Kapitel C

# Mathematische Logik und Beweistechniken

*Mathematics, rightly viewed, possesses not only truth,*
*but supreme beauty [...] The true spirit of delight, [...]*
*is to be found in mathematics as surely as poetry.*

Bertrand Russel (1872–1970), Nobelpreis 1950

# Inhalt dieses Kapitels C

1. Aussagenlogik
   - Aussagen und Wahrheitswerte
   - Aussagenlogische Formeln und Tautologien
   - Nützliche Rechenregeln der Aussagenlogik
   - Aussagenlogische Formeln und Junktoren
2. Schlussregeln und Beweisverfahren
   - Schnittregel, Kettenschluss, Fallunterscheidung
   - Kontraposition und Beweis durch Widerspruch
3. Prädikate und Quantoren
   - Rechenregeln für Existenz- und Allquantor
   - Existenz und Eindeutigkeit
4. Induktion: the road to infinity!
   - Das Prinzip der vollständigen Induktion
   - Starke Induktion als nützliche Variante
5. Glanzlicht: komplexe Spiele, induktive Lösungen

# Zielsetzung

In der Mathematik wollen wir **wahre Aussagen** effizient auffinden, präzise formulieren und streng beweisen. Ebenso müssen wir **falsche Aussagen** als unwahr erkennen und ebenso begründet zurückweisen. Algorithmisch führt das direkt zu einem der Millenium-Probleme C1K!

Solide und bescheiden benötigen wir mathematisches Handwerkszeug. Grundlegend und allgegenwärtig sind die Regeln der **Aussagenlogik**; sie strukturieren unser Vorgehen und vereinfachen die Kommunikation. Dazu präsentiere ich Ihnen in diesem Kapitel die nötigen Grundlagen.

Unser akribisches logisches Vorgehen hat viele gute Gründe:
(1) Sie sollen verstehen, was ich tue und auch warum ich es tue.
(2) Sie sollen selbstständig nachprüfen, dass ich es richtig mache.
(3) Sie sollen selbst wahre Aussagen finden und beweisen lernen.
(4) Sie sollen selbst nachprüfen können, dass Sie es richtig machen.
(5) Wir wollen uns darüber verständigen, was wahr und was falsch ist.
(6) Sie sollen Ihre Erkenntnisse richtig anwenden und weitergeben.

Kurzum: Die Logik benötigen und nutzen Sie überall.

# Zielsetzung

*Tradition ist nicht die Bewahrung der Asche,*
*sondern die Weitergabe des Feuers.*
nach Jean Jaurès (1859–1914)

Als Anfänger macht man zunächst viele Fehler, das ist völlig normal.
Aber dabei soll es nicht bleiben. Wachsen Sie über sich hinaus!
Sie sollen in Ihrem Studium möglichst rasch und gründlich lernen,
diese Fehler zu *erkennen* und dann auch zu *vermeiden*.

Auch ich mache gelegentlich Fehler, das ist leider unvermeidlich,
aber Sie können die Fehler *erkennen* und sollen sie *korrigieren*.
Das ist ein Grundprinzip der Mathematik: Es geht nicht um Autorität,
Überredung oder Einschüchterung, sondern um schlüssige Argumente.

Unser gemeinsames Ziel ist die nachvollziehbare Verständigung über
und die nachhaltige Erarbeitung von mathematischen Sachverhalten.
Lernen wir also die mathematische Sprache! Lernen wir Logik!

*Habe Mut, dich deines eigenen Verstandes zu bedienen!*
Immanuel Kant (1724–1804)

# Zweck und Nutzen der Logik: Korrektheit

Sie sollen mit Aussagen und ihren Wahrheitswerten sicher rechnen: **korrekt und kritisch, kreativ und effizient.** Das ist nicht leicht! Dazu gehört insbesondere auch das Beweisen: Ein Beweis ist nichts anderes als die Berechnung des Wahrheitswerts der Behauptung.

Sie sollen mathematische Beweise und Beweisversuche prüfen, und dabei gültige von ungültigen Argumenten unterscheiden lernen. Dazu müssen Sie wie oben genannt *korrekt und kritisch* arbeiten. Das ist solides Handwerk, Sie lernen es am besten durch Übung.

Auch kleine Fehler können entscheidend sein, scheinbar zwingende Schlüsse können zu absurden Ergebnissen führen! Das hat auch sportlich-spielerische Aspekte: Immer wieder wurden und werden Paradoxien formuliert und als logische Herausforderung behandelt.

*Seit man begonnen hat, die einfachsten Behauptungen zu beweisen, erwiesen sich viele von ihnen als falsch.*

Bertrand Russell (1872–1970)

# Zweck und Nutzen der Logik: Erkenntnis

Mit zunehmender Übung und mathematischer Erfahrung sollen Sie auch selbst Beweise finden, erarbeiten und ausformulieren lernen.
Dazu müssen Sie wie oben genannt *kreativ und effizient* arbeiten.
Hierbei hilft es, sich an bewährten Vorbildern zu orientieren.

Oft wird der Mathematik vorgeworfen, dass sie nur „richtig“ oder „falsch“ kenne, und dies wird als übertrieben streng, ja grausam empfunden.
Sehen wir das Positive: Die Mathematik kennt richtig und falsch!
Dies können Sie nutzen und damit Klarheit schaffen.

Müssen wir alles so genau nehmen? Präzision ist Fluch und Segen:
Als Anwender mathematischer Ergebnisse schätzen Sie die Garantie.
Als Hersteller mathematischer Ergebnisse spüren Sie die Pflicht.
Ihre Vorbereitung von heute ist Ihr Nutzen von morgen!

*Die mit Tränen säen, werden mit Freuden ernten.*

Die Bibel, Psalm 126:5

# Zweck und Nutzen der Logik: Sprache

Sprache ist ungeheuer wichtig! Sie soll möglichst praktisch und präzise sein, doch nicht unnötig pedantisch und prätentiös. Das fordert Disziplin.

Jura: Verträge, Gesetze, Regeln müssen klar und eindeutig sein, soweit möglich vollständig und möglichst nicht mehrdeutig.

Physik: qualitative und quantitative Vorhersagen zu Experimenten. Nur diese sind prüfbar, wichtiger noch: Sie müssen widerlegbar sein.

Informatik: Spezifikationen für Software, Pflichtenheft bei Arbeitsteilung. Unklare Vereinbarungen führen zu unnötigem Kummer und Leid.

Mathematik: Logik und Mengenlehre dienen als gemeinsame Sprache für die gesamte Mathematik, in diversen Dialekten je nach Teilgebiet. Exploration: erste Formulierung von Ideen, Hypothesen, Versuchen. Konsolidierung: Präzisierung, Beweis, Archivierung, Weitergabe.

*Die Grenzen meiner Sprache bedeuten die Grenzen meiner Welt.*
Ludwig Wittgenstein (1889-1951), *Tractatus logico-philosophicus*

# Zweck und Nutzen der Logik: Kalkül

Eines der Ziele und Werkzeuge der Mathematik ist gute Notation.

*By relieving the brain of all unnecessary work, a good notation sets it free to concentrate on more advanced problems.*

Alfred North Whitehead (1861–1947), *An Introduction to Mathematics* (1911)

Idealerweise lassen sich dadurch komplexe Aufgaben routiniert lösen.
Es kann sogar dazu verleiten, sich blind auf den Kalkül zu verlassen:

*Die Mathematik ist eine gar herrliche Wissenschaft, aber die Mathematiker taugen oft den Henker nicht. Es ist fast mit der Mathematik, wie mit der Theologie. [...] so verlangt sehr oft der so genannte Mathematiker für einen tiefen Denker gehalten zu werden, ob es gleich darunter die größten Plunderköpfe gibt, die man nur finden kann, untauglich zu irgend einem Geschäft, das Nachdenken erfordert, wenn es nicht unmittelbar durch jene leichte Verbindung von Zeichen geschehen kann, die mehr das Werk der Routine, als des Denkens sind.*

Georg Christoph Lichtenberg (1742–1799), *Sudelbuch K.185*

# Klarheit der Sprache und des Denkens

Wir wollen **wahre und falsche Aussagen** als solche erkennen.

Wissenschaft sucht Erkenntnis, nachvollziehbar und begründet.
Oberstes Ziel wissenschaftlicher Kommunikation ist daher Klarheit!
Idealerweise ist sie redlich und transparent, eindeutig und klar, objektiv / intersubjektiv, überprüfbar / widerlegbar. Grundlage dafür ist die Logik!

Dramatische Beispiele: Welche der folgenden Aussagen sind wahr?

☺ Sorgfalt bei Primzahlen:
A: „Wenn $1, 2, 3$ prim sind, dann heiße ich Rumpelstilzchen.“

☺ Mathematische Urlaubsgrüße:
B: „Immer wenn es geregnet hat, haben Aliens unser Zelt geklaut.“

☺ Doch keine Verschwörung:
C: „Ist die Erde eine Scheibe, dann war die Mondlandung inszeniert.“

Full disclosure: Ich heiße Michael Eisermann, kenne bislang keine Belege für Aliens, und die Erde ist eine Kugel (mit Unebenheiten).
Was soll ich von den obigen Aussagen halten: wahr oder falsch?

# Klarheit der Sprache und des Denkens

Ich halte alle drei Aussagen für wahr und kann dies gut begründen.
Auch Sie können diese schockierenden Behauptungen überprüfen:

A: Wir haben eine präzise Definition: $1$ ist keine Primzahl!
Alles weitere ist dann irrelevant, die Aussage A ist wahr.

B: Wir dürfen weiterhin davon ausgehen, dass keine Aliens die Erde besuchen. Es hat während des Urlaubs einfach nicht geregnet!

C: Die Erde ist keine Scheibe, sondern eine Kugel (mit Unebenheiten).
Alles weitere ist dann irrelevant, die Aussage C ist wahr.

In diesen anschaulichen Beispielen ist Ihnen die Logik vermutlich klar.
Das ändert sich, sobald Sie über neue, unbekannte Dinge nachdenken.

