Auch hier gibt es mehrere Sprech-Varianten :

- $p$  und  $q$  äquivalent
- $p$  und  $q$  implizieren einander
- $p$  genau dann wenn („gdw.“)  $q$
- $p$  hinreichend und notwendig für  $q$

$$p \leftrightarrow q \iff (p \rightarrow q) \wedge (q \rightarrow p) .$$

Abschließend:

- ***KNF***

Die Konjunktive Normal-Form ist eine aussagen-logische Konjunktion bestehend aus Disjunktionen von „Literalen“ (negativen/positiven booleschen Variablen).

- ***k-SAT***

Bei *k-SATISFIABILITY* treten in jeder einzelnen Disjunktion maximal  $k$  Literale in einer KNF auf, letztere nun betrachtet als aussagen-logisches Erfüllbarkeits-Problem. Dabei geht es um die Frage, ob die gegebene Formel so mit Wahrheits-Werten belegt werden kann, dass sie zu „true“ evaluiert (bzw. sicher sagen zu können, dass dies mit keiner der exponentiell vielen Belegungs-Varianten geht).<sup>2</sup> Fokussiert man auf  $k \in \{2, 3\}$ , so ergeben sich zwei prominente Spezial-Fälle; zwischen diesen beiden verläuft ein sogenannter „Phasen-Übergang“, bezogen auf den Schwierigkeits-Grad der Problem-Lösung: 2- und 3-SAT gehören (wohl) unterschiedlichen Berechnungs-Komplexitätsklassen der Theoretischen Informatik an.<sup>3</sup>

<sup>2</sup>Eine Lösung hierzu ist, zumindest prinzipiell, immer „berechenbar“, da der Suchraum endlich ist.

<sup>3</sup>Der erste Fall ist linear, der zweite scheint exponentieller Natur (siehe folg. Unter-Abschnitt 3.2.2).

### 3.2.2 Belegungs-Möglichkeiten

Gegeben sind  $n$  verschiedene boolesche Variablen; dann gilt folgender Sachverhalt :

1. # verschiedener Codierungen:  $2^n$  [Binär-Darstellungen der Zahlen 0 bis  $2^n - 1$ ] ;
2. # verschiedener Funktionen:  $2^{(2^n)}$  [Codierungs-# im Exponenten] .

<b>p</b>	<b>q</b>	<b>r</b>	$f_b$
0	0	0	0, 1
0	0	1	0, 1
0	1	0	0, 1
0	1	1	0, 1
1	0	0	0, 1
1	0	1	0, 1
1	1	0	0, 1
1	1	1	0, 1

**Abb. 3.9:** # Codierungen + Gedanken-Schema # Boole-Funktionen

Abbildung 3.9 erlaubt einen ersten Einblick in beide Formeln. Die Beweise finden sich im Unter-Abschnitt 4.1.1 ab Seite 43 als vorgerechnete Beispiele („5.“ und „6.“) zur Induktion mit natürlichen Zahlen.

### 3.3 Gesetzmäßigkeiten

Im Folgenden lernen wir die bekanntesten Booleschen Gesetze englisch-sprachig kennen.

- contradiction:  $p \wedge \neg p \iff \text{false}$
- tautology:  $p \vee \neg p \iff \text{true}$
- double negation:  $\neg\neg p \iff p$
- commutativity:  $p \wedge q \iff q \wedge p$  ;  $p \vee q \iff q \vee p$
- associativity:  $(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$  ;  $(p \vee q) \vee r \iff p \vee (q \vee r)$
- distributivity:  $p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$  ;  $p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$
- dominance:  $\text{false} \wedge p \iff \text{false}$  ;  $\text{true} \vee p \iff \text{true}$
- identity:  $\text{true} \wedge p \iff p$  ;  $\text{false} \vee p \iff p$
- idempotence<sup>4</sup>:  $p \wedge p \iff p$  ;  $p \vee p \iff p$
- absorption  $p \wedge (p \vee q) \iff p$  ;  $p \vee (p \wedge q) \iff p$

---

<sup>4</sup>Mindestens die deutsche Übersetzung braucht hier, gerade anfangs, jedes Buchstaben-Pärchen  $\sim$

- De Morgan  $\neg(\bigwedge_{i=1}^n p_i) \iff \bigvee_{i=1}^n (\neg p_i)$  ;  $\neg(\bigvee_{i=1}^n p_i) \iff \bigwedge_{i=1}^n (\neg p_i)$
- exportation  $p \rightarrow (q \rightarrow r) \iff (p \wedge q) \rightarrow r$ .

Die ersten elf Gesetze leuchten schnell ein; die letzte Äquivalenz lässt sich einfach zeigen:

$$\begin{aligned} p \rightarrow (q \rightarrow r) &\iff p \rightarrow (\neg q \vee r) \iff \\ \neg p \vee \neg q \vee r &[=: \text{linke Seite}] \iff [=\text{rechte Seite}:] \neg(p \wedge q) \vee r \iff \\ (p \wedge q) \rightarrow r &. \end{aligned}$$

Wir erkennen die Mengen-Gesetze aus Abschnitt 2.3 wieder;<sup>5</sup> sie finden in der Booleschen Algebra ihre sichtbare Entsprechung — eine Art „Dualität“. Umgekehrt kann man auch in der „exportation“-Regel eine Mengen-Aussage sehen; nach Bildung des „Universums“ lauten o. g. „linke“ und „rechte Seite“ in der Mengen-Variante wie folgt:

$$U := P \cup Q \cup R ; \quad P^C \cup Q^C \cup R \stackrel{\text{De Morgan}}{\iff} (P \cap Q)^C \cup R .$$

Es gibt weitere Analogien zwischen Mengen-Lehre und Boolescher Algebra. So ist zum Beispiel die Anzahl der Elemente in der Potenz-Menge einer  $n$ -elementigen Grund-Menge identisch mit der Anzahl Zeilen in einer Werte-Tafel mit  $n$  booleschen Variablen; schließlich stellt eine „1“ das Vorhandensein eines Elements, eine „0“ das Gegenteil dar. Die leere Menge ist demnach durch die Codierung „ $(0, \dots, 0)$ “ repräsentiert, die Grund-Menge selbst via „ $(1, \dots, 1)$ “; entsprechende Darstellungen ergeben sich für die Misch-Belegungen. Daraufhin halten sowohl die Potenz-Menge als auch die Werte-Tafel jeweils  $2^n$  verschiedene Einträge bereit.

---

<sup>5</sup>Die beiden dort ab Seite 18 im „complement“ zusammengefassten Aussagen haben hier 2 gesonderte Bezeichnungen („contradiction“ und „tautology“).

# 4 Beweis-Prinzipien

Dieses Kapitel stellt die drei gängigsten Methoden der mathematischen Beweisführung vor. Wir beginnen mit der grundlegenden Technik der *Induktion*, fahren fort mit dem *Direkten Beweis* und schließen mit dem *Indirekten Beweis*. (Die auch für die Informatik wichtige *Diagonalisierung* hebe ich für die Vorlesung *Formale Grundlagen* auf; sie findet sich im hinten gelisteten Informatik-Werk  $\ddot{\text{S}}$ .)

## 4.1 Induktion

Das *induktive* Prinzip besprechen wir zum einen auf natürlichen Zahlen sowohl hinsichtlich einer Original-Eingabe  $n$  als auch bzgl. eines Logarithmus-Wertes (Ebenen-Nummer/Such-Tiefe im Entscheidungs-Baum mit einheitlichem Verzweigungs-Grad) — und zum anderen auf Zeichen-Ketten („Wörtern“), um typische Behauptungen der Informatik-Sprachtheorie beweisen zu können.<sup>1</sup> (Die für die Informatik interessante *Strukturelle Induktion* halte ich ebenfalls für o. g. Vorlesungs-Äquivalent *Theoretische Informatik* zurück, auch um das Ganze hier nicht zu überfrachten — und vor allem damit's nicht zu „abgefahren“  $\ddot{\text{S}}$  daherkommt.)

### 4.1.1 Natürliche Zahlen

Das Induktions-Prinzip folgt immer dem gleichen Schema: Zunächst zeigt man die Gültigkeit auf einer sehr elementaren *Basis*<sup>2</sup> ( $n_0$ ), nimmt die zu beweisende Behauptung für einen allgemeinen Fall (z. B.  $n-1$ ) als gültige *Hypothese* an und zeigt dann in einem konstruktiven realen *Schritt* (z. B. von  $n-1$  nach  $n$ ), dass sich diese Hypothese hierdurch auf die nächst größere Struktur (z. B.  $n$ ) erweitern lässt — welche exakt der Behauptung entspricht.<sup>3</sup> (Notationell wird die Ersetzung der Vorgänger-Struktur durch die Hypothesen-Formel im jeweiligen Schritt durch „!“ signalisiert.) Somit zeigt man, dass die Struktur der zu beweisenden Aussage durch das konstruktive Problemlösungs-Prinzip von der Lösungs-Formel für unendlich viele Fälle abgedeckt wird.<sup>4</sup> Folgende Beispiele illustrieren diese traditionelle Beweis-Technik:

<sup>1</sup>Verschiedene Wörter werden zunächst der Länge nach betrachtet/geordnet. Das „leere“ Wort  $\varepsilon$  hat die Länge 0, ein Wort bestehend aus nur einem Zeichen (eines gegebenen Alphabets) hat die Länge 1, ein Wort bestehend aus zwei Zeichen die Länge 2, usw. Wörter gleicher Länge werden lexikografisch (in der Regel aufsteigend) sortiert. So kann man jeder beliebigen Zeichen-Kette eine eindeutige natürliche Zahl zuordnen — weshalb man doch wieder in der bekannten Menge  $\mathcal{N}$  landet, und alles ist wie gehabt.

<sup>2</sup>optimalerweise kleinstmögliche Zahl (meist 0 oder 1, selten 2 oder 3, manchmal 4 oder 5)

<sup>3</sup>Formaler: Sei  $A(n)$  die Aussage, die es für beliebiges  $n$  zu beweisen gilt; hierzu zeigt man zunächst  $A(n_0)$  und konstruiert dann, basierend auf  $A(n-1)$ , mit einem problem-abhängigen Folge-Schritt  $A(n)$ .

<sup>4</sup>Die Sinnhaftigkeit dieses Vorgehens liegt im letzten Peano-Axiom begründet (siehe vorne ab S. 3).

### 1. Anzahl Kanten im „vollständigen Graphen“

Ein (allgemeiner) Graph besteht aus einer Menge  $V$  („vertices“) von  $n$  Knoten („nodes“) und einer Menge  $E$  („edges“) von Kanten. In der hier vorgestellten Spezial-Ausprägung führt von jedem Knoten genau eine Kante zu jedem anderen Knoten; Richtungen gibt es dabei keine — nur ungerichtete Verbindungen.

Sei  $n := |V|$ ,  $e_n := |E|$ ; dann gilt folgende Behauptung :

$$e_n = \frac{n \cdot (n - 1)}{2} .$$

Beweis: Induktion über  $n$  :

(a) Basis:  $n_0 := 1$

Prinzip:  $e_{1_p} = 0$  ( $\not\exists$  Kante bei nur 1 Knoten) ;

Formel:  $e_{1_F} = 1 \cdot (1 - 1)/2 = 0 = e_{1_p}$  .

Das Prinzip aus der realen Welt wird also von der Formel abgedeckt .

(b) Hypothese:

$$e_{n-1} = \frac{(n - 1) \cdot ((n - 1) - 1)}{2} \left[ = \frac{(n - 1) \cdot (n - 2)}{2} \right] .$$

(c) Schritt:  $(n_0 \leq) n - 1 \rightarrow n (> n_0)$

Idee: Die Kanten des nächst kleineren vollständigen Graphen werden weiterhin gebraucht, und der Knoten mit der Nummer  $n$  wird zu allen vorhandenen  $n - 1$  Knoten via jeweils einer weiteren Kante angebunden :

$$\begin{aligned} e_{n_p} &= e_{n-1} + (n - 1) \\ &\stackrel{!}{=} \frac{(n - 1) \cdot (n - 2)}{2} + \frac{2 \cdot (n - 1)}{2} \\ &= \frac{(n - 2 + 2) \cdot (n - 1)}{2} \\ &= \frac{n \cdot (n - 1)}{2} = e_{n_F} . \end{aligned}$$

Der Beweis der Behauptung ergibt sich demnach durch das Aufsetzen eines konstruktiven Schrittes auf die Hypothese und somit durch das prinzipielle Überführen eines Welt-Ausschnitts in eine Formel.

### 2. Anzahl Knoten im „Entscheidungs-Baum“

Gegeben ist ein Baum mit Verzweigungs-Faktor<sup>5</sup>  $b$  und Entwicklungs-Stufe<sup>6</sup>  $l$  (hier die Anzahl beteiligter Variablen reflektierend). Im Bild 4.1 sehen wir einen, wie in der Informatik üblich, nach unten hängenden Binär-Baum ( $b := 2$ ) mit 3

---

<sup>5</sup>(Entscheidungs-Grad) engl.: branching factor

<sup>6</sup>engl.: level

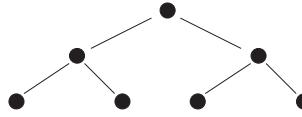


Abb. 4.1: Entscheidungs-Baum

Ebenen, welche die Stufen-Nummern 0 (Wurzel-Ebene), 1 (mittlere Ebene hier) und 2 (=:  $l$ , „Blatt-Ebene“) als Namen tragen. Wir können es so interpretieren: Die Wurzel-Position entspricht unserem Stand-Punkt. Von hier verzweigen wir bei der Entscheidung bzgl. Variable 1 gemäß „if\_then\_else“ nach links zu „then“ und nach rechts zu „else“, auf der nächsten Entscheidungs-Ebene bzgl. Variable 2 nach links wieder zu „then“ und nach rechts wieder zu „else“, usw.; wenn wir alle Variablen in Betracht ziehen, so haben wir auf der (letzten) Blatt-Ebene  $l$  genau  $2^l$  „Blätter“. Liest man „then“ als *true* („1“) und „else“ als *false* („0“), so finden sich auf dieser Ebene  $l$  von rechts nach links die Binär-Kodierungen, rechts anfangend bei der kleinsten Zahl 0 bis links hin zur größten Zahl  $2^l - 1$ , womit  $2^l$  Zahlen kodiert wären. Dies entspricht der Anzahl Zeilen einer booleschen Wertetafel, die für  $l$  Variablen so alle  $2^l$  *false/true*-Belegungs-Kombinationen darstellt.

Wir interessieren uns, bspw. zur Bestimmung des Speicher-Bedarfs in der Spiele-Programmierung, für die Gesamt-Anzahl an Knoten (Spiel-Konfigurationen) im Baum, wenn jede Ebene vollständig besetzt ist, man also auf allen Positionen die volle Entscheidungs-Freiheit hat.

Sei  $b_{[> 1]} :=$  Verzweigungs-Faktor,

$l :=$  Such-Tiefe (letzte Entscheidungs-Ebene),

$s_b(l) :=$  Summe aller Knoten über alle Ebenen (von 0 bis  $l$ ); dann gilt folgende

Behauptung (*geometrische Reihe*<sup>7</sup>) :

$$s_b(l) = \frac{b^{(l+1)} - 1}{b - 1} .$$

Beweis: Induktion über  $l$  [ $= \log_b(b^l) \in \mathcal{N}$ ] :

(a) Basis:  $l_0 := 0$

Prinzip:  $s_b(0)_P = 1$  ( $\exists!$  Knoten: Wurzel) ;  
Formel:  $s_b(0)_F = (b^{(0+1)} - 1)/(b - 1) = (b - 1)/(b - 1) = 1 = s_b(0)_P$  .

(b) Hypothese:

$$s_b(l - 1) = \frac{b^{((l-1)+1)} - 1}{b - 1} \quad \left[ = \frac{b^l - 1}{b - 1} \right] .$$

<sup>7</sup> mit  $a_0 := 1$ ,  $a_i :=_{[i > 0]} a_{i-1} \cdot b_{\text{Bruch}}$ ;  $\sum_{i=0}^l a_i = \sum_{i=0}^l b^i =: s_b(l)$

(c) Schritt:  $(l_0 \leq) l - 1 \rightarrow l (> l_0)$

Zur bisherigen Summe kommen auf der neuen Ebene  $l$  noch  $b^l$  Knoten hinzu:

$$\begin{aligned}
 s_b(l)_P &= s_b(l-1) + b^l \\
 &\stackrel{!}{=} \frac{b^l - 1}{b - 1} + \frac{(b-1) \cdot b^l}{b-1} \\
 &= \frac{b^l - 1 + b^{(l+1)} - b^l}{b-1} \\
 &= \frac{b^{(l+1)} - 1}{b-1} = s_b(l)_F
 \end{aligned} .$$

### 3. Anzahl vollbesetzter Ebenen im „Fibonacci-Baum“

Gegeben ist folgende (zunächst) rekursive Bildung der Fibonacci-Zahlen :

$$F_0 := 0, \quad F_1 := 1; \quad F_{n[>1]} := F_{n-1} + F_{n-2}, \quad n \geq 2 .$$

Wir berechnen bspw.  $F_6$ . Dieser Index 6 (die Eingabe-Größe  $n$ ) ist (üblicherweise) unter den beiden gegebenen Index-Basen 0 (in  $F_0$ ) und 1 (in  $F_1$ ) nicht vertreten; sein  $F$ -Wert lässt sich nicht direkt ablesen. Wir ersetzen den allgemeinen Index  $n$  mit der konkreten Eingabe 6 und nehmen die Rekursion als Rechen-Vorschrift :

$$F_6 := F_{6-1} + F_{6-2} .$$

Auch  $F_5$  steht nicht unmittelbar zur Verfügung, weshalb wir auch dies (wiederum rekursiv) herleiten, usw. Es ergibt sich der in Bild 4.2 dargestellte Binär-Baum von Rekursions-Aufrufen der Fib-Funktion:

Sei  $c_n := \#$  vollständig<sup>8</sup> besetzter  $F$ -Ebenen beim Aufruf-Index  $n$ ; es gilt folgende Behauptung :

$$c_n = 1 + \left\lfloor \frac{n}{2} \right\rfloor .$$

Beweis: Induktion über  $n$  :

(a) Basis:

- i.  $n_0 := 0$ 
  - $c_{0_P} = 1$  (Top-Level:  $F_0$ ) ,
  - $c_{0_F} = 1 + \left\lfloor \frac{0}{2} \right\rfloor = 1 = c_{0_P}$  ;
- ii.  $n_1 := 1$ 
  - $c_{1_P} = 1$  (Top-Level:  $F_1$ ) ,
  - $c_{1_F} = 1 + \left\lfloor \frac{1}{2} \right\rfloor = 1 = c_{1_P}$  .

---

<sup>8</sup>engl.: completely

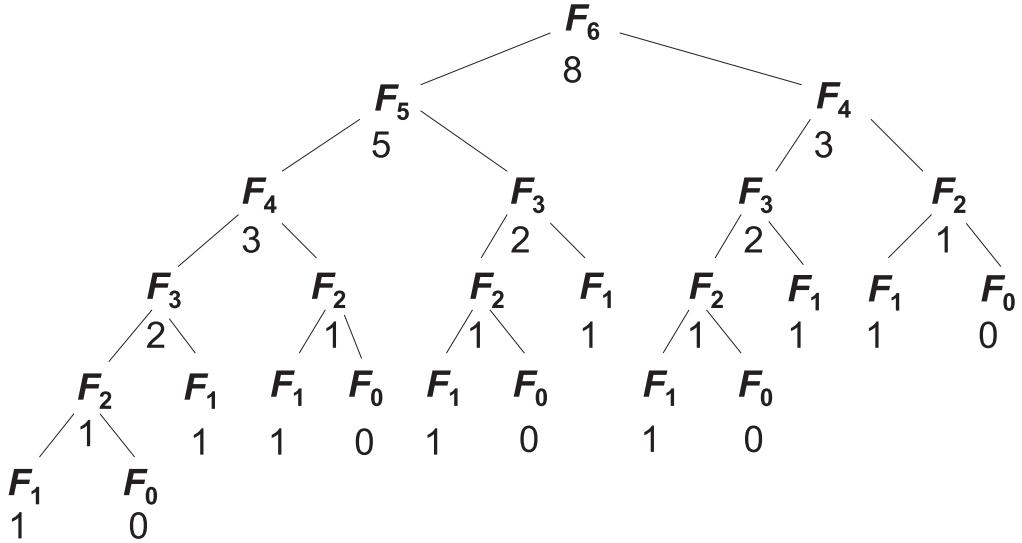


Abb. 4.2: Fib-Baum

(b) Hypothese:

$$c_{n-1} = 1 + \left\lfloor \frac{n-1}{2} \right\rfloor, \quad c_{n-2} = 1 + \left\lfloor \frac{n-2}{2} \right\rfloor.$$

(c) Schritt:  $(n_0 \leq) n-2, n-1 \rightarrow n (> n_1 > n_0)$ 

Idee: Wir nehmen das Minimum der beiden Vorgänger-Werte, da es nur um die vollständig besetzten Ebenen geht; durch den neuen Aufruf-Index  $n$  wird eine weitere (Top-)Ebene<sup>9</sup> eingezogen, weshalb man 1 addiert :

$$\begin{aligned} c_{n_P} &= 1 + \min\{c_{n-1}, c_{n-2}\} \\ &= 1 + \min \left\{ 1 + \left\lfloor \frac{n-1}{2} \right\rfloor, 1 + \left\lfloor \frac{n-2}{2} \right\rfloor \right\} \\ &= 1 + \begin{cases} \frac{2+(n-2)}{2} &; \text{gerade}(n) \\ \frac{2+((n-2)-1)}{2} &; \text{ungerade}(n) \end{cases} \\ &= 1 + \begin{cases} \frac{n}{2} &; \text{gerade}(n) \\ \frac{n-1}{2} &; \text{ungerade}(n) \end{cases} \\ &= 1 + \left\lfloor \frac{n}{2} \right\rfloor = c_{n_F} \end{aligned}.$$

<sup>9</sup>mit neuer Wurzel zur Verbindung der 2 vorherigen (Teil-)Bäume mit den Indizes  $n-1$  und  $n-2$

Laut vorherigem („2.“) Beispiel geht die Ebenen-Nummer als Exponent in die Formel zur Bestimmung der Knoten-Anzahl im Baum ein — weshalb man leicht sieht, dass bereits durch die vollständig besetzten Ebenen die Anzahl der Funktions-Aufrufe exponentiell bezogen auf den Eingabe-Index ausfällt.<sup>10</sup>

Es gibt natürlich einen linearen Algorithmus, der — „bottom-up“ (iterativ) — bei den Basis-Indizes anfangend, sich nacheinander zum Index  $n$  nach vorne hängelt und somit einfach proportional zur Eingabe-Größe nach  $n$  Schritten  $F_n$  ausgibt. Wir betreiben jedoch hier keine Algorithmitik, sondern explizieren lediglich das Induktions-Prinzip.

Nun, es gibt noch eine Methode, deren Rechen-Zeit sich sogar „konstant“, bezogen auf den Eingabe-Index  $n$ , verhält:<sup>11</sup>

#### 4. Binet's geschlossene „Fib-Formel“

Sei  $\phi := (1 + \sqrt{5}) / 2$ ,  $\psi := (1 - \sqrt{5}) / 2$ ; dann gilt folgende Behauptung für die Fibonacci-Zahl mit Eingabe-Index  $n$  :

$$f_n = \frac{\phi^n - \psi^n}{\sqrt{5}} \quad [\in \mathbb{N}] \quad .$$

Beweis: Induktion über  $n$  :

(a) Basis:

$$\begin{aligned} \text{i. } n_0 &:= 0 & & ; \\ \bullet f_{0_P} &= 0 & \text{(erster gegebener Basis-Wert)} & ; \\ \bullet f_{0_F} &= (\phi^0 - \psi^0) / \sqrt{5} = (1 - 1) / \sqrt{5} = 0 = f_{0_P} & & ; \end{aligned}$$

$$\begin{aligned} \text{ii. } n_1 &:= 1 & & ; \\ \bullet f_{1_P} &= 1 & \text{(letzter gegebener Basis-Wert)} & ; \\ \bullet f_{1_F} &= (\phi^1 - \psi^1) / \sqrt{5} = ((1 + \sqrt{5}) / 2 - (1 - \sqrt{5}) / 2) / \sqrt{5} = \\ &= ((1 + \sqrt{5}) - (1 - \sqrt{5})) / (2\sqrt{5}) = (1 - 1 + 2\sqrt{5}) / (2\sqrt{5}) = \\ &= 1 = f_{1_P} & & . \end{aligned}$$

(b) Hypothese:

$$f_{n-1} = \frac{\phi^{(n-1)} - \psi^{(n-1)}}{\sqrt{5}} \quad ;$$

$$f_{n-2} = \frac{\phi^{(n-2)} - \psi^{(n-2)}}{\sqrt{5}} \quad .$$

(c) Schritt:  $(n_0 \leq) n - 2, n - 1 \rightarrow n (> n_1 > n_0)$

$$f_{n_P} = f_{n-1} + f_{n-2} \stackrel{!}{=} \quad$$

---

<sup>10</sup>Zur Nutzung der Behauptung auf S. 37:  $l := c_n$ ; da  $c_n$  linear von  $n$  abhängt, gilt o. g. Bemerkung.

<sup>11</sup>Wir betrachten keinen Speicher-Platz.

$$\begin{aligned}
& \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-1)} - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-1)}}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-2)} - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-2)}}{\sqrt{5}} \\
= & \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-2)} \cdot \left(\frac{1+\sqrt{5}}{2} + 1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-2)} \cdot \left(\frac{1-\sqrt{5}}{2} + 1\right)}{\sqrt{5}} \\
= & \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-2)} \cdot \frac{(1+\sqrt{5}+2) \cdot 2}{2 \cdot 2} - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-2)} \cdot \frac{(1-\sqrt{5}+2) \cdot 2}{2 \cdot 2}}{\sqrt{5}} \\
= & \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-2)} \cdot \frac{1+2\sqrt{5}+5}{2^2} - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-2)} \cdot \frac{1-2\sqrt{5}+5}{2^2}}{\sqrt{5}} \\
= & \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{(n-2)} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{(n-2)} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} \\
= & \frac{\phi^n - \psi^n}{\sqrt{5}} = f_{n_F}
\end{aligned}$$

[Ausritt:  $\phi - Fib - GGT$ ]

- Binet's Formel eignet sich nicht im Reich der endlichen Zahlen-Darstellung des Computers. Wir kommen daher zurück auf das Nacheinander-Ausrechnen. Wenn wir nun eine kleine Abweichung akzeptieren, so schaffen wir es, nur auf 1 Vorgänger zurückzugreifen (und nicht auf 2 angewiesen zu sein). Holen wir zunächst das eben eingeführte  $\phi$  wieder hervor :

$$\phi := \frac{1 + \sqrt{5}}{2}$$

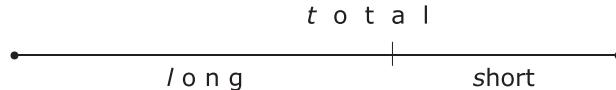
Wir beobachten (bzgl. der Fibonacci-Zahl mit Index  $i$  bzw. letztlich  $n$ ) :

$$\begin{aligned}
\frac{f_{i-1}}{f_{i-2}} < \phi < \frac{f_i}{f_{i-1}} ; i := 2k+1, k \in \mathcal{N} \setminus \{0\} [= \{1, 2, 3, \dots\}] ; \\
\lim_{n \rightarrow \infty} \frac{f_n}{f_{n-1}} = \phi & \quad [\approx \frac{8}{5}] \\
f_n \approx \phi \cdot f_{n-1} & ; n \geq 6
\end{aligned}$$

$\phi$  findet sich auch in anderen Bereichen wieder; es ist der „Goldene Sch.<sup>12</sup>“. In der (klassischen) Architektur repräsentiert er die als harmonisch angesehene Aufteilung einer Front-Ansicht in zwei unterschiedlich breite Teile, dargestalt, dass das Verhältnis der Gesamt-Länge zur längeren Teil-Seite identisch ist mit dem der längeren zur kürzeren Teil-Seite, wie in etwa in Bild 4.3 skizziert:

---

<sup>12</sup> ↗ Schnitt

**Abb. 4.3:** Goldener Schnitt

$$t := l + s ; \quad \frac{t}{l} = \frac{l}{s} .$$

$$\phi := \frac{l}{s} = \frac{t}{l} | \cdot ls \iff$$

$$l^2 = ts \iff$$

$$l^2 - ts = 0 \iff$$

$$l^2 - (l + s)s = 0 \iff$$

$$l^2 - sl - s^2 = 0 \iff$$

$$l = \frac{s}{2} \pm \sqrt{\left(-\frac{s}{2}\right)^2 - (-s^2)} \iff$$

$$l = \frac{s}{2} \pm \sqrt{\frac{s^2 + 4s^2}{4}} \iff$$

$$l = \frac{s}{2} \pm \sqrt{\left(\frac{s}{2}\right)^2 \cdot 5} \iff$$

$$l = \frac{s}{2} \cdot \left(1 \pm \sqrt{5}\right) [ > 0 ] \implies$$

$$l = \frac{1 + \sqrt{5}}{2} \cdot s | : s \iff$$

$$\frac{l}{s} = \frac{1 + \sqrt{5}}{2} =: \phi := \frac{t}{l} .$$

- Sei  $\text{GGT} :=$  größter gemeinsamer Teiler zweier Zahlen. Es gilt, ohne Beweis:

$$Fib(\text{GGT}(m, n)) = \text{GGT}(Fib(m), Fib(n)) .$$

Beispiel :

$$m := 6 , n := 9 ;$$

$$Fib(\text{GGT}(6, 9)) = Fib(\text{GGT}(3 \cdot 2, 3 \cdot 3)) = Fib(3) = 2 .$$

$$\text{GGT}(Fib(6), Fib(9)) = \text{GGT}(8, 34) = \text{GGT}(2 \cdot 4, 2 \cdot 17) = 2 .$$

### 5. Anzahl Zeilen in *boolescher* Werte-Tafel

Sei  $r_n := \#$  Zeilen<sup>13</sup> einer Werte-Tabelle für  $n$  *boolesche* Variablen; es gilt die Behauptung

$$r_n = 2^n$$

Beweis: Induktion über  $n$

(a) Basis:  $n_0 := 1$

$$\begin{array}{rcl} r_{1_p} & = & 2 \\ r_{1_F} & = & 2^1 = r_{1_p} \end{array} \quad [= |\{\text{false}, \text{true}\}|] ;$$

(b) Hypothese:

$$r_{n-1} = 2^{(n-1)}$$

(c) Schritt:  $(n_0 \leq) n - 1 \rightarrow n (> n_0)$

$$r_{n_p} = 2 \cdot r_{n-1} \stackrel{!}{=} 2^1 \cdot 2^{(n-1)} = 2^n = r_{n_F} .$$

Im aktuellen Beispiel stellt der Inhalt dieser  $2^n$  Zeilen die Binär-Notation der  $2^n$  Zahlen 0 bis  $2^n - 1$  dar. Hat man vorher  $2^{(n-1)}$  Zeilen, so bleiben diese bisherigen Zahlen durch Ergänzen einer führenden 0 erhalten, und es ergeben sich  $2^{(n-1)}$  neue größere Zahlen durch Voranstellen einer führenden 1, s. d. letztlich doppelt so viele Zahlen (hier Zeilen) zur Verfügung stehen wie vorher.