Wir werden bald komplexe, mathematische Sachverhalte bearbeiten, zu denen Sie (noch) keine Anschauung haben. Sie können dann nicht auf vage Intuition bauen, Sie müssen die Logik sicher beherrschen!

 Die Logik ist zum Glück nicht schwer, sondern solides Handwerk.
Dazu gehen wir die grundlegenden Regeln der Logik schrittweise durch.

# Klarheit der Sprache und des Denkens

Vielleicht finden Sie die obigen Beispiele allzu konstruiert und denken „In der Natur kommen logische Probleme nicht vor". Oh, weit gefehlt! Beispiele von unklaren oder unlogischen Formulierung gibt es zuhauf.


**Beispiel:** Ein Fall für das Gesetz. . .
von Augustus De Morgan (1806–1871).
Was genau ist hier verboten und strafbar?

„Euer Ehren, ich habe nur gepflückt,
aber nicht auch noch ausgegraben,
denn beides zugleich ist verboten.“

— „Angeklagter, beides ist verboten!
Sie machen sich also bereits strafbar,
wenn Sie pflücken *oder* ausgraben.“

— „Euer Ehren, hier muss ein bedauerlicher
Irrtum vorliegen, auf dem Schild steht *und*.
Ich habe nicht gepflückt *und* ausgegraben.“

# Klarheit der Sprache und des Denkens

Das Verbot habe ich tatsächlich beim Spaziergang im Wald *gefunden*. Die Feld-Wald-und-Wiesen-Seifenoper dazu ist natürlich frei *erfunden*.

Kommunikation kann auf viele Weisen scheitern. Zwei typische Quellen logischer Fehlschlüsse sind Inkompetenz und Bösartigkeit, sowohl auf Seite des Senders als auch auf Seite des Empfängers.

*Sophistik ist nach Aristoteles die Philosophie des Scheins,*
*das heißt die Kunst, durch falsche Dialektik*
*das Wahre mit dem Falschen zu verwirren*
*und durch Disputieren, Widerspruch und Schönschwatzen*
*Beifall und Reichtum zu erwerben; sophistisch heißt demnach*
*trügerisch, Sophisterei ein verfängliches Räsonnement.*

Kirchner, Michaëlis: *Wörterbuch der Philosophischen Grundbegriffe* (1907)

Wir bauen auf Logik, wir vermeiden Polemik. Daher müssen wir zuerst erklären, was wir unter Logik verstehen und wie sie zu benutzen ist! Idealerweise löst das Verständnisprobleme schon bevor sie entstehen und macht Sie wehrhaft gegen (Selbst)Betrug und Schönschwatzen.

# Klarheit der Sprache und des Denkens

Das vorige Beispiel scheint Ihnen allzu fiktiv? Wie ist es mit folgendem?

> *The fee for new UK and EU students starting in 2020 is £9,250. [. . .]*
> *The fee for new overseas (non-UK or EU) undergraduates is £21,570.*
>
> London School of Economics am 05.01.2020.

Benötigt man für die erste Klausel die doppelte Staatsangehörigkeit?
Gilt die zweite Klausel für deutsche Studierende? Sind Sie „*overseas*“?
Wie programmieren Sie die Buchhaltung für die Gebührenerhebung?

Nach Rückfrage und Klärung ist vermutlich folgendes gemeint:

```
1 if isUKCitizen or isEUCitizen:
2     print("Your fee is 9250 pounds stirling.")
3 if (not isUKCitizen) and (not isEUCitizen):
4     print("Your fee is 21570 pounds stirling.")
```

 Präzise Formulierung und korrekte Logik sind unabdingbar,
wenn Sie genaue Regeln formulieren oder programmieren wollen.
Genau diese Klarheit und Präzision schulden wir uns auch gegenseitig.

# Klarheit der Sprache und des Denkens

Hätten Sie sich dieses Jahr neben Stuttgart auch an der London School of Economics (LSE) beworben, dann stünden Sie vor der dringenden und kniffligen Frage: Wie viel Studiengebühren müssen Sie zahlen? Wie sollten „*and*“, „*or*“, „*non*“ hier verwendet und verstanden werden?

Zugegeben, im Alltag sind viele Aussagen nicht eindeutig wahr oder falsch, meist gibt es vage Graubereiche und mehr oder weniger große Spielräume. Das ist unvermeidlich selbst in einfachsten Beispielen.

Es gibt aber oft genug auch Fragen, die mit einem klaren „ja“ oder „nein“ beantwortet werden können, gar müssen, so wie hier: Zahlen Sie die niedrigen Gebühren? Oder zahlen Sie die hohen Gebühren? Natürlich könnten Sie nachfragen, aber auch dann sollte eine klare Regel zugrundeliegen und keine Willkür.

Für viele Anwendungen ist diese Klarheit wünschenswert, gar essentiell: Gesellschaft: Hat Kandidat $X$ die Wahl gewonnen? Sport: Gilt das Tor? Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen? Naturwissenschaft und Technik: Hat das Instrument angeschlagen?

# Klarheit der Sprache und des Denkens

Wie würden Sie die obigen Klauseln als Programm implementieren?
Logische Präzision und sprachliche Klarheit sind dazu unerlässlich,
etwa für Datenbanken, Expertensysteme, Künstliche Intelligenzen, etc.

☺ Die Formulierung als Computerprogramm zwingt uns zur Präzision.
Das ist auch in vielen anderen Situationen ein strenger, aber guter Test.
Manche sagen: „Du hast es erst dann verstanden, wenn du es einem Computer beibringen kannst.“ Das ist etwas extrem, aber doch nützlich.

☺ Leichter zu schreiben und zu lesen ist die äquivalente Formulierung,
in der wir Zeile 3 `if ...:` durch `else:` ersetzen. Eleganter und klarer!

Beide Formulierungen sind äquivalent dank der Regel von De Morgan:
Die Aussage „nicht( $p$ oder $q$)“ ist äquivalent zu „(nicht $p$) und (nicht $q$)“.
Die Aussage „nicht( $p$ und $q$)“ ist äquivalent zu „(nicht $p$) oder (nicht $q$)“.

Bitte beachten Sie die Klammern: Diese sind hier ganz wesentlich!
Beim Sprechen fallen sie oft weg, das stiftet dann große Verwirrung.
Wenn wir Klammern weglassen, müssen wir erklären, was wir meinen.

# Klarheit der Sprache und des Denkens

 Mit dem Brexit fällt die Ausnahme für Studierende aus der EU weg. Das vereinfacht die Logik, aber verdoppelt ihre Studiengebühren:

> *The fee for new UK students starting in 2021 is £9,250. [. . .]*
> *The fee for new overseas (non-UK) undergraduates is £22,430.*
> London School of Economics am 03.10.2020.

Logische Aussagen begegnen uns überall – auch viel komplexere!

- Zulassung, Prüfungsordnung,
- Verträge, Gesetze, Spielregeln,
- Gebrauchsanweisung, Spezifikation,
- Formulierung / Hypothesen zu Naturgesetzen,
- mathematisch-statistische Analyse von Daten.

Nahezu immer und überall benötigen wir verlässliche präzise Aussagen. Die Logik ist daher keine theoretische Haarspalterei, sondern praktische Notwendigkeit: Davon hängen handfeste Entscheidungen ab!

# Aussagen und Wahrheitswerte

Wir wollen wahre und falsche **Aussagen** erkennen und nachweisen. Als Handwerkszeug entwickeln wir hierzu sorgsam die **Aussagenlogik** und ihre **Schlussregeln**, sodass wir mit Aussagen sicher rechnen können.

Die Mathematik nutzt einen strengen und präzisen Wahrheitsbegriff – für manche Anwendungen zu streng, dafür wunderbar einfach und klar.

*If people do not believe that mathematics is simple,*
*it is only because they do not realize how complicated life is.*
John von Neumann (1903–1957)

## Definition C1A: Aussage und Wahrheitswert

Eine **Aussage** $A$ ist ein sprachlicher Ausdruck, dem ein eindeutiger Wahrheitswert $\langle A \rangle$ zugeordnet ist: entweder $0 =$ falsch oder $1 =$ wahr.

Wir lassen vorerst offen, was genau ein „sprachlicher Ausdruck“ $A$ ist. Wichtig ist nur, ihn zu einem Wahrheitswert $\langle A \rangle$ auswerten zu können.

Zunächst nutzen wir die Umgangssprache (C1B). Später präzisieren wir Sprache (Syntax) und Bedeutung (Semantik) und Wahrheitswerte (C1D).

# Aussagen und Wahrheitswerte

Im Alltag sind viele Aussagen nicht eindeutig wahr oder falsch, oft gibt es Graubereiche und Ermessensfragen. Das ist unvermeidlich selbst in einfachsten Beispielen wie „die Nudeln sind al dente“ oder „es regnet“, erst recht bei Urteilen wie „diese Impfung ist sicher und wirksam“.

Die Mathematik bietet dazu sehr erfolgreiche und ausgefeilte Methoden, etwa Wahrscheinlichkeit als Grad der Un/Gewissheit, entweder subjektiv als Mangel an Information oder objektiv als physikalisches Grundprinzip.

Zum Aufbau der Mathematik jedoch beginnen wir mit den Grundlagen, und diese beruhen auf der klassischen, zweiwertigen **Aussagenlogik**. Hier arbeiten wir nur mit genau zwei **Wahrheitswerten**:

$0 =$ falsch, alternative Schreibweise: $\bot =$ falsum $=$ false $=$ faux

$1 =$ wahr, alternative Schreibweise: $\top =$ verum $=$ true $=$ vrai

Für viele Anwendungen ist diese Vereinfachung sinnvoll, gar essentiell: Gesellschaft: Hat Kandidat $X$ die Wahl gewonnen? Sport: Gilt das Tor? Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen?

# Aussagen und Wahrheitswerte

## Beispiel C1B: Aussage oder nicht? wahr oder falsch?

Wir untersuchen die folgenden umgangssprachlichen Ausdrücke:

$A =$ (Alle Primzahlen sind ungerade.)

$\neg A =$ (Es gibt eine gerade Primzahl.)

$B =$ (Dieses Beispiel C1B ist nicht leicht aber hilfreich.)

$\neg B =$ (Dieses Beispiel C1B ist leicht oder nicht hilfreich.)

$C =$ (Diese Aussage $C$ ist falsch.)

$D =$ (Diese Aussage $D$ ist wahr.)

$E =$ (Ein Quadrat mit Seitenlänge $\ell$ hat den Flächeninhalt $4\ell$.)

$F =$ (Ist jedes Quadrat ein Rechteck oder umgekehrt?)

$G =$ (Jede gerade Zahl $n \geq 4$ ist Summe zweier Primzahlen.)

$H =$ (Nächste Saison gewinnt der VfB Stuttgart die Meisterschaft.)

Welche dieser Ausdrücke sind Aussagen? wahr? falsch?

# Aussagen und Wahrheitswerte

**Aufgabe:** Welche dieser Ausdrücke sind Aussagen? wahr? falsch?

**Lösung:** Die Frage ist weit und offen, ich gebe hier nur eine Skizze.

Die Aussage $A$ ist falsch: Nicht alle Primzahlen sind ungerade.
Ihre Negation $\neg A$ ist wahr, denn $2$ ist eine gerade Primzahl.

Die Ausdrücke $B$ und $\neg B$ sind subjektive **Meinungsäußerungen**
ohne objektiven Wahrheitswert, es gibt dazu verschiedene Meinungen.

⚠ Die umgangssprachliche Konjunktion „aber“ bedeutet logisch „und“.
Zusätzlich drückt sie eine Bewertung aus, etwa einen Gegensatz, eine Einschränkung, einen Einwand, eine Entgegnung, eine Überraschung.
Für die logische Verknüpfung ist diese Bewertung überflüssig.

⚠ Beachten Sie die korrekt ausformulierte Verneinung von $B$ zu $\neg B$:
Aus „und“ wird „oder“ gemäß der Regel von De Morgan! Ausführlich:
Die Aussage „nicht( $p$ und $q$)“ ist äquivalent zu „(nicht $p$) oder (nicht $q$)“.
Die Aussage „nicht( $p$ oder $q$)“ ist äquivalent zu „(nicht $p$) und (nicht $q$)“.

# Aussagen und Wahrheitswerte

Der selbstbezügliche Ausdruck $C$ ist das berüchtigte **Lügner–Paradox**:
Ist $C$ wahr, dann ist $C$ falsch. Ist $C$ falsch, dann ist $C$ wahr.
Der Ausdruck $C$ ist somit in sich widersprüchlich:
Er kann weder wahr noch falsch sein.

⚠ Wir lassen den Ausdruck $C$ nicht als Aussage zu,
da ihm kein Wahrheitswert zugeordnet werden kann.

Ausdruck $D$ kann sowohl wahr als auch falsch sein, das ist vollkommen beliebig. Einen eindeutigen Wahrheitswert hat also auch $D$ nicht.

⚠ Vorsichtshalber lassen wir auch $D$ nicht als Aussage zu.
da ihm kein eindeutiger Wahrheitswert zugeordnet ist.

Sie sehen bereits an diesen einfachen umgangssprachlichen Beispielen, dass die Frage nach dem Wahrheitswert erstaunlich vertrackt sein kann. Das sollte Sie vor naiver Sorglosigkeit warnen und zu mathematischer Sorgfalt motivieren: Selbst für die einfachsten Grundbegriffe müssen wir umsichtig vorgehen, wenn wir Widersprüche vermeiden wollen.

# Aussagen und Wahrheitswerte

Ausdruck $E$ ist missverständlich formuliert! Soll $E$ heißen „Mindestens ein Quadrat…“? Dann ist ein Quadrat mit $\ell = 4$ ein Beleg, also $E$ wahr. Oder soll $E$ heißen „Ein beliebiges Quadrat…“, also eigentlich „Jedes Quadrat…“? Dann ist ein Quadrat mit $\ell = 3$ ein Gegenbeispiel, somit $E$ falsch. Wir müssen präzise und unmissverständlich formulieren!

⚠ Streng genommen müssen wir auch den Ausdruck $E$ als Aussage zurückweisen, da ihm kein eindeutiger Wahrheitswert zugeordnet ist.

Ausdruck $F$ ist keine Aussage sondern eine Frage. Die logisch korrekte Antwort lautet: „Ja, jedes Quadrat ist ein Rechteck oder umgekehrt.“

⚠ Eine Alternativfrage wie diese ist meist eine implizite Aufforderung an den Gefragten, die zutreffende/n Alternative/n explizit zu nennen. Eine freundlichere, hilfreichere Antwort wäre daher: „Ja, jedes Quadrat ist ein Rechteck, aber umgekehrt ist nicht jedes Rechteck ein Quadrat.“

⚠ Auch Aufforderungen („Rechnen wir!“) und Annahmen („Sei $x = 2$.“) sind logisch gesehen keine Aussagen: Sie haben keinen Wahrheitswert.

# Aussagen und Wahrheitswerte

Ausdruck $G$ ist eine **Vermutung von Christian Goldbach** (1690-1764). Ihr Wahrheitswert ist bislang unbekannt (Stand 2020): Trotz großer Anstrengungen (und zwischenzeitlich einem Preisgeld von 1 Million Dollar) wurde weder ein Beweis noch ein Gegenbeispiel gefunden. Die Aussage gilt für $4 \leq n \leq 4 \cdot 10^{18}$ dank maschineller Prüfung.

⚠ Ist $G$ eine Aussage oder nicht? Die **klassische Sichtweise** ist, dass jeder wohlgeformte Ausdruck $A$ einen Wahrheitswert $\langle\, A \,\rangle$ hat, egal ob wir ihn kennen oder nicht. Die **konstruktive Sichtweise** ist strenger: Sie verlangt einen Beweis für $A$ oder einen Beweis für die Negation $\neg A$, der Wahrheitswert muss also explizit durch einen Beweis belegt sein.

Diese stärkere Anforderung eines Nachweises ist natürlich und nützlich. Sie bereitet wesentlich mehr Mühe und ist manchmal sogar unmöglich: Es gibt Aussagen, analog zu $c$, die nachweislich unentscheidbar sind. Dies ist der berühmte **Unvollständigkeitssatz** von Kurt Gödel (1931).

*Fun fact:* Wäre $G$ unentscheidbar, also weder $G$ noch $\neg G$ beweisbar, dann wäre $G$ wahr, denn jedes Gegenbeispiel lässt sich entscheiden.

# Aussagen und Wahrheitswerte

Auch das Beispiel $H$ ist noch nicht entscheidbar: Wer Meister wird, stellt sich erst gegen Ende der nächsten Saison heraus und ist jetzt, zu Beginn dieser Saison, keineswegs sicher. Jeder Fußballfan kann sich zwar eine gefühlte Wahrscheinlichkeit einbilden und vielleicht sogar begründen, aber das ersetzt keine Auswertung zu wahr oder falsch.

Ebenso ist $K = (\text{Am Ende der nächsten Saison jubeln die VfB-Fans.})$ noch nicht entscheidbar. Hingegen ist $H \Rightarrow K$ eine wahre Aussage. Ähnliche Phänomene begegnen uns tatsächlich auch in der Mathematik.

⚠ Vorsichtigerweise sollten wir $G, H, K$ als Vermutungen betrachten, wie „zukünftige Aussagen“, deren Wahrheitswert noch unbekannt ist. Für die weitere Arbeit ist es bequem, sie wie Aussagen zu behandeln, auch wenn die klassische Sichtweise hier an ihre Grenzen stößt.

🙂 Im Folgenden vermeiden wir Paradoxien und Unentscheidbarkeit. Die Problematik der Beweisbarkeit bzw. Unentscheidbarkeit ist ganz real und konkret, doch wir wollen und können ihr vorerst sorgsam ausweichen und dabei viel gute Mathematik entwickeln.

# Verknüpfung von Aussagen

## Definition C1c: logische Verknüpfungen

Sind $A$ und $B$ Aussagen, so auch die folgenden Ausdrücke:

| Aussage | Bedeutung | Name |
|---|---|---|
| $\neg A$ | nicht $A$ | Negation |
| $(A \wedge B)$ | $A$ und $B$ | Konjunktion |
| $(A \vee B)$ | $A$ oder $B$ | (inklusive) Disjunktion |
| $(A \dot{\vee} B)$ | entweder $A$ oder $B$ | exklusive Disjunktion |
| $(A \Leftrightarrow B)$ | $A$ gilt genau dann, wenn $B$ gilt | Äquivalenz (Bijunktion) |
| $(A \Rightarrow B)$ | wenn $A$ gilt, dann gilt $B$ | Implikation (Subjunktion) |

Die zugehörigen Wahrheitswerte definieren wir wie folgt:

| $\langle A \rangle$ | $\langle B \rangle$ | $\langle \neg A \rangle$ | $\langle A \wedge B \rangle$ | $\langle A \vee B \rangle$ | $\langle A \dot{\vee} B \rangle$ | $\langle A \Leftrightarrow B \rangle$ | $\langle A \Rightarrow B \rangle$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 |

# Verknüpfung von Aussagen

 Die Wahrheitstabelle *definiert* diese logischen Verknüpfungen, klar und unmissverständlich, besser als jede Prosa. Hier die Prosa:

Die Negation $\neg p$ kehrt den Wahrheitswert um, von $0$ zu $1$ und von $1$ zu $0$: Die Aussage $\neg p$ ist falsch, wenn $p$ wahr ist, und wahr, wenn $p$ falsch ist. Alternative Schreibweisen für die Negation $\neg p$ sind $\sim p$ oder $\overline{p}$, oder `!p` wie in C/C++ oder `not p` wie in Python.