$2^n$  entspricht auch der Anzahl der Elemente in der Menge aller Teilmengen (Potenz-Menge) einer  $n$ -elementigen Grund-Menge. Das hier benutzte Induktions-Schema (Verdoppeln der Vorgänger-Struktur beim Übergang von  $n-1$  nach  $n$ ) findet sich demnach auch beim Bilden einer neuen größeren Potenz-Menge: Die  $2^{(n-1)}$  bisher vorhandenen Teilmengen bleiben alle erhalten, und zu jeder dieser Mengen wird als weitere Variante zusätzlich das neue Element gesteckt, weshalb man letztlich doppelt so viele Elemente in der Potenz-Menge wie vorher erhält — reflektiert durch den vorher genannten konstruktiven Schritt [in (c)] „ $2 \cdot$ “.

### 6. Anzahl *boolescher* Funktionen

Sei  $d_n := \#$  aller verschiedenen<sup>14</sup>  $n$ -stelligen *booleschen* Funktionen; es gilt die Behauptung

$$d_n = 2^{(2^n)}$$

Hintergrund: Ähnlich wie vorhin nehmen wir die Gesamtzahl möglicher Eingaben in den Exponenten der Potenz zur Basis 2 (da jede der  $2^n$  möglichen Input-Zeilen einen binären Funktions-Output hat).

Beweis: Induktion über  $n$

---

<sup>13</sup>engl.: *rows*

<sup>14</sup>engl.: *different*

(a) Basis:  $n_0 := 0$

$$\begin{aligned} d_{0_p} &= 2 [= |\{( \text{no input}, \text{false output}), (\text{no input}, \text{true output})\}|] , \\ d_{0_F} &= 2^{(2^0)} = 2^1 = d_{0_p} \\ \text{oder: } n'_0 &:= 1 \\ d_{1_p} &= 4 [= |\{(f_{in}, f_{out}), (f_{in}, t_{out}), (t_{in}, f_{out}), (t_{in}, t_{out})\}|] , \\ d_{1_F} &= 2^{(2^1)} = 2^2 = d_{1_p} \end{aligned} .$$

(b) Hypothese:

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

(c) Schritt:  $(n_0 \leq) n - 1 \rightarrow n (> n_0)$

Mit dem nächstgrößeren  $n$  verdoppelt sich gemäß vorigem Beispiel die Zeilen-Zahl, was sich im hiesigen Induktions-Schritt entsprechend bemerkbar macht:

$$\begin{aligned} d_{n_p} &= |\mathcal{B}|^{\# \text{Zeilen}_n} =_{\substack{\text{Schritt} \\ 5. \text{ Beispiel}}} 2^{(2 \cdot \# \text{Zeilen}_{n-1})} \\ &= (2^{\# \text{Zeilen}_{n-1}})^2 = (d_{n-1})^2 \stackrel{!}{=} (2^{(2^{(n-1)})})^2 \\ &= 2^{(2^{(n-1)} \cdot 2^1)} = 2^{(2^n)} = d_{n_F} \end{aligned} .$$

### 4.1.2 Wort-Längen

Idee: Das sogenannte „leere“<sup>15</sup> Wort  $\varepsilon$  hat die Länge 0; haben wir bereits ein Wort und hängen einen Buchstaben an, so erhalten wir ein neues Wort, welches 1 Zeichen mehr hat. Es lassen sich so alle möglichen Zeichenketten beliebiger Länge bilden. Obwohl ein zugrunde liegendes Alphabet selbst nur endlich viele Zeichen zur Auswahl bereitstellt, sind unendlich viele Wörter möglich; jedes davon ließe sich letztlich einer natürlichen Zahl eindeutig zuordnen.

Ein potentieller Induktions-Beweis geht nun folglich über die Wort-Länge („Breite“).<sup>16</sup>

Sei  $a$  ein Alphabet-Zeichen,  $\varepsilon$  das leere Wort sowie  $u, v$  und  $w$  beliebige Wörter; es gilt:

$$\begin{aligned} \varepsilon w &= w \varepsilon = w && , \\ (u v) w &= u (v w) && ; \\ |w| &:= \text{Wort-Breite} && : \\ |\varepsilon| &:= 0 && , \\ |u v| &= |u| + |v| && \Rightarrow \\ |v a| &= |v| + 1 && . \end{aligned}$$

3 Bemerkungen:

---

<sup>15</sup>engl.: empty

<sup>16</sup>Wir leisten hier Vor-Arbeit für das Thema *Formale Sprachen* im Bereich *Theoretische Informatik*.

- Letzteres gilt unter der syntaktischen Berücksichtigung eines Zeichens als ein Wort der Länge 1.
- Das Hintereinander-Platzieren zweier Wörter ist nicht kommutativ<sup>17</sup>; demnach gilt i. Allg.:  $uv \neq vu$ , was kommutative Spezial-Fälle natürlich nicht ausschließt.
- Die Klammern sind nicht Teil des Alphabets; sie mögen lediglich die Reihenfolge der Abarbeitung/Betrachtung verdeutlichen.

Anwendung: Wort-Umkehr<sup>18</sup>  $\rho: \rho(c_1 c_2 \dots c_n) = c_n \dots c_2 c_1$ ,  $c_{[1 \leq i \leq n]} := \text{Zeichen}^{19}$  :

$$\begin{aligned}\rho(\varepsilon) &= \varepsilon \\ \rho(va) &= a\rho(v)\end{aligned};$$

Ein längeres Wort, welches gegenüber „vorher“ um einen Buchstaben verlängert wurde, wird dadurch umgekehrt, indem man den Buchstaben am Ende entfernt und nach vorne bringt sowie den bereits „vorhandenen“ Wort-Stamm (bspw. nach dem gleichen Prinzip) ebenfalls umdreht. Es gilt ganz allgemein folgende Behauptung :

$$\rho(uv) = \rho(v)\rho(u);$$

Beweis: Induktion über die Wort-Länge  $n$  :

$$\begin{aligned}(a) \text{ Basis: } |w| := 0 & [= n_0; w := \varepsilon] \\ \text{Regel: } \rho(\varepsilon) &= \rho(\varepsilon\varepsilon) = \rho(\varepsilon)\rho(\varepsilon) \\ \text{Prinzip: } \rho(\varepsilon\varepsilon) &= \rho(\varepsilon) = \varepsilon = \varepsilon\varepsilon = \rho(\varepsilon)\rho(\varepsilon) \\ \text{oder: } \rho(uv) &:= \rho(u\varepsilon) = \rho(u) = \varepsilon\rho(u) = \rho(\varepsilon)\rho(u) = \rho(v)\rho(u).\end{aligned};$$

(b) Hypothese:

$$\begin{aligned}\rho(c_1 c_2 \dots c_n) &= c_n \dots c_2 c_1 \\ \rho(uv) &= \rho(v)\rho(u)\end{aligned};$$

$$(c) \text{ Schritt: } (n_0 \leq |v| \Rightarrow n \xrightarrow{\text{hierr}} n+1 \quad (= |va| > n_0))$$

$$\begin{aligned}w &:= va \\ \rho(uw) &= \rho(u(va)) = \rho((uv)a) = a\rho(uv) \\ &\stackrel{!}{=} a(\rho(v)\rho(u)) = (a\rho(v))\rho(u) \\ &= \rho(va)\rho(u) = \rho(w)\rho(u)\end{aligned};$$

Wir konnten beweisen, dass jedes beliebige Wort dadurch umgekehrt werden kann, indem man einen hinteren (Wort-)Teil umgedreht nach vorne und den alten vorderen Teil umgedreht nach hinten bringt — unabhängig der Wort-Länge.

<sup>17</sup>man denke nur an die Reihenfolge von Vor- und Nach-Namen

<sup>18</sup>engl.: reverse (hier via o. g. griech. Buchstaben „rho“)

<sup>19</sup>engl.: character

## 4.2 Direkter Beweis

Bei diesem Vorgehen startet man bei einer gesicherten Ausgangs-Basis, macht einige gültige Schritte („Äquivalenz-Transformationen“), um *direkt* die Behauptung zu liefern. Um Ihnen/dir den Vergleich verschiedener Beweis-Verfahren zu erleichtern, vollziehen wir das Prinzip *Direkter Beweis* auf den bereits im vorherigen Abschnitt vorgestellten ersten beiden Beispielen.

1. Illustration: Es gilt die inzwischen aus Unter-Abschnitt 4.1.1 (1. Beispiel)<sup>20</sup> bekannte Behauptung :

$$e_n = \frac{n \cdot (n - 1)}{2} .$$

Beweis: direkt :

$$\begin{aligned} e_n &= e_{n-1} + (n - 1) &= 1 + 2 + 3 + \dots + (n - 3) + (n - 2) + (n - 1); \\ &+ &[ (n - 1) + (n - 2) + (n - 3) + \dots + 3 + 2 + 1 ] \end{aligned}$$


---

$$2 \cdot e_n = n \cdot (n - 1) | : 2$$

$$\iff e_n = \frac{n \cdot (n - 1)}{2} .$$

(Diese Formel zur Summe der ersten  $n - 1$  natürlichen Zahlen ist „common folklore“.)

2. Illustration: Es gilt die inzwischen aus Unter-Abschnitt 4.1.1 (2. Beispiel)<sup>21</sup> bekannte Behauptung :

$$s_{b[>1]}(l) := \sum_{i:=0}^l b^i = \frac{b^{(l+1)} - 1}{b - 1} .$$

Beweis: direkt :

$$\begin{aligned} 1 \cdot s_b(l) &= b^0 + b^1 + b^2 + \dots + b^{(l-1)} + b^l &| \cdot b \\ - [b \cdot s_b(l)] &= b^1 + b^2 + b^3 + \dots + b^l + b^{(l+1)} \end{aligned}$$


---

$$(1 - b) \cdot s_b(l) = 1 - b^{(l+1)} | : (1 - b)$$

<sup>20</sup>Seite 36

<sup>21</sup>Seite 37

$$\begin{aligned} \iff s_b(l) &= \frac{1 - b^{(l+1)}}{1 - b} & | \cdot \frac{-1}{-1} \\ \iff s_b(l) &= \frac{b^{(l+1)} - 1}{b - 1} \end{aligned} .$$

Man notiert die Ausgangs-Lage nur etwas ausführlicher, wählt „geschickt“<sup>22</sup> eine einfache mathematische Operation, macht einige wenige Schritte, und das Ding ist bewiesen.

## 4.3 Indirekter Beweis

Diese Philosophie basiert auf der „contrapositive“-Äquivalenz<sup>23</sup> der Booleschen Algebra:

$$a \rightarrow c \iff \neg c \rightarrow \neg a ;$$

die Werte-Tafel in Bild 4.4 zeigt anschaulich die Gültigkeit dieses Prinzips.

<b>a</b>	<b>c</b>	<b>a → c</b>	<b>¬c → ¬a</b>	<b>¬c</b>	<b>¬a</b>
0	0	1	1	1	1
0	1	1	1	0	1
1	0	0	0	1	0
1	1	1	1	0	0

**Abb. 4.4:** Indirekter Beweis

Wir negieren zunächst die Aussagen-Variable  $c$  — in der Hoffnung, nach sauberen Transformations-Schritten bei der Negation der Ausgangs-Basis ( $\neg a$ ) zu landen — ein sogenannter Widerspruchs-Beweis. Wie auch beim *direkten* Beweis wird  $a$  aber eigentlich als gesichert angesehen; kommen wir jedoch hier nun zwischenzeitlich zu dem Punkt, dass  $a$  doch nicht zu gelten scheint, dann kann es nur an der falschen Annahme ( $\neg c$ ) gelegen haben — weshalb also doch  $c$  gilt, was man so auf *indirektem* Weg gezeigt hat.

Beispiel: Das Quadrieren einer natürlichen Zahl ist invariant hinsichtlich ihrer Parität (*gerade/ungerade* zu sein), und die Wurzel(-Ausgabe) einer Quadrat-Zahl hat die gleiche Parität wie deren Eingabe.

Vorbemerkungen zur Parität  $p$

- $p(2i) = \text{gerade} \neq \text{ungerade} = p(2i + 1)$  ,
- $p(i) = \text{gerade} \oplus p(i) = \text{ungerade} ; \quad \forall i \in \mathcal{N}$  .

---

<sup>22</sup>ok, auf genau diese vorher präsentierte Idee muss man natürlich erst einmal kommen ☺

<sup>23</sup>ausgehend von: „antecedent“ → „consequent“; siehe Unter-Abschnitt 3.2.1, Seite 32

(Man kann sie als Funktion ansehen; damit hat jede natürliche Zahl genau 1 Parität.)

Für jedes beliebige  $n \in \mathbb{N}$  gilt folgende, im laufenden Beispiel bereits textuell genannte, Behauptung:

$$p(n^2) = p(n).$$

Wir teilen den Beweis auf

1.  $p(n^2) = \text{gerade} \implies p(n) = \text{gerade},$
2.  $p(n^2) = \text{ungerade} \implies p(n) = \text{ungerade};$
3.  $p(n) = \text{gerade} \implies p(n^2) = \text{gerade},$
4.  $p(n) = \text{ungerade} \implies p(n^2) = \text{ungerade}.$

Die zweite Hälfte können wir uns schenken; kümmern wir uns um die ersten zwei Fälle:

Beweis: indirekt

1. Zu zeigen:  $p(n^2) = \text{gerade} \implies p(n) = \text{gerade} :$

$$\begin{aligned} p(n) &\neq \text{gerade} [p(n) = \text{ungerade}] \implies n := 2i+1; \\ p(n^2) &= p((2i+1)^2) = p(4i^2+4i+1) = p(2 \cdot (2i^2+2i)+1) \\ &= [p(1) =] \text{ ungerade} \neq \text{gerade}_{\text{Ausgangs-Basis}} \implies \\ p(n) &= \text{ungerade} [\neq \text{gerade}] \implies p(n^2) = \text{ungerade} [\neq \text{gerade}] \\ &\quad \iff_{\text{indirekter Beweis}} \end{aligned}$$

$$p(n^2) = \text{gerade} \implies p(n) = \text{gerade}.$$

2. Zu zeigen:  $p(n^2) = \text{ungerade} \implies p(n) = \text{ungerade} :$

$$\begin{aligned} p(n) &\neq \text{ungerade} [p(n) = \text{gerade}] \implies n := 2i; \\ p(n^2) &= p((2i)^2) = p(4i^2) = p(2 \cdot 2i^2) \\ &= [p(0) =] \text{ gerade} \neq \text{ungerade}_{\text{Ausgangs-Basis}} \implies \\ p(n) &= \text{gerade} [\neq \text{ungerade}] \implies p(n^2) = \text{gerade} [\neq \text{ungerade}] \\ &\quad \iff_{\text{indirekter Beweis}} \end{aligned}$$

$$p(n^2) = \text{ungerade} \implies p(n) = \text{ungerade}.$$

# 5 Zähl-Techniken

Wir kommen nun zum Höhepunkt im hinteren Teil dieses Buches. Zunächst beleuchten wir einige grundlegende Techniken wie Summen-, Produkt- und Quotienten-Regel<sup>1</sup> sowie das Schubfach-Prinzip. Anschließend betrachten wir den sich abwechselnd gestaltenden Ein-/Ausschluss von Mengen-Ausdrücken, hauptsächlich zur Bestimmung der Anzahl der Elemente in der Vereinigung mehrerer nicht-schnittfreier Mengen. Sodann wenden wir uns meiner Lieblings-Technik, der Rekurrenz-Relation, zu. Dabei versuche ich, Sie mit auf eine Kreativitäts-Reise zu nehmen; schließlich ist der Hauptzweck eines solchen Werkzeugs einer geschlossenen (Zähl-)Formel kreativ auf die Spur zu kommen. Danach behandeln wir die Klassiker unter den Zähl-Problemen: die Anzahl verschiedener Reihenfolgen (Permutationen) bzw. Auswahlen (Kombinationen); dabei unterscheiden wir zwischen Objekten verschiedenen und gleichen Typs. Abschließend lernen Sie die Stirling-Zahlen erster und zweiter Art, inklusive deren für uns wichtigeren Interpretation als Zyklen- resp. Teilmengen-Zahl, kennen, sowie die Bell-Zahlen — sie sind das Letzte ☺. (Weiterführendes findet sich in meinem hinten gelisteten Informatik-Buch, 1. Kapitel, wo ich im Abschnitt „1.4 Zähltechniken“ [S. 14–16] u. a. aus der beliebten ausgangssperren-freien Bar-Welt ein Schmankerl zum „Ziehen mit Zurückgeben“ ☺ präsentiere. [Dort im Anschluss lauert ebenso noch ein Einstieg in die *Kryptologie* — die *Eulersche*  $\phi$ -Funktion {für die endliche Gruppen-Ordnung}, der *Kleine* ☺ *Satz von Euler-Fermat* sowie dessen Einsatz im Spezial-Fall einer *Prim*-Zahl im *RSA*-Verfahren.])

## 5.1 Grundlegendes

### 5.1.1 Summen-Regel

Gegeben seien  $m$  unterschiedliche Fälle à  $n_i$  ( $1 \leq i \leq m$ ) verschiedener Optionen; dann ist die (An-)Zahl differierender Möglichkeiten

$$z = \sum_{i:=1}^m n_i .$$

Lassen Sie uns ein Mini-Beispiel aus der Informatik betrachten:

Die (Zeichen-)Länge  $l$  eines Zugangs-Kennwortes soll zwischen 1 und 3 liegen; bei  $l := 1$  darf beliebig eine Ziffer oder ein Vokal benutzt werden, bei  $l := 2$  muss eine Ziffer vorangestellt werden und bei  $l := 3$  zusätzlich vorne zwingend ein Vokal stehen.

Frage: Wie viele Möglichkeiten der Bildung eines solchen<sup>2</sup> Kennwortes gibt es ?

<sup>1</sup>alle nicht zu verwechseln mit gleichlautenden Begriffen der Differential-Analysis

<sup>2</sup>zugegebenermaßen recht unsicheren

Antwort :

$$\begin{aligned} z &= \sum_{i:=1}^3 n_i = |\{0, 1, 2, \dots, 9\} \cup \{\text{a, e, i, o, u}\}| + 10 \cdot 15 + 5 \cdot 150 = \\ &15 \cdot (1 + 10 + 5 \cdot 10) = 15 \cdot 61 = 915 . \end{aligned}$$

Zusatz-Frage :

Welches  $z$  ergibt sich, wenn wir die Zeichenkette nun von der anderen Seite kommend entwickeln, d. h. bei  $l := 1$  zunächst einen Vokal fordern, bei  $l := 2$  dahinter eine Ziffer verlangen und bei  $l := 3$  abschließend entweder eine Ziffer oder einen Vokal vorsehen? Bevor Sie's ausrechnen: Wird nicht eh das Gleiche dabei herauskommen? Hier nun die Zusatz-Antwort :

$$\begin{aligned} z &= \sum_{i:=1}^3 n_i = 5 + 5 \cdot 10 + 50 \cdot 15 = \\ &5 \cdot (1 + 10 + 10 \cdot 15) = 5 \cdot 161 = 805 \neq 915 . \end{aligned}$$

Einer der 3 in der Summen-Formel genannten Summanden ist jedoch selbstverständlich identisch mit dem gleichnamigen Summanden aus der ersten Antwort. Welches  $n_i$  ist's?<sup>3</sup>

Eine komplexere Erweiterung findet sich im hinten zitierten Informatik-Buch (S. 16–21).

### 5.1.2 Produkt-Regel

Gegeben seien  $m$  (unterschiedliche) Schritte (Positionen) à  $n_i$  ( $1 \leq i \leq m$ ) verschiedener Optionen (bzw. Belegungen); dann ist die (An-)Zahl differierender Möglichkeiten

$$z = \prod_{i:=1}^m n_i .$$

Lassen Sie uns ein Standard-Beispiel aus der Informatik betrachten:

die Bestimmung der (An-)Zahl der Kodier-Möglichkeiten eines  $m$ -stelligen Bit-Vektors<sup>4</sup>.

Frage: Wie viele Möglichkeiten der Bildung eines solchen „Wortes“ gibt es ?

Antwort :

$$z = \prod_{i:=1}^m n_i = |\mathcal{B}|^m = 2^m [= |\mathcal{B}^m|] .$$

---

<sup>3</sup> $n_m$  (=hier  $n_3$ ) =  $50 \cdot 15 = 5 \cdot 150 = 750$ )

<sup>4</sup>Binär-Zeichenkette mit vorgegebener Länge  $l := m$  und Belegungs-Optionen auf jeder Position aus der 2-wertigen Menge  $\mathcal{B} := \{0, 1\}$

### 5.1.3 Quotienten-Regel

Gegeben sei eine Aufteilung einer  $n$ -elementigen Menge  $S$  in gleichgroße Teilmengen à  $(0 <) m (< n)$  Elemente; dann ist die (An-)Zahl dieser Teilmengen

$$z = \frac{n}{m}$$

Betrachten wir ein interessantes Beispiel aus der Welt der Permutationen (ab S. 73): die (An-)Zahl unterschiedlicher zyklischer Vertauschungen  $m$  verschiedener Elemente.

Frage:

Wie viele verschiedene Möglichkeiten der Anordnung<sup>5</sup> von  $m$  Personen an einem Rund-Tisch gibt es, wobei es auf die Platzierungs-Positionen am Tisch selbst nicht ankommt?

(Hierbei lässt sich das !-Zeichen für die „Fakultät“ schön einbringen; siehe das hier bald folgende letzte Rekurrenz-Beispiel sowie der anschließende Abschnitt „Permutationen“.)

Antwort:  $z = n/m = m!/m = (m-1)! \cdot m/m = (m-1)!$

Erläuterung:

$S :=$  Menge aller prinzipiell möglichen Anordnungen von  $m$  Personen;  $|S| = m! =: n$ . Jeweils  $m$  gleichwertige Rund-Anordnungen lassen sich durch 1 Repräsentanten vertreten. Dann gibt  $z = n/m$  die (An-)Zahl unterschiedlicher Repräsentanten an, wobei jeder eine Teilmenge aller Anordnungen nur zyklisch verschobener Elemente darstellt.

### 5.1.4 Schubfach-Prinzip

Diese einfache, jedoch sehr nützliche, Überlegung<sup>6</sup> ist auch bekannt unter dem Begriff „pigeonhole principle“ bzw. „Verteilung in Taubenhöhlen“:  $t$  Tauben fliegen in  $h$  Höhlen; dann gibt es zumindest 1 Höhle mit mindestens folgender Anzahl Tauben :

$$z = \left\lceil \frac{t}{h} \right\rceil$$

Beispiel: Prüfungs-Organisation

$$\begin{aligned} t &:= \# \text{ StudentINNen} \\ h &:= \# \text{ Prüfungs-Räumlichkeiten} \end{aligned}$$

Dann ist es nicht möglich, dass in jedem Prüfungsraum weniger als  $z$  Studierende sitzen; positiv formuliert: es gibt (zumindest) 1 Raum mit mindestens  $z := \lceil t/h \rceil$  Studierenden.

Illustration: Gegeben sind die beiden Werte  $t := 65$  und  $h := 3$ .

Frage: Welche Zahl ergibt sich für  $z$  ?

---

<sup>5</sup>bezogen auf „befindet sich genau 1 Position links (bzw. „rechts“, je nach Blick-Richtung) neben“

<sup>6</sup>aus 1834 — Johann Peter Gustav Lejeune Dirichlet

Antwort

$$z = \left\lceil \frac{65}{3} \right\rceil = \left\lceil \frac{63+2}{3} \right\rceil = \left\lceil 21 + \frac{2}{3} \right\rceil = 22$$

Interpretation:

Es reicht nicht aus, in jeden Raum nur 21 Stühle zu platzieren; zumindest in einem Raum müssen mindestens 22 stehen (nicht Studierende, sondern Stühle zur Verfügung).

## 5.2 Ein-/Ausschluss

Hier geht es um das Zählen der Elemente in der Vereinigung von Mengen, welche nicht disjunkt<sup>7</sup> sein müssen. Zunächst einmal beziffern wir für  $n$  gegebene Mengen die Zahl nicht-leerer Kombinationen<sup>8</sup>

$$\sum_{i=1}^n \binom{n}{i} = \sum_{i=0}^n \binom{n}{i} - \binom{n}{0} = 2^n - 1$$

Dies ist die Anzahl der Terme im nun folgenden Ausdruck zur Berechnung der Anzahl der  $v$  Elemente in der Mengen-Vereinigung

$$v = \left| \bigcup_{k=1}^n A_k \right| = \sum_{k=1}^n \left( (-1)^{(k+1)} \cdot \sum_{1 \leq i_1 < \dots < i_k \leq n} |\cap A_{i_j}| \right)$$

Was zunächst unhandlich daherkommt, wird klar anhand folgender Konkretisierungen:

i)  $n := 1$

Aufbau

$$\bigcup_{k=1}^1 A_k = A ;$$

(Zähl-)Formel

$$\begin{aligned} \left| \bigcup_{k=1}^1 A_k \right| &= \sum_{k=1}^1 \left( (-1)^{(k+1)} \cdot \sum_{1 \leq i_1 < \dots < i_k \leq 1} |\cap A_{i_j}| \right) = \\ &(-1)^{(1+1)} \cdot |\cap A_1| = (-1)^2 \cdot |\cap A| = |A| \end{aligned}$$

---

<sup>7</sup>schnitt-frei (kein [gemeinsames] Element im [leeren] Mengen-Schnitt)

<sup>8</sup>Die folgende Notation  $\binom{n}{k}$ , manchmal  $C(n, k)$  geschrieben, wird im Unter-Abschnitt 5.4.2 (ab S. 76) vorgestellt: die Anzahl Möglichkeiten, aus einer  $n$ -elementigen Menge  $k$  Elemente auszuwählen.

ii)  $n := 2$ 

Aufbau

$$\bigcup_{k:=1}^2 A_k = A_1 \cup A_2 ;$$

(Zähl-)Formel

$$\left| \bigcup_{k:=1}^2 A_k \right| = \sum_{k:=1}^2 \left( (-1)^{(k+1)} \cdot \sum_{1 \leq i_1 < \dots < i_k \leq 2} |\cap A_{i_j}| \right) =$$

$$(-1)^{(1+1)} \cdot (|A_1| + |A_2|) + (-1)^{(2+1)} \cdot |A_1 \cap A_2| =$$

$$|A_1| + |A_2| - |A_1 \cap A_2|$$

iii)  $n := 3$ 

Aufbau

$$\bigcup_{k:=1}^3 A_k = A_1 \cup A_2 \cup A_3 ;$$

(Zähl-)Formel

$$\left| \bigcup_{k:=1}^3 A_k \right| = \sum_{k:=1}^3 \left( (-1)^{(k+1)} \cdot \sum_{1 \leq i_1 < \dots < i_k \leq 3} |\cap A_{i_j}| \right) =$$

$$(-1)^{(1+1)} \cdot (|A_1| + |A_2| + |A_3|) +$$

$$(-1)^{(2+1)} \cdot (|A_1 \cap A_2| + |A_1 \cap A_3| + |A_2 \cap A_3|) +$$

$$(-1)^{(3+1)} \cdot |A_1 \cap A_2 \cap A_3| =$$

$$|A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3| .$$

Zwei Beispiele mögen die Anwendung dieses Zähl-Prinzips verdeutlichen :

a) Eine Fußball-Trainerin findet folgende Situation vor :

$$\begin{aligned}
 S &:= \text{Menge aller Spielerinnen im Kader } (S := D \cup F \cup N, \text{ siehe gleich}), |S| := 13 , \\
 D &:= \text{Menge der Fußballerinnen, welche Verteidigung spielen können}, |D| := 9 , \\
 F &:= \text{Menge der Fußballerinnen, welche im Sturm spielen können}, |F| := 6 , \\
 N &:= \text{Menge der Nicht-Spielerinnen (zu schlecht oder verletzt)}, |N| := 2 ; \\
 M &:= \text{Menge der Mittelfeld-Spielerinnen (midfielders)} :=_{\text{hier}} D \cap F , \\
 D_o &:= \text{Menge der reinen Verteidigerinnen (defenders}_{\text{only}}\text{)} , \\
 F_o &:= \text{Menge der reinen Stürmerinnen (forwards}_{\text{only}}\text{)} .
 \end{aligned}$$

Die Trainerin interessiert sich bei der Mannschaftsaufstellung für die Beantwortung der Frage:

Haben wir genug Mittelfeld-Spielerinnen; wie viele Fußballerinnen können nur hinten in der Verteidigung, wie viele nur vorne als Stürmerinnen eingesetzt werden?

Antwort:

$$\begin{aligned}
 |D \cup F| &= |D| + |F| - |D \cap F| \iff \\
 |D \cap F| &= |D| + |F| - |D \cup F| = 9 + 6 - (|S| - |(D \cup F)^c|) = 15 - (13 - |N|) = 2 + 2 = 4 = |M| ; \\
 |D_o| &= |D \setminus M| =_{[D \supseteq M]} |D| - |M| = 9 - 4 = 5 , \\
 |F_o| &= |F \setminus M| =_{[F \supseteq M]} |F| - |M| = 6 - 4 = 2 .
 \end{aligned}$$

Die Torhüterin zählt mit zur „Verteidigung“ — das Spiel kann beginnen:  $5+4+2 = 11$ .