Die Konjunktion $p \wedge q$ ist das logische Und: Die Aussage $p \wedge q$ ist wahr, wenn $p$ und $q$ wahr sind. Die Aussage $p \wedge q$ ist falsch, wenn $p$ oder $q$ falsch ist. (Letzteres ist die Regel von De Morgan, siehe C135)

Die Disjunktion $p \vee q$ ist das inklusive Oder: Die Aussage $p \vee q$ ist wahr, wenn $p$ oder $q$ wahr ist. Die Aussage $p \vee q$ ist falsch, wenn $p$ und $q$ falsch sind. (Letzteres ist die Regel von De Morgan, siehe C135)

Das exklusive Oder schreiben wir $p \dot{\vee} q$ und sagen ausdrücklich „entweder $p$ oder $q$“. Die Aussage $p \dot{\vee} q$ ist wahr, wenn entweder $p$ oder $q$ wahr ist, also genau eine, nicht beide. Die Aussage $p \dot{\vee} q$ ist falsch, wenn $p$ und $q$ falsch sind, aber auch, wenn $p$ und $q$ beide zugleich wahr sind.

# Beispiel: Wenn Spinat, dann Nachtisch?

(1) Die strengen Eltern mahnen ihre Kinder: „Wenn ihr euren Spinat nicht aufesst, dann bekommt ihr heute keinen Nachtisch.“ Die Kinder essen tapfer ihren Spinat, bekommen aber dennoch keinen Nachtisch.

Können sie ihre Eltern auf Herausgabe des Nachtischs verklagen?
Nein! Für diesen Fall haben die Eltern keine Zusage gemacht.

(2) Die Dozentin mahnt: „Wenn Sie nicht fleißig üben, kommt kein Aha.“ Die Studierenden üben fleißig, aber es kommt (vorerst noch) kein Aha.

Hat die Dozentin nun gelogen oder doch die Wahrheit gesagt?
Über diesen Fall hat die Dozentin keine Aussage gemacht.

(3) Für $n \in \mathbb{N}_{\geq 1}$ sei $A(n)$ die Aussage: „Wenn $n$ Quadrat einer Primzahl ist, dann hat $n$ als Teiler genau drei verschiedene natürliche Zahlen.“

Diese Aussage $A(n)$ ist wahr für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$, unabhängig davon, ob $n$ Quadrat einer Primzahl ist oder nicht.

Um die Aussage $A(n)$ zu beweisen, müssen Sie lediglich zeigen:
Wenn die Voraussetzung wahr ist, dann ist die Folgerung wahr.

# Implikationen

 Sie sehen an diesen einfachen Beispiele bereits sehr deutlich, wie wichtig unsere klare und unmissverständliche Definition C1c ist.

Wir nennen „$p \Rightarrow q$“ eine **Implikation** oder **Schlussfolgerung**, $p$ heißt die **Voraussetzung** oder **Prämisse** und $q$ die **Folgerung**.

Gilt $p \Rightarrow q$, so ist $p$ eine **hinreichende Bedingung** für $q$:
Wann immer $p$ wahr ist, dann ist auch $q$ wahr.

Gilt $p \Rightarrow q$, so ist $q$ ist **notwendige Bedingung** für $p$:
Wenn $q$ nicht gilt, dann kann auch $p$ nicht gelten.

Die Implikation $p \Rightarrow q$, wie oben definiert, mag überraschen:
Wenn die Prämisse nicht gilt, so ist die Implikation dennoch wahr!
Von allen logischen Operationen ist diese anfangs die Schwierigste, am wenigsten intuitiv, und läuft dem Alltagsgebrauch entgegen.

Bitte folgen Sie streng der Definition und machen Sie sich mit möglichst vielfältigen Beispielen vertraut, alltäglichen und mathematischen.
Auch die Logik verlangt und belohnt gewissenhafte Übung.

# Verknüpfung von Wahrheitswerten

Wie zuvor nutzen wir die beiden Wahrheitswerte $0$ (falsch) und $1$ (wahr).
Die Negation ist die Abbildung $\neg : \{0,1\} \to \{0,1\}$ mit $\neg 0 = 1$ und $\neg 1 = 0$.
Wir definieren die Verknüpfungen $\wedge, \vee, \dot{\vee}, \Rightarrow, \Leftrightarrow : \{0,1\} \times \{0,1\} \to \{0,1\}$:

| $a$ | $b$ | $a \wedge b$ | $a \vee b$ | $a \mathbin{\dot{\vee}} b$ | $a \Rightarrow b$ | $a \Leftrightarrow b$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 1 |

Für alle $a, b \in \{0,1\}$ gilt $(a \wedge b) = \min\{a, b\}$ und $(a \vee b) = \max\{a, b\}$.
Damit können wir alle anderen ausdrücken: $(a \Rightarrow b) = (\neg a \vee b)$
sowie $(a \Leftrightarrow b) = ((a \Rightarrow b) \wedge (b \Rightarrow a))$ und $(a \mathbin{\dot{\vee}} b) = \neg(a \Leftrightarrow b)$.

| $a$ | $b$ | $\neg a$ | $\neg a \vee b$ | $a \Rightarrow b$ | $b \Rightarrow a$ | $(a \Rightarrow b) \wedge (b \Rightarrow a)$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 0 |
| 0 | 0 | 1 | 1 | 1 | 1 | 1 |

# Verknüpfung von Wahrheitswerten

 Genau so rechnen Sie mit Wahrheitswerten, ganz einfach.
Dies sind elementare Rechenoperationen auf den Werten $0$ und $1$, inspiriert, extrahiert und abstrahiert von unseren vorigen Beispielen.

Bitte beachten Sie, dass die logischen Verknüpfungssymbole $\neg, \wedge, \vee, \dot{\vee}, \Rightarrow, \Leftrightarrow$ hier in zwei verschiedenen Rollen auftreten:

1. Bei der Verknüpfung von Aussagen sind dies verbindende Symbole. Sind zum Beispiel $a, b$ aussagenlogische Variablen, so ist „$a \wedge b$“ eine Abfolge von drei Symbolen, eine Zeichenkette der Länge $3$.
2. Beim Rechnen mit Wahrheitswerten $0, 1$ sind dies Operationen. So ergibt die Operation $0 \wedge 1$ den Wert $0$, kurz $0 \wedge 1 = 0$. Hier geht es um den Wert, nicht den Ausdruck.

Aus dem Kontext der Verknüpfung ist jeweils klar, was gemeint ist.

Die folgende Definition C1D erklärt die Sichtweise (1) noch ausführlicher, also was genau wir unter einer aussagenlogischen Formel verstehen.
Die Definition C1E leistet die Übersetzung von aussagenlogischen Formeln zur Auswertung der Wahrheitswerte in $\{0, 1\}$ wie in (2).

# Verknüpfung von Wahrheitswerten

Alle logischen Operationen lassen sich auf $\neg$, $\wedge$ und $\vee$ zurückführen!

$$(a \Rightarrow b) = (\neg a \vee b)$$

$$\begin{aligned}(a \Leftrightarrow b) &= ((a \Rightarrow b) \wedge (b \Rightarrow a)) \\ &= ((\neg a \vee b) \wedge (a \vee \neg b)) \\ &= ((a \wedge b) \vee (\neg a \wedge \neg b))\end{aligned}$$

$$\begin{aligned}(a \dot{\vee} b) &= \neg(a \Leftrightarrow b) \\ &= \neg((\neg a \vee b) \wedge (a \vee \neg b)) \\ &= ((a \wedge \neg b) \vee (\neg a \wedge b))\end{aligned}$$

 Definition C1G erklärt die konjunktive und disjunktive Normalform, und Satz C1H zeigt, dass wir jeden Junktor so darstellen können.

Insbesondere das Exklusiv-Oder $\dot{\vee}$ lassen wir daher meistens weg; bei Bedarf können wir jederzeit $(a \dot{\vee} b) = \neg(a \Leftrightarrow b)$ vereinbaren.

Die Implikation $\Rightarrow$ und die Äquivalenz $\Leftrightarrow$ hingegen werden sehr häufig gebraucht, sodass wir diese bequeme Notation beibehalten wollen.

# Verknüpfung von Wahrheitswerten

Wir haben oben die wichtigsten logischen Verknüpfungen erklärt.
Es gibt daneben noch einige weitere, wie zum Beispiel:

$$\text{NAND} \quad a \mathbin{\overline{\wedge}} b := \neg(a \wedge b)$$
$$\text{NOR} \quad a \mathbin{\overline{\vee}} b := \neg(a \vee b)$$

**Übung:** Wie viele Verknüpfungen $\{0,1\} \times \{0,1\} \to \{0,1\}$ gibt es?
Zählen Sie alle Möglichkeiten explizit auf. (Lösung auf Seite C142)

☺ Es ist eine gute Übung, neu definierte Objekte aufzuzählen.
Das verschafft Ihnen einen guten Überblick und mehr Sicherheit.

**Übung:** Jede logische Verknüpfung $\neg, \vee, \wedge, \ldots$ lässt sich aufbauen
(1) alleine aus NAND sowie alternativ (2) alleine aus NOR.

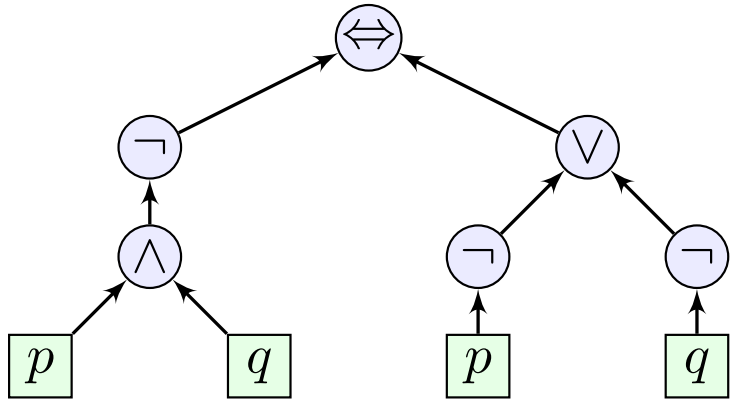
☺ Das hilft beispielsweise zur Herstellung von Computerchips, um alle logischen Schaltungen aus einem einzigen Grundbaustein herzustellen.

**Übung:** Allein aus $\wedge$ und $\vee$ lassen sich nicht alle Verknüpfungen $\{0,1\} \times \{0,1\} \to \{0,1\}$ aufbauen: Alle daraus gebauten Formeln $f(a,b)$ sind monoton, das heißt, aus $a \leq a'$ und $b \leq b'$ folgt $f(a,b) \leq f(a',b')$.

# Aussagenlogische Variablen und Formeln

Wir wollen aussagenlogische Formeln aufbauen, wie zum Beispiel

$$\begin{aligned}
\neg(p \wedge q) &\Leftrightarrow (\neg p \vee \neg q) \\
\neg(p \vee q) &\Leftrightarrow (\neg p \wedge \neg q) \\
((p \Rightarrow q) \wedge (q \Rightarrow p)) &\Leftrightarrow (p \Leftrightarrow q) \\
((p \Rightarrow q) \wedge (q \Rightarrow r)) &\Rightarrow (p \Rightarrow r)
\end{aligned}$$




Als Bausteine haben wir dazu

- die Konstanten $\bot$ (falsum, falsch) und $\top$ (verum, wahr),
- die Verknüpfungen $\neg$, $\wedge$, $\vee$, $\Rightarrow$, $\Leftrightarrow$ mit Klammern $($ und $)$,
- die Variablen $p, q, r, \ldots$ als freie Symbole (noch nicht belegt).

Daraus bauen wir alle Formeln rekursiv auf:

## Definition C1D: aussagenlogische Formeln

Konstanten und Variablen $x$ sind Formeln der Komplexität $\kappa(x) = 0$.

Sind $a, b$ Formeln, so auch $\neg a$ mit Komplexität $\kappa(\neg a) = 1 + \kappa(a)$
und $c = (a \wedge b), (a \vee b), (a \Rightarrow b), (a \Leftrightarrow b)$, mit $\kappa(c) = 1 + \kappa(a) + \kappa(b)$.

# Aussagenlogische Variablen und Formeln

Das erklärt den formalen Aufbau aller aussagenlogischen Formeln.
Wir nutzen folgende Konventionen, um Klammern zu sparen:

- Wir können äußere Klammern weglassen.
  Beispiel: Wir kürzen $(p \Rightarrow q)$ ab zu $p \Rightarrow q$.
- Die Negation $\neg$ bindet stärker als $\wedge$ und $\vee$.
  Beispiel: $(\neg p \wedge q) \neq \neg(p \wedge q)$ und $(\neg p \vee q) \neq \neg(p \vee q)$
- die Verknüpfungen $\wedge$ und $\vee$ binden stärker als $\Leftrightarrow$ und $\Rightarrow$.
  Beispiel: Wir können $(p \wedge q) \Leftrightarrow (q \wedge q)$ abkürzen zu $p \wedge q \Leftrightarrow q \wedge q$.

Prinzip der Klarheit: Eine Bezeichnung / Abkürzung ist nur sinnvoll, wenn der gemeinte Gegenstand daraus unmissverständlich hervorgeht.

Test: Können Sie auf einem Computer die Ersetzung programmieren? Können Sie umgekehrt die Baumstruktur eindeutig rekonstruieren? Spätestens hier bemerken Sie Unklarheiten und Unstimmigkeiten.

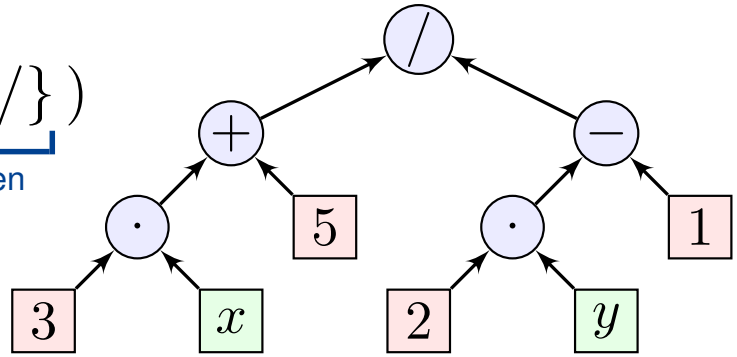
Die obigen Konventionen zum Sparen von Klammern erinnern an die Regel „Punkt-vor-Strich“, die Sie noch gut aus der Schule kennen. Tatsächlich besteht hier eine sehr enge und schöne Analogie.

# Aussagenlogische Variablen und Formeln

Sie kennen das Prinzip von rationalen Ausdrücken:

$$\mathrm{RAT} = \mathscr{F}(\underbrace{\mathbb{Z}}_{\text{Konstanten}}, \underbrace{\{x, y, z, \ldots\}}_{\text{Variablen}}, \underbrace{\{+, -, \cdot, /\}}_{\text{Verknüpfungen}})$$

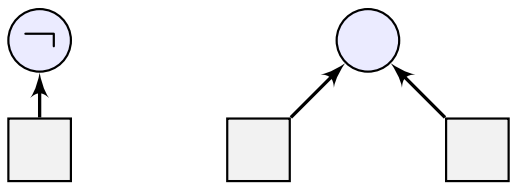
$$\frac{3x+5}{2y-1} = ((3 \cdot x) + 5)/((2 \cdot y) - 1)$$




Ebenso konstruieren wir alle aussagenlogischen Formeln:

$$\mathrm{ALF} = \mathscr{F}(\underbrace{\{\bot, \top\}}_{\text{Konstanten}}, \underbrace{\{p, q, r, \ldots\}}_{\text{Variablen}}, \underbrace{\{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\}}_{\text{Verknüpfungen}})$$

**Aufgabe:** Wir betrachten die Konstanten $\bot, \top$ und drei Variablen $p, q, r$. Wie viele aussagenlogische Formeln der Komplexität $0, 1, 2$ gibt es?




**Lösung:** Es gibt genau $5 + 4 \cdot 5^2 = 105$ Formeln der Komplexität $1$. Komplexität $2$ empfehle ich als Übung. Lesen Sie die Definition!

# Aussagenlogische Variablen und Formeln

Definition C1D erklärt den Aufbau aller aussagenlogischen Formeln.
Jede Formel entspricht genau einer Baumstruktur wie oben skizziert.
Zur Betonung: Nichts anderes ist eine aussagenlogische Formel.

Es ist oft lehrreich, neu definierte Objekte zu zählen. Dies zwingt dazu, die Definition genau zu verstehen und klärt so Missverständnisse auf.
*Defendit numerus.* [Die Zahl gibt Schutz.] Juvenal (58–138 n.Chr.), *Satiren*

Jede Variable $p$ ist ein Platzhalter und hat noch keinen Wahrheitswert.
Wir können jede beliebige Aussage $A$ für $p$ einsetzen, geschrieben $p \mapsto A$, gelesen „ersetze der Variable $p$ überall durch die Aussage $A$“.

**Beispiel:** Durch die beiden Ersetzungen $p \mapsto (\text{die Sonne scheint})$ und $q \mapsto (\text{ich gehe ins Freibad})$ wird aus der allgemeinen Formel $(p \Rightarrow q)$ die spezielle Aussage $(\text{die Sonne scheint}) \Rightarrow (\text{ich gehe ins Freibad})$, gesprochen „Wenn die Sonne scheint, dann gehe ich ins Freibad.“

Wir wollen von Sonnenschein und Freizeitaktivitäten abstrahieren, mit allgemeinen aussagenlogischen Formeln arbeiten und rechnen.
Besonders nützlich sind Tautologien, also Formeln, die immer gelten.

# Auswertungen und Tautologien

## Definition C1E: Auswertungen und Tautologien

Eine **Belegung** der Variablen ist eine Abbildung $\beta : \{p, q, r, \ldots\} \to \{0, 1\}$:
Sie ordnet jeder Variablen $x$ einen Wahrheitswert $\beta(x) \in \{0, 1\}$ zu.

Diese Abbildung setzen wir fort zu einer Auswertung aller Formeln:
Die Konstanten $\bot$ und $\top$ werten wir aus zu $\beta(\bot) = 0$ und $\beta(\top) = 1$.
Zusammengesetzte Formeln werten wir daraufhin rekursiv aus:

$$\begin{aligned}
\beta(\neg a) &= \neg\beta(a) \\
\beta(a \wedge b) &= \beta(a) \wedge \beta(b) \\
\beta(a \vee b) &= \beta(a) \vee \beta(b) \\
\beta(a \Rightarrow b) &= \beta(a) \Rightarrow \beta(b) \\
\beta(a \Leftrightarrow b) &= \beta(a) \Leftrightarrow \beta(b)
\end{aligned}$$

Eine Formel $a$ heißt **erfüllbar**, wenn sie für eine Belegung wahr ist.
Eine Formel $a$ heißt **Tautologie**, wenn sie für jede Belegung wahr ist.
Zwei Formeln $a, b$ heißen **äquivalent**, wenn $a \Leftrightarrow b$ eine Tautologie ist.

# Auswertungen und Tautologien

Definition C1D erklärt die **Sprache** (Syntax) aussagenlogischer Formeln und C1E ihre **Interpretation** (Semantik) bezüglich einer Belegung $\beta$. Wir betrachten jede Belegung $\beta$ als ein **Beispiel** oder ein **Modell**, erst dadurch wird eine Formel zur Aussage, also wahr oder falsch.

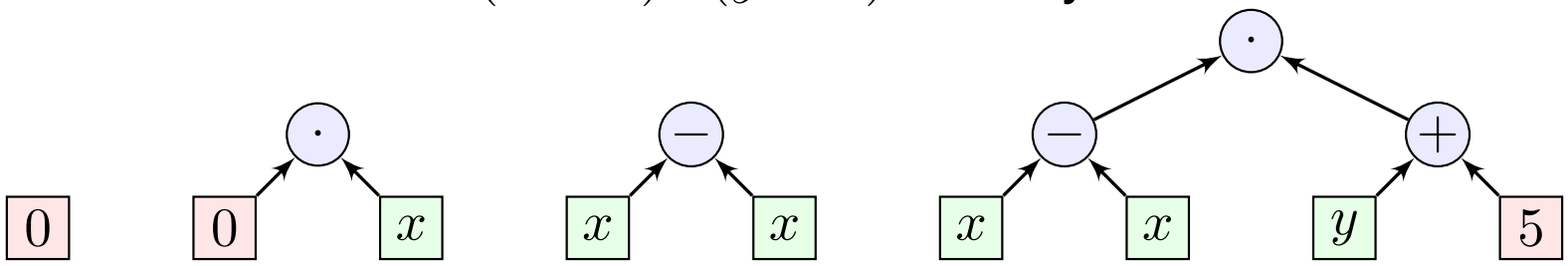
Zwei Formeln $a$ und $b$ sind **gleich**, wenn sie identisch aufgebaut sind, also durch denselben Text dargestellt werden, somit denselben Baum. Zur Betonung sagen wir, $a$ und $b$ sind **syntaktisch gleich**. Das ist leicht zu prüfen: Es genügt $a$ und $b$ Buchstabe für Buchstabe zu vergleichen.