Die Anzahl der Mittelfeld-Spielerinnen lässt sich aber noch etwas eleganter bestimmen:

$$\begin{aligned}
 |S| &:= |(D \cup F) \cup N| =_{\substack{\text{Partition} \\ \text{auf } 2, \text{ „}\cup\text{“}}} (|D| + |F| - |D \cap F|) + |N| \iff \\
 |D \cap F| &= |D| + |F| + |N| - |S| = 9 + 6 + 2 - 13 = 4 = |M| .
 \end{aligned}$$

b) Bei der Prüfungsplanung maximal zu erwartender # Klausuren wär's bspw. wie folgt:

$$\begin{aligned}
 DM &:= \text{Menge der Prüflinge in Diskrete Mathematik}; & |DM| &:= 60 , \\
 FG &:= \text{Menge der Prüflinge in Formale Grundlagen}; & |FG| &:= 50 , \\
 KI &:= \text{Menge der Prüflinge in Künstliche Intelligenz}; & |KI| &:= 40 ; \\
 DM \cap FG &:= \text{Menge der Prüflinge, welche in } DM \text{ und in } FG \text{ sind}; & |DM \cap FG| &:= 40 , \\
 DM \cap KI &:= \text{Menge der Prüflinge, welche in } DM \text{ und in } KI \text{ sind}; & |DM \cap KI| &:= 30 , \\
 FG \cap KI &:= \text{Menge der Prüflinge, welche in } FG \text{ und in } KI \text{ sind}; & |FG \cap KI| &:= 20 , \\
 DM \cap FG \cap KI &= : & K &:=
 \end{aligned}$$

Menge der Prüflinge, welche alle 3 genannten Klausuren mitschreiben;  $|K| := k := 10$ .  
 $S := DM \cup FG \cup KI$  Menge aller Mit-Schreiber;  $|S| =: s$ . Interessant zu wissen ist die Frage:

Wie viele Studierende schreiben welche Klausur(en) mit:  
mindestens 1, genau 2 der 3 möglichen bzw. nur 1 — welche?

Antwort:

$$\begin{aligned} s &= |DM \cup FG \cup KI| = \\ &\quad |DM| + |FG| + |KI| - (|DM \cap FG| + |DM \cap KI| + |FG \cap KI|) + k = \\ &\quad 60 + 50 + 40 - (40 + 30 + 20) + 10 = 160 - 90 = 70 \end{aligned} .$$

70 Studierende schreiben demnach mindestens eine Klausur mit.

$$\begin{aligned} |(DM \cap FG) \setminus K| &=_{[DM \cap FG \supseteq K]} |DM \cap FG| - |K| = 40 - k = 30 . \\ |(DM \cap KI) \setminus K| &=_{[DM \cap KI \supseteq K]} |DM \cap KI| - |K| = 30 - k = 20 . \\ |(FG \cap KI) \setminus K| &=_{[FG \cap KI \supseteq K]} |FG \cap KI| - |K| = 20 - k = 10 . \end{aligned}$$

30 (der 70) Studierende schreiben genau die beiden Klausuren  $DM$  und  $FG$ , noch 20 Studierende genau  $DM$  und  $KI$ , und nur 10 Studierende schreiben genau  $FG$  und  $KI$ .

$$\begin{aligned} |DM_{\text{exkl.}}| &= |S \setminus (FG \cup KI)| =_{[S \supseteq FG \cup KI]} s - (|FG| + |KI| - |FG \cap KI|) = \\ &\quad 70 - (50 + 40 - 20) = 0 . \\ |FG_{\text{exkl.}}| &= |S \setminus (DM \cup KI)| =_{[S \supseteq DM \cup KI]} s - (|DM| + |KI| - |DM \cap KI|) = \\ &\quad 70 - (60 + 40 - 30) = 0 . \\ |KI_{\text{exkl.}}| &= |S \setminus (DM \cup FG)| =_{[S \supseteq DM \cup FG]} s - (|DM| + |FG| - |DM \cap FG|) = \\ &\quad 70 - (60 + 50 - 40) = 0 . \end{aligned}$$

Niemand hat exakt lediglich nur eine Klausur vor sich;  $0 \cdot 3 + (30 + 20 + 10) + k = s$ .

## 5.3 Rekurrenz-Relation

Diese Technik kommt hauptsächlich dann zum Einsatz, wenn man bei Zähl-Problemen ad-hoc keine geschlossene Form parat hat, man also für einen Eingabe-Fall  $n$  nicht direkt die Zahl  $z(n)$  angeben kann, welche das gesuchte Ergebnis des entsprechenden Zähl-Problems darstellt. Was Einem jedoch bleibt ist die Beobachtung, was bei einer gewissen Vergrößerung eines Problems passiert, z. B. beim in der Informatik häufig vorkommenden Verlängern eines Bit-Vektors der Länge  $n-1$  um 1 Bit-Position auf  $n$ .<sup>9</sup>

Nehmen wir jedoch zunächst die Gaußsche Summen-Formel<sup>10</sup> der einfachsten *arithmetischen Reihe*<sup>11</sup>  $g(n) := \sum_{i=1}^n i$ ; die geschlossene Form<sup>12</sup>  $g_n = n \cdot (n+1)/2$  sei uns noch

---

<sup>9</sup>Eine solche Erhöhung der Eingabe-Größe um 1 verdoppelt die Anzahl der Kodier-Möglichkeiten (# verschiedener Zeichen-Ketten) und stellt das Hintergrund-Rauschen für nahezu jedes Beispiel auf dem Terrain der Bit-Vektoren dar.

<sup>10</sup>aufgaben-mäßig als inkrementelle Formel (hier fortwährend zunehmende Summe) formuliert

<sup>11</sup>mit  $a_0 := 0$ ,  $a_i := [i > 0] a_{i-1} + d_{\text{Differenz}}$ ;  $\sum_{i=0}^n a_i = \sum_{i=1}^n a_i = \sum_{i=1}^n d \cdot i = d \cdot (n \cdot (n+1)/2)$

<sup>12</sup>Eingabe  $n$  als Index notiert (in o. g. inkrementeller Form  $n$  noch als Variable geschrieben)

unbekannt. Wir beobachten aber sehr einfach, dass beim Schritt von  $n - 1$  nach  $n_{[> 0]}$  genau  $n$  auf  $g_{(n-1)}$  addiert wird — also folgende Rekursion gilt :

$$g_n := g_{(n-1)} + n ;$$

d. h., wir kennen die de-/inkrementelle Konstruktion von  $g_n$ .

Dieses Prinzip können wir nun auf diesen Vorgänger-Fall anwenden :

$$g_{(n-1)} := g_{(n-2)} + (n - 1) ,$$

und somit

$$g_n := g_{(n-2)} + (n - 1) + n ,$$

dann

$$g_n := g_{(n-3)} + (n - 2) + (n - 1) + (n - 0) ,$$

usw. Wie weit zurück können wir diese Vorgänger-Konstruktion(en) bilden? Wir gehen  $n$  Schritte zurück, bis zu  $g_0 (= 0)$  und bekommen

$$g_n = 0 + 1 + 2 + 3 + \cdots + (n - 2) + (n - 1) + n .$$

Dieser Weg nennt sich „Rückwärts-Ersetzung“. Startet man bei

$$g_0 := 0 ,$$

bildet

$$g_1 := g_{(1-1)} + 1 = g_0 + 1 = 0 + 1 = 1 ,$$

$$g_2 := g_1 + 2 = 1 + 2 = 3 ,$$

usw., so landet man natürlich — nach  $n$  Schritten — bei der gleichen Summe für  $g_n$ ; dieses Vorgehen nennt man „Vorwärts-Ersetzung“. Unter Vernachlässigung des neutralen Elements der Addition (vorne) fassen wir nun geschickt zusammen: das erste Element, die 1, mit dem letzten Element  $n$ , das zweite Element, 2, mit dem zweit-letzten Element  $n - 1$ , das dritte Element, 3, mit dem dritt-letzten Element  $n - 2$ , usw. Dies funktioniert zunächst bis zur Mitte  $\lfloor \frac{n}{2} \rfloor$ ; ist  $n$  ungerade, müssen wir  $\lceil \frac{n}{2} \rceil$  einfache<sup>13</sup> hinzuaddieren. Wir erhalten :

$$g_n = \sum_{i:=1}^{\lfloor \frac{n}{2} \rfloor} (i + (n - (i - 1))) + \begin{cases} 0 & ; \text{gerade}(n) \\ \lceil \frac{n}{2} \rceil & ; \text{ungerade}(n) \end{cases} =$$

$$\begin{cases} \sum_{i:=1}^{\frac{n}{2}} (i + n - i + 1) & ; \text{gerade}(n) \\ \sum_{i:=1}^{\frac{n-1}{2}} (n + 1) + \lceil \frac{n}{2} \rceil & ; \text{ungerade}(n) \end{cases} =$$

<sup>13</sup>eben nicht zweifach — was bei ungeradem  $n$  passiert, wenn wir in oben folgendem „Wir erhalten“ ohne Fall-Unterscheidung der Parität die Summen-Obergrenze gleich nach oben falsch gerundet hätten

$$\begin{cases} \frac{n}{2} \cdot (n+1) & ; \text{ gerade}(n) \\ \frac{n-1}{2} \cdot (n+1) + \frac{n+1}{2} & = ((n-1)+1) \cdot \frac{n+1}{2} ; \text{ ungerade}(n) \end{cases} = \frac{n \cdot (n+1)}{2}$$

Ein traditioneller Induktions-Beweis würde abschließend die Behauptung bestätigen.

Das Ganze mag bucklig erscheinen — erst recht, wenn uns die Gaußsche Summen-Formel bereits bekannt ist. Wir sind auch erst beim „Warm-up“ — um einen Einblick in die prinzipielle Vorgehensweise zu gewinnen.

Es kommt bei praktischen Zähl-Problemen häufig vor, dass man den direkten Ansatz nicht vor Augen hat, jedoch die inkrementelle Struktur durchschaut; und dann ist es hilfreich, die Rekurrenzrelation im Köcher (der Problem-Lösungs-Techniken) zu haben.

Fassen wir die Grund-Bausteine zusammen:

- Schema: ähnlich wie bei inkrementeller Rekursion (Eingabe bzw. Einsicht  $\ddot{\dots}$ )
- Idee: Rekursions-Eliminierung, hin zu einer geschlossenen Formel
- Struktur
  - Basis-Wert
  - Konstruktions-Prinzip
    - \* aufbauend auf Vorgänger-Wert
    - \* konstruktiver Schritt (kreativer Teil)
  - Entwicklung/Ersetzung (zwei Alternativen)
    - \* rückwärts
    - \* vorwärts
- Beweis (der gefundenen Behauptung — oft per ähnlich gestrickter Induktion).

1. Illustration:  $n$ -stelliger Bit-Vektor (Binär-Zeichen-Kette der Länge  $n$ )

Wir zählen gern mit  $z_n$  die Anzahl Möglichkeiten, dass, ausgehend von  $n$  Positionen, an genau einer Stelle das jeweilige Bit *false*<sup>14</sup> (hier als „0“ besprochen) ausweist. (Dass es offensichtlich  $n$  sind, sei hier zweitrangig; wir nehmen diese Fragestellung nur, um die Grund-Struktur einer Rekurrenz aufzuzeigen.)

Basis-Wert:  $z_0 := 0$  ;

Prinzip :  $z_{n[>0]} := z_{(n-1)} + 1$  .

---

<sup>14</sup> *true* (also eine „1“) würde das gleiche Ergebnis produzieren

Warum? Ein  $(n-1)$ -stelliger Bit-Vektor kann vorne nur entweder um eine 1 ( $\text{:= } \text{true}$ ) oder eine 0 ( $\text{:= } \text{false}$ ) zu einer  $n$ -steligen Zeichen-Kette erweitert werden. Was passiert, wenn vorne eine 1 ergänzt wird? Dies kann natürlich nicht die gesuchte Anzahl erhöhen, da wir auf das Auftreten einer 0 fokussieren. Was passiert, wenn vorne eine 0 ergänzt wird? Nur im (einzigsten) Fall, dass an allen  $n-1$  vorherigen Positionen nirgends *false* auftrat (also alle Einträge *true* sind), bildet sich mit einer neuen führenden 0 ein Bit-Vektor der gesuchten Form. (Es wird auch keiner zerstört — bspw. einer, der bereits genau eine 0 auf einer der bisherigen  $n-1$  Positionen aufweist, da dieser, wie eben erwähnt, mit einer neuen führenden 1 erhalten bleibt.) Demnach ergibt sich, für  $n > 0$ :

$$z_n := z_{(n-1)} + \binom{n-1}{0},$$

wobei der letzt-genannte Summand, der „Binomial-Koeffizient“<sup>15</sup>, hier ausdrückt wie oft bei  $n-1$  Bit-Positionen genau 0-mal *false* auftreten kann — von  $2^{(n-1)}$  booleschen Belegungs-Möglichkeiten ist dies genau einmal der Fall (siehe eben genanntes „Prinzip“). Abbildung 5.1 will genau dies illustrieren.

Wir zeigen nun, dass beide Substitutions-Wege zur Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned} z_n &:= z_{(n-1)} + 1 &:= (z_{(n-2)} + 1) + 1 \\ &= z_{(n-2)} + 2 &:= (z_{(n-3)} + 1) + 2 \\ &= z_{(n-3)} + 3 &:= (z_{(n-4)} + 1) + 3 \\ &= z_{(n-4)} + 4 \\ &\quad \vdots \\ &:= z_{(n-n)} + n \\ &= z_0 + n \\ &:= 0 + n \\ &= n \end{aligned};$$

- Vorwärts-Ersetzung

$$\begin{aligned} z_1 &:= z_0 + 1 &:= 0 + 1 &= 1 \\ z_2 &:= z_1 + 1 &:= 1 + 1 &= 2 \\ z_3 &:= z_2 + 1 &:= 2 + 1 &= 3 \\ z_4 &:= z_3 + 1 &:= 3 + 1 &= 4 \\ &\quad \vdots \\ z_n &:= z_{(n-1)} + 1 &:= (n-1) + 1 &= n \end{aligned}.$$

---

<sup>15</sup>wird im Unter-Abschnitt 5.4.2 (ab Seite 76) vorgestellt

0
1

0	0
0	1
1	0

1	1
---	---

0	0	0
0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

**Abb. 5.1:** Bitmuster-Rekurrenz

Behauptung:  $z_n = n \quad [= \binom{n}{1}]$

Beweis: Induktion über  $n$

- Basis<sup>16</sup>:  $z_0 := 0$ 
  - Prinzip:  $z_0 = 0$  [Initial-Wert:  $0 \times \text{false}$ ]
  - Formel:  $z_0 = 0 \hat{=} \text{Prinzip}$
- Hypothese:  $z_{(n-1)} = n - 1$

---

<sup>16</sup>alternativ:  $n_0 := 1$

- Prinzip:  $z_1 = 1$
- Formel:  $z_1 = 1$

- Schritt:  $(n_0 \leq) n - 1 \rightarrow n (> n_0)$

$$\begin{aligned} - \text{ Prinzip: } z_n &:= z_{(n-1)} + 1 \stackrel{!}{=} (n-1) + 1 = n \\ - \text{ Formel: } z_n &= n \stackrel{\hat{=}}{=} \text{Prinzip} . \end{aligned}$$

2. Illustration: Anzahl Kanten im vollständigen Graphen mit  $n$  Knoten

Wir zählen mit  $e_n$  die Anzahl aller ungerichteten Kanten in einem Graphen, in dem jeder der  $n_{[>0]}$  Knoten genau  $1 \times$  mit jedem der  $n - 1$  anderen Knoten verbunden ist.

Basis-Wert:  $e_1 := 0$  ;

Prinzip :  $e_n := e_{(n-1)} + (n - 1)$  .

Warum? Ein vollständiger Graph mit  $n - 1$  Knoten kann bei einer Erweiterung um genau einen Knoten nur dann „vollständig“ bleiben, wenn der neue („ $n$ .“) Knoten, zusätzlich zu den bereits vorhandenen  $e_{(n-1)}$  Kanten<sup>17</sup>, zu allen schon vorher existierenden  $n - 1$  Knoten durch je eine weitere Kante angebunden wird. Demnach ergibt sich, für  $n > 1$ , das soeben dargestellte Konstruktions-Prinzip.

Wir zeigen nun, dass beide Substitutions-Wege zur Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned} e_n &:= e_{(n-1)} + (n - 1) \\ &:= e_{(n-2)} + (n - 2) + (n - 1) \\ &:= e_{(n-3)} + (n - 3) + (n - 2) + (n - 1) \\ &\quad \vdots \\ &:= e_{(n-(n-1))} + (n - (n - 1)) + \cdots + (n - 3) + (n - 2) + (n - 1) \\ &= e_1 + \sum_{i:=1}^{n-1} i \\ &:= 0 + \sum_{i:=1}^n i - n \\ &= \frac{n \cdot (n + 1)}{2} - \frac{n \cdot 2}{2} \\ &= \frac{n \cdot ((n + 1) - 2)}{2} \\ &= \frac{n \cdot (n - 1)}{2} ; \end{aligned}$$

---

<sup>17</sup>es darf ja keine gelöscht werden

- Vorwärts-Ersetzung

$$e_2 := e_1 + 1 := 0 + 1 = 1$$

$$e_3 := e_2 + 2 := 1 + 2 = 3$$

$$e_4 := e_3 + 3 := 3 + 3 = 6$$

⋮

$$e_n = \sum_{i=0}^{n-1} i = \stackrel{\text{laut Gauß}}{=} \frac{(n-1) \cdot n}{2} .$$

Behauptung:  $e_n = \frac{n \cdot (n-1)}{2}$

Beweis: siehe Unter-Abschnitt 4.1.1, 1. Beispiel (Seite 36)

3. Illustration: Anzahl Kanten im  $h$ -dimensionalen Hyper-Würfel mit  $n_h$  Knoten

Ein sogenannter „hypercube“ der Dimension  $h_{[> 0]}$  mit genau 1 Knoten an jeder der  $n_h$  ( $= 2^h$ ) Ecken lässt sich aus seiner Vorgänger-Struktur der Dimension  $h-1$  konstruieren, indem zunächst dieses Vorgänger-Gebilde verdoppelt und von jeder Ecke dieses Hyper-„Würfels“ der Dimension  $h-1$  zur korrespondierenden („gleichen“) Ecke seiner eigenen Kopie eine neue Kante gezogen wird — wie in Bild 5.2 ersichtlich. Somit verdoppelt

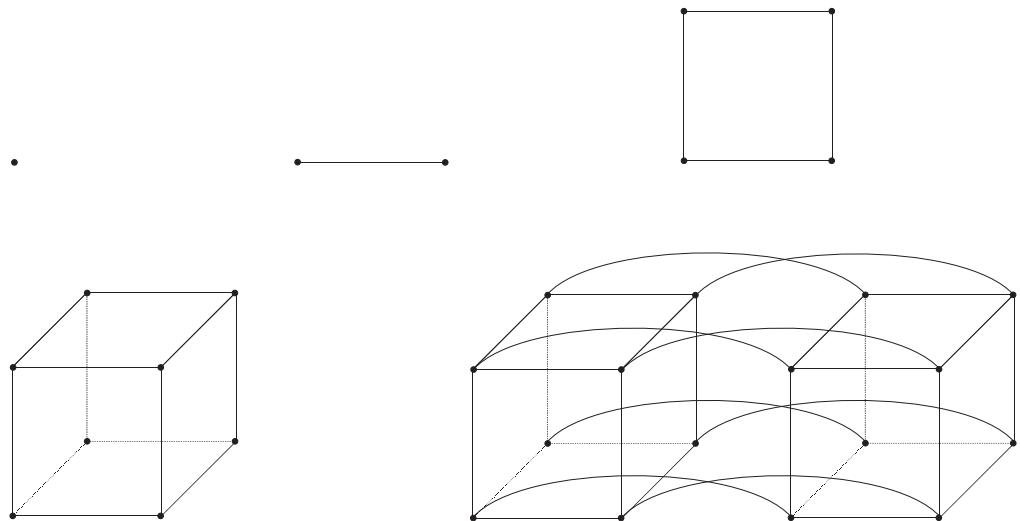


Abb. 5.2:  $h$ -dimensionaler Hyper-Würfel

sich bei jeder Erhöhung der Dimension die Knoten-Anzahl ( $n_h = 2 \cdot n_{h-1}$ ); anders ausgedrückt: der Hyper-Würfel der Dimension  $h-1$  hat halb so viele Knoten wie der

$h$ -dimensionale:  $n_{h-1} = n_h / 2$ . Hier möge jedoch, wie im vorherigen Beispiel, die Anzahl der Verbindungen ( $\#$  „connections“  $=: c_h$ ) interessieren. Der Einfachheit halber fungiert nun aber nicht die Knoten-Anzahl, sondern die Dimension als Parameter der Rekurrenz.

Basis-Wert:  $c_0 := 0$  ;

Prinzip :  $c_h := 2 \cdot c_{h-1} + n_{h-1} = 2 \cdot c_{h-1} + 2^{h-1}$  .

Warum? Durch die Erhöhung der Dimension (von  $h-1$  nach  $h$ ) erzeugen wir zunächst eine Kopie eines Hyper-Würfels der Dimension  $h-1$  und erhalten hiermit bereits das Doppelte an Kanten; zusätzlich werden ecken-korrespondierend so viele Verbindungen eingezogen, wie die Vorgänger-Struktur Knoten hatte. Dadurch ergibt sich, für  $h > 0$ , das genannte Rekurrenz-Prinzip.

Wir zeigen nun, dass beide Substitutions-Wege zu einer geschlossenen Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned}
 c_h &:= 2 \cdot c_{h-1} + 2^{h-1} \\
 &:= 2 \cdot (2 \cdot c_{h-2} + 2^{h-2}) + 2^{h-1} \\
 &= 4 \cdot c_{h-2} + 2^1 \cdot 2^{h-2} + 2^{h-1} \\
 &= 4 \cdot c_{h-2} + 2^{h-1} + 2^{h-1} \\
 &:= 4 \cdot (2 \cdot c_{h-3} + 2^{h-3}) + 2 \cdot 2^{h-1} \\
 &= 8 \cdot c_{h-3} + 2^2 \cdot 2^{h-3} + 2 \cdot 2^{h-1} \\
 &= 8 \cdot c_{h-3} + 1 \cdot 2^{h-1} + 2 \cdot 2^{h-1} \\
 &= 2^3 \cdot c_{h-3} + 3 \cdot 2^{h-1} \\
 &:= 2^3 \cdot (2 \cdot c_{h-4} + 2^{h-4}) + 3 \cdot 2^{h-1} \\
 &= 2^4 \cdot c_{h-4} + 1 \cdot 2^{h-1} + 3 \cdot 2^{h-1} \\
 &= 2^4 \cdot c_{h-4} + 4 \cdot 2^{h-1} \\
 &\quad \vdots \\
 &:= 2^h \cdot c_{h-h} + h \cdot 2^{h-1} \\
 &= n_h \cdot c_0 + h \cdot 2^{h-1} \\
 &:= h \cdot 2^{h-1} ;
 \end{aligned}$$

- Vorwärts-Ersetzung

$$\begin{aligned}
 c_1 &:= 2 \cdot c_0 + 2^0 := 2 \cdot 0 + 2^0 = 1 \cdot 2^0 \\
 c_2 &:= 2 \cdot c_1 + 2^1 := 2 \cdot 2^0 + 2^1 = 2 \cdot 2^1 \\
 c_3 &:= 2 \cdot c_2 + 2^2 := 2 \cdot 2^1 + 1 \cdot 2^2 = 3 \cdot 2^2 \\
 c_4 &:= 2 \cdot c_3 + 2^3 := 2 \cdot (3 \cdot 2^2) + 2^3 = 3 \cdot 2^3 + 1 \cdot 2^3 = 4 \cdot 2^3 \\
 c_5 &:= 2 \cdot c_4 + 2^4 := 2 \cdot (4 \cdot 2^3) + 2^4 = 4 \cdot 2^4 + 1 \cdot 2^4 = 5 \cdot 2^4 \\
 &\quad \vdots \\
 c_h &:= h \cdot 2^{h-1}
 \end{aligned}$$

Behauptung:  $c_h = h \cdot 2^{h-1}$

Beweis: Induktion über  $h$   $[= \log_2(2^h) =: \underset{\text{dualis}}{\text{logarithmus}} \text{ld}(n_h)]$

- Basis:  $h_0 := 0$

- Prinzip:  $c_0 = 0$  [der 0-dimens. Punkt hat keine Verbindung]
- Formel:  $c_0 = 0 \cdot \dots = 0 \hat{=} \text{Prinzip}$

- Hypothese:  $c_{(h-1)} = (h-1) \cdot 2^{(h-1)-1}$

- Schritt:  $(h_0 \leq) h-1 \rightarrow h (> h_0)$

$$\begin{aligned} \text{– Prinzip: } c_h &:= 2 \cdot c_{h-1} + 2^{h-1} \\ &\stackrel{!}{=} 2^1 \cdot ((h-1) \cdot 2^{(h-1)-1}) + 1 \cdot 2^{h-1} \\ &= ((h-1)+1) \cdot 2^{h-1} \\ &= h \cdot 2^{h-1} \end{aligned}$$

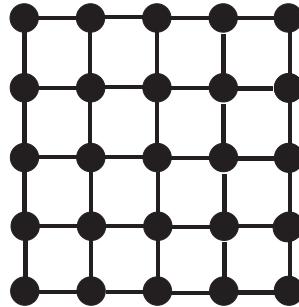
$$\text{– Formel: } c_h = h \cdot 2^{h-1} \hat{=} \text{Prinzip}$$

Ergebnis:  $c_h(n_h) = \text{ld}(n_h) \cdot 2^h \cdot 2^{-1} = h \cdot n_h / 2$

Logisch  $\hookrightarrow$ : Im  $h$ -dimensionalen Hyper-Würfel gehen eigentlich von jeder der  $n_h$  Ecken  $h$  Kanten ab; da keine dieser gedachten  $h \cdot n_h$  Kanten gerichtet ist (eine Verbindung zwischen zwei Ecken existiert nicht 2-fach), wird das gerade erwähnte Produkt halbiert.

4. Illustration: Durchmesser im quadratischen Gitter-Netz mit  $n$  Knoten

Der „Durchmesser“ eines Graphen ist die Distanz (auf kürzestem Weg) der beiden am weitesten voneinander entfernten Punkte, wobei nur Schritte entlang des gegebenen Kanten-Musters erlaubt sind. Hier liegt nun eine quadratische Gitternetz-Struktur zugrunde. Bild 5.3 zeigt ein  $(5 \times 5)$ -Muster:  $n_5 := 5^2 = 25$ . Allgemein:  $n_r := r^2$ ,



**Abb. 5.3:** Gitter-Netz

$r = \sqrt{n_r}$ ; wir haben demnach sowohl  $r$  Zeilen als auch  $r$  Spalten. Dieses  $r$  spielt nun sinnigerweise die Rolle des Rekurrenz-Parameters — siehe die hier folgende Erläuterung.

Basis-Wert:  $d_1 := 0$  ;

Prinzip :  $d_r := d_{r-1} + 1 \cdot 2$  .

Warum? Durch die Hinzunahme je einer weiteren Zeile (von bisher  $r - 1$  auf jetzt  $r$ ) und Spalte müssen wir zur vorherigen Distanz je 1 zusätzlichen Schritt in jeder der 2 Dimensionen tätigen. Dadurch ergibt sich, für  $r > 1$ , das genannte Rekurrenz-Prinzip.

Wir zeigen nun, dass beide Substitutions-Wege zu einer geschlossenen Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned}
 d_r &:= d_{r-1} + 1 \cdot 2 \\
 &:= (d_{r-2} + 1 \cdot 2) + 1 \cdot 2 &= d_{r-2} + 2 \cdot 2 \\
 &:= (d_{r-3} + 1 \cdot 2) + 2 \cdot 2 &= d_{r-3} + 3 \cdot 2 \\
 &:= (d_{r-4} + 1 \cdot 2) + (4-1) \cdot 2 &= d_{r-4} + 4 \cdot 2 \\
 &:= (d_{r-5} + 1 \cdot 2) + (5-1) \cdot 2 &= d_{r-5} + 5 \cdot 2 \\
 &:= (d_{r-6} + 1 \cdot 2) + (6-1) \cdot 2 &= d_{r-6} + 6 \cdot 2 \\
 &\vdots \\
 &:= (d_{r-(r-1)} + 1 \cdot 2) + ((r-1)-1) \cdot 2 &= d_1 + (r-1) \cdot 2 \\
 &:= 2 \cdot (r-1) & ;
 \end{aligned}$$

- Vorwärts-Ersetzung

$$\begin{aligned}
 d_2 &:= d_1 + 1 \cdot 2 &:= 0 + 1 \cdot 2 &= 1 \cdot 2 &= (2-1) \cdot 2 \\
 d_3 &:= d_2 + 1 \cdot 2 &:= 1 \cdot 2 + 1 \cdot 2 &= 2 \cdot 2 &= (3-1) \cdot 2 \\
 d_4 &:= d_3 + 1 \cdot 2 &:= 2 \cdot 2 + 1 \cdot 2 &= 3 \cdot 2 &= (4-1) \cdot 2 \\
 d_5 &:= d_4 + 1 \cdot 2 &:= 3 \cdot 2 + 1 \cdot 2 &= 4 \cdot 2 &= (5-1) \cdot 2 \\
 d_6 &:= d_5 + 1 \cdot 2 &:= 4 \cdot 2 + 1 \cdot 2 &= 5 \cdot 2 &= (6-1) \cdot 2 \\
 &\vdots \\
 d_r &:= d_{r-1} + 1 \cdot 2 &= ((r-1)-1) \cdot 2 + 1 \cdot 2 &= (r-1) \cdot 2
 \end{aligned}$$

Behauptung:  $d_r = 2 \cdot (r-1)$  .