Hingegen sind $a$ und $b$ **logisch äquivalent**, wenn sie immer dasselbe Ergebnis liefern, egal auf welches Beispiel / Modell wir sie anwenden. Das bedeutet $a \Leftrightarrow b$ ist eine Tautologie, also wahr für jede Belegung $\beta$. Zur Betonung sagen wir, $a$ und $b$ verhalten sich **semantisch gleich**.

Letzteres ist mühsamer zu prüfen. Für den syntaktischen Vergleich von zwei Formeln $a$ und $b$ der Länge $\leq \ell$ benötigen wir $\leq \ell$ Schritte. Für den semantischen Vergleich bezüglich aller Belegungen der $n$ Variablen benötigen wir $2^n$ Rechnungen: Das ist exponentiell in $n$.

# Auswertungen und Tautologien

Sie kennen das Prinzip von rationalen Ausdrücken: Die vier Ausdrücke $0$ und $0 \cdot x$ und $x - x$ und $(x - x) \cdot (y + 5)$ sind syntaktisch verschieden:




Alle vier sind jedoch semantisch gleich: Sie liefern dasselbe Ergebnis, egal welche (ganzzahligen) Werte wir für die Variablen $x, y$ einsetzen. Alle vier definieren dieselbe Funktion $f : \mathbb{Z} \times \mathbb{Z} \mapsto \mathbb{Z} : (x, y) \mapsto f(x, y)$.

Zum Schluss einer Rechnung versuchen Sie, Ihre Antwort soweit wie möglich zu vereinfachen, also unter den semantisch gleichen Lösungen eine syntaktisch möglichst einfache herzustellen, manchmal sogar *die* Normalform: Zum Beispiel möchten Sie Brüche vollständig kürzen.

Wir werden daher penibel zwischen Formel und Funktion unterscheiden. Mit der Formel können wir explizit arbeiten und das Objekt benennen. Die Funktion hingegen sagt uns, was die Formel bei Auswertung tut. Verschiedene Formeln können dieselbe Funktion definieren!

# Auswertungen und Tautologien

Sie haben in der Schule gelernt, wie man solche Formeln, sagen wir in $\mathscr{F}(\mathbb{Q}, \{x\}, \{+, -, \cdot\})$, als Polynome in eine geeignete Normalform bringt und somit schließlich bequem vergleichen kann: Koeffizientenvergleich!

Solche Normalformen sind Fluch und Segen: Sie dürfen sich freuen, sie zu nutzen, doch Sie müssen sich etwas mühen, sie herzustellen. Sie kennen das von Hausaufgaben und vor allem Klausuren.

Auch für aussagenlogische Formeln gibt es solche Normalformen, CNF und DNF, diese werden wir unten definieren und Beispiele erarbeiten. Bemerkenswerterweise ist jedoch der semantische Vergleich von zwei aussagenlogischen Formeln rechnerisch sehr aufwändig. Das führt uns zu einer der größten ungelösten Fragen der Komplexitätstheorie: C1K.

Sie sehen hier ein eindrückliches Beispiel für die sinnvolle Trennung zwischen der *Definition* eines Begriffs (konkret: Erfüllbarkeit, Tautologie, Äquivalenz) und möglichen *Algorithmen* zu seiner expliziten Berechnung (Wahrheitstabelle, Normalform, . . . ?). Die Trennung ist notwendig und schafft Klarheit: (1) Was wollen wir wissen? (2) Wie berechnen wir es?

# Doppelte Verneinung und das ausgeschlossene Dritte

Als einfache Illustration untersuchen wir die folgenden Ausdrücke:

| $p$ | $\neg p$ | $\neg\neg p$ | $p \wedge \neg p$ | $\neg(p \wedge \neg p)$ | $p \vee \neg p$ | $p \dot{\vee} \neg p$ |
|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 0 | 1 | 1 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 | 1 |

*Mein Hund gehorcht mir aufs Wort. Wenn ich sage „Komm her oder nicht!“, dann kommt er her oder nicht, und zwar sofort!* (Otto Waalkes)

## Satz C1F: doppelte Verneinung und das ausgeschlossene Dritte

Folgende Ausdrücke sind Tautologien, also allgemeingültig:

| | |
|---|---|
| $\neg\neg p \Leftrightarrow p$ | die doppelte Verneinung |
| $\neg(p \wedge \neg p)$ | der ausgeschlossene Widerspruch |
| $p \vee \neg p$ | das ausgeschlossene Dritte, *Tertium non datur* |
| $p \dot{\vee} \neg p$ | beides zusammengefasst |

Lesen Sie dies laut vor! Das klingt tautologisch? Ja, klar! Jetzt haben wir die Sprache, dies zu formulieren, und auch die Technik, es zu beweisen.

# Doppelte Verneinung und das ausgeschlossene Dritte

In der klassischen Aussagenlogik ist die Formel $p \vee \neg p$ eine Tautologie, also immer wahr. So werden wir es im Folgenden bequem verwenden.

Die konstruktive Sichtweise ist hier wesentlich strenger: Zum Beweis der Disjunktion $p \vee q$ fordert die Konstruktivistin einen Nachweis von $p$ oder einen Nachweis von $q$. Das ist viel informativer, aber auch schwieriger! Insbesondere ist für eine Konstruktivistin die Formel $p \vee \neg p$ noch nicht automatisch bewiesen, sie fordert einen Nachweis von $p$ oder von $\neg p$.

**Beispiel:** Wir erinnern uns an die Goldbachsche Vermutung:

$$G = (\text{Jede gerade Zahl } n \geq 4 \text{ ist Summe zweier Primzahlen.})$$

Klassisch gilt $G \vee \neg G$. Konstruktiv bleibt die Aussage offen: Wir wissen (noch) nicht, ob die Vermutung $G$ gilt, oder ob ihre Negation $\neg G$ gilt.

**Beispiel:** „Ich bin verzweifelt: Ich habe meine Schlüssel verbummelt. Das war entweder in der Mensa oder in der Bahn.“ Das ist prinzipiell gut zu wissen, sagt uns aber leider noch lange nicht, wo wir suchen sollen! Für viele praktische Fragen ist die konstruktive Sichtweise hilfreicher.

# Nützliche Rechenregeln

Die folgenden einfachen Tautologien sind allgegenwärtig und hilfreich:

(1) Kommutativität

$$(p \wedge q) \Leftrightarrow (q \wedge p)$$
$$(p \vee q) \Leftrightarrow (q \vee p)$$

(2) Assoziativität

$$((p \wedge q) \wedge r) \Leftrightarrow (p \wedge (q \wedge r))$$
$$((p \vee q) \vee r) \Leftrightarrow (p \vee (q \vee r))$$

(3) Distributivität

$$(p \vee (q \wedge r)) \Leftrightarrow ((p \vee q) \wedge (p \vee r))$$
$$(p \wedge (q \vee r)) \Leftrightarrow ((p \wedge q) \vee (p \wedge r))$$

(4) Idempotenz

$$(p \wedge p) \Leftrightarrow p$$
$$(p \vee p) \Leftrightarrow p$$

(5) Absorption

$$(p \vee (p \wedge q)) \Leftrightarrow p$$
$$(p \wedge (p \vee q)) \Leftrightarrow p$$

(6) De Morgan

$$\neg(p \wedge q) \Leftrightarrow (\neg p \vee \neg q)$$
$$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$$

Damit können Sie rechnen, Formeln umformen und vereinfachen.

# Nützliche Rechenregeln

**Aufgabe:** Beweisen Sie, dass dies Tautologien sind! Was ist zu tun?

**Lösung:** Wir prüfen dies als Wahrheitstabelle, hier exemplarisch für (6):

| $p$ | $q$ | $p \wedge q$ | $p \vee q$ | $\neg p$ | $\neg q$ | $(\neg p) \vee (\neg q)$ | $(\neg p) \wedge (\neg q)$ |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 |
| 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 |

Die Negation der dritten/vierten Spalte ergibt die siebte/achte Spalte.
Die verbleibenden Rechnungen (1–5) empfehle ich als Übung.

**Aufgabe:** Ist $\Rightarrow$ kommutativ / assoziativ? Ist $\Leftrightarrow$ kommutativ / assoziativ?

**Lösung:** Nein, $\Rightarrow$ ist nicht kommutativ: $(1 \Rightarrow 0) = 0$ und $(0 \Rightarrow 1) = 1$, ebensowenig assoziativ: $((0 \Rightarrow 1) \Rightarrow 0) = 0$ und $(0 \Rightarrow (1 \Rightarrow 0)) = 1$.

⚠ Zum Beweis einer Tautologie müssen wir (laut Definition) die gesamte Wahrheitstabelle prüfen. Zum Widerlegen genügt ein Gegenbeispiel! Die Rechnung für $\Leftrightarrow$ empfehle ich als Übung.

# Konventionen für mehrfache Verknüpfungen

Die mehrfache Konjunktion definieren wir als Linksklammerung:

$$\bigwedge_{i=1}^{n} p_i \;:=\; p_1 \wedge p_2 \wedge \cdots \wedge p_n \;:=\; (\cdots(p_1 \wedge p_2) \wedge \cdots) \wedge p_n$$

Das ist wahr, wenn $p_i$ für jeden Index $i \in \{1, \ldots, n\}$ wahr ist.
Hierfür schreiben wir abkürzend auch $\forall i \in \{1, \ldots, n\} : p_i$.

Die mehrfache Disjunktion definieren wir als Linksklammerung:

$$\bigvee_{i=1}^{n} p_i \;:=\; p_1 \vee p_2 \vee \cdots \vee p_n \;:=\; (\cdots(p_1 \vee p_2) \vee \cdots) \vee p_n$$

Das ist wahr, wenn $p_i$ für (mind.) einen Index $i \in \{1, \ldots, n\}$ wahr ist.
Hierfür schreiben wir abkürzend auch $\exists i \in \{1, \ldots, n\} : p_i$.

 Dank Assoziativität dürfen wir beliebig umklammern
und dank Kommutativität zudem beliebig umordnen.

Die mehrfache Implikation bzw. Äquivalenz definieren wir durch

$$p_1 \Rightarrow p_2 \Rightarrow \ldots \Rightarrow p_n \;:=\; (p_1 \Rightarrow p_2) \wedge (p_2 \Rightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Rightarrow p_n),$$
$$p_1 \Leftrightarrow p_2 \Leftrightarrow \ldots \Leftrightarrow p_n \;:=\; (p_1 \Leftrightarrow p_2) \wedge (p_2 \Leftrightarrow p_3) \wedge \cdots \wedge (p_{n-1} \Leftrightarrow p_n).$$

# Konjunktive und disjunktive Normalformen

Jede polynomielle Formel $f \in \mathrm{POL} = \mathscr{F}(\mathbb{C}, \{x\}, \{+, -, \cdot\})$ können Sie umformen in eine **Summe von Produkten** $a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ und ebenso in ein **Produkt von Summen** $a_n (x - z_1)(x - z_2) \cdots (x - z_n)$.

Ebenso können Sie jede aussagenlogische Formel

$$a \in \mathrm{ALF} = \mathscr{F}(\{\bot, \top\}, \{p, q, r, \ldots\}, \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\})$$

umformen in eine äquivalente **Disjunktion von Konjunktionen** und ebenso in eine **Konjunktion von Disjunktionen**. Zum Beispiel:

$$((p \wedge q) \vee (\neg p \wedge \neg q)) \quad \Leftrightarrow \quad ((\neg p \vee q) \wedge (p \vee \neg q))$$

## Definition C1G: konjunktive und disjunktive Normalform

Wir nennen $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ eine **konjunktive Normalform** (CNF) und $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ eine **disjunktive Normalform** (DNF); hierbei ist $a_{ij}$ ein Literal, also eine Variable $x$ oder ihre Negation $\neg x$, und jede Klausel $\bigvee_{j=1}^{m_i} a_{ij}$ bzw. $\bigwedge_{j=1}^{m_i} a_{ij}$ enthält jede Variable höchstens einmal.

# Konjunktive und disjunktive Normalformen

**Beispiel:** Die Formel $p \wedge (\neg p \vee q) \wedge (q \vee r)$ ist eine CNF, aber keine DNF. Die Formel $(p \wedge q) \vee (p \wedge q) \vee (\neg p \wedge r) \vee q$ ist eine DNF, aber keine CNF. Die Formeln $\neg p \vee q$ und $p \wedge q \wedge \neg r$ sind sowohl CNF als auch DNF; dasselbe gilt für jede Disjunktion und jede Konjunktion von Literalen.

In jedem konkreten Beispiel ist das leicht: Eine CNF ist eine Konjunktion von Disjunktionen, und eine DNF ist eine Disjunktion von Konjunktionen. Zur Ausformulierung dieser Idee benötigen wir eine geeignete Notation, nur so können wir sie präzise definieren und effizient mit ihr arbeiten.

Ausführlich: Ein **Literal** ist eine Variable $x$ oder ihre Negation $\neg x$. Eine **disjunktive Klausel** $d_i = \bigvee_{j=1}^{m_i} a_{ij}$ ist eine Disjunktion von Literalen $a_{ij}$ ohne doppelte Variablen. Eine **konjunktive Normalform** $c = \bigwedge_{i=1}^{\ell} d_i$ ist eine Konjunktion von disjunktiven Klauseln $d_i$, also $c = \bigwedge_{i=1}^{\ell} (\bigvee_{j=1}^{m_i} a_{ij})$.

Dual ist eine **konjunktive Klausel** $c_i = \bigwedge_{j=1}^{m_i} a_{ij}$ eine Konjunktion von Literalen $a_{ij}$ ohne doppelte Variablen. Eine **disjunktive Normalform** $d = \bigvee_{i=1}^{\ell} c_i$ ist eine Disjunktion von konjunktiven Klauseln $c_i$, also ausgeschrieben $d = \bigvee_{i=1}^{\ell} (\bigwedge_{j=1}^{m_i} a_{ij})$. Soweit das Vokabular.

# Konjunktive und disjunktive Normalformen

☺ Konjunktive und disjunktive Normalformen sind dual durch Negation:
Für jede CNF $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ ist die Negation $\neg c$ äquivalent zur DNF $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} b_{ij}$, mit $b_{ij} = \neg x$ falls $a_{ij} = x$ und $b_{ij} = x$ falls $a_{ij} = \neg x$.

☺ Doppelte Variablen lassen sich leicht und effizient kürzen!

In der Disjunktion $\bigvee_{j=1}^{m_i} a_{ij}$ können wir jede doppelte Variable $p$ kürzen, entweder dank Idempotenz $(p \vee p) \Leftrightarrow p$ und $(\neg p \vee \neg p) \Leftrightarrow \neg p$ oder dank $(p \vee \neg p) \Leftrightarrow \top$ und in $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ wird diese Disjunktion gelöscht.

In jeder Konjunktion $\bigwedge_{j=1}^{m_i} a_{ij}$ gilt entsprechend dieselbe Kürzungsregel, entweder dank Idempotenz $(p \wedge p) \Leftrightarrow p$ und $(\neg p \wedge \neg p) \Leftrightarrow \neg p$ oder dank $(p \wedge \neg p) \Leftrightarrow \bot$ und in $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ wird diese Konjunktion gelöscht.

☺ Die kleinen Längen $\ell \leq 2$ schreibe ich zur Deutlichkeit explizit aus:

$$\bigvee_{i=1}^{2} p_i = p_1 \vee p_2, \qquad \bigvee_{i=1}^{1} p_i = p_1, \qquad \bigvee_{i=1}^{0} p_i = \bot,$$
$$\bigwedge_{i=1}^{2} p_i = p_1 \wedge p_2, \qquad \bigwedge_{i=1}^{1} p_i = p_1, \qquad \bigwedge_{i=1}^{0} p_i = \top.$$

Letzteres entspricht unserer Definition für leere Summen $\sum_{i=1}^{0} s_i = 0$ und leere Produkte $\prod_{i=1}^{0} t_i = 1$, jeweils durch das neutrale Element.

# Junktoren

Wir kennen die logischen Verknüpfungen $\wedge, \vee, \Rightarrow, \Leftrightarrow : \{0,1\}^2 \to \{0,1\}$.
Ein $n$–stelliger **Junktor** ordnet jedem $n$–Tupel $a = (a_1, a_2, \ldots, a_n)$ mit Einträgen $a_1, a_2, \ldots, a_n \in \{0,1\}$ einen Wert $J(a) \in \{0,1\}$ zu, kurz

$$J : \{0,1\}^n \to \{0,1\} : a \mapsto J(a).$$

**Aufgabe:** Wie viele $n$–Tupel $a \in \{0,1\}^n$ gibt es? Wie viele $n$–stellige Junktoren gibt es? Berechnen Sie dies explizit für $n = 0, 1, 2, \ldots, 8$.

**Lösung:** Für $n \in \mathbb{N}$ gibt es genau $2^n$ Tupel und $2^{2^n}$ Junktoren.

| $n$ | Anzahl der $n$–Tupel | Anzahl der $n$–Junktoren |
|---|---|---|
| $0$ | $2^0 = 1$ leeres Tupel | $2^1 = 2$ |
| $1$ | $2^1 = 2$ Elemente | $2^2 = 4$ |
| $2$ | $2^2 = 4$ Paare | $2^4 = 16$ |
| $3$ | $2^3 = 8$ Tripel | $2^8 = 256$ |
| $4$ | $2^4 = 16$ Quadrupel | $2^{16} = 65\,536$ |
| $5$ | $2^5 = 32$ Quintupel | $2^{32} = 4\,294\,967\,296$ |
| $6$ | $2^6 = 64$ Sextupel | $2^{64} \approx 1.84 \cdot 10^{19}$ |
| $7$ | $2^7 = 128$ Septupel | $2^{128} \approx 3.40 \cdot 10^{38}$ |
| $8$ | $2^8 = 256$ Octupel | $2^{256} \approx 1.16 \cdot 10^{77}$ |

# Junktoren

**Aufgabe:** Nennen Sie alle zweistelligen Junktoren $J : \{0,1\}^2 \to \{0,1\}$.

| $c_0$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 0 |

| $\overline{\vee}$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 0 |

| $<$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 0 | 0 |

| $\overline{\mathrm{pr}_1}$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 0 |

| $>$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 0 |

| $\overline{\mathrm{pr}_2}$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 0 |

| $\dot{\vee}$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

| $\overline{\wedge}$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 0 |

| $\wedge$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

| $=$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 0 | 1 |

| $\mathrm{pr}_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 0 | 1 |

| $\leq$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |

| $\mathrm{pr}_1$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |

| $\geq$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 0 |
| 1 | 1 | 1 |

| $\vee$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 1 |

| $c_1$ | 0 | 1 |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 1 | 1 |

# Von Formeln zu Junktoren

Sei $V = \{x_1, x_2, \ldots, x_n\}$ die Menge der betrachteten Variablen und $f \in \mathscr{F}(\{\bot, \top\}, V, \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\})$ eine aussagenlogische Formel.
Der zugehörige Junktor $J_f : \{0,1\}^n \to \{0,1\}$ ist die Wahrheitstabelle:

| $x_1$ | $x_2$ | $x_3$ | $f = x_1 \wedge (x_2 \vee x_3)$ | $(x_1 \wedge x_2) \vee (x_1 \wedge x_3)$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 0 |
| 1 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 |

Ausführlich entsteht diese Tabelle wie folgt: Jedes $n$–Tupel $b \in \{0,1\}^n$ definiert die zugehörige Belegung $\beta : V \to \{0,1\} : x_1 \mapsto b_1, \ldots, x_n \mapsto b_n$.
Wir definieren $J_f(b) := \beta(f)$, also $f$ ausgewertet mit der Belegung $\beta$.