Beweis: Induktion über  $r$  [=  $\sqrt{n_r}$ ] :

- Basis:  $r_0 := 1$

– Prinzip:  $d_1 = 0$  [keine Nachbar-Zellen: 0 Schritte]

– Formel:  $d_1 = 2 \cdot (1-1) = 0 \hat{=} \text{Prinzip}$  .

- Hypothese:  $d_{(r-1)} = 2 \cdot ((r-1) - 1)$
- Schritt:  $(r_0 \leq) r-1 \rightarrow r (> r_0)$ 
  - Prinzip:  $d_r := d_{r-1} + 1 \cdot 2$   
 $\stackrel{!}{=} 2 \cdot ((r-1) - 1) + 2 \cdot 1$   
 $= 2 \cdot ((r-1) - 1) + 1$   
 $= 2 \cdot (r-1)$
  - Formel:  $d_r = 2 \cdot (r-1) \hat{=} \text{Prinzip}$

Ergebnis:  $d_r = 2 \cdot (r-1) = 2 \cdot (\sqrt{n_r} - 1) =: d(n_r)$

Man ist ungünstigerweise in einer Ecke und möchte in die diametral liegende; in jeder der beiden Dimensionen sind noch  $r-1$  Schritte zu gehen, macht zusammen  $2 \cdot (\sqrt{n_r} - 1)$ .

Anwendungen

(zum *Durchmesser* in der aktuellen Illustration):

- Beim Routen einer elektronischen Nachricht auf einer Grid-Architektur kann man sich gut vorstellen, dass das Rekurrenz-Prinzip von Interesse ist: Beim Vergrößern des Netzes um je 1 Spalte und Zeile möge der Netzwerk-Guru die Schritt-Zahl bedenken, die eine Nachricht im „worst case“ länger benötigt:  $2 \cdot$ . Diese Zusatz-Schritt-Anzahl fällt demnach unabhängig der angestrebten Netzwerk-Größe aus.
- Realisiert man in der Spiele-Programmierung auf dem Grid-Tableau die kürzeste Strecken-Länge von einem Feld in einer der 4 Ecken zum am weitesten schräg gegenüber liegenden, so braucht man auf diesem quadratischen Gitternetz mit  $r \times r$  Feldern bei optimaler Bedienung  $d_r$  Schritte bis zum Ziel-Feld. Uns interessiert nun, bspw. via Rekurrenz zu bekommen, die geschlossene Formel  $d_r$ .

5. Illustration: Anzahl Verbindungen im quadratischen  $(r \times r)$ -Gitter-Netz

Wie bei der („3.“) Illustration im Hyper-Würfel zählen wir die Verbindungen innerhalb einer Netzwerk-Architektur und benutzen wieder die übliche englisch-sprachige Bezeichnung # „connections“, zunächst bezogen auf die Eingabe-Größe  $r$ , der Spalten- bzw. Zeilen-Anzahl in der gegebenen Matrix; diese Bezugnahme erweitern wir abschließend spielend auf den an  $r$  gekoppelten Input-Parameter  $n_r$ , die Knoten-Anzahl im Netzwerk.

Basis-Wert:  $c_0 := 0$  ;

Prinzip :  $c_r := c_{r-1} + 4 \cdot (r-1)$

Warum? Betrachten wir das vorherige Gitternetz-Bild. Will man eine neue „ $r$ .“ Zeile aufmachen, so muss man zu den bestehenden  $r-1$  Knoten in der Vorgänger-Zeile (die aufgrund der quadratischen Struktur genauso viele Spalten und so diese  $r-1$  Einträge in dieser Zeile hat) je eine Verbindung vertikal ziehen und auf dieser neuen Zeile diese neuen  $r-1$  Knoten horizontal verbinden, was mit  $r-2$  Verbindungen über die Bühne geht. Nun binden wir nur noch den neuen Eck-Knoten in der horizontalen Dimension an. Da das Ganze in einer Dimension symmetrisch zu der anderen ist, gilt es die genannten Operationen schließlich zu verdoppeln — fertig ist, für  $r > 0$ , das Rekurrenz-Prinzip :

$w :=$  weitere Verbindungen:  $w_r = 2 \cdot ((r-1) + (r-2) + 1) = 2 \cdot (2 \cdot r - 2) = 4 \cdot (r-1) =$

$$w(n_r) = 4 \cdot \sqrt{n_{r-1}} .$$

Wir zeigen nun, dass beide Substitutions-Wege zu einer geschlossenen Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned}
 c_r &:= c_{r-1} + 4 \cdot (r-1) \\
 &:= c_{r-2} + 4 \cdot (r-2) + 4 \cdot (r-1) = c_{r-2} + 8 \cdot r - 12 \\
 &:= c_{r-3} + 4 \cdot (r-3) + 8 \cdot r - 12 = c_{r-3} + 12 \cdot r - 24 \\
 &:= c_{r-4} + 4 \cdot (r-4) + 12 \cdot r - 24 = c_{r-4} + 16 \cdot r - 40 \\
 &:= c_{r-5} + 4 \cdot (r-5) + 16 \cdot r - 40 = c_{r-5} + 20 \cdot r - 60 \\
 &:= c_{r-6} + 4 \cdot (r-6) + 20 \cdot r - 60 = c_{r-6} + 24 \cdot r - 84 \\
 &= c_{r-6} + 4 \cdot 6 \cdot r - 4 \cdot 21 \\
 &= c_{r-6} + 4 \cdot (6 \cdot r - \sum_{i:=1}^6 i) \\
 &= z := \# \text{Zeilen bis zur Basis-Zeilen-Nummer } 0 \quad c_{r-z} + 4 \cdot (z \cdot r - \sum_{i:=1}^z i) \\
 &\stackrel{\text{Summen-Formel}}{=} c_{r-z} + 4 \cdot (z \cdot r - z \cdot (z+1) / 2) \\
 &= c_{r-z} + 4 \cdot z \cdot \frac{2 \cdot r - (z+1)}{2} \\
 &= c_{r-z} + 2 \cdot z \cdot (2 \cdot r - z - 1) \\
 &\vdots \\
 &:= c_{r-r} + 2 \cdot r \cdot (2 \cdot r - r - 1) \\
 &= c_0 + 2 \cdot r \cdot (r-1) \\
 &:= 0 + 2 \cdot r \cdot (r-1) \\
 &= 2 \cdot r \cdot (r-1)
 \end{aligned}
 ;$$

- Vorwärts-Ersetzung

$$\begin{aligned}
 c_1 &:= c_0 + 4 \cdot 0 := 0 + 0 = 0 := 4 \cdot 0 \\
 c_2 &:= c_1 + 4 \cdot 1 := 0 + 4 = 4 = 4 \cdot 1 \\
 c_3 &:= c_2 + 4 \cdot 2 := 4 + 8 = 12 = 4 \cdot 3
 \end{aligned}$$

$$\begin{aligned}
c_4 &:= c_3 + 4 \cdot 3 := 12 + 12 = 24 = 4 \cdot 6 \\
c_5 &:= c_4 + 4 \cdot 4 := 24 + 16 = 40 = 4 \cdot 10 \\
c_6 &:= c_5 + 4 \cdot 5 := 40 + 20 = 60 = 4 \cdot 15 \\
&\vdots \\
c_r &:= 4 \cdot \sum_{i=0}^{r-1} i \\
&\stackrel{\text{Gauß}}{=} 4 \cdot \frac{(r-1) \cdot r}{2} \\
&= 2 \cdot r \cdot (r-1)
\end{aligned}$$

Behauptung:  $c_r = 2 \cdot r \cdot (r-1)$

Beweis: Induktion über  $r [= \sqrt{n_r}]$

- Basis:  $r_0 := 0$ 
  - Prinzip:  $c_0 = 0$  [keine (Computer-)Zeile/Spalte, keine Vernetzung]
  - Formel:  $c_0 = 2 \cdot 0 \cdot (\dots) = 0 \hat{=} \text{Prinzip}$
- Hypothese:  $c_{(r-1)} = 2 \cdot (r-1) \cdot ((r-1)-1)$
- Schritt:  $(r_0 \leq r-1 \rightarrow r (> r_0))$ 
  - Prinzip:  $c_r := c_{r-1} + 4 \cdot (r-1)$ 
 $\stackrel{!}{=} 2 \cdot (r-1) \cdot ((r-1)-1) + 4 \cdot (r-1)$ 
 $= 2 \cdot (r-1) \cdot ((r-2)+2)$ 
 $= 2 \cdot (r-1) \cdot r$
  - Formel:  $c_r = 2 \cdot r \cdot (r-1) \hat{=} \text{Prinzip}$

Ergebnis:  $c_r = 2 \cdot (r^2 - r) = 2 \cdot (n_r - \sqrt{n_r}) =: c(n_r)$

Anwendung (der Verbindungs-Anzahl bezogen auf beide Parameter  $r$  und  $n_r$ ):

Beim Entwurf einer Grid-Architektur ist der funktionale Zusammenhang zwischen der Zeilen-/Spalten-Anzahl  $r$  bzw. der Anzahl  $n_r$  an Computern und dem Vernetzungsaufwand  $c_r$  bzw.  $c(n_r)$  interessant — welcher sich bzgl. des Parameters  $r$  quadratisch und bezogen auf den Parameter  $n_r$  linear darstellt. Ist das Netzwerk in Betrieb, stellt sich üblicherweise im Laufe der Zeit für den Netzwerk-Guru die Frage nach den Zusatz-Kosten bei einer notwendigen Erweiterung: Wie viele Kabel benötigen wir zusätzlich,

wenn an das bisherige Gitter-Netz je eine neue Zeile und Spalte angeflanscht werden sollen? Von der prinzipiellen Größenordnung her kommen in Bezug auf die Zeilen-/Spalten-Anzahl linear viele Kabel, bzgl. der Computer-Anzahl „wurzel-mäßig“ viele Kabel hinzu.

Beispiel:

Eingabe-Wert:  $r - 1 := 5$

Ausgabe-Art: direkt über die geschlossene Formel:

$$c_{r-1} = 2 \cdot (r-1) \cdot ((r-1)-1) = 2 \cdot 5 \cdot (5-1) = 10 \cdot 4 = 40 = c_5$$

Eingabe-Wert:  $n_{r-1} := 5^2 = 25$

Ausgabe-Art: direkt über die geschlossene Formel:

$$c(n_{r-1}) = 2 \cdot (n_{r-1} - \sqrt{n_{r-1}}) =_{r=5}^{r-1} 2 \cdot (25 - \sqrt{5^2}) = 2 \cdot 20 = 40 = c(n_5)$$

Eingabe-Werte:  $c_{r-1}$  und  $r := (r-1)+1 := (6-1)+1 = 6$

Ausgabe-Art: rekursiv über die Rekurrenz-Relation:

$$c_r = c_{r-1} + \underline{4 \cdot (r-1)} = c_{6-1} + 4 \cdot (6-1) = c_5 + 4 \cdot 5 = 40 + 20 = 60 = c_6$$

Es ging um den linearen Zuwachs; die absolute Verbindungs-Anzahl gäbe es auch direkt:

$$c_6 = 2 \cdot 6 \cdot (6-1) = 60.$$

Eingabe-Werte:  $c(n_{r-1})$  und  $r := (r-1)+1 := (6-1)+1 = 6$

Ausgabe-Art: rekursiv über die Rekurrenz-Relation:

$$\begin{aligned} c(n_r) &= c(n_{r-1}) + \underline{4 \cdot \sqrt{n_{r-1}}} = c(n_{6-1}) + 4 \cdot \sqrt{n_{6-1}} = c(n_5) + 4 \cdot \sqrt{n_5} = \\ &40 + 4 \cdot 5 = 60 = c(n_6) \end{aligned}$$

Es ging um den wurzelmäßigen Zuwachs; die absolute Kabel-Anzahl gäbe es auch direkt:

$$c(n_6) = 2 \cdot (n_6 - \sqrt{n_6}) = 2 \cdot (6^2 - 6) = 60.$$

6. Illustration: Knoten-Zuwachs auf einer quadratischen Gitternetz-Architektur

Wir verweilen auf dem Verbindungs-Muster der zwei vorherigen Illustrationen. Haben wir  $r$  Zeilen (und auch Spalten), so gibt  $r^2 =: n_r$  die dazugehörige Anzahl Knoten an, wobei wir die Knoten jetzt als Pixel interpretieren. Wir kennen bereits den quadratischen Zusammenhang zwischen der Knoten-Anzahl  $n_r$  und dem Zeilen-/Spalten-Parameter  $r (= \sqrt{n_r})$ . Hier interessieren wir uns für das Rekurrenz-Prinzip an sich — um wie viele Knoten ein existierendes Pixel-Muster bestehend aus  $r - 1$  Zeilen (bzw. Spalten) durch Aufstockung um eine weitere Zeile und Spalte knoten-mäßig anwächst. (Dies geht anders<sup>18</sup> schneller als nun im Folgenden gezeigt; interessant ist jedoch, wie sich die Rekurrenz auch hier als hilfreich erweist.) Vom Prinzip her ist es doch so, dass mit einer neuen Zeilen-Nummer  $r (> 0)$  und dieser neuen Spalten-Nummer  $r$  prinzipiell jedes Mal genauso viele Knoten hinzukommen ( $2 \cdot r$ ); damit der gemeinsame neue Eck-Knoten nicht doppelt gezählt wird, müssen wir aber 1 abziehen, demnach:  $n_r := n_{r-1} + 2 \cdot r - 1$ . Wir testen nun diese Idee hinsichtlich der Differenz zweier Knoten-Anzahlen, bei denen die Zeilen-/Spalten-Nummer um 1 differiert, mit diesem Rekurrenz-Prinzip — und überprüfen dabei, ob die quadratische Struktur erhalten bleibt. (Dies ist aufwändig, aber ich will diese weitere Möglichkeit ja nur in den Köcher der Zähl-Techniken legen.)

$$\text{Basis-Wert: } n_0 := 0 ;$$

$$\text{Prinzip : } n_r := n_{r-1} + 2 \cdot r - 1 .$$

Warum? Jede Dimension liefert zunächst  $r$  Knoten, den Eck-Knoten aber nicht doppelt.

Wir zeigen nun, dass beide Substitutions-Wege zu der bekannten Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned}
 n_r &:= n_{r-1} + 2 \cdot r - 1 \\
 &:= n_{r-2} + 2 \cdot (r-1) - 1 + 2 \cdot r - 1 = n_{r-2} + 4 \cdot r - 4 \\
 &:= n_{r-3} + 2 \cdot (r-2) - 1 + 4 \cdot r - 4 = n_{r-3} + 6 \cdot r - 9 \\
 &:= n_{r-4} + 2 \cdot (r-3) - 1 + 6 \cdot r - 9 = n_{r-4} + 8 \cdot r - 16 \\
 &:= n_{r-5} + 2 \cdot (r-4) - 1 + 8 \cdot r - 16 = n_{r-5} + 10 \cdot r - 25 \\
 &:=^z :=^{\# \text{ Zeilen}}_{\text{bis zur Basis-Zeilen-Nummer 0}} n_{r-z} + (2 \cdot z) \cdot r - z^2 \\
 &\quad \vdots \\
 &:= n_{r-r} + 2 \cdot r^2 - r^2 \\
 &= n_0 + r^2 \\
 &= 0 + r^2 \\
 &= r^2 ;
 \end{aligned}$$

---

<sup>18</sup>  $n_r = n_{r-1} + x \iff x = n_r - n_{r-1} = r^2 - (r-1)^2 = r^2 - (r^2 - 2r + 1) = r^2 - r^2 + 2r - 1 = 2r - 1$

- Vorwärts-Ersetzung

$$\begin{aligned}
 n_1 &:= n_0 + 2 \cdot 1 - 1 = 0 + 1 = 1 \\
 n_2 &:= n_1 + 2 \cdot 2 - 1 = 1 + 3 = 4 \\
 n_3 &:= n_2 + 2 \cdot 3 - 1 = 4 + 5 = 9 \\
 n_4 &:= n_3 + 2 \cdot 4 - 1 = 9 + 7 = 16 \\
 n_5 &:= n_4 + 2 \cdot 5 - 1 = 16 + 9 = 25 \\
 &\vdots \\
 n_r &= r^2
 \end{aligned}$$

Behauptung:  $n_r = r^2$

Beweis: Induktion über  $r [= \sqrt{n_r}]$

- Basis:  $r_0 := 0$

$$\begin{aligned}
 - \text{ Prinzip: } n_0 &= 0 \quad [\text{keine Zeilen, keine (Pixel-)Knoten vorhanden}] \\
 - \text{ Formel: } n_0 &= 0^2 = 0 \quad \hat{=} \quad \text{Prinzip}
 \end{aligned}$$

- Hypothese:  $n_{(r-1)} = (r-1)^2$

- Schritt:  $(r_0 \leq) r-1 \rightarrow r (> r_0)$

$$\begin{aligned}
 - \text{ Prinzip: } n_r &:= n_{r-1} + 2 \cdot r - 1 \\
 &\stackrel{!}{=} (r-1)^2 + 2 \cdot r - 1 \\
 &= r^2 - 2 \cdot r + 1 + 2 \cdot r - 1 \\
 &= r^2
 \end{aligned}$$

$$- \text{ Formel: } n_r = r^2 \quad \hat{=} \quad \text{Prinzip}$$

Fazit: In der Tat haben wir für's Vergrößern eines Grids die richtige Rekurrenz gefunden.

Beispiel: Computer-Monitor, Fernseh-Bildschirm, Mobil-Display.

Wir gehen von einer bisher benutzten Zeilen- (und Spalten-)Anzahl  $r_a :=_{\text{hier}} 1.024$  aus, womit uns eine  $(1.024 \times 1.024)$ -Pixel-Matrix zur Verfügung steht.

Frage:

Wie viele weitere Pixel gewinnen wir, wenn wir die Zeilen-/Spalten-Anzahl um 1 erhöhen?

Antwort:

Sei  $r_e := r_a + 1$ ,  $w := n_{r_e} - n_{r_a}$ .

Die Rekurrenz-Vorschrift  $n_{r_e} := n_{r_a} + w$  liefert uns die gesuchte Anzahl Zusatz-Pixel:

$$w := n_{r_e} - n_{r_a}$$

$$\begin{aligned}
 &:= n_{(r_a+1)} - n_{r_a} \\
 &:= n_{r_a} + 2 \cdot r_e - 1 - n_{r_a} \\
 &= 2 \cdot r_e - 1 \\
 &:= 2 \cdot (r_a + 1) - 1 \\
 &= 2 \cdot (1.024 + 1) - 1 = 2.050 - 1 = 2.049
 \end{aligned} \quad .$$

Es gilt selbstverständlich:  $1.024^2 + 2.049 = 1.025^2$  (keine Fußnote  $\smile$ ) .

Dieser Blick auf das Rekurrenz-Prinzip ist eher ungewöhnlich; er soll hier lediglich ergänzend angeboten werden. Hier war der Gag der Rekurrenz die inkrementelle Struktur an sich, also der nächste Schritt, relativ bzgl. einer vorliegenden Situation; das Inkrement war linear:  $w_{r_e} := 2 \cdot r_e - 1$ . Üblicherweise strebt man weitergehend einen absoluten funktionalen Zusammenhang an, der hier quadratischer Natur ist:  $n(r) = r^2$ .

## 7. Illustration:

### Anzahl Bijektionen bei $n$ Elementen

Wir zählen hier mit  $b_n$  die Anzahl verschiedener *Bijektionen* aus einer  $n$ -elementigen Definitions-Menge in eine entsprechende (selbstverständlich gleich-große) Werte-Menge.

Basis-Wert:  $b_1 := 1$  ;

Prinzip :  $b_n := b_{(n-1)} \cdot n$  .

Warum? Eine Bijektion bedeutet, dass nicht nur jedes Element aus der Ausgangs-Menge genau ein Element aus der Ziel-Menge zugewiesen bekommt, sondern unterschiedliche Ausgangs-Werte auch unterschiedliche Ziel-Werte erhalten sowie alle zur Verfügung stehenden Werte aus der Ziel-Menge tatsächlich ausgewählt werden. Da natürlich beide Mengen gleich groß sind, entspricht diese Funktion einfach einer ganz speziellen Reihenfolge der Ziel-Elemente. Jede dieser möglichen Reihungen stellt eine andere Abbildung dar. Es geht um die Anzahl Möglichkeiten, die Ziel-Objekte verschiedenartig ansteuern zu können. Gab es bei einer Menge mit  $n-1$  Elementen  $b_{n-1}$  Reihungen, so hat das neue („n.“) Element  $n$  verschiedene Möglichkeiten, genau eines der nun  $n$  Ziel-Elemente auszuwählen — ungeachtet der möglichen Permutationen<sup>19</sup> unter  $n-1$  Elementen. Da dies multiplikativ zu sehen ist, ergibt sich, für  $n > 1$ , das dargestellte Konstruktions-Prinzip.

Wir zeigen nun, dass beide Substitutions-Wege zur Formel führen.

- Rückwärts-Ersetzung

$$\begin{aligned}
 b_n &:= b_{(n-1)} \cdot n \\
 &:= b_{(n-2)} \cdot (n-1) \cdot n \\
 &:= b_{(n-3)} \cdot (n-2) \cdot (n-1) \cdot n \\
 &\vdots
 \end{aligned}$$

---

<sup>19</sup>siehe Unter-Abschnitt 5.4.1, in dem auch das folgende „Fakultät“-Zeichen „!“ erläutert wird

$$\begin{aligned}
 &:= b_{(n-(n-1))} \cdot (n - (n-2)) \cdot \dots \cdot (n-2) \cdot (n-1) \cdot n \\
 &= b_1 \cdot \prod_{i:=2}^n i \\
 &:= 1 \cdot \prod_{i:=2}^n i \\
 &= \prod_{i:=1}^n i \\
 &=: n! \quad ;
 \end{aligned}$$

- Vorwärts-Ersetzung

$$b_2 := b_1 \cdot 2 := 1 \cdot 2 = 2$$

$$b_3 := b_2 \cdot 3 := 2 \cdot 3 = 6$$

$$b_4 := b_3 \cdot 4 := 6 \cdot 4 = 24$$

 $\vdots$ 

$$b_n = \prod_{i:=1}^{n-1} i \cdot n$$

$$= \prod_{i:=1}^n i$$

$$=: n!$$

Behauptung:  $b_n = n!$

Beweis: Induktion über  $n$

- Basis:  $n_0 := 1$

– Prinzip:  $b_1 = 1$  [das einzige Element kann man nur  $1 \times$  auswählen]  
 – Formel:  $b_1 = 1! = 1 \hat{=} \text{Prinzip}$ .

- Hypothese:  $b_{(n-1)} = (n-1)!$

- Schritt:  $(n_0 \leq) n-1 \rightarrow n (> n_0)$

– Prinzip:  $b_n := n \cdot b_{n-1}$   
 $\stackrel{!}{=} n \cdot (n-1)!$   
 $= n!$

– Formel:  $b_n = n! \hat{=} \text{Prinzip}$ .

## 5.4 Reihenfolgen und Auswahlen

### 5.4.1 Permutationen

Hier geht es um die Anzahl verschiedener Reihenfolgen von  $n$  Objekten; sind alle  $n$  verschieden, bietet sich folgende Überlegung an: Objekt 1 hat natürlich nur 1 Reihenfolge. Objekt 2 kann vor das erste oder hinter das erste Objekt platziert werden:  $1 \cdot 2 = 2$ . Objekt 3 kann vor's erste, vor's zweite oder hinter's zweite gesetzt werden, unabhängig der 2 Möglichkeiten der Platzierung dieser zwei anderen Objekte — also  $2 \cdot 3 = 6$ . Objekt 4 kann vor's erste, vor's zweite, vor's dritte oder hinter's dritte gelegt werden, unabhängig der 6 Möglichkeiten der Platzierung dieser drei anderen Objekte, demnach  $6 \cdot 4 = 24$ , usw. Das gesuchte Ergebnis ergibt sich somit per inkrementellem Produkt:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot n =: \prod_{i=1}^n i =: n!$$

— genannt „ $n$  Fakultät“. (Ein einfacher Induktions-Beweis würde dies leicht bestätigen.) Dabei gilt  $0! = 1$ , da  $(n-1)! = n!/n_{[>0]}$ . Die nächsten 7 Fälle sollte man auch noch parat haben, zur Not via  $n! := (n-1)! \cdot n_{[>0]} : \dots, 7! = 5040$ . Die Fakultät liefert früh große Werte; diese Funktion wächst gar exponentiell, was einfach zu sehen ist und sich ebenso locker beweisen ließe.<sup>20</sup> So ist bspw.  $13!$  bereits  $6.227.020.800$  und  $69! > 10^{98}$ .

Wie sieht es aus, wenn man nur irgendwelche  $k$  Objekte permuiert (verschieden stellt)? Diese Zahl nennt man *Permutations-Koeffizient* :

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

da es auf die verschiedenen Platzierungen der restlichen  $n - k$  Objekte nicht ankommt.

Eine andere Bezeichnung hierfür ist die *fallende Faktorielle* von  $n$  auf  $k$  :

$$n^k = \frac{n!}{(n-k)!} = \frac{(n-k)! \cdot \prod_{i=1}^k (n-k+i)}{(n-k)!} = \prod_{i=0}^{k-1} (n-i).$$

Wie  $P(n, k)$  zur Lösung von Aufgaben beiträgt, mögen folgende vier Beispiele aufzeigen:

1. In einer aus  $n_{[\geq 3]}$  Mitgliedern bestehenden Organisation sind 3 Funktions-Träger-Innen zu wählen, sagen wir Präsident/in, Vize-Präsi und Geschäftsführer/in. Der Gesellschaft soll es vorbehalten bleiben, dass die 3 Personen mit den meisten Stimmen die konkrete Besetzung der Funktionen unter sich ausmachen.

Frage: Wie viele Möglichkeiten gibt es zur Zusammenstellung des Führungs-Trios?

Antwort:  $P(n, 3) [= (n-2) \cdot (n-1) \cdot n]$ .

---

<sup>20</sup> $n! = \prod_{i=1}^n i >_{[n \geq 4]} \prod_{i=1}^n 2 = 2^n$ ; links wächst der Faktor weiter — rechts nicht.

2. Ein Klausur-Raum mit  $n$  Stühlen wird von  $k$  Studierenden geentert.

Frage: Wie viele Sitz-Ordnungen sind möglich ?

Antwort:  $P(n, k)$ .

3. Es geht um eine einfache Konstruktion eines aus 2 Teilen bestehenden Codes: für den vorderen Teil („Präfix“) sollen aus  $n_1$  Ziffern  $k_1$  verschiedene ausgewählt werden, und für den hinteren Teil („Suffix“) wähle man aus  $n_2$  Buchstaben  $k_2$  verschiedene aus.

Frage: Wie viele gültige Kennwörter stehen zur Verfügung ?

Antwort:  $P(n_1, k_1) \cdot P(n_2, k_2)$ .

4. Gegeben zwei endliche Mengen mit deren Kardinalitäten  $|D| =: k$  sowie  $|C| =: n$ .

Frage: Wie viele Injektionen  $\hookrightarrow$  von  $D$  nach  $C$  sind möglich ?

Antwort:  $P(n, k)$ .

Illustration:<sup>21</sup>

Ausgehend von  $k$  Elementen in der Definitions-Menge („domain“)  $D$  werden  $k$  Elemente in der potenziellen Werte-Menge („co-domain“)  $C$  getroffen; dazu gibt es  $\binom{n}{k}$  Möglichkeiten.<sup>22</sup> Belegt man in jeder dieser Konfigurationen die gewählten  $k$  Objekte ( $\in C$ ) mit einer Platzierungs-Nummer  $(1, \dots, k)$  und bringt sie gedanklich in jede beliebige Reihenfolge (entspricht jeweils einer Funktion), so gibt es dafür  $k!$  Möglichkeiten — macht insgesamt<sup>23</sup> :

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

Die letzte Bruch-Notation lässt sich auch unmittelbar erklären: Der Zähler ist klar:  $n!$  potenzielle Reihungen der  $n$  Elemente in  $C$ . Da nur  $k$  beteiligt sind, treten  $n - k$  nicht in Erscheinung — und damit auch nicht ihre Um-Ordnungen, d. h. 1 Repräsentant reicht als Vertreter dieser  $(n - k)!$  Nicht-Möglichkeiten, womit wir beim Nenner angelangt wären. In Schul-Sprache ausgedrückt könnte man ergänzen: Da das Ganze keine „Strich-“<sup>24</sup> sondern eine „Punkt-“ Aufgabe<sup>25</sup> ist, wird tendenziell nichts abgezogen sondern  $n!$  durch  $(n-k)!$  dividiert. Diese Bruch-Schreibweise entspricht dem Permutations-Koeffizienten  $P(n, k)$  [ $= n^k$ ].

Testen wir zum Abschluss der Betrachtung von  $P(n, k)$  noch dessen Spezial-Fall  $P(n, n)$ , die Anzahl verschiedener Anordnungen aller  $n [=: k]$  Objekte — ergibt  $\#$  Bijektionen.

Frage: Gilt  $P(n, n) = n!$  ?

Antwort: Ja !

<sup>21</sup> Die anderen 3 o. g. Szenarien sind offensichtlich — hier die Darlegung der  $\#$  injektiver Abbildungen.

<sup>22</sup> Der vertikale Klammer-Ausdruck („Binomial-Koeffizient“) wird, wie vorher erwähnt, im Unter-Abschnitt 5.4.2 (ab Seite 76) detailliert vorgestellt; er bedeutet (hier): aus  $n$  Elementen  $k$  auszuwählen.

<sup>23</sup> siehe die vorangegangene Fußnote 22

<sup>24</sup> „+“ bzw. „-“

<sup>25</sup> „.“ bzw. „,:“

Illustration:

$$P(n, n) = n^n = \frac{n!}{(n-n)!} = n! .$$

$$P(n, n) = \prod_{i:=1}^n (n - n + i) = \prod_{i:=1}^n i = n! .$$

$$P(n, n) = \prod_{i:=0}^{n-1} (n - i) = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1 = n! .$$

Kommen wir nun zur *steigenden Faktoriellen* von  $k$  auf  $n$  :

$$n^{\bar{k}} := \prod_{i:=0}^{k-1} (n+i) .$$

Wir testen hier nur den Spezial-Fall  $1^{\bar{n}}$ , das Produkt aller 1-Nachfolger bis hoch zu  $n$ .

Frage: Gilt  $1^{\bar{n}} = n!$  ?

Antwort: Ja !

Illustration:

$$1^{\bar{n}} = \prod_{i:=0}^{n-1} (1+i) = \prod_{i:=1}^n i = n! [= n^n] .$$

Interessant zu wissen ist noch die Lösung folgender Fragestellung:

Wie viele sichtbar verschiedene Anordnungen von  $n$  Objekten gibt es, wenn einige gleich sind — wenn gar mehrere verschiedene Gruppen jeweils identischer Objekte existieren?

Wir hätten  $k_1$  Objekte des Typs 1,  $k_2$  des Typs 2,  $k_3$  des Typs 3, usw.,  $k_j$  des Typs  $j$ ;  $\sum_{i:=1}^j k_i =: n$ . Dann bringt uns folgende Überlegung die gesuchte Lösung :

$$a_{n,(k_1, \dots, k_j)} = \frac{(\sum_{i:=1}^j k_i)!}{k_1! \cdot \dots \cdot k_j!} = \frac{n!}{\prod_{i:=1}^j (k_i)!} .$$

Die Erläuterung des Bruches läuft ähnlich wie im 4. Anwendungs-Beispiel von  $P(n, k)$  auf Seite 74 bei der Darlegung der # injektiver Abbildungen; hier reicht nun jeweils 1 Repräsentant jeden Typs  $i$  ( $1 \leq i \leq j$ ) als Vertreter für die jeweiligen  $k_i!$  nicht-verschiedenen Anordnungen, weshalb man  $n!$  durch alle  $k_i!$  durch-dividiert.

Folgende drei Beispiele wenden die genannte Formel an :

1.

$$a_{3,(2,1)} = \frac{3!}{2! \cdot 1!} = \frac{2! \cdot 3}{2! \cdot 1} = 3 ; \quad \text{Illustration :}$$

$$|\{(true, true, false), (true, false, true), (false, true, true)\}| = 3 .$$

2.

$$a_{4,(2,1,1)} = \frac{4!}{2! \cdot 1!^2} = \frac{2! \cdot 3 \cdot 4}{2! \cdot 1} = 12 ; \quad \text{Illustration :}$$

$$\begin{aligned} |\{AABC, AACB, ABAC, ACAB, ABCA, ACBA, \\ BAAC, CAAB, BACA, CABA, CBA\}| &= 12 . \end{aligned}$$

3.

$$a_{5,(2,3)} = \frac{5!}{2! \cdot 3!} = \frac{3! \cdot 4 \cdot 5}{3! \cdot 2 \cdot 1} = 10 ; \quad \text{Illustration :}$$

$$\begin{aligned} |\{(b, b, g, g, g), (b, g, b, g, g), (b, g, g, b, g), (b, g, g, g, b), (g, b, b, g, g), \\ (g, b, g, b, g), (g, b, g, g, b), (g, g, b, b, g), (g, g, b, g, b), (g, g, g, b, b)\}| = 10 . \end{aligned}$$

Testen wir abschließend den Spezial-Fall, dass alle  $n$  untereinander verschieden sind :

Frage: Gilt  $a_{n,(k_1, \dots, k_n)} = n!$  ?

Antwort: Ja !

Illustration:

$$a_{n,(k_1, \dots, k_n)} = \frac{n!}{\prod_{i=1}^n (k_i!)} = \frac{n!}{1!^n} = n! .$$

## 5.4.2 Kombinationen

Hier geht es um die Anzahl verschiedener Auswahlen von  $k$  aus  $n$  Objekten, also wie viele  $k$ -elementige Teilmengen sich aus einer  $n$ -elementigen Grundmenge bilden lassen<sup>26</sup> — # verschiedener Kombinationen<sup>27</sup>; dies wird durch den *Kombinations-Koeffizienten*  $C(n, k)$  ausgedrückt. Der geläufigere Name lautet: „Binomial-Koeffizient“ — gesprochen „ $n$  über  $k$ “; mathematisch ergibt er sich wie folgt :

$$\binom{n}{k} = \frac{n!}{k! \cdot (n - k)!} \quad \left[ = \begin{cases} 0 & ; n < k \quad (\text{definiert}) \\ 1 & ; (n = k) \vee (n \geq k = 0) \end{cases} \right] .$$

Der Unterschied zu bzw. Zusammenhang mit  $P(n, k)$  ist offensichtlich: Hier kommt es nicht auf die Reihenfolge der gewählten  $k$  Objekte an, weshalb wieder 1 Repräsentant

<sup>26</sup> „#  $k$ -Teilmengen einer  $n$ -Menge“

<sup>27</sup> engl.: combinations

als Vertreter dieser  $k!$  möglichen Reihungen ausreicht — was man dadurch erreicht, indem man den Permutations-Koeffizienten durch genau diese  $k!$  dividiert :

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

Folgende Überlegung lässt die Ausrechnung im unteren Zahlenbereich etwas handlicher ausfallen; dazu setzen wir  $m := \max(k, n - k)$  und schreiben wie folgt :

$$\binom{n}{k} = \frac{m! \cdot (m+1) \cdot (m+2) \cdot \dots \cdot n}{m! \cdot \min(k, n-k)!} = \frac{\prod_{i=1}^{n-m} (m+i)}{\min(k, n-k)!} .$$

Folgende vier Beispiele wenden die genannte Formel an :

1.

$$\begin{aligned} \binom{4}{2} &= \left[ \frac{\max(2, 4-2)! \cdot (2+1) \cdot (2+(4-2))}{\max(2, 2)! \cdot \min(2, 2)!} \right] \\ &\quad \frac{\prod_{i=1}^{4-2} (2+i)}{2!} = \frac{3 \cdot 4}{2} = \frac{3 \cdot 2 \cdot 2}{2} = 6 ; \\ \text{anstatt : } \binom{4}{2} &= \frac{4!}{2! \cdot 2!} = \frac{24}{2 \cdot 2} = \frac{24}{4} = 6 . \end{aligned}$$

2.

$$\begin{aligned} \binom{7}{3} &= \left[ \frac{\max(3, 7-3)! \cdot (4+1) \cdot (4+2) \cdot (4+(7-4))}{\max(3, 4)! \cdot \min(3, 4)!} \right] \\ &\quad \frac{\prod_{i=1}^{7-4} (4+i)}{3!} = \frac{5 \cdot 6 \cdot 7}{6} = 35 ; \\ \text{anstatt : } \binom{7}{3} &= \frac{7!}{3! \cdot 4!} = \frac{5040}{6 \cdot 24} = \frac{5040}{144} = \dots = 35 . \end{aligned}$$

3.

$$\begin{aligned} \binom{9}{4} &= \left[ \frac{\max(4, 9-4)! \cdot (5+1) \cdot (5+2) \cdot (5+3) \cdot (5+(9-5))}{\max(4, 5)! \cdot \min(4, 5)!} \right] \\ &\quad \frac{\prod_{i=1}^{9-5} (5+i)}{4!} = \frac{6 \cdot 7 \cdot 8 \cdot 9}{24} = \frac{(6 \cdot 4) \cdot 2 \cdot 7 \cdot 9}{24} = 126 ; \\ \text{anstatt : } \binom{9}{4} &= \frac{9!}{4! \cdot 5!} = \frac{7! \cdot 8 \cdot 9}{24 \cdot 120} = \frac{5040 \cdot 8 \cdot 3 \cdot 3}{120 \cdot 24} = \dots = 126 . \end{aligned}$$

4.

$$\binom{11}{3} = \left[ \frac{\max(3, 11-3)! \cdot (8+1) \cdot (8+2) \cdot (8+(11-8))}{\max(3, 8)! \cdot \min(3, 8)!} \right] \\ \frac{\prod_{i=1}^{11-8} (8+i)}{3!} = \frac{9 \cdot 10 \cdot 11}{6} = \frac{3 \cdot 3 \cdot 2 \cdot 5 \cdot 11}{3 \cdot 2} = 165; \\ \text{anstatt: } \binom{11}{3} = \frac{11!}{3! \cdot 8!} = \frac{11!}{6 \cdot 5040 \cdot 8} = \frac{11!}{6 \cdot 40320} = \dots = 165.$$

Es wird halt am Anfang fehlerfrei gekürzt; die Zahlen bleiben, so gut es geht, handlich.

Kommen wir nun zu einer sofort einleuchtenden Eigenschaft: Die Anzahl Möglichkeiten, aus einer  $n$ -elementigen Menge  $k$  Elemente zu wählen ist identisch mit der Anzahl Möglichkeiten,  $n - k$  Elemente auszuwählen. Schließlich lässt man im ersten Fall  $n - k$  liegen und im zweiten Fall  $k$ ; man vertauscht nur die Semantik<sup>28</sup> der betrachteten Objekte — sie genommen oder nicht genommen zu haben. Da die beiden Fälle symmetrisch zueinander sind, spricht man von der *Binomial-Symmetrie*, mit gleicher Syntax<sup>29</sup>:

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

Dieser bequeme Sachverhalt lässt sich *direkt* beweisen :

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

Das wohl von der Schule her bekannte „*Pascalsche Dreieck*“ kann man ähnlich zeigen:

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

---

<sup>28</sup>Bedeutung

<sup>29</sup>Struktur

$$\begin{aligned}
 & \frac{(n-1)!}{k! \cdot (n-k-1)!} \cdot \frac{n}{n} + \frac{k}{k} \cdot \frac{(n-1)!}{(k-1)! \cdot (n-k)!} \cdot \frac{n}{n} = \\
 & \frac{n!}{k! \cdot (n-k-1)! \cdot n} + \frac{n! \cdot k}{k! \cdot (n-k)! \cdot n} = \\
 & \frac{n!}{k!} \cdot \left( \frac{n-k}{(n-k-1)! \cdot (n-k) \cdot n} + \frac{k}{(n-k)! \cdot n} \right) = \\
 & \frac{n!}{k!} \cdot \left( \frac{n-k}{(n-k)! \cdot n} + \frac{k}{(n-k)! \cdot n} \right) = \\
 & \frac{n!}{k! \cdot (n-k)!} \cdot \frac{n-k+k}{n} = \\
 & \frac{n!}{k! \cdot (n-k)!}
 \end{aligned}$$

Der Binomial-Koeffizient lässt sich somit bisher auf mindestens zwei Arten berechnen: geschlossen<sup>30</sup> und rekursiv<sup>31</sup>. Nun bieten wir eine weitere Berechnungs-Variante an: sukzessiv<sup>32</sup>, und zwar als fortwährende (inkrementelle<sup>33</sup>) Summe :

$$\binom{n}{k} = \sum_{[0 \leq] i := k-1}^{[0 \leq] n-1} \binom{i}{k-1}$$

Abbildung 5.4 möge dies illustrieren.

Bringen wir nun noch einige interessante Sachverhalte.

Der „zentrale“ Binomial-Koeffizient ist derjenige, bei dem der untere Parameter halb so groß wie der obere ist. Stellt man sich die Anordnung aller möglichen  $C(n, k)$  in einem Teilmengen-Verband mit  $n+1$  Ebenen<sup>34</sup> vor — unten  $C(n, 0)$ , darüber die mit nächstgrößerem  $k$ , usw., bis hoch zu  $C(n, n)$  — so ist die Anzahl der Elemente auf der mittleren Ebene mit der Nummer  $\lfloor n/2 \rfloor$  maximal<sup>35</sup>  $C(n, \lfloor n/2 \rfloor) \geq C(n, k), \forall k$ . Ist  $n$  gerade, gibt es natürlich nichts zu runden; ist  $n$  ungerade, so soll das eher unübliche Rundungs-Zeichen den Umstand signalisieren, dass es egal ist, ob man nach unten oder oben rundet [ $C(n, (n-1)/2) = C(n, (n+1)/2)$ ], wegen der bekannten Binomial-Symmetrie:

$$\binom{n}{\lfloor \frac{n}{2} \rfloor} = \begin{cases} \binom{\frac{n}{2}}{\frac{n}{2}} & ; \text{gerade}(n) \\ \binom{\frac{n}{2}}{\frac{n-1}{2}} & ; \text{ungerade}(n) \end{cases} = \begin{cases} \binom{\frac{n}{2}}{\frac{n}{2}} & ; \text{gerade}(n) \\ \binom{\frac{n}{2}}{\frac{n+1}{2}} & ; \text{ungerade}(n) \end{cases}.$$

<sup>30</sup>hier als Quotient von Fakultäten

<sup>31</sup>rückführend auf Vorheriges — hier via der gerade gezeigten Addition

<sup>32</sup>schriftweise

<sup>33</sup>der untere Summen-Index (hier der obere Binomial-Parameter) wächst, wie üblich, um 1

<sup>34</sup>nummeriert von 0 bis  $n$ , den möglichen Werten von  $k$  (siehe Abb. 1.1 ab Seite 11 in Abschnitt 1.3)

<sup>35</sup>weshalb der oben folgende  $C$ -Ausdruck auch der *maximale* Binomial-Koeffizient genannt wird

	<b>k</b>	0	1	2	3	4	...
<b>n</b>							
0		1	0	0	0	0	...
1		1	1	0	0	0	...
2		1	2	1	0	0	...
3		1	3	3	1	0	...
4		1	4	6	4	1	...
⋮							⋮

Abb. 5.4: Binom-Summe

Illustration

$$\binom{1}{\lfloor \frac{1}{2} \rfloor} = \binom{1}{\frac{1-1}{2}} = \binom{1}{0} = \binom{1}{0} = \\ \binom{1}{\frac{1+1}{2}} = \binom{1}{\frac{2}{2}} = \binom{1}{1} [= 1] .$$

$$\binom{3}{\lfloor \frac{3}{2} \rfloor} = \binom{3}{\frac{3-1}{2}} = \binom{3}{\frac{2}{2}} = \binom{3}{1} = \\ \binom{3}{\frac{3+1}{2}} = \binom{3}{\frac{4}{2}} = \binom{3}{2} [= 3] .$$

Ist  $n$  gerade, existiert der zentrale Binomial-Koeffizient nur  $1 \times$ ; ist  $n$  jedoch ungerade, taucht er doppelt auf; dies gilt es bei entsprechenden Zähl-Aufgaben zu berücksichtigen.

Der Binomial-Koeffizient ist Haupt-Bestandteil des sogenannten *Binomial-Theorems*<sup>36</sup>

$$(a+b)^n = \sum_{k:=0}^n \left( \binom{n}{k} \cdot a^{(n-k)} \cdot b^k \right) .$$

Hiermit lässt sich überzeugend eine früher mal strittige Behauptung beweisen:  $0^0 = 1$ :

$$1 = 1^0 = (0+1)^0 = \binom{0}{0} \cdot 0^{(0-0)} \cdot 1^0 = 1 \cdot 0^0 \cdot 1 = 0^0 .$$

---

<sup>36</sup>, „Binomischer Lehrsatz“

In der wichtigen Spezialisierung  $a := b := 1$  ergibt sich Folgendes :

$$(1+1)^n = \sum_{k=0}^n \left( \binom{n}{k} \cdot 1^{(n-k)} \cdot 1^k \right) \iff \sum_{k=0}^n \binom{n}{k} = 2^n.$$

Da  $C(n, k)$  die Anzahl  $k$ -elementiger Teil-Mengen einer endlichen  $n$ -elementigen Menge angibt, stellt die soeben dargelegte Formel klar, dass die Menge aller („unechten“) Teilmengen exakt  $2^n$  Elemente hat — es also exponentiell viele Teilmengen gibt.

Für die ersten 14  $n$ -Werte sollte man die jeweilige 2er-Potenz parat haben.<sup>37</sup>

Wie  $C(n, k)$  zur Lösung von Aufgaben beiträgt, mögen folgende fünf Beispiele aufzeigen:

1. In einer aus  $n$  Mitgliedern bestehenden Organisation sind  $k$  Verlässliche zu wählen.

Frage: Wie viele Auswahlen sind möglich (falls Alle in Frage kommen  $\supseteq$ ) ?

Antwort:  $C(n, k)$ .

2. Aus einem Kader bestehend aus  $n$  Fußballern sind  $k$  Spieler zu nominieren.<sup>38</sup>

Frage: Wie viele vollständige Nominierungs-Bögen sind zu Spiel-Beginn möglich?

Antwort:  $C(n, k)$ .

3. Wir betrachten wieder die gängige Welt der Bit-Vektoren<sup>39</sup>.

Frage: Wie viele  $n$ -stellige Bit-Vektoren mit mindestens  $k \times true$  sind machbar?<sup>40</sup>

Antwort:  $\sum_{i=k}^n C(n, i)$ .

4. Bleiben wir noch kurz in diesem für die Informatik wichtigen Anwendungs-Bereich.

Frage: Wie viele  $n$ -stellige Binär-Ketten gibt es, wenn  $\# false$ -Bits =  $\# true$ -Bits?

Antwort :

$$\begin{cases} 0 & ; \text{ ungerade}(n) \\ \binom{n}{\frac{n}{2}} & ; \text{ gerade}(n) \end{cases}.$$

In diesem Beispiel sehen wir auch den zentralen Binomial-Koeffizienten in Aktion.

5. Lassen Sie uns abschließend in die Welt der Spiele-Programmierung eintauchen. Wir sind im Zentrum des Koordinaten-Systems, 2d-mäßig lokalisiert durch „ $(0, 0)$ “.

Frage: Wie viele minimale achsen-parallele Schrittfolgen vom Ursprungs-Punkt zu einem Punkt „ $(a, b)$ “<sup>41</sup> sind gangbar ( $|a|$  Schritte horizontal,  $|b|$  vertikal)<sup>42</sup> ?

Antwort (siehe Bild 5.5) :

<sup>37</sup>  $2^0 = 1, \dots, 2^{10} = 1024, \dots, 2^{13} = 8192; 2^i := \sum_{[i>0]} 2^{(1)} \cdot 2^{(i-1)}$ .

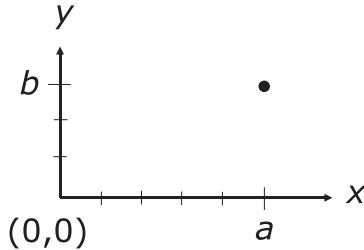
<sup>38</sup> Beim FCB  $\supseteq$  bspw. herrscht natürlich „Selektions-Druck“:  $k < n$ ; aber auch für  $k = n$  und  $k > n$  liefert der gesuchte Ansatz die richtige Antwort.

<sup>39</sup> Zeichen-Ketten bestehend aus *false* („0“) oder/und *true* („1“)

<sup>40</sup> bei stabilem  $n$  — führende 0-Werte (*false*-Bits) demnach vorne erlaubt

<sup>41</sup>  $\in \mathbb{Z}^2 \setminus (0, 0)$ ; unabhängig der Vorzeichen — wir haben eine Symmetrie bzgl. der Achsen  $x$  und  $y$

<sup>42</sup>  $|z| := \text{hier}$  (Absolut-)Betrag einer Zahl



**Abb. 5.5:** 2d-Trajektorie

$$\binom{|a| + |b|}{|a|} = \stackrel{\text{Binomial-}}{\underset{\text{Symmetrie}}{=}} \binom{|a| + |b|}{(|a| + |b|) - |a|} = \binom{|a| + |b|}{|b|} = \binom{|b| + |a|}{|b|},$$

was auch die Antwort für die symmetrische<sup>43</sup> Fragestellung nach der Anzahl verschiedener Bewegungs-Muster zum Punkt „ $(b, a)$ “ darstellen würde: Bei der Gesamt-Anzahl diskreter Schritte kommt es auf die Summe der Bewegungen sowohl in  $x$ - als auch in  $y$ -Richtung an, also auf die Addition der beiden Koordinaten-Beträge, nicht auf die Reihenfolge der Begehung der einzelnen Dimensionen — was auch ganz allgemein die Formeln für die jeweils minimalen Weg-Längen erklärt:

1. Betrachtung: Wir begeben uns auf unserem Weg, welcher  $|a| + |b|$  Schritte benötigt, zunächst auf die  $y$ -Achse, um schrittweise zur Position  $b$  zu gelangen; dabei drückt uns  $|a|$ -mal eine Windböe 1 Schritt horizontal in  $x$ -Richtung.<sup>44</sup> Die Anzahl verschiedener Möglichkeiten hierzu, wann/wo dies geschieht, gibt uns  $C(|a| + |b|, |a|)$ .

2. Betrachtung: Wir begeben uns auf unserem Weg, welcher  $|a| + |b|$  Schritte benötigt, zunächst auf die  $x$ -Achse, um schrittweise zur Position  $a$  zu gelangen; dabei drückt uns  $|b|$ -mal ein kleiner Erdstoß 1 Schritt vertikal in  $y$ -Richtung.<sup>45</sup> Die Anzahl verschiedener Möglichkeiten hierzu, wann/wo dies geschieht, gibt uns  $C(|a| + |b|, |b|)$ .

Wir erzielen die Formel auch aus einer ganz anderen Überlegung heraus; schließlich haben wir aus Unter-Abschnitt 5.4.1 (S. 75) eine Herangehensweise im Köcher, welche uns erlaubt, die # Konfigurationen von  $n$  Objekten zu zählen, wenn verschiedene Gruppen jeweils identischer Objekte existieren: Die 2 Dimensionen ( $x$ - und  $y$ -Richtung) stellen nun die verschiedenen Gruppen-Typen dar, und das Identische ist die auf jeweils einer Dimension stattfindende Bewegungs-Richtung<sup>46</sup>; mit

$$k_1 := |a|, \quad k_2 := |b|, \quad n := k_1 + k_2 := |a| + |b|$$

<sup>43</sup>zur Winkel-Halbierenden durch die ungeraden Quadranten

<sup>44</sup> $a < 0$  Ost-,  $a > 0$  West-Wind;  $a = 0$  Wind-Stille — man gelangt direkt auf der  $y$ -Achse zu  $b$ .

<sup>45</sup>Bei negativem  $b$  fallen wir bei jeder vertikalen Bewegung 1 Stufe tiefer — wie bei 2d-Spielen üblich.

<sup>46</sup>Die Pixel werden in fortlaufender „Laufrichtung“ vom Ursprung aus in 1er-Schritten angesteuert.

erhalten wir dann für die Anzahl möglicher 2-dimensionaler Trajektorien :

$$\frac{(\sum_{i=1}^2 k_i)!}{\prod_{i=1}^2 (k_i!)} = \frac{(|a| + |b|)!}{|a|! \cdot |b|!} = \frac{(|a| + |b|)!}{|a|! \cdot ((|a| + |b|) - |a|)!} = \binom{|a| + |b|}{|a|}.$$

Komplexere Zwischenstationsszenarien zeigt hinten zitiertes Informatik-Buch, S. 12–14.

## 5.5 Stirling- und Bell-Zahlen

### 5.5.1 Stirling-Zahlen 1. Art

Eigentlich handelt es sich hier um die Koeffizienten von  $x^k$  in der Summen-Schreibweise des Ausdrückes  $\prod_{i=0}^{n-1} (x-i) =: j_1$ ; wir bezeichnen sie nach James Stirling mit  $s_1(n, k)$ :

$$j_1 = \sum_{k=0}^n (s_1(n, k) \cdot x^k) .$$

Folgende Rekursion definiert  $s_1(n, k)$  :=

$$\begin{cases} 0 & ; \quad (n < k) \vee (n > k = 0) \\ 1 & ; \quad n = k \\ s_1(n-1, k-1) - (n-1) \cdot s_1(n-1, k) & ; \quad n > k > 0 \end{cases} .$$

Sei  $n := 3$ ,  $M := \{0, \dots, n\}$ ; dann ergeben sich folgende  $|M|$  Werte für  $s_1(n, k)$ ,  $k \in M$ :  $(-)0, 2, -3, 1$ .

Interessant für uns ist die Interpretation als (*Stirling-*)*Zyklus-Zahl* via  $|s_1(n, k)| =:$

$$\begin{bmatrix} n \\ k \end{bmatrix} , \quad \text{Sprechvorschlag : } n \text{ Zyklus } k ,$$

der Anzahl sogenannter „zyklischer“ Partitionen einer  $n$ -elementigen Menge in  $k$  nicht-leere „Zyklen“: Man partitioniert eine  $n$ -Menge in  $k$  nicht-leere Bereiche, betrachtet aber in jedem Teil alle Möglichkeiten einer kreis-förmigen Anordnung<sup>47</sup> der Objekte — als wenn sie um einen Rund-Tisch herum drapiert wären, wobei es weder auf die absolute Platzierungs-Positionen am Tisch selbst noch auf die Zuordnung zu einem bestimmten Tisch ankommt<sup>48</sup>; siehe auch den Spezial-Fall  $|s_1(m, 1)|$ , der die Frage bei der Illustration der Quotienten-Regel im Unter-Abschnitt 5.1.3 (ab S. 51) gelöst hätte.<sup>49</sup>

Zeichnung 5.6 illustriert die Stirling-Zahl 1. Art für  $k$  Tische mit je mindestens 1 Person:

<sup>47</sup>bezogen auf „befindet sich genau 1 Position links (bzw. „rechts“, je nach Blick-Richtung) neben“

<sup>48</sup>jedoch auf die relative Anordnung am jeweiligen Tisch gemäß der Nachbarschafts-Relation „neben“

<sup>49</sup>hier: alle  $n := m$  „Objekte“ an  $k := 1$  Tisch:  $(m-1)!$

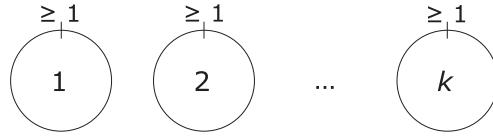


Abb. 5.6: Stirling-1

Beispiel

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix} = |s_1(4, 2)| =_{\text{rekursiv}} \dots = |11| = 11 =_{\text{z. B. explizit}}$$

$$\begin{aligned} & |\{(1), (2, 3, 4)\}, \{(1), (2, 4, 3)\}, \{(2), (1, 3, 4)\}, \{(2), (1, 4, 3)\}, \\ & \{(3), (1, 2, 4)\}, \{(3), (1, 4, 2)\}, \{(4), (1, 2, 3)\}, \{(4), (1, 3, 2)\}, \\ & \{(1, 2), (3, 4)\}, \{(1, 3), (2, 4)\}, \{(1, 4), (2, 3)\}\}| \end{aligned}$$

Spielt man für gegebenes  $n$  die einzelnen Belegungen von  $k$  schrittweise durch, so stellt man fest, dass bei jeder Erhöhung von  $k$  um 1 das Vorzeichen von  $s_1(n, k)$  wechselt<sup>50</sup>. Da die Zyklus-Zahl selbst nur positiv sein kann, ergibt sich hier folgender Zusammenhang:

$$\begin{aligned} s_1(n, k) &= (-1)^{(n-k)} \cdot \begin{bmatrix} n \\ k \end{bmatrix} \quad | : (-1)^{(n-k)} \iff \\ \begin{bmatrix} n \\ k \end{bmatrix} &= \frac{s_1(n, k)}{(-1)^{(n-k)}} = \begin{cases} -s_1(n, k) ; \text{ungerade}(n-k), s_1(n, k) \leq 0 \\ +s_1(n, k) ; \text{gerade}(n-k) , s_1(n, k) \geq 0 \end{cases} \end{aligned}$$

(Die Fälle sind strukturell bewusst nicht disjunkt; der einzige gemeinsame [„= 0“-]Fall wird jedoch wertmäßig in beiden Fällen gleich behandelt, siehe auch den Klammer-Inhalt der Fußnote 50.)

$$\begin{aligned} &= |s_1(n, k)| = |s_1(n-1, k-1) - (n-1) \cdot s_1(n-1, k)| \\ &= \begin{cases} \left| - \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} - (n-1) \cdot (+ \begin{bmatrix} n-1 \\ k \end{bmatrix}) \right| ; s_1(n-1, k) \geq 0 \\ \left| + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} - (n-1) \cdot (- \begin{bmatrix} n-1 \\ k \end{bmatrix}) \right| ; s_1(n-1, k) \leq 0 \end{cases} \\ &= \begin{cases} \left| - \left( \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} \right) \right| ; \text{ungerade}(n-k) \\ \left| + \left( \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} \right) \right| ; \text{gerade}(n-k) \end{cases} \end{aligned}$$

<sup>50</sup>, „alterniert“ (wobei die 0 abwechselnd mal als negative und mal als positive Zahl interpretiert wird)

$$= \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} .$$

Behauptung

$$z(n) := \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} = n! \quad (= n \cdot (n-1)! = n \cdot \begin{bmatrix} n \\ 1 \end{bmatrix}) .$$

Beweis: Induktion über  $n$

Start:  $n_{0_{\text{initial}}} := 0$

$$z_{\text{Prinzip}}(0) := \sum_{k=0}^0 \begin{bmatrix} 0 \\ k \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} = 1 = 0! = z_{\text{Formel}}(0).$$

Im noch kommenden Induktions-Schritt wird es komfortabel sein,  $n-1 \geq 1$  zu haben.

Basis:  $n_0 := 1$

$$z_{\text{P}}(1) := \sum_{k=0}^1 \begin{bmatrix} 1 \\ k \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 0 + 1 = 1 = 1! = z_{\text{F}}(1) .$$

Hypothese:

$$z(n-1) := \sum_{k=0}^{n-1} \begin{bmatrix} n-1 \\ k \end{bmatrix} = (n-1)! .$$

Schritt:  $(n_0 \leq) n-1 \rightarrow n (> n_0)$

$$\begin{aligned} z_{\text{P}}(n) &:= \sum_{k=0}^n \begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n \\ 0 \end{bmatrix} + \sum_{k=1}^n \left( (n-1) \cdot \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \right) \\ &= 0 + (n-1) \cdot \sum_{k=1}^n \begin{bmatrix} n-1 \\ k \end{bmatrix} + \sum_{k=1}^n \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} \\ &= (n-1) \cdot \left( \sum_{k=1}^{n-1} \begin{bmatrix} n-1 \\ k \end{bmatrix} + \begin{bmatrix} n-1 \\ n \end{bmatrix} \right) + \sum_{k=1}^{n-1} \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} \\ &= (n-1) \cdot \left( \sum_{k=0}^{n-1} \begin{bmatrix} n-1 \\ k \end{bmatrix} - \begin{bmatrix} n-1 \\ 0 \end{bmatrix} + 0 \right) + \\ &\quad \sum_{k=0}^{n-1} \begin{bmatrix} n-1 \\ k \end{bmatrix} - \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} + \begin{bmatrix} n-1 \\ n-1 \end{bmatrix} \\ &\stackrel{!}{=} (n-1) \cdot (n-1)! + (n-1)! = ((n-1)+1) \cdot (n-1)! = n \cdot (n-1)! \\ &= n! = z_{\text{F}}(n) . \end{aligned}$$

### 5.5.2 Stirling-Zahlen 2. Art

Eigentlich handelt es sich hier um die Koeffizienten von  $\prod_{i=0}^{k-1} (x - i) =: j_2$  in  $x^k$  als Summe von Produkten geschrieben; wir bezeichnen sie nach James Stirling mit  $s_2(n, k)$ :

$$x^n = \sum_{k=0}^n (s_2(n, k) \cdot j_2) .$$

Folgende Rekursion definiert  $s_2(n, k)$

$$\begin{cases} 0 & ; (n < k) \vee (n > k = 0) \\ 1 & ; (n = k) \vee (n > k = 1) \\ s_2(n-1, k-1) + k \cdot s_2(n-1, k) & ; n > k > 1 \end{cases} .$$

Sei  $M := \{0, \dots, 5\}$ ; die Tabelle 5.7 zeigt uns nun die  $|M|^2$  Werte für  $s_2(n, k)$  [ $k, n \in M$ ].

<b><i>n</i></b>	0	1	2	3	4	5	...
<b><i>k</i></b>	1	0	0	0	0	0	
0	1	0	0	0	0	0	
1	0	1	0	0	0	0	
2	0	1	1	0	0	0	
3	0	1	3	1	0	0	
4	0	1	7	6	1	0	
5	0	1	15	25	10	1	

Abb. 5.7: Stirling-2

In inkrementeller Summen-Notation bekommen wir die Gleichung  $s_2(n, k) =$

$$\sum_{i=k-1}^{n-1} \left( \binom{n-1}{i} \cdot s_2(i, k-1) \right) .$$

Die Stirling-Zahlen 2. Art stehen in einem besonderen Verhältnis zu den Stirling-Zahlen 1. Art, wie wir gleich sehen; aufgrund des alternierenden Vorzeichens von  $s_1(n, k)$  — im Gegensatz zum permanent positiven in  $s_2(n, k)$  — neutralisieren sie sich in folgender Produkt-Summe :

$$\sum_{k=0}^n (s_1(n, k) \cdot s_2(k, i)) = \sum_{k=0}^n (s_2(n, k) \cdot s_1(k, i)) = \begin{cases} 1 & ; n = i \\ 0 & ; n \neq i \end{cases} .$$

Interessant für uns ist die Interpretation als (*Stirling-*) *Teilmengen-Zahl* via  $s_2(n, k) =:$

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \quad , \quad \text{Sprechvorschlag: } n \text{ Aufteilung } k \quad ,$$

die Anzahl Partitionen einer  $n$ -elementigen Menge in  $k$  Teilmengen: Man teilt eine  $n$ -Menge in  $k$  Bereiche auf, betrachtet aber in keinem Teil irgendwelche Reihenfolgen. Dies bedeutet automatisch :

$$\left\{ \begin{matrix} n \\ k \end{matrix} \right\} \leq \left[ \begin{matrix} n \\ k \end{matrix} \right] .$$

Für  $k \in \{n - 1, n\}$  gilt die Gleichheit :

$$\left\{ \begin{matrix} n \\ n - 1 \end{matrix} \right\} =_{n > 0} \left[ \begin{matrix} n \\ n - 1 \end{matrix} \right] =_{n > 1} \left[ \begin{matrix} n - 2 \\ n - 2 \end{matrix} \right] \cdot \binom{n}{2} = n \cdot (n - 1)/2 : .$$

Zunächst sind  $n - 1$  Teil-Mengen zu bilden, womit sich in  $n - 2$  Teil-Mengen jeweils nur 1 Element befindet (ohne weitere Zyklus-Varianten) und sich die restlichen 2 Elemente in der 1 noch verbliebenen Teil-Menge tummeln (ebenfalls ohne weitere Zyklus-Varianten); für die letzt-genannte Auswahl gibt es  $C(n, 2)$  Möglichkeiten, und für die erst-genannte Aufteilung hat man keine weitere Wahl mehr<sup>51</sup>:  $|s_1(n - 2, n - 2)| = 1$  .

$$\left\{ \begin{matrix} n \\ n \end{matrix} \right\} = \left[ \begin{matrix} n \\ n \end{matrix} \right] = 1 =_{n > 0} \left\{ \begin{matrix} n \\ 1 \end{matrix} \right\} : .$$

Im ersten Fall sind  $n$  Teil-Mengen zu bilden, womit sich in jeder Teil-Menge nur 1 Element befindet; im mittleren Fall können es deshalb nicht mehr Zyklen<sup>52</sup> sein, was jeweils nur genau  $1 \times$  möglich ist — wie im letzt-genannten Fall des Ablieferns nur 1 nicht-leeren (Teil-)Menge, in der  $1 \times$  alle Elemente enthalten sind.

Folgendes Beispiel aus der Welt der Abbildungen zeigt eine Anwendung von  $s_2(n, k)$  :

Frage: Wie viele surjektive Funktionen aus einer  $n$ - in eine  $k$ -Menge sind möglich ?

Antwort: Sei  $n := |D|$ ,  $k := |C|$ ;  $f : D \rightarrow C$ . Dann gibt es  $k! \cdot s_2(n, k)$  Surktionen.

Illustration: Schließlich müssen alle  $k$  Elemente aus  $C$  getroffen werden, weshalb die  $n$  Elemente aus  $D$  zu  $k$  Gruppen zusammenzufassen sind<sup>53</sup> — und für eine spezielle Abbildungs-Reihenfolge von  $k$  Objekten gibt es genau  $k!$  Möglichkeiten.

Testen wir zum Abschluss dieser Anwendung noch deren Spezial-Fall  $k = n$ , um die uns bekannte einfache Formel zur Berechnung der # Bijektionen bestätigt zu bekommen:  
 $n! \cdot s_2(n, n) = n!$  — ok<sup>54</sup>.

---

<sup>51</sup>  $\exists! 1$  Aufteilungs-Möglichkeit von  $n - 2$  Elementen in  $n - 2$  Zyklen der „Länge“ ( $:= \# \text{ Elemente}$ ) 1  
<sup>52</sup> der Länge 1

<sup>53</sup>  $n > k$  erlaubt — Injektivität wird hier nicht vorausgesetzt

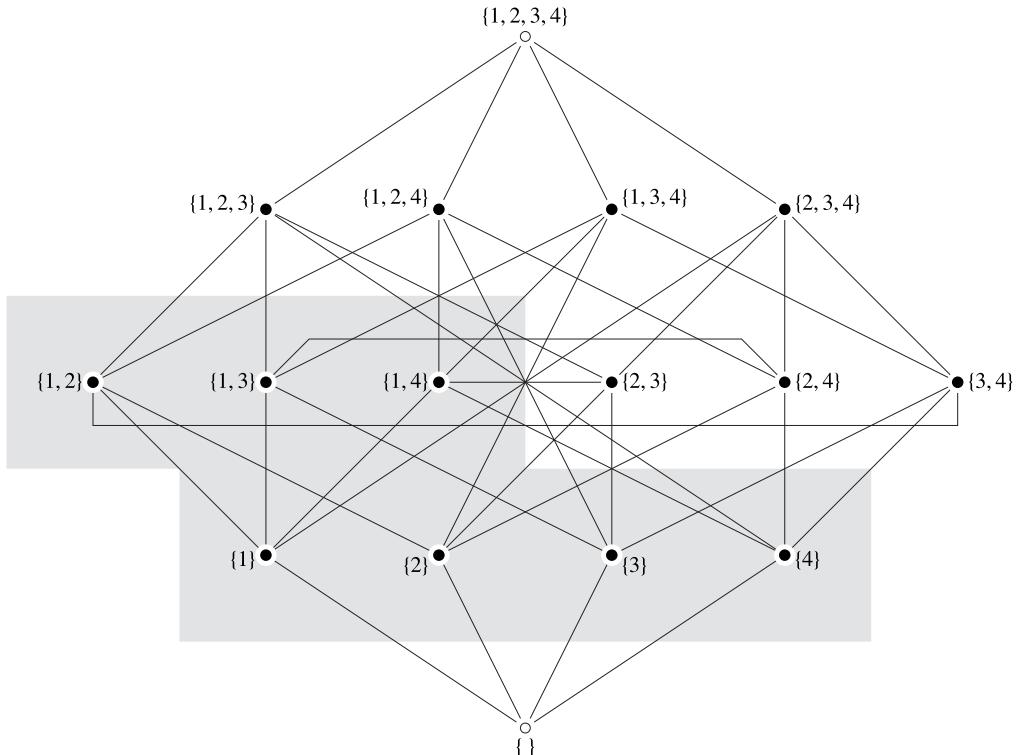
<sup>54</sup> siehe auch den Spezial-Fall  $P(n, n)$  im Unter-Abschnitt 5.4.1 (Seite 74)

Als Glanzlicht dieses Kapitels präsentiere ich die Herleitung der geschlossenen Formel im Sonder-Fall  $s_2(n, 2)$  für beliebiges  $n_{[> 0]}$ ; diese Formel bringt die Anzahl Möglichkeiten, eine gegebene nicht-leere Menge von  $n$  Elementen in 2 nicht-leere Bereiche aufzuteilen:

$$\begin{aligned} \binom{n}{2} &= \sum_{i:=1}^{\lfloor \frac{n}{2} \rfloor} \binom{n}{i} - \begin{cases} \frac{\binom{n}{\frac{n}{2}}}{2}; \text{ gerade}(n) \\ 0; \text{ ungerade}(n) \end{cases} = \\ \frac{\sum_{i:=0}^n \binom{n}{i}}{2} - \binom{n}{0} &= \frac{2^n}{2^1} - 1 = 2^{(n-1)} - 1 : \end{aligned}$$

Zunächst zur Differenz mit der Fall-Unterscheidung:

Man startet bei 1-elementigen Teilmengen und steckt jeweils die restlichen  $n-1$  Elemente in die andere Teil-Menge, in der Zeichnung 5.8 strich-punktiert; die Kardinalität



**Abb. 5.8:** Hälftige Aufteilung

der klein-elementigen Teil-Mengen wird bis zur „Hälfte“ (von  $n$  bzw. des Teil-Mengen-Verbandes<sup>55</sup>) nacheinander erhöht.

<sup>55</sup>siehe Abschnitt 1.3 (ab Seite 11)

Darüber hinaus kann man nicht gehen, da die „dahinter liegende“ zweite Hälfte bereits als Partner für Teil-Mengen aus der ersten Hälfte dient. Für ungerades  $n$  hätte man es damit klar.<sup>56</sup> Für gerades  $n$  muss man sich vergegenwärtigen, dass die Partner der Teil-Mengen auf „halber Höhe“ sich selbst auch auf dieser mittleren Ebene befinden, d. h., man also im Teil-Mengen-Verband auf dieser breitesten<sup>57</sup> Ebene  $n/2$  nur eine Hälfte des zentralen Binomial-Koeffizienten nehmen darf, da die andere Hälfte bereits als Partner auftaucht — im Bild gestrichelt.<sup>58</sup> Da die Elemente auf dieser besagten mittleren Ebene durch den oberen Summen-Index bereits alle mit-summiert wurden, müssen wir die Hälfte dieser  $C(n, n/2)$  Elemente letztlich subtrahieren. (Den oberen Summen-Index nach oben zu runden wäre falsch im ungeraden Fall, da wir die mittlere Ebene sonst doppelt und damit  $1 \times$  zuviel gezählt hätten.)

Nun zur Subtraktion des Binomial-Koeffizienten  $C(n, 0)$  vom o. g. Bruch:

Die vorhin diskutierte Formel entspricht — ungeachtet der Parität<sup>59</sup> von  $n$  — der dort folgenden Differenz aus der halbierten Gesamt-Summe und dem Binomial-Koeffizienten  $C(n, 0)$ . Die Anzahl Knoten in der „unteren“ Hälfte des Teilmengen-Verbandes entspricht aufgrund der Symmetrie des Binomial-Koeffizienten exakt der Hälfte der Gesamt-Anzahl;<sup>60</sup> da wir nur nicht-leere Teil-Mengen betrachten, blenden wir die Möglichkeit kein Element auszuwählen aus — weshalb wir  $C(n, 0) [= 1]$  am Ende abziehen.

Nun zur geschlossenen Form:

Für die Summe im Zähler haben wir bereits den Ausdruck  $2^n$  an der Hand, davon nehmen wir natürlich nur die Hälfte und subtrahieren die 1 Nicht-Möglichkeit — fertig.

$$\text{Beispiel: } s_2(4, 2) = 2^{(4-1)} - 1 = 2^3 - 1 = 8 - 1 = 7 =_{\text{z. B.}}$$

$$|\{\{\{1\}, \{2, 3, 4\}\}, \{\{2\}, \{1, 3, 4\}\}, \{\{3\}, \{1, 2, 4\}\}, \{\{4\}, \{1, 2, 3\}\}, \\ \{\{1, 2\}, \{3, 4\}\}, \{\{1, 3\}, \{2, 4\}\}, \{\{1, 4\}, \{2, 3\}\}\}| \leq |s_1(4, 2)|.$$

### 5.5.3 Bell-Zahlen

Zählen wir abschließend die Gesamt-Zahl aller möglichen Partitionen einer gegebenen Menge der Kardinalität  $n$  [ $\geq 0$ ], unabhängig der Anzahl der jeweils resultierenden Teile. Indem wir alle Fälle von  $k$  [ $\in \{0, \dots, n\}$ ] in  $s_2(n, k)$  durchspielen, erhalten wir durch die Summe dieser Stirling-Aufteilungen die sogenannten *Bell-Zahlen* :

$$B(n) = \sum_{k=0}^n s_2(n, k) = \sum_{k=0}^n \left\{ \begin{matrix} n \\ k \end{matrix} \right\} .$$

Folgende Rekursion definiert

$$B(n) :=$$

$$\begin{cases} 1 & ; \quad n \leq 1 \\ \sum_{i=0}^{n-1} \left( \binom{n-1}{i} \cdot B(i) \right) & ; \quad n \geq 1 \end{cases} .$$

<sup>56</sup>Ist  $n$  ungerade, so hat der Teilmengen-Verband eine gerade Anzahl ( $n + 1$ ) Ebenen (Nr. 0 …  $n$ ).

<sup>57</sup># Elemente (pro Ebene) ist hier maximal

<sup>58</sup>Wir zählen nur die Anzahl verschiedener Aufteilungs-Möglichkeiten von  $n$  Elementen in 2 Bereiche.

<sup>59</sup>„gerade“ bzw. „ungerade“ zu sein

<sup>60</sup>Im „geraden“ Fall bedeutet der Bruch-Strich das Halbieren des Teilmengen-Verbandes mitten durch den zentralen Binomial-Koeffizienten auf der Ebene  $n/2$  (wie in Abbildung 5.8), im „ungeraden“ Fall die Trennung zwischen den beiden auftretenden gleich-großen mittleren Ebenen  $\lfloor n/2 \rfloor$  und  $\lceil n/2 \rceil$ .

Diese nicht-disjunkte Fall-Unterscheidung erlaubt für den einzigen gemeinsamen Fall ( $n = 1$ ) den Funktions-Wert auch über die Replikation der Rekursions-Verankerung ( $n := 0$ ) unmittelbar zu erhalten:

$$B(1) \quad [= B(0)] \quad := \quad 1 \quad .$$

Betrachten wir einige konkrete Werte

$$\begin{aligned} B(0) &= 1, \\ B(1) &= \sum_{i:=0}^{1-1} \left( \binom{0}{i} \cdot B(i) \right) = 1 \cdot B(0) = 1, \\ B(2) &= \sum_{i:=0}^{2-1} \left( \binom{1}{i} \cdot B(i) \right) = 1 \cdot B(0) + 1 \cdot B(1) = 2, \\ B(3) &= \sum_{i:=0}^{3-1} \left( \binom{2}{i} \cdot B(i) \right) = 1 \cdot B(0) + 2 \cdot B(1) + 1 \cdot B(2) = 5 =_{\text{z. B.}} \\ |\{\{\{a, b, c\}\}, \{\{a\}, \{b, c\}\}, \{\{b\}, \{a, c\}\}, \{\{c\}, \{a, b\}\}, \{\{a\}, \{b\}, \{c\}\}\}|, \\ B(4) &= \sum_{i:=0}^{4-1} \left( \binom{3}{i} \cdot B(i) \right) = 1 \cdot B(0) + 3 \cdot B(1) + 3 \cdot B(2) + 1 \cdot B(3) \\ &\qquad\qquad\qquad = 1 \cdot 1 + 3 \cdot 1 + 3 \cdot 2 + 1 \cdot 5 = 15 \end{aligned}$$

Kurz zur Interpretation im Vergleich zu den dazugehörigen Stirling-Teilmengen-Zahlen  $s_2(4, k)$  [ $1 \leq k \leq 4$ ]: Wir stellen uns vor, wir könnten bei der Verteilung von 4 Briefen beliebig zwischen 1, 2, 3 und 4 Säcken wählen.<sup>a</sup> Steckt man alle Briefe in einen Sack, so gibt es dafür nur 1 Möglichkeit. Nimmt man zwei Säcke, so gibt es 7 Möglichkeiten. Hat man drei Säcke, kann man die vier Briefe auf 6 verschiedene Arten verteilen. Stehen vier Säcke zur Verfügung, haben wir nur 1 letzte Möglichkeit: die Briefe alle einzeln in Isolations-Haft zu nehmen. So erhalten wir:  $B(4) = \sum_{k:=0}^4 s_2(4, k) = 0 + 1 + 7 + 6 + 1 = 15$ .

---

<sup>a</sup>Es kommt nicht auf die „Location“ an, sondern lediglich was/wer mit wem zusammen ist — wie im richtigen Leben. Mathematisch spiegelt sich dies in der Mengen-Schreibweise wider, bei der ja auch die Reihenfolge keine Rolle spielt.

$$\begin{aligned} &=_{\text{5.9}}^{\text{Bild}} B(3) + ((B(1) + B(2)) + (B(2) + B(3))) = \\ &\qquad 1 \cdot B(1) + (1+1) \cdot B(2) + (1+1) \cdot B(3) = \\ &\qquad 1 \cdot B(0) + (2 \cdot B(1) + 1 \cdot B(2)) + \\ &\qquad ((1 \cdot B(2) + (1 \cdot B(1) + 1 \cdot B(2))) + 1 \cdot B(3)) = \\ &\qquad \binom{3}{0} \cdot B(0) + \binom{3}{1} \cdot B(1) + \binom{3}{2} \cdot B(2) + \binom{3}{3} \cdot B(3) . \end{aligned}$$

Diese rekursive Vorgehensweise sehen wir in der Grafik 5.9 als schrittweise Addition.

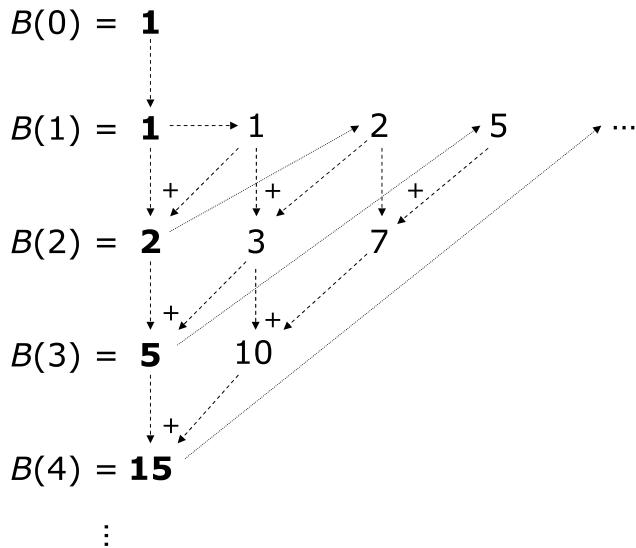


Abb. 5.9: Bell-Zahlen

Die Bell-Zahlen wachsen sehr schnell

$$B(14) = 190.899.322 ,$$

$$B(15) = 1.382.958.545 ,$$

exponentiell:  $2^{(n-1)} \leq B(n) \leq n!$  ;

es gilt:  $4 < n < 2^n < B(n) < n!$  .



# 6 Wahrscheinlichkeits-Theorie

Mit diesem Kapitel beschließen wir thematisch das vorliegende Werk. Im ersten Abschnitt geht es um die *Allgemeine Wahrscheinlichkeit*, im zweiten Abschnitt behandeln wir die *Bedingte Wahrscheinlichkeit*. Lassen Sie uns dabei zunächst mit einigen womöglich bekannten Allgemeinheiten, mit Beispielen garniert, beginnen. Wir kommen sodann zu zwei Varianten der Formel von Thomas Bayes im Bereich der Bedingtheiten, beide mit je einer Anwendung illustriert: das erste Beispiel aus der Welt des Roulette und das zweite zum Thema „Unterschied zwischen Theorie und Praxis“ ☺. Viel Spaß!

## 6.1 Allgemeine Wahrscheinlichkeit

Wir führen hier die nötigen Begriffe ein und erläutern sie anhand gängiger Beispiele.

Es beginnt mit der Festlegung des

*Ereignis-Raums*

:

$\Omega :=$  Menge aller möglichen Ausprägungen von Ereignissen<sup>1</sup> (s. u.) .

Die # Elemente in dieser Menge der Möglichkeiten ist die *Ereignisraum-Größe* :

$|\Omega|$  .

Ein gewünschtes *Ereignis* ist ganz allgemein eine Teil-Menge aller Möglichkeiten:

$E \subseteq \Omega$  .

Die *Ereignis-Kardinalität* ist demnach:

$|E|_{[\leq |\Omega|]}$  .

Ein *Elementar-Ereignis* ist ein Ereignis-„Singleton“ ( $\exists!$  Element:  $|E| = 1$ ).

Bei fairem Ausgang eines „Experiments“ ergibt sich sodann die *Wahrscheinlichkeit* :

$$p_\Omega(E) = \frac{|E|}{|\Omega|} .$$

Dass diese Wahrscheinlichkeit (engl.: *probability*)  $p$  nur positiv sein und 100 % nicht übersteigen kann, sieht man schon allein darin, dass  $E$  stets eine Teilmenge von  $\Omega$  ist :

$$0 = p(\{\}) \leq p(E) \leq p(\Omega) = 1 =_{[\Omega \ni e_i]}$$

<sup>1</sup>was alles passieren kann („alles was geht“ ☺)

$$p\left(\bigcup_{i:=1}^{|\Omega|} \{e_i\}\right) =_{\substack{\text{Partition} \\ e_i \text{ disjunkt}}} \sum_{i:=1}^{|\Omega|} p(e_i).$$

Betrachten wir  $n$  Ereignis-Mengen, welche ggf. gemeinsame Elemente vorweisen, so gilt — nach George Boole — die sofort einleuchtende Ungleichung :

$$p\left(\bigcup_{i:=1}^n E_i\right) \leq \sum_{i:=1}^n p(E_i).$$

Im allgemeinen Fall der Vereinigung eventuell nicht-disjunkter Ereignis-Mengen greifen wir auf das Ein-/Ausschluss-Prinzip zurück; es liest sich bei nur zwei Mengen wie folgt:

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

Im Spezial-Fall zweier doch disjunkter Mengen haben wir einen leeren Durchschnitt<sup>2</sup>; es liegt demnach eine Partition vor (s. o.), und wir können schnittfrei argumentieren :

$$p(A \cup B) = p(A) + p(B).$$

Teilt sich unser gesamtes  $\Omega$  in zwei völlig unabhängige Teilbereiche auf, so erhalten wir:

$$\begin{aligned} p(\Omega) &=_{\text{Partition}} p(A) + p(B) = 1 & | - p(B) &\iff \\ p(A) &= 1 - p(B) &&. \end{aligned}$$

Beispiel: Fußballplatz-Seitenwahl („fairer Münz-Wurf“)<sup>3</sup>

$$\begin{aligned} \Omega &:= \{Kopf, Zahl\}; \\ p(K) &= 1 - p(Z) =_{\text{fair}} 1 - p(K) \iff_{:2}^{+p(K)} p(K) = \frac{1}{2} = p(Z). \end{aligned}$$

Die folgenden vier aus dem Alltag bekannten Beispiele illustrieren größere Partitionen:

### 1. 1 Würfel

- $\Omega := \{1, 2, 3, 4, 5, 6\}$
- $|\Omega| = 6$
- $E :=$  gewünschte „Augen“-Zahl,  $|E| = 1$
- $p_\Omega(E) = p(e_i) = |E|/|\Omega| = 1/6$ ,  $\forall_{[1 \leq i \leq |\Omega|]}$
- $p(\Omega) = p\left(\bigcup_{i:=1}^{|\Omega|} \{e_i\}\right) = \sum_{i:=1}^{|\Omega|} p(e_i) = 6 \cdot 1/6 = 1$

<sup>2</sup>weshalb es nichts abzuziehen gibt

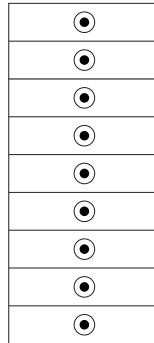
<sup>3</sup>Das Ding möge auf eine flache Seite zu liegen kommen und nicht auf der Kante stehen bleiben. ☺

## 2. 2 verschieden-farbige Würfel

- $\Omega := \{(1,1), (1,2), (1,3), \dots, (1,6), (2,1), \dots, (2,6), \dots, (6,1), \dots, (6,6)\}$
- $|\Omega| = 6^2 = 36$
- $E :=$  spezieller Doppel-Wurf<sup>4</sup>,  $|E| = 1$
- $p_\Omega(E) = p(e_i) = |E|/|\Omega| = 1/36$ ,  $\forall_{[1 \leq i \leq |\Omega|]}$
- $p(\Omega) = p(\bigcup_{i=1}^{|\Omega|} \{e_i\}) = \sum_{i=1}^{|\Omega|} p(e_i) = 36 \cdot 1/36 = 1$

## 3. Würfel-Pärchen

- $\Omega := \{(j,k) \mid 1 \leq j, k \leq 6\}$
- $|\Omega| = 6^2 = 36$  — alles wie eben
- $E := \{(j,k) \mid 1 \leq j = k \leq 6\} = \{(j,j) \mid 1 \leq j \leq 6\}$
- $|E| = 6$
- $p_\Omega(E) = p(\bigcup_{i=1}^{|E|} \{e_i\}) = \sum_{i=1}^{|E|} p(e_i) = 6 \cdot 1/36 = |E|/|\Omega| = 1/6$

4. Spiel-Automat<sup>5</sup> (siehe Skizze 6.1)**Abb. 6.1:** Spiel-Automat

- $\Omega := \{(b_{n-1}, b_{n-2}, \dots, b_0) \mid b_i \in \mathcal{B} [= \{0,1\}], n-1 \geq i \geq 0\} [= \mathcal{B}^n]$
- $|\Omega| = |\mathcal{B}|^{\{n-1, n-2, \dots, 0\}} = 2^n [= |\mathcal{B}^n|]$
- $E := \{(1, 1, \dots, 1)\}$
- $|E| = 1$

---

<sup>4</sup> $(j,k) \neq_{[j \neq k]} (k,j)$

<sup>5</sup>Vereinfachte Sichtweise im Sinne eines Bit-Vektors, bei dem nacheinander jedes Bit *true* werden soll; man muss bei jedem Tasten-Druck erfolgreich sein, bis man auf der höchsten Stufe angelangt ist.

$$\bullet \quad p_{\Omega}(E) = |E|/|\Omega| = 1/2^n = 2^0/2^n = 2^{-n} .$$

Konkret: Es möge eine faire boolesche Taste vorliegen; müsste man nun für die sogenannte „Serie“ bspw. 9 (=:  $n$ ) mal hintereinander einen erfolgreichen Tasten-Druck schaffen, so läge die Schluss-Wahrscheinlichkeit ( $\approx_{[<]} 0,2\%$ ) nahe bei 2% — ein im dortigen Milieu durchaus anzutreffender Wert.  $\smile$

Bisher haben wir die Wahrscheinlichkeiten summiert, nun werden wir sie multiplizieren — und zwar beim gleichzeitigen Auftreten „unabhängiger“ Ereignisse.

*Unabhängig* sind  $n$  Ereignisse, wenn folgende Gleichheit gilt:

$$p(\bigcap_{i:=1}^k E_{j_i}) = \prod_{i:=1}^k p(E_{j_i}), \forall_{[2 \leq]} k \leq n \geq j_k > j_{k-1} > \dots > j_2 > j_1 \geq 1 .$$

Illustration

$$\bullet \quad n := 2$$

$$p(E_1 \cap E_2) = p(E_1) \cdot p(E_2)$$

$$\bullet \quad n := 3$$

$$p(E_1 \cap E_2) = p(E_1) \cdot p(E_2)$$

$$p(E_1 \cap E_3) = p(E_1) \cdot p(E_3)$$

$$p(E_2 \cap E_3) = p(E_2) \cdot p(E_3)$$

$$p(E_1 \cap E_2 \cap E_3) = p(E_1) \cdot p(E_2) \cdot p(E_3) .$$

Beispiel: 2 verschiedene Würfel (wie vorhin)

$$\bullet \quad \Omega := \{1, 2, 3, 4, 5, 6\}$$

$$\bullet \quad |\Omega| = 6 \text{ (pro Würfel)}$$

$$\bullet \quad E_i := \text{gewünschte „Augen“-Zahl Würfel}_i, \quad 1 \leq i \leq 2 =: n =: k$$

$$\bullet \quad E := E_1 \cap E_2$$

$$\bullet \quad p_{\Omega}(E) = p(\{e_1\} \cap \{e_2\}) = p(e_1) \cdot p(e_2) = (1/6)^2 = 1/6^2 = 1/36 .$$

## 6.2 Bedingte Wahrscheinlichkeit

Dieser letzte Abschnitt behandelt die Wahrscheinlichkeit eines Ereignisses  $A$  unter der *Bedingung* eines gegebenen Ereignisses  $B$ ; diese berechnet sich wie folgt — gesprochen: „ $p$  von  $A$  gegeben  $B$ “ :

$$p(A|B) = \frac{p(A \cap B)}{p(B)_{[>0]}} \iff p(A \cap B) = p(A|B) \cdot p(B) .$$

Sind  $A$  und  $B$  unabhängig, so ergibt sich das wenig überraschende Resultat :

$$p(A|B) = \frac{p(A) \cdot p(B)_{[>0]}}{p(B)_{[>0]}} = p(A) .$$

(Schließlich kommt es hier beim Auftreten von  $A$  nicht auf die *Bedingung*  $B$  an.)

Eine einfache Vertauschung der Namen bringt korrespondierende Sachverhalte hervor :

$$p(B|A) = \frac{p(B \cap A)}{p(A)_{[>0]}} \iff p(B \cap A) = p(B|A) \cdot p(A) .$$

Sind  $A$  und  $B$  unabhängig, so ergibt sich entsprechend :

$$p(B|A) = \frac{p(B) \cdot p(A)_{[>0]}}{p(A)_{[>0]}} = p(B) .$$

Wir kommen sodann zur Formel von Thomas Bayes zur *bedingten Wahrscheinlichkeit* :

$$p(A|B) = \frac{p(A \cap B)}{p(B)_{[>0]}} = \frac{p(B \cap A)}{p(B)_{[>0]}} = \frac{p(B|A) \cdot p(A)}{p(B)} .$$

Im Spezial-Fall  $A \subseteq B$  fällt das Ganze entsprechend einfacher aus:

$$\begin{aligned} p(A|B) &= \frac{p(A \cap B)}{p(B)_{[>0]}} = \frac{p(A)}{p(B)} \iff \\ p(A \cap B) &= \frac{p(A)}{p(B)_{[>0]}} \cdot p(B)_{[>0]} = p(A) ; \\ p(B|A) &= \frac{p(B \cap A)}{p(A)_{[>0]}} = \frac{p(A)}{p(A)_{[>0]}} = 1 \iff \\ p(B \cap A) &= 1 \cdot p(A)_{[>0]} = p(A) . \end{aligned}$$

$p(B|A_{[\subseteq B]}) = 100\%$ , weil die „unwahrscheinlichere“ Ereignis-Menge  $A$  gegeben und somit bereits erfüllt ist — und die Ober-Menge  $B$  als Disjunktion („ODER“-Verknüpfung) von Ereignissen damit ebenfalls erfüllt ist.

Diese spezielle *bedingte Teilmengen-Wahrscheinlichkeit* lässt sich auch so herleiten:

$$p(A|B) = p(B|A) \cdot \frac{p(A)_{[>0]}}{p(B)_{[>0]}} = 1 \cdot \frac{p(A)_{[>0]}}{p(B)_{[>0]}} = \frac{p(A)}{p(B)} ,$$

wie bereits vorhin angegeben.

Wir kommen nun zu den *totalen Wahrscheinlichkeiten* :

Voraussetzung: Bedingende Ereignisse  $B_1, B_2, \dots, B_n$  bilden eine Partition von  $\Omega$  :

$$\begin{aligned} \bigcup_{i:=1}^n B_i &= \Omega & , \\ B_j \cap B_k &= \{\} & , \quad \forall [1 \leq] j < k [\leq n] \\ \sum_{i:=1}^n p(B_i) &= p(\Omega) = 1 & . \end{aligned}$$

Da  $A \subseteq \Omega =_{\text{partition}} \bigcup_{i:=1}^n B_i$  gegeben ist, erhalten wir  $p(A)$  als Summe aller  $n$  Einzel-Wahrscheinlichkeiten von  $A$  im jeweiligen Schnitt mit den unter sich disjunkten  $B_i$  :

$$p(A) = \sum_{i:=1}^n p(A \cap B_i) = \sum_{i:=1}^n (p(A|B_i) \cdot p(B_i)) .$$

Wir stellen nun die allgemeine Formel für *bedingte totale Wahrscheinlichkeiten* dar:

Voraussetzung:  $A \subseteq \Omega \supseteq B_s \in \{B_1, B_2, \dots, B_n\}$  ;

insgesamt erzielen wir folgenden Zusammenhang :

$$\begin{aligned} p(B_s|A) &= \frac{p(B_s \cap A)}{p(A)} = \frac{p(A \cap B_s)}{p(A)} = \frac{p(A|B_s) \cdot p(B_s)}{p(A)} = \\ &\frac{p(A|B_s) \cdot p(B_s)}{\sum_{i:=1}^n (p(A|B_i) \cdot p(B_i))} . \end{aligned}$$

Im Sonder-Fall  $n := 1 [= s]$  ergibt sich die bedingte totale Wahrscheinlichkeit von 100 %:

$$p(B_s|A) = \frac{p(A|B_s) \cdot p(B_s)}{\sum_{i:=1}^1 (p(A|B_i) \cdot p(B_i))} = \frac{p(A|B_s) \cdot p(B_s)}{p(A|B_s) \cdot p(B_s)} = 1 ,$$

was man schon aus dem Spezial-Fall  $A \subseteq B_{(s)}$  der bedingten Wahrscheinlichkeit erhält:

$$p(B_s|A) = p(\Omega|A[\subseteq \Omega]) = 1 .$$

Wie angekündigt runden zwei Beispiele den Themen-Kanon des vorliegenden Buches ab — ein offensichtliches und ein nicht-offensichtliches<sup>6</sup> :

### 1. Beispiel: Roulette

Unter Vernachlässigung der *Zero* spielen wir eine Farbe.

---

<sup>6</sup>auf den ersten Blick — den Unterschied zwischen Theorie und Praxis offenbarend ☺

- Erster Lauf: *Rouge*; zweiter Lauf: Spiel .
- Mit welcher Wahrscheinlichkeit käme *Noir* ?
- $A := \{(\underline{R}, N)\}$ ,  $B := \{(\underline{R}, N), (\underline{R}, R)\} =_{\text{hier}} \Omega$  .
- $p(A_{[\subseteq B]} | B) = \frac{p(A)}{p(B)} = \frac{50\%}{100\%} = \frac{1}{2}$  .
- Mit welcher Wahrscheinlichkeit käme stattdessen wiederum  $R$  ?
- $p(\{(\underline{R}, R)\}_{[\subseteq B]} | \Omega) = \frac{50\%}{100\%} = \frac{1}{2}$  .
- Wir beobachten, dass beide Farben gleich wahrscheinlich sind, wir das Folge-Ereignis also nicht vorhersagen können — was zu erwarten war; der Ausgang des ersten Laufs hat keinerlei Einfluss auf den Ausgang des zweiten Laufs.

## 2. Beispiel: „Hinter der Tür“

Bei einem Spiel-Wettbewerb versteckt sich hinter genau einer von drei Türen ein vorher ausgelobter Gewinn-Preis. Die Kandidatin soll nun erraten, hinter welcher Tür sich dieser Preis befindet.

- Tür-Menge  $T := \{A, B, C\}$
- Ereignis  $H_X$ : hinter Tür  $X (\in T)$  befindet sich der Gewinn
- Wahrscheinlichkeit  $p(H_X) = \frac{1}{3}, \forall X_{[\in T]}$  (gleich-verteilt — „fair“)
- Ereignis  $O_X$ : Tür  $X$  offen
- Die Lady legt los — und rät richtig:<sup>7</sup>  $H_A$  (dies sei das dargebotene Szenario).
- Zum Charakter des Spiels gehört es, dass der Moderator der Kandidatin nun eine der beiden nicht von ihr genannten Türen öffnet<sup>8</sup> und ihr dann anbietet, ihre Tür-Wahl nochmals zu überdenken. (Der Moderator öffnet nach dem ersten Raten nie sofort ihre angesagte Tür.) Versteckt sich der Gewinn wirklich hinter  $A$ , so kann der Moderator beliebig  $B$  oder  $C$  öffnen; ist der Preis hinter  $B$  oder  $C$ , so öffnet er die jeweils andere Tür ( $C$  oder  $B$ ), aber nicht  $A$ . Er öffnet jetzt bspw.  $B$ .
- Was scheint nun günstiger für die Kandidatin — es bei ihrer ursprünglichen Wahl  $A$  zu belassen oder nach  $C$  zu wechseln? Oder ist es gar egal?
- Sie schätzt zunächst ab, warum Tür  $B$  geöffnet wurde (und nicht  $C$ )<sup>9</sup> :

$$p(O_B | H_C) = 1 ,$$

$$p(O_B | H_B) = 0 ,$$

$$p(O_B | H_A) = p(O_C | H_A) = \frac{1}{2} , \quad p(O_A | H_A) = 0 ;$$

$$\sum_{X \in T} p(O_X | H_A) = 0 + \frac{1}{2} \cdot 2 = 1 , \quad \text{ok} .$$

<sup>7</sup>was sie zu dem Zeitpunkt noch nicht weiß

<sup>8</sup>eine, hinter der sich der Gewinn nicht befindet (stattdessen bspw. eine Ziege [„Ziegen-Problem“])

<sup>9</sup> $A$  fällt aufgrund der Spielregeln beim ersten Öffnen weg.

- Sie prüft die Voraussetzungen bzgl. der Partitionierung des Ereignis-Raumes:

$$\bigcup_{X \in T} H_X = \Omega ,$$

$$H_A \cap H_B = H_A \cap H_C = H_B \cap H_C = \{\} ;$$

$$\sum_{X \in T} p(H_X) = \frac{1}{3} \cdot 3 = 1 = p(\Omega) , \text{ ok} .$$

(Schließlich ist der Preis hinter irgendeiner Tür, aber nicht hinter mehreren; dürfte man hingegen alle Türen öffnen, so wäre der Preis zu 100% „safe“.)

- Nun berechnet die Kandidatin die bedingten totalen Wahrscheinlichkeiten, um ihre zweite Ansage vorzubereiten:  $A$  („so lassen“) oder  $C$  („wechseln“) :

$$\begin{aligned} p(H_A|O_B) &= \frac{p(O_B|H_A) \cdot p(H_A)}{\sum_{X \in T} (p(O_B|H_X) \cdot p(H_X))} = \frac{\frac{1}{2} \cdot \frac{1}{3}}{(\frac{1}{2} + 0 + 1) \cdot \frac{1}{3}} \\ &= \frac{1/2}{3/2} = \frac{1}{2} \cdot \frac{2}{3} = \frac{1}{3} ; \\ p(H_C|O_B) &= \frac{p(O_B|H_C) \cdot p(H_C)}{\sum_{X \in T} (p(O_B|H_X) \cdot p(H_X))} = \frac{\frac{1}{2} \cdot \frac{1}{3}}{\frac{3}{2} \cdot \frac{1}{3}} = \frac{2}{3} \\ &= 2 \cdot p(H_A|O_B) . \end{aligned}$$

- Die Lady ist begeistert und geht „all in“; sie lässt sich hinreißen — zum Wechsel ihrer Position<sup>10</sup>. Es kommt zum Showdown; der Moderator öffnet, wie gewünscht,  $C$  — der Preis ist jedoch nicht dahinter ( $H_A; \neg H_B, \neg H_C$ ) .
- Wurden alle Partitions-Fälle (nach Öffnen der Tür  $B$ ) bedacht? Voilà :

$$\begin{aligned} \sum_{X \in T} p(H_X|O_B) &= p(H_A|O_B) + p(H_B|O_B) + p(H_C|O_B) = \\ &\quad \frac{1}{3} + 0 + \frac{2}{3} = 1 . \end{aligned}$$

- Die Lady war „tough“ und hat alles gegeben, der Moderator auch; selbst *Diskrete Mathematik* — Grundlage der Informatik — lässt immer noch einen Spalt offen, für den erfrischenden Unterschied zwischen Theorie und Praxis.

---

<sup>10</sup>Die erste beizubehalten wäre hier attraktiver gewesen; siehe den durch Fußnote 7 erläuterten Text.

# A Anhang

## A.1 Übung: Grundstock

### Aufgaben

- Funktionen

1. Geben Sie bei den folgenden Zuordnungen an, ob sie überhaupt Funktionen sind — und dann ggf. ob sie sogar bijektiv, oder wenigstens injektiv oder surjektiv sind („Hauptsache objektiv“ ☺) + begründen Sie Ihre Antworten!

$$D := \{0, 1, 2\}, C := \{\alpha, \beta, \gamma, \delta\}; f_i: D \rightarrow C, 1 \leq i \leq 3.$$

(a)  $f_1(0) := \alpha, f_1(1) := \beta, f_1(2) := \alpha$

(b)  $f_2(0) := \alpha, f_2(1) := \beta, f_2(2) := \gamma$

(c)  $f_3(0) := \alpha, f_3(1) := \beta, f_3(2) := \gamma, f_3(0) := \delta$

2. Kann eine Funktion bijektiv sein im Falle  $|D| \neq |C|$  — warum (nicht ☺)?

3. Berechnen Sie nachstehende Werte:

a)  $[0/1]$

b)  $[0/1]$

c)  $[1/1]$

d)  $[1/1]$

e)  $[0/1]$

f)  $[1/1]$

g)  $[1/2]$

h)  $[1/2]$

- Relationen

1.  $X := \{0, 1, 2\}, Y := \{1, 2, 3\}$ . Berechnen Sie Folgendes (jeweils  $\subset X \times Y$ ):

a)  $<(X, Y)$

b)  $>(X, Y)$

2.  $\mathcal{B} := \{0, 1\}$ .

Welcher (Formel-)Wert ergibt sich für  $|\mathcal{B}^n|$ ?

## Lösungen

- Funktionen

1. 1 Injektion  $\hookrightarrow$ , 2 x weder Surjektion noch Bijektion; 1 x objektiv  $\hookleftarrow$  gar keine:

- (a) Die Funktion  $f_1$  ist keine spezielle im vorhin genannten Sinne:
  - i.  $f_1(0) = f_1(2) \implies \neg \text{ injektiv} \implies \neg \text{ bijektiv}$
  - ii.  $|C| > |D| \implies \neg \text{ surjektiv} \quad (\implies \neg \text{ bi...} \hookrightarrow)$
- (b)  $f_2$  ist injektiv, aber nicht surjektiv:
  - i. Alle Funktions-Werte sind verschieden  $\implies f_2$  injektiv
  - ii. s. o.  $\implies \neg \text{ bijektiv}$
- (c) Die gedachte Abbildung ist gar keine Funktion:  $\alpha =: f_3(0) := \delta$  .

2. Eine Funktion kann mit  $|D| \neq |C|$  nie bijektiv sein:

- (a) bijektiv  $\iff$  injektiv  $\wedge$  surjektiv
- (b) injektiv  $\implies |D| \leq |C|$
- (c) surjektiv  $\implies |D| \geq |C|$
- (d) bijektiv  $\implies |D| \leq |C| \leq |D| \iff |D| = |C|$
- (e) contrapositive:  $|D| \neq |C| \implies \neg \text{ bijektiv}$

3. Bei den ersten 6 Brüchen gibt's nichts zu runden, lediglich die letzten 2:

- (a) 0
- (b) 0
- (c) 1
- (d) 1
- (e) 0
- (f) 1
- (g) 1
- (h) 0

- Relationen

1. Die Relationsmengen sind echte Teilmengen des *Cartesischen Produkts* ( $CP$ ):

- (a)  $\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}$
- (b)  $\{(2, 1)\}$  mit (salopp notiert)  $|(b)| = 1 < 6 = |(a)| < |CP| = 3^2 = 9$

2.  $|\mathcal{B}^n| = |\mathcal{B}|^n = 2^n$

## A.2 Übung: Mengen-Lehre

### Aufgaben

- Begriffe / Kardinalität Endlicher Mengen
  1. Konstruieren Sie zwei endliche Mengen  $A$  und  $B$  mit mindestens einem gemeinsamen Element (also mit nicht-leerem Schnitt), s. d. gilt:  $|A| = |B| + 2$ .
    - Visualisieren Sie mit einem Schaubild die Kardinalität der Mengen-Vereinigung ( $|A \cup B| = |A| + |B| - |A \cap B|$ ). Argumentieren Sie somit, warum man die Schnitt-Elemente einmal subtrahieren muss.
    - Berechnen Sie  $|A \setminus B|$  über die entsprechende Formel ( $|A| - |A \cap B|$ ) und vergleichen Ihre Antwort mit der Herangehensweise, zuerst die Mengen-Differenz zu bilden und nur diese (verbleibenden) Elemente zu zählen.
    - Berechnen Sie  $|A \oplus B|$  über die bekannte ( $\smile$ ) Formel und vergleichen diese Antwort mit dem Vorgehen, zuerst die Symmetrische Differenz zu bilden und gleich nur diese Elemente zu zählen.
  2. Gegeben sei die Menge  $S := \{1, 2, 3, 4, \alpha, \beta, \gamma, \text{false}, \text{true}\}$ ; wir produzieren nun die Partition  $P := \{A_1, A_2, A_3\}$  mit  $A_1 := \{1, 2, 3, 4\}$ ,  $A_2 := \{\alpha, \beta, \gamma\}$ ,  $A_3 := \{\text{false}, \text{true}\}$ .

Bestimmen Sie:

$$\text{a)} \quad |P|$$

$$\text{b)} \quad |S|$$

- Gesetzmäßigkeiten

Sei unser kleines Universum die Welt der Dezimal-Ziffern:  $U := \{0, 1, 2, \dots, 9\}$ .

1.  $E := \{0, 2, 4, 6, 8\}$ . Bilden Sie: a)  $E^c$  b)  $(E^c)^c$ .
2. Erstellen Sie im folgenden Beispiel alle Ausdrücke der beiden *De-Morgan*-Varianten und erhellen so den Zusammenhang im jeweiligen Gesetz:  $n := 3$ ;  $S_1 := \{1, 2, 3, 4, 5\}$ ,  $S_2 := \{2, 4, 6, 8\}$ ,  $S_3 := \{3, 6, 9\}$ .

- Über-/Abzählbarkeit Unendlicher Mengen

Wie schafft man es eine Menge zu konstruieren, welche eine höhere Kardinalität hat als eine beliebige gegebene Menge  $S$ , selbst wenn  $S$  bereits unendlich groß ist? (Dies würde bedeuten, dass es unendlich viele Unendlichkeits-Stufen gibt.)

## Lösungen

- Begriffe / Kardinalität Endlicher Mengen

1. Interessant ist's für 2 Mengen, welche weder Teil- noch Ober-Mengen sind.  
Nehmen könnten Sie die eben definierte Menge  $E =: A$  und  $B := \{1, 6, 9\}$ .

- (a) Sie visualisieren natürlich Ihr eigenes Beispiel personalisiert. ↗  
Sei der Bequemlichkeit halber  $A \cap B =: T$ . Nun sehen Sie Folgendes:

$$\begin{aligned} |A \cup B| &= |A \cup (B \setminus (A \cap B))| =_{\text{Partition}} |A| + (|B \setminus (A \cap B)|) =_{B \supset T} \\ |A| + (|B| - |A \cap B|) &=_{\text{Assoziativ-Gesetz}} |A \cup B| \quad [=_{\text{o.g. Beispiel 7}}]. \end{aligned}$$

Bei der Berechnung der  $|\cup|$  ist der Schnitt (wegen Teilmenge zu jeder der beiden vorliegenden Mengen) 2-fach enthalten — weshalb  $|\cap|$  1-mal subtrahiert werden muss.

- (b) Hier ist gemeint, dass Sie zunächst die Formel konkret auswerten und dann das Ergebnis vergleichen mit dem direkten Zählen der Elemente ausschließlich in der Differenz-Menge — was das Gleiche bringen müsste. [Im o. g. Beispiel sollten Sie auf 4 kommen.]
- (c) s. o. via „(b)“, bezogen halt auf die Symmetrische Differenz [=o.g. Bsp. 6].
2. Die Grund-Menge  $S$  wird in drei Teile partitioniert, woraus sich die 3-gliedrige Partition  $P$  ergibt;  $S$  (mit ihren 9 Elementen) behält ihre Grund-Kardinalität.
- (a)  $|P| = 3$
- (b)  $|S| = \sum_{i=1}^{|P|} |A_i| = 4 + 3 + 2 = 9$

- Gesetzmäßigkeiten

Hier geht's um das was einer Menge im Vergleich zum Universum noch fehlt.

1. Gegeben  $E :=$  Menge der **geraden**<sup>1</sup> 10er-Ziffern.

- Demnach fehlen zu  $U$  die **ungeraden** Dezimal-Ziffern.
- Komplementiert man erneut („zurück“), so landet man wieder bei der gegebenen Menge ( $E$ ); dabei führt man diese doppelte Komplement-Bildung erst gar nicht konkret durch — was hier der Clou sein soll ☺.

2. Einmal zeigen wir's für's Komplement<sup>2</sup> der  $\cap$ - und ebenso der  $\cup$ -Menge:

– Komplement des Gesamt-Schnitts = Vereinigung aller Einzel-Komplemente:

$$\text{i. } \left( \bigcap_{i=1}^3 S_i \right)^c = \{ \ }^c = U$$

$$\text{ii. } \bigcup_{i=1}^3 S_i^c = \{0, 6, 7, 8, 9\} \cup \{0, 1, 3, 5, 7, 9\} \cup \{0, 1, 2, 4, 5, 7, 8\} = U$$

– Komplement der Gesamt-Vereinigung = Schnitt aller Einzel-Komplemente:

$$\text{i. } \left( \bigcup_{i=1}^3 S_i \right)^c = \{1, 2, 3, 4, 5, 6, 8, 9\}^c = \{0, 7\}$$

$$\text{ii. } \bigcap_{i=1}^3 S_i^c = \{0, 6, 7, 8, 9\} \cap \{0, 1, 3, 5, 7, 9\} \cap \{0, 1, 2, 4, 5, 7, 8\} = \{0, 7\}$$

- Über-/Abzählbarkeit Unendlicher Mengen

$$|\mathcal{P}(\omega_i)| >_{[(\text{verallgemeinerte}) \text{ Kontinuums-Hypothese}]} \omega_i$$

---

<sup>1</sup>englisch „even“ (deutsch ginge auch, da ich kein Kürzel für **ungerade** bräuchte [ $U :=$  Universum])

<sup>2</sup>ohne „i“ (in der Mitte) ☺

## A.3 Übung: Boolesche Algebra

### Aufgaben

- Werte-Tafeln sowie logische Kombinatorik

1. Zeigen Sie die folgenden Äquivalenzen:

- $p \oplus q \iff (p \vee q) \wedge (p \mid q)$
- $\text{Implication} \iff \neg p \vee q \iff \text{Contrapositive}$
- $\text{Converse} \iff \text{Inverse}$
- $\text{Equivalence} \iff \text{Implication AND Converse}$

2. Gegeben  $n$  boolesche Variablen; begründen Sie die jeweilige Standard-Formel:

- # verschiedener Codierungen
- # verschiedener Funktionen

- Gesetzmäßigkeiten

Beweisen Sie, ggf. in beiden Varianten:

1. Absorption
2. De Morgan
3. Exportation

**Lösungen**

- Werte-Tafeln sowie logische Kombinatorik

1. Äquivalenzen via jeweiliger Logik-Tabelle:

$$(a) \ p \oplus q \iff (p \vee q) \wedge (p \mid q)$$

$p$	$q$	$p \oplus q$	$p \vee q$	$p \mid q$	$(p \vee q) \wedge (p \mid q)$
0	0	<b>0</b>	0	1	<b>0</b>
0	1	<b>1</b>	1	1	<b>1</b>
1	0	<b>1</b>	1	1	<b>1</b>
1	1	<b>0</b>	1	0	<b>0</b>

$$(b) \text{ Implication} \iff \neg p \vee q \iff \text{Contrapositive}$$

$p$	$q$	$p \rightarrow q$	$\neg p$	$\neg p \vee q$	$\neg q$	$\neg q \rightarrow \neg p$
0	0	<b>1</b>	1	<b>1</b>	1	<b>1</b>
0	1	<b>1</b>	1	<b>1</b>	0	<b>1</b>
1	0	<b>0</b>	0	<b>0</b>	1	<b>0</b>
1	1	<b>1</b>	0	<b>1</b>	0	<b>1</b>

$$(c) \text{ Converse} \iff \text{Inverse}$$

Wie eben bei *Implication*  $\iff$  *Contrapositive*, nur  $p$  mit  $q$  vertauscht.

$$(d) \text{ Equivalence} \iff \text{Implication AND Converse}$$

$p$	$q$	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
0	0	<b>1</b>	1	1	<b>1</b>
0	1	<b>0</b>	1	0	<b>0</b>
1	0	<b>0</b>	0	1	<b>0</b>
1	1	<b>1</b>	1	1	<b>1</b>

2. Hier die Herleitungen für die Aufgaben-Formeln bei  $n$  booleschen Variablen:

- (a) # verschiedener Codierungen

Die Kardinalität dieses speziellen Cartesischen Produkts auf der gemeinsamen Basis-Menge  $\mathcal{B}$  beläuft sich auf  $2^n$ ; Ausführlicheres siehe Seite 9.

- (b) # verschiedener Funktionen

Jede der  $2^n$  Belegungen aus „(a)“ stellt eine konkrete Ausprägung dar, welche in einer vorliegenden Formel<sup>3</sup> zu **true** oder **false** evaluiert — was zu  $2^{(2^n)}$  verschiedenen ( $\mathcal{B}$ -)Funktionen führt; den Beweis können Sie sich gern auf Seite 43 reinziehen — ist 'ne herrliche Induktions-Übung.

- Gesetzmäßigkeiten

1. Absorption

$p$	$q$	$p \vee q$	$p \wedge (p \vee q)$	$p \wedge q$	$p \vee (p \wedge q)$
<b>0</b>	0	0	<b>0</b>	0	<b>0</b>
<b>0</b>	1	1	<b>0</b>	0	<b>0</b>
<b>1</b>	0	1	<b>1</b>	0	<b>1</b>
<b>1</b>	1	1	<b>1</b>	1	<b>1</b>

2. De Morgan

$p$	$q$	$p \wedge q$	$\neg(p \wedge q)$	$\neg p$	$\neg q$	$\neg p \vee \neg q$
0	0	0	<b>1</b>	1	1	<b>1</b>
0	1	0	<b>1</b>	1	0	<b>1</b>
1	0	0	<b>1</b>	0	1	<b>1</b>
1	1	1	<b>0</b>	0	0	<b>0</b>

$p$	$q$	$p \vee q$	$\neg(p \vee q)$	$\neg p$	$\neg q$	$\neg p \wedge \neg q$
0	0	0	<b>1</b>	1	1	<b>1</b>
0	1	1	<b>0</b>	1	0	<b>0</b>
1	0	1	<b>0</b>	0	1	<b>0</b>
1	1	1	<b>0</b>	0	0	<b>0</b>

---

<sup>3</sup> bspw. KNF, welche ja entweder „erfüllt“ oder eben „nicht erfüllt“ ist (die Basis für die SAT-Theorie)

## 3. Exportation

$p$	$q$	$r$	$q \rightarrow r$	$p \rightarrow (q \rightarrow r)$	$p \wedge q$	$(p \wedge q) \rightarrow r$
0	0	0	1	<b>1</b>	0	<b>1</b>
0	0	1	1	<b>1</b>	0	<b>1</b>
0	1	0	0	<b>1</b>	0	<b>1</b>
0	1	1	1	<b>1</b>	0	<b>1</b>
1	0	0	1	<b>1</b>	0	<b>1</b>
1	0	1	1	<b>1</b>	0	<b>1</b>
1	1	0	0	<b>0</b>	1	<b>0</b>
1	1	1	1	<b>1</b>	1	<b>1</b>

## A.4 Übung: Beweis-Prinzipien

### Aufgaben

- Induktion

1. Beweisen Sie:  $n! > 2^n$ ,  $\forall n \geq n_0$ .

2. Laurence E. Sigler, Fibonacci's Liber Abaci — A Translation into Modern English of Leonardo Pisano's Book of Calculation, Seite 397, Springer, 2003, 978-0-387-40737-1 (Original vermutlich aus 1202):

*„On Him Who Went into the Pleasure Garden to Collect Apples.*

A certain man entered a certain pleasure garden through 7 doors, and he took from there a number of apples; when he wished to leave he had to give the first doorkeeper half of all the apples and one more; to the second doorkeeper he gave half of the remaining apples and one more. He gave to the other 5 doorkeepers similarly, and there was one apple left for him.“

$a_t := \#$  Äpfel zum Passieren von  $t$  Türwächtern (s. d. 1 Apfel übrig bleibt).

Finden Sie die Formel für den allgemeinen Fall  $a_n$  und beweisen Ihre Aussage!

- Direkter Beweis

Leiten Sie die Gauß-Formel, die Summe der ersten  $n$  natürlichen Zahlen, her.

- Indirekter Beweis

Zeigen Sie, dass für zwei natürliche Zahlen gilt:  $a < b \iff a^2 < b^2$ .

## Lösungen

- Induktion

1. Behauptung:  $n! > 2^n$ ,  $\forall n \geq n_0 := 4$ .

Basis:

$$n_0 := 4 ; \quad 4! = 24 > 16 = 2^4$$

Hypothese [=: H.]:

$$(n-1)! > 2^{(n-1)}, \quad n-1 \geq 4$$

Schritt:

$$[4 \leq] n-1 \rightarrow n [> 4]$$

$$n! = (n-1)! \cdot n >_{[\text{H.}]} ^! 2^{(n-1)} \cdot n >_{[n > n_0 > 2]} 2^{(n-1)} \cdot 2^1 = 2^{[(n-1)+1]} = 2^n .$$

2. <https://educ.ethz.ch/unterrichtsmaterialien/informatik/recurrence-relations.html>  
 $\rightarrow$  Recurrence Relations and Induction Proofs  $\rightarrow$  Download  
oder via hinten zitiertem deutschen Werk (S. 25/26)  $\circlearrowleft$ .

- Direkter Beweis

Ersetzen Sie zum Erhalt der Gauß-Formel auf Seite 46 einfach  $n-1$  durch  $n$ , oder eleganter — und höchstwahrscheinlich historischer — wie folgt :

$$\begin{aligned} \sum_{i=1}^n i &= \left[ \sum_{i=1}^n i + \sum_{i=0}^{n-1} (n-i) \right] / 2 = \left[ \sum_{i=1}^n (i + [n - (i-1)]) \right] / 2 \\ &= \left[ \sum_{i=1}^n (i + n - i + 1) \right] / 2 = \left[ \sum_{i=1}^n (n+1) \right] / 2 = \frac{n \cdot (n+1)}{2} \end{aligned}$$

- Indirekter Beweis

Eine  $\leftrightarrow$ -Behauptung sieht bekanntermaßen  $\circlearrowleft$  so aus:  $l \rightarrow r \wedge r \rightarrow l$ .

Aus Rücksicht auf die Erst-Semestler/innen zeigen wir hier keine berüchtigte „Hin-Richtung“<sup>4</sup>  $\circlearrowleft$ , sondern lediglich die „Rück-Richtung“ (das letzte UND-Kettenglied), die aufgrund des *Contrapositive* einfach wie folgt indirekt bewiesen werden kann:

$$\begin{aligned} \neg(a < b) &\iff a \geq b \implies a =_{[\beta \geq 1]} \beta \cdot b \implies a^2 = \beta^2 \cdot b^2 \\ &\implies_{[\beta^2 \geq 1]} a^2 \geq b^2 \iff \neg(a^2 < b^2) \hat{=} \neg l \rightarrow \neg r . \end{aligned}$$

---

<sup>4</sup>  $l \rightarrow r \iff_{\text{Contrapositive}} \neg r \rightarrow \neg l$ , was sich ähnlich wie oben leicht bewerkstelligen lässt)

## A.5 Übung: Zähl-Techniken

### Aufgaben

- Schubfach-Prinzip (*pigeonhole principle* [=: PP])

$$s := \# \text{ Studierende} := 60, \quad v := \# \text{ Vorlesungen}.$$

Das PP würde uns sagen: es gibt eine Vorlesung mit mindestens 9 Studierenden.

(Diese Zähl-Technik wird hier nicht in der üblichen Art und Weise angewendet.)

Wie viele Vorlesungen werden angeboten?

- Ein-/Ausschluss

$$A \cap B \cap C =: D.$$

Beantworten Sie in diesen beiden Teil-Aufgaben jeweils folgende Frage:

Gibt es ein Element ( $\in D$ ), welches zu jeder Menge gehört; ist also  $|D| > 0$  ?

1.  $|A| := 1, |B| := 2, |C| := 3,$   
 $|A \cap B| := |B \cap C| := 1, |A \cap C| := 0,$   
 $|A \cup B \cup C| := 4$
2.  $|A| := 2, |B| := 3, |C| := 4,$   
 $|A \cap B| := |B \cap C| := 2, |A \cap C| := 1,$   
 $|A \cup B \cup C| := 5$

- Permutationen

Uns stehen die folgenden Buchstaben zur Verfügung:  $A, B, C, D, E, F, I$ ; sowohl das „E“ als auch das „I“ sind doppelt vorhanden. Wir haben demnach die Vokale (=:  $V$ )  $A, E, E, I, I$  und die Konsonanten (=:  $K$ )  $B, C, D, F$ .

Wie viele sichtbar verschiedene Arrangements bei der Bildung eines Wortes aus diesen 9 Buchstaben sind möglich, wenn die Zeichenkette wie folgt aussehen soll:

$$V | K | V | K | V | K | V | K | V \quad ?$$

## Lösungen

- Schubfach-Prinzip (PP):

$$p := \text{PP-#} := \left\lceil \frac{s}{v} \right\rceil$$

$$v = \left\lceil \frac{s}{p} \right\rceil =_{\text{hier}} \left\lceil \frac{60}{9} \right\rceil = \left\lceil \frac{9 \cdot 6 + 6}{9} \right\rceil = \left\lceil 6 \frac{2}{3} \right\rceil = 7$$

Test:

$$\left\lceil \frac{60}{8} \right\rceil = 8 < p = \left\lceil \frac{60}{7} \right\rceil = \left\lceil \frac{7 \cdot 8 + 4}{7} \right\rceil = \left\lceil 8 \frac{4}{7} \right\rceil = 9 < 10 = \left\lceil \frac{60}{6} \right\rceil$$

- Ein-/Ausschluss

$$1. |A \cap C| := 0 \implies |D| = 0 \neq 0 \implies$$

Nein, es gibt kein solches Element in der globalen Schnitt-Menge!

$$2. |A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$$

$$\iff |D| = 5 - (2 + 3 + 4) + (2 + 1 + 2) = 5 - 9 + 5 = 1 > 0 \implies$$

Ja, diesmal gibt es 1 solches Element!

- Permutationen

$$a = \frac{\frac{9!}{1! \cdot 1! \cdot 1! \cdot 1! \cdot 1! \cdot 2! \cdot 2!}}{9!} = \frac{5! \cdot 4!}{2! \cdot 2!} = \frac{(2! \cdot 3 \cdot 4 \cdot 5) \cdot (2! \cdot 3 \cdot 4)}{2! \cdot 2!} = \frac{5! \cdot 4!}{5! \cdot 4!}$$

$$(3 \cdot 4)^2 \cdot 5 = \frac{1440}{2} = 720$$

oder (kompakter):

$$\frac{5!}{1! \cdot 2! \cdot 2!} \cdot 4! = \frac{2! \cdot 3 \cdot 4 \cdot 5}{2! \cdot 2!} \cdot 2! \cdot 3 \cdot 4 = 12^2 \cdot 5 = \frac{1440}{2} = 720 .$$

## A.6 Übung: Wahrscheinlichkeits-Theorie

### Aufgaben

- Allgemeine Wahrscheinlichkeit

Bestimmen Sie die Wahrscheinlichkeit  $p_n$ , dass in einem  $n$ -steligen Bit-Vektor an genau zwei Positionen *false* auftritt. Berechnen Sie noch  $p_i$  für die sechs Fälle  $i \in \{0, 1, 2, 3, 4, 5\}$  und beweisen abschließend die allgemeine Formel.

- Bedingte Wahrscheinlichkeit

Bestimmen Sie die Wahrscheinlichkeit (jetzt in %), dass bei einem fairen Münzwurf nach vorherigem Erscheinen von *Kopf* ( $=: H$ ) nun *Zahl* ( $=: T$ ) auftritt.<sup>5</sup> Bewerten Sie's kurz zum Abschluss!

---

<sup>5</sup>Die deutschen Anfangs-Buchstaben lassen sich in der Lösung zu krass — daher englisch abgekürzt.

## Lösungen

- Allgemeine Wahrscheinlichkeit

$$1. \ p(E) := |E|/|\Omega| = \frac{\frac{n \cdot (n-1)}{2^n}}{2^n} = n \cdot (n-1) \cdot 2^{(-1)} \cdot 2^{(-n)} = (n-1) \cdot n \cdot 2^{[-(n+1)]}.$$

Illustration: Rekurrenz-Relation für  $|E| =: e$

$$e_{\text{Prinzip}}(0) = 0$$

$$e_{\text{P}}(n_{[>0]}) := e_{\text{P}}(n-1) + \binom{n-1}{1} = e_{\text{P}}(n-1) + (n-1)$$

$\uparrow$                      $\uparrow$   
neues **true** vorne    **false** vorne neu

Rückwärts-Ersetzung:

$$\begin{aligned} e_{\text{P}}(n) &:= [e_{\text{P}}(n-2) + (n-2)] + (n-1) \\ &:= [e_{\text{P}}(n-3) + (n-3)] + [(n-2) + (n-1)] \\ &\quad \vdots \\ &:= [e_{\text{P}}(n-n) + (n-n)] + [\cdots + (n-3) + (n-2) + (n-1)] \\ &:= e_{\text{P}}(0) + \sum_{i=0}^{n-1} i = 0 + (n-1) \cdot [(n-1)+1]/2 = n \cdot (n-1)/2 \\ &=: e_{\text{Formel}}(n) \end{aligned}$$

Beweis: Induktion über  $n$ :

$$e_{\text{Prinzip}}(0) = 0 = e_{\text{Formel}}(0)$$

$$\begin{aligned} e_{\text{P}}(n) &= e_{\text{P}}(n-1) + (n-1) = (n-1) \cdot [(n-1)-1]/2 + (n-1) \\ &= (n-1) \cdot [(n-2)+2]/2 = n \cdot (n-1)/2 = e_{\text{F}}(n). \end{aligned}$$

2.  $n = 0 : p(E) = 0$ , ebenso für  $n = 1$

$$n = 2 : p(E) = 2/8 = 1/4$$

$$n = 3 : p(E) = 6/16 = 3/8 = 12/32, \text{ also ebenso für } n = 4$$

$$n = 5 : p(E) = 20/64 = 5/16$$

3. Induktion über  $n$ :

Basis:

$$n := 0 : p_{\text{Prinzip}}(E_0) = 0 = p_{\text{Formel}}(0)$$

Ind.-Hyp.:

$$p_F(E_{n-1}) = (n-2) \cdot (n-1) \cdot 2^{(-n)}$$

Ind.-Schritt:

$$n - 1 \rightarrow n$$

$$p_P(E_n) := |E_n| / |\Omega_n| = \frac{e_n}{2^n} = \frac{e_{(n-1)} + (n-1)}{2^{(n-1)} \cdot 2} = p_P(n-1) \cdot 2^{(-1)} + \frac{n-1}{2^n}$$

=!

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

$$(n-1) \cdot 2^{[-(n+1)]} \cdot [(n-2) + 2] =$$

$$(n-1) \cdot n \cdot 2^{[-(n+1)]} =$$

$$p_F(n)$$

.

- Bedingte Wahrscheinlichkeit

$$A := \{(\underline{H}, T)\}, \quad B := \{(\underline{H}, H), (\underline{H}, T)\};$$

$$P(A|B) =_{[B \supseteq A]} P(A)/P(B)_{[>0]} =_{\text{hier}} P(A)/P(\Omega) = \frac{1}{2}/1 = 50\%.$$

Der *Zahl*-Würfel hat keine Ahnung was vorher (bspw.  $H$ ) gelaufen ist (wie die Roulette-Kugel); ihn als *kopflos* zu bezeichnen würde ihn die Fairness kosten. ☺

# B      Bonus-Track      ☺

## B.1      Übung: Grundstock

### **Neue Aufgabe**

Gegeben die Bijektionen  $f: A \rightarrow B$ ,  $g: B \rightarrow C$ ,  $h := g \circ f$ ;  $|A| =: a$ ,  $|B| =: b$ ,  $|C| =: c_{[>0]}$

Wie viele bijektive Kompositionen sind möglich für  $h$ ?

Welche gängigen Fehler lauern — und warum ist's einfach, doch nicht zu grätschen? ☺

## Neue Lösung

$a! (= b! [= c!])$ , Beweis: ab Seite 71.

Illustration:  $a := 3 (= c)$ ;  $A := \{\alpha, \beta, \gamma\}$ ,  $C := \{x, y, z\}$ . # Bijektionen =  $3! = 6$ :

$$\begin{aligned} h_1 : \quad & h_1(\alpha) := x, h_1(\beta) := y, h_1(\gamma) := z; \\ h_2 : \quad & h_2(\alpha) := x, h_2(\beta) := z, h_2(\gamma) := y; \\ h_3 : \quad & h_3(\alpha) := y, h_3(\beta) := x, h_3(\gamma) := z; \\ h_4 : \quad & h_4(\alpha) := y, h_4(\beta) := z, h_4(\gamma) := x; \\ h_5 : \quad & h_5(\alpha) := z, h_5(\beta) := x, h_5(\gamma) := y; \\ h_6 : \quad & h_6(\alpha) := z, h_6(\beta) := y, h_6(\gamma) := x. \end{aligned}$$

Folgende Grätschen ☺ sind berüchtigte „Soll-Bruchstellen“:

- Eine Bijektion an sich:

$$\neq |C|^2 \quad (\text{im Fall } c \neq 1 \text{ natürlich})$$

Für  $2 \leq c \leq 3$  ist die korrekte Lösung gar kleiner als die hier genannte falsche, weil bei der Quadrat-Idee ja alle Elemente noch als greifbar angenommen werden; sie ist ab  $c \geq 4$  größer, da nun die volle Permutations-Explosion zuschlägt (welche eine exponentiell große Zahl erzeugt [wobei besagte 4 bei einem Induktions-Beweis das  $n_0 (=: c_0)$  darstellen würde]).

- Die Komposition kompliziert zu sehen:

Man könnte dem Gedanken verfallen, erst die Kombinatorik der # f-Bijektionen ( $=: k$ ) zu bestimmen und dann darauf aufbauend die # g-Bijektionen ( $=: l$ ), um die „Gesamt“-# der h-Bijektionen ( $=: m$ ) zu erhalten, bspw. wie folgt:

$$m := l := k! := c!! \neq_{[c > 2]} c! \quad —$$

vielleicht verführerisch, aber zugleich gruselig.

Am einfachsten blickt man's, wenn man — wie hier gleich durchgezogen — die Wirkung einer Komposition direkt mit Original-Eingabe der Funktion  $f$  (und noch anschließender Zwischen-Funktion  $[g]$ ) die # Ausgabe-Möglichkeiten der Funktion  $h$  bedenkt; dabei kann sich dann die Permutations-Dramatik nicht noch weiter dramatisieren. ☺

## B.2 Übung: Mengen-Lehre

### **Neue Aufgabe**

Welche Bedingung muss für folgende Aussage gelten:  $|\bigcup_{i=1}^n S_i| = \sum_{i=1}^n |S_i|$  ?

**Neue Lösung**

Alle  $S_i$ -Paare sind untereinander disjunkt.

## B.3 Übung: Boolesche Algebra

### **Neue Aufgabe**

Zeigen Sie ohne Werte-Tafel mit logischen Schritten die Basis für den indirekten Beweis:

$$p \rightarrow q \iff \neg q \rightarrow \neg p.$$

**Neue Lösung**

$$p \longrightarrow q$$

 $\iff$ 

$$\neg p \vee q$$

 $\iff$ 

$$q \vee \neg p$$

 $\iff$ 

$$\neg\neg q \vee \neg\neg(\neg p)$$

 $\iff$ 

$$\neg(\neg q) \vee \neg(\neg\neg p)$$

 $\iff$ 

$$\neg(\neg q) \vee \neg p$$

 $\iff$ 

$$\neg q \longrightarrow \neg p$$

## B.4 Übung: Beweis-Prinzipien

### Neue Aufgabe

Sie können nun entweder die folgende Betrags-Variante<sup>1</sup> oder die gleichwertige Notation der [Stirling-]Zyklus-Zahl<sup>2</sup> nehmen.

Beweisen Sie durch Induktion über  $n[> 0]$ :  $z_n := |s_1(n, 1)| = (n - 1)!$ .

---

<sup>1</sup>aufwändig :-)

<sup>2</sup>bequem (empfehlenswert) ☺

**Neue Lösung**

Betrag-Variante:  $z_n := |s_1(n, 1)|$

i) Basis:  $n_0 := 1$

$$\begin{aligned} z_{1_{\text{Prinzip}}} &:= |s_1(1, 1)| = |1| = 1 \\ z_{1_{\text{Formel}}} &:= (1 - 1)! = 0! = 1 = z_{1_p} . \end{aligned}$$

ii) Hypothese:  $z_{n-1} := |s_1(n-1, 1)| = ((n-1)-1)!$

iii) Schritt:  $n - 1_{[\geq n_0]} \rightarrow n_{[> n_0]} ; z_{n_p} := |s_1(n, 1)|$

$$= \begin{cases} +s_1(n, 1) ; \text{ gerade}(n-1) \\ -s_1(n, 1) ; \text{ ungerade}(n-1) \end{cases}$$

$$= \begin{cases} +(s_1(n-1, 0) - (n-1) \cdot s_1(n-1, 1)) ; \text{ gerade}(n-1) \\ -(s_1(n-1, 0) - (n-1) \cdot s_1(n-1, 1)) ; \text{ ungerade}(n-1) \end{cases}$$

$$= \begin{cases} +(0 - (n-1) \cdot s_1(n-1, 1)) ; \text{ gerade}(n-1) \\ -(0 - (n-1) \cdot s_1(n-1, 1)) ; \text{ ungerade}(n-1) \end{cases}$$

$$= (n-1) \cdot \begin{cases} (-s_1(n-1, 1)) ; \text{ ungerade}((n-1)-1) \\ (+s_1(n-1, 1)) ; \text{ gerade}((n-1)-1) \end{cases}$$

$$= (n-1) \cdot |s_1(n-1, 1)| = (n-1) \cdot z_{n-1} \stackrel{!}{=} (n-1) \cdot ((n-1)-1)!$$

$$= (n-1)! = z_{n_F}$$

Zyklus-Notation:  $z_n := \left[ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right]$

i) Basis:  $n_0 := 1$

$$\begin{aligned} z_{1_{\text{Prinzip}}} &:= \left[ \begin{smallmatrix} 1 \\ 1 \end{smallmatrix} \right] = 1 \\ z_{1_{\text{Formel}}} &:= (1-1)! = 0! = 1 = z_{1_p} . \end{aligned}$$

ii) Hypothese:  $z_{n-1} := \left[ \begin{smallmatrix} n-1 \\ 1 \end{smallmatrix} \right] = ((n-1)-1)!$

iii) Schritt:  $n - 1_{[\geq n_0]} \rightarrow n_{[> n_0]}$

$$z_{n_p} := \left[ \begin{smallmatrix} n \\ 1 \end{smallmatrix} \right] = \left[ \begin{smallmatrix} n-1 \\ 0 \end{smallmatrix} \right] + (n-1) \cdot \left[ \begin{smallmatrix} n-1 \\ 1 \end{smallmatrix} \right] = 0 + (n-1) \cdot z_{n-1}$$

$$\stackrel{!}{=} (n-1) \cdot ((n-1)-1)! = (n-1)! = z_{n_F}$$

## B.5 Übung: Zähl-Techniken

### Neue Aufgabe

Beim Fußball-Training haben wir  $p_{[>1]}$  Spieler und würden gern 2 Teams mit in etwa gleich vielen Kickern auf jeder Seite formieren.

Die Frage in den folgenden 3 Fällen<sup>3</sup> [a), b), c)] ist jeweils:

Wie viele verschiedene *Formationen* [=:  $f(p) = \dots$ ] sind möglich?

a)  $p := 5$

b)  $p := 6$

c)  $p := n$  (der allgemeine Fall mit einer beliebigen Spieler-Anzahl) [ohne Beweis]

---

<sup>3</sup>Die 2 o. g. kleinen  $p$ -Zahlen tauchten bei unserem Hochschul-Hallensport damals wirklich mal auf.

**Neue Lösung** (siehe auch S. 11/12 in meinem hinten zitierten Informatik-Buch)

a)

$$f(5) = C(5, \lfloor 5/2 \rfloor) = C(5, 3) = C(5, 2) = 5 \cdot 4 / 2 = 10 ; \quad \text{die Spieler heißen } A, \dots, E :$$

$$AB|CDE, AC|BDE, AD|BCE, AE|BCD, BC|ADE, BD|ACE, BE|ACD, CD|ABE, CE|ABD, DE|ABC .$$

Es ist nicht egal, ob man in einem 2er- oder 3er-Team spielt; daher kommt bei einer ungeraden  $\#$  Spieler der volle Binomial-Koeffizient zum Tragen.

b)

$$f(6) = C(6, 3) / 2 = 6! / (3! \cdot (6-3)!) / 2 = (3! \cdot 4 \cdot 5 \cdot 6) / (3! \cdot 3!) / 2 = (2 \cdot 2 \cdot 5) / 2 = 10 \stackrel{\circ}{=}$$

$$f(6-1) = f(5) ; \quad \text{die Spieler heißen } A, \dots, F :$$

$$ABC|DEF, ABD|CEF, ABE|CDF, ABF|CDE, ACD|BEF, ACE|BDF, ACF|BDE, ADE|BCF, ADF|BCE, AEF|BCD .$$

Bei gerader  $\#$  Teilnehmer/innen kommt es für einen Spieler auf die  $\#$  Möglichkeiten der verschiedenen Team-Formierungen mit  $n/2 - 1$  Mitspielerinnen an, allgemein also

$$\binom{n-1}{\frac{n}{2}-1} =: x =_{[\text{Bin.-Sym.}]} y := \binom{n-1}{n/2} .$$

c)

$$f(n) = C(n, \lfloor n/2 \rfloor) / \begin{cases} 1 & \text{ungerade}(n) \\ 2 & \text{gerade}(n) \end{cases}$$

oder: if `gerade(n)` then  $p := n - 1$ ;  $f(n) := C(p, \lfloor n/2 \rfloor)$  — hierzu folgender

$$\begin{aligned} \text{Hintergrund: } f(n) &=_{[\text{gerade}(n)]} \frac{C(n, n/2)}{2} =_{[\text{PASCALSches Dreieck}]} \frac{C(n-1, n/2-1) + C(n-1, n/2)}{2} \\ &=_{[\text{Bin.-Sym.}]} \frac{2 \cdot C(n-1, n/2)}{2} = C(n-1, n/2) =_{[\text{ungerade}(p)]}^{[n-1 =: p < n]} C(p, n/2). \end{aligned}$$

Die im Fall „b“ eingeführten Binomial-Größen  $x$  und  $y$  helfen, das Ganze hier weiter zu illustrieren: Da  $x + y =_{[\text{gerade}(n)]} z =_{[\text{PASCALSches Dreieck}]} C(n, n/2)$ , gilt:  $x = y = z/2$ .

In einer solchen Situation mit einer geraden  $\#$  Spieler/innen zeigt der uninteressante Fall  $n := 2$  sehr schön, dass es egal ist auf welcher Seite man kickt [ $f(2) = C(2, 1)/2 = 1$ ].

## B.6 Übung: Wahrscheinlichkeits-Theorie

### **Neue Aufgabe**

Gesucht ist die Wahrscheinlichkeit  $p_n$  (in %), dass in einem  $n_{[>0]}$ -stelligen Bit-Vektor die Werte-Belegung für das erste und das letzte ⋮ Bit gleich ist.

**Neue Lösung**

$$p_n = \frac{|E|}{|\Omega|}$$

$$= \begin{cases} \frac{2}{2} & ; \quad n = 1 \quad (\text{erstes Bit } \stackrel{\smile}{=} \text{ letztes Bit}) \\ \frac{2}{4} & ; \quad n = 2 \quad (\text{es existieren nur die 2 Bits}) \\ \frac{2 \cdot 2^{(n-2)}}{2^n} & ; \quad n > 2 \quad (\text{gefragtes Paar, Rest-Bits beliebig}) \end{cases}$$

$$= \begin{cases} 1 & ; \quad n = 1 \\ \frac{1}{2} & ; \quad n = 2 \\ 2^{[1+(n-2)-n]} & ; \quad n > 2 \end{cases}$$

$$= \begin{cases} 1 & ; \quad n = 1 \\ 2^{(-1)} & ; \quad n \geq 2 \end{cases}$$

$$= \begin{cases} 100\% & ; \quad n = 1 \\ 50\% & ; \quad n > 1 \end{cases}$$

# Literaturverzeichnis

Arnold, André / Guessarian, Irène: *Mathématiques pour l'informatique*, 4<sup>e</sup> édition, Dunod, 2005.

Beeler, Robert A.: *How to Count: An Introduction to Combinatorics and Its Applications — A problem-based approach to learning Combinatorics*, Springer International Publishing, 2015.

Biggs, Norman L.: *Discrete Mathematics*, 2<sup>nd</sup> edition, reprinted with corrections, Oxford University Press, 2005.

Ferland, Kevin: *Discrete Mathematics and Applications*, 2<sup>nd</sup> edition, Routledge / CRC / Chapman and Hall / Taylor & Francis, 2017.

Graham, Ronald L. / Knuth, Donald E. / Patashnik, Oren: *Concrete Mathematics — A Foundation for Computer Science*, 2<sup>nd</sup> edit., 20<sup>th</sup> pr., Pearson, Addison-Wesley, 2006.

Hower, Walter: *Informatik-Bausteine — Eine komprimierte Einführung*, Springer Nature Vieweg Fachmedien, Softcover 978-3-658-01279-3, eBook 978-3-658-01280-9, 2019; Rezension: <https://doi.org/10.1007/s00287-020-01237-8>, 2020.

Rosen, Kenneth H.: *Discrete Mathematics and Its Applications*, 8<sup>th</sup> edition, McGraw-Hill, 2019.

Rosen, Kenneth H. / Shier, Douglas R. / Goddard, Wayne (eds.): *Handbook of Discrete and Combinatorial Mathematics*, 2<sup>nd</sup> edition, Routledge / CRC / Chapman and Hall / Taylor & Francis, 2018.



# Register

- $\mathcal{B}$ , 9  
 $\mathcal{N}$ , 3  
GGT, 42  
 $glb$ , 11  
 $lub$ , 11  
 $\#$ , 13  
*Boole*  
    -Algebra, 29  
    -Ungleichung, 94  
*De Morgan*, 19, 34  
*NAND*, 30  
*NOR*, 31  
*NOT*, 29  
*OR*, 30  
*Pascalsches Dreieck*, 78  
*XOR*, 31  
*contradiction* (Widerspruch), 33  
*contrapositive*, 32  
*converse*, 32  
*inverse*, 32  
*symmetric difference*, 10
- Absorption, 33  
Analogie *Boole*-Algebra|Mengenlehre, 34  
Assoziativität, 33
- Bell-Zahlen, 89  
Beweis  
    direkter, 46  
    indirekter, 47  
    Induktions-, 35  
Bi-Konditional (Äquivalenz), 32  
Bijektionen-#, 71  
Binet-Formel (Fibonacci-Zahl), 40  
Binomial  
    -Symmetrie, 79  
    -Theorem  
        allgemein: Binom. Lehrsatz, 80  
        spezialisiert:  $\sum_{k=0}^n \binom{n}{k} = 2^n$ , 81
- Cartesisches Produkt (Kreuz-Prod.), 8  
Disjunktion, 30  
Distributivität, 33  
Dominanz, 33  
Dualität, 34
- Ein-/Ausschluss ( $| \cup |$ ), 52  
Entscheidungs-Grad, 36  
Ereignis, 93  
    -Mengen, 94  
    Elementar-, 93  
Exportation, 34
- Faktorielle  
    fallende, 73  
    steigende, 75  
Fakultät, 73  
Fibonacci  
    -Baum, 38  
    -Zahlen, 38  
Funktion, 4  
    bijektive, 6  
    injektive, 6  
    inverse, 6  
    partielle, 4  
    surjektive, 6  
    totale, 4
- Gitter-Netz (quadratisch), 63  
Goldener Schnitt, 41  
Graph  
    -Durchmesser, 63  
    vollständiger, 36
- hinreichend, 31  
Hyper-Würfel (beliebig dimensional), 61
- Idempotenz, 33  
Identität, 33

- Implikation (Konditional), 31
- Induktion
  - auf natürlichen Zahlen, 35
  - hinsichtlich Wort-Länge, 44
- Infix-Notation, 29
- Injektionen-#, 74
- Inklusion, 5
- Kardinalität, 13
- Kette, 11
- KNF, 32
- Kodierungs-#, 33
- Kombination (Auswahl)
  - (Binomial)-Koeffizient
    - Definition / Formel, 76
    - zentraler/maximaler, 79
    - #, 77
- Kommutativität, 33
- Komposition, 7
- Konjunktion, 29
- Kontinuums-Hypothese
  - einfache  $\cup$ , 27
  - verallgemeinerte, 27
- Literal, 32
- Menge
  - über-abzählbare, 26
  - abzählbare, 13
  - Bild-, 5
  - Definitions-, 5
  - Differenz-, 16
  - Komplement-, 16
  - Multi-, 13
  - Ober-, 15
  - Potenz-, 14
  - Schnitt-, 16
  - Standard-, 13
  - Teil-, 15
  - Vereinigungs-, 16
  - Werte-, 5
- Nachfolger ( $n + 1$  einer nat. Zahl  $n$ ), 3
- Negation
  - doppelte, 33
  - einfache, 29
- notwendig, 31
- Ordinal, 25
  - Grenz-, 25
  - Nachfolger-, 26
- Partial/Vor-Ordnung, 10
- Partition
  - $p$ -gliedrige, 17
  - #, 89
  - zyklische, 83
- Peano-Axiome, 3
- Peirce-Pfeil, 31
- Permutation (Reihenfolge)
  - Koeffizient, 73
  - #, 73
- poSet, 10
- Präfix-Notation, 30
- Produkt-Zählregel, 50
- Projektion, 5
- Quotienten-Zählregel, 51
- Reihe
  - arithmetische, 55
  - geometrische, 37
- Rekurrenz, 55
  - Rückwärts-Ersetzung, 56
  - Vorwärts-Ersetzung, 56
- Rekursion, 56
- Relation
  - Äquivalenz-, 10
  - anti-symmetrische, 10
  - asymmetrische, 10
  - Binär-, 8
  - Differenz-, 10
  - intransitive, 10
  - irreflexive, 9
  - Komplement-, 9
  - Kompositions-, 9
  - reflexive, 9
  - Schnitt-, 10
  - symmetrische, 10
  - transitive, 10
  - Vereinigungs-, 10
- SAT, 32
- Schubfach-Prinzip, 51
- Sheffer-Strich, 30

- Stirling-Zahlen
  - erster Art, 83
  - zweiter Art, 86
- Summen-Zählregel, 49
- Surjektionen-#, 87
- Symmetrische Differenz (*eXklusiv-OdeR*)
  - Menge, 17
  - Relation, 10
- Tautologie, 33
- Tupel, 9
- Unendlichkeit, 15
  - über-abzählbar, 15
  - abzählbar, 15
- Universum, 16
- unvergleichbar, 10
- Verband
  - lattice, 11
  - Teilmengen-, 11
- vergleichbar, 10
- Verzweigungs-Faktor, 36
- Wahrheits-Wert, 29
- Wahrscheinlichkeit
  - allgemeine, 93
  - bedingte, 97
  - totale, 98
- Ziegen-Problem ('Hinter der Tür'), 99