# Von Formeln zu Junktoren

Zwei verschiedene Formeln $f \neq g$ können denselben Junktor $J_f = J_g$ definieren; $f$ und $g$ sind dann äquivalent, $f \Leftrightarrow g$ ist eine Tautologie (C1E). Die Formeln $f, g$ sind syntaktisch verschieden, aber semantisch gleich: Sie liefern dasselbe Ergebnis, egal welche Belegung $\beta$ wir auswerten.

Wir haben oben die Variablen $x_1, x_2, \ldots, x_n$ nummeriert, um es konkret und einfach zu machen; Belegungen $\beta$ entsprechen dann $n$–Tupeln $(a_1, a_2, \ldots, a_n) \in \{0,1\}^n$ von Wahrheitswerten $a_1, a_2, \ldots, a_n \in \{0,1\}$. Die folgende Sichtweise ist eleganter und allgemeiner und abstrakter:

Sei $V = \{x_1, x_2, \ldots, x_n\}$ die Menge der hier betrachteten Variablen. Mit $\{0,1\}^V$ bezeichnen wir die Menge aller Belegungen dieser Variablen, also der Abbildungen $\beta : V \to \{0,1\}$. Jeder Variablen $x_i \in V$ wird ein Wert $\beta(x_i) \in \{0,1\}$ zugeordnet. Sortiert wie oben sind dies $n$–Tupel.

Sei $f \in \mathscr{F}(\{\bot, \top\}, V, \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow\})$ eine aussagenlogische Formel. Diese definiert einen Junktor $J_f : \{0,1\}^V \to \{0,1\}$ gemäß $J_f(\beta) = \beta(f)$, das heißt $J_f$ ausgewertet auf $\beta$ ist $f$ ausgewertet mit der Belegung $\beta$. Anders gesagt: Der Junktor $J_f$ ist die Wahrheitstabelle der Formel $f$.

# Von Junktoren zu Formeln

Jede aussagenlogische Formel $f$ in den Variablen $x_1, \ldots, x_n$ definiert einen Junktor $J_f : \{0,1\}^n \to \{0,1\}$. Lässt sich umgekehrt jeder Junktor $J : \{0,1\}^n \to \{0,1\}$ durch eine Formel $f$ darstellen? Ja, sogar in DNF!

**Aufgabe:** Finden Sie Formeln (in DNF) für die folgenden Junktoren:

| $x_1$ | $x_2$ | $x_3$ | $J_1$ | $J_2$ | $J_3$ | $J_4$ |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 1 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 1 | 0 | 1 | 1 |

**Lösung:** Es gelingt mit $f_1 = x_1 \wedge x_2 \wedge x_3$ und $f_2 = \neg x_1 \wedge x_2 \wedge x_3$ sowie $f_3 = f_1 \vee f_2 = (x_1 \wedge x_2 \wedge x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) = x_2 \wedge x_3$ und schließlich $f_4 = (\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (\neg x_1 \wedge x_2 \wedge x_3) \vee (x_1 \wedge \neg x_2 \wedge x_3) \vee (x_1 \wedge x_2 \wedge x_3)$.

# Von Junktoren zu Formeln

Sie sehen hier ein sehr schönes Beispiel für mathematisches Vorgehen. Zunächst einmal sollten Sie lernen, mit offenen Augen durch die Welt zu gehen, naheliegende Fragen zu erkennen und sich explizit zu stellen! Hier geht es um ein **Umkehrproblem**, das tritt sehr häufig auf (B3A).

Bitte nehmen Sie sich die Zeit, versuchen Sie die Frage zunächst selbst, dann schrittweise anhand der vorgeschlagenen Beispiele und Aufgaben. Dann fällt der folgende Satz C1H für Sie nicht unerwartet vom Himmel, sondern Sie können ihn selbst entdecken und auch selbst beweisen!

☹ Die Frage scheint auf den ersten Blick schwierig, gar überwältigend. Vermutlich sehen Sie zunächst keine Lösung, keinen Ansatz, keine Idee.

☺ In solchen Fällen gibt es verschiedene Strategien. Betrachten Sie Beispiele, zunächst ganz kleine und einfache. . . dann etwas größere und kompliziertere. . . . Mit etwas Glück erkennen Sie dann ein Muster.

☺ Dieses Muster können Sie nun weiter testen. Schließlich können Sie damit eine Vermutung formulieren und idealerweise sogar beweisen. Genau dies geschieht hier. Es gelingt auch sonst erfreulich häufig!

# Von Junktoren zu Formeln

**Aufgabe:** Extrahieren Sie aus den Beispielen eine allgemeine Lösung!

**Lösung:** Wir beschaffen uns zunächst eine bequeme Schreibweise.

Sei $a = (a_1, \ldots, a_n) \in \{0,1\}^n$. Zu jeder Variablen $x_1, \ldots, x_n$ definieren wir das zugehörige Literal $[a_i]x_i$ durch $[1]x_i = x_1$ und $[0]x_i = \neg x_i$.

Für jede Belegung $\beta : x_i \mapsto b_i \in \{0,1\}$ gilt somit

$$\beta([a_i]x_i) = (a_i \Leftrightarrow b_i) = \begin{cases} 1 & \text{falls } a_i = b_i, \\ 0 & \text{falls } a_i \neq b_i. \end{cases}$$

Die konjunktive Klausel $c = \bigwedge_{i=1}^{n} [a_i]x_i$ definiert somit den Junktor $J_c : \{0,1\}^n \to \{0,1\}$ mit $J_c(b) = 1$ für $b = a$ und $J_c(b) = 0$ für $b \neq a$.

Allgemeiner sei $A \subseteq \{0,1\}^n$ eine beliebige Teilmenge.
Dann ist $d = \bigvee_{a \in A} \bigwedge_{i=1}^{n} [a_i]x_i$ eine disjunktive Normalform mit

$$J_d(b) = \begin{cases} 1 & \text{falls } b \in A, \\ 0 & \text{falls } b \notin A. \end{cases}$$

# Von Junktoren zu Formeln

## Satz C1H: kanonische Darstellung eines Junktors

Sei $n \in \mathbb{N}$. Jeder $n$–stellige Junktor $J : \{0,1\}^n \to \{0,1\}$ lässt sich durch eine aussagenlogische Formel $f$ darstellen: Es existiert $f$ mit $J_f = J$.

Genauer: Dies gelingt in disjunktiver / konjunktiver Normalform vermöge

$$d_J = \bigvee_{a\,:\,J(a)=1} \bigwedge_{i=1}^{n} [a_i] x_i,$$
$$c_J = \bigwedge_{a\,:\,J(a)=0} \bigvee_{i=1}^{n} [\neg a_i] x_i.$$

Wir nennen $d_J$ die **kanonische disjunktive Normalform** (CDNF) und $c_J$ die **kanonische konjunktive Normalform** (CCNF) des Junktors $J$.

**Beweis:** Sei $A = \{\, a \in \{0,1\}^n \mid J(a) = 1 \,\}$ die Menge aller $a \in \{0,1\}^n$, für die $J$ den Wert $J(a) = 1$ annimmt. Das nennen wir den Träger von $J$. Für $d = \bigvee_{a \in A} \bigwedge_{i=1}^{n} [a_i] x_i$ gilt $J_d = J$, wie in der Aufgabe ausgerechnet.

Der Junktor $\neg J$ wird demnach dargestellt durch $\bigvee_{a\,:\,\neg J(a)=1} \bigwedge_{i=1}^{n} [a_i] x_i$.
Somit wird $J = \neg\neg J$ dargestellt durch $c = \bigwedge_{a\,:\,J(a)=0} \bigvee_{i=1}^{n} [\neg a_i] x_i$. QED

# Normalform und Entscheidungsproblem

Wir wollen prüfen, ob eine aussagenlogische Formel $f$ eine Tautologie ist, also $\beta(f) = 1$ für *jede* Belegung $f$, oder wenigstens erfüllbar ist, also $\beta(f) = 1$ für *irgendeine* Belegung $\beta$. In Normalform gelingt dies leicht:

## Satz C1I: eine Lösung des Entscheidungsproblems

(1) Sei $c = \bigwedge_{i=1}^{\ell} \bigvee_{j=1}^{m_i} a_{ij}$ eine konjunktive Normalform.
Genau dann ist $c$ eine Tautologie, wenn $\ell = 0$ gilt, also $c = \top$.

(2) Sei $d = \bigvee_{i=1}^{\ell} \bigwedge_{j=1}^{m_i} a_{ij}$ eine disjunktive Normalform.
Genau dann ist $d$ unerfüllbar, wenn $\ell = 0$ gilt, also $d = \bot$.

**Beweis:** (1) Ist $\ell = 0$, so ist $c = \top$ eine Tautologie. Sei umgekehrt $\ell \geq 1$.
Für jedes Literal $a_{1j}$ gilt $a_{1j} = x$ oder $a_{1j} = \neg x$ mit einer Variablen $x$.
Im ersten Falle setzen wir $\beta(x) = 0$, im zweiten Falle hingegen $\beta(x) = 1$.
Jede Variable tritt höchstens einmal auf, also entsteht kein Widerspruch.
Für jede nicht-auftretende Variable $y$ setzen wir willkürlich $\beta(y) = 0$.
Für diese Belegung $\beta$ gilt $\beta(\bigvee_{j=1}^{m_1} a_{1j}) = 0$ und somit $\beta(c) = 0$.

Aussage (2) beweist man analog. Versuchen Sie es als Übung! QED

# Normalform und Entscheidungsproblem

Gegeben sei eine aussagenlogische Formel $f$ mit Variablen $x_1, \ldots, x_n$.
Gesucht ist eine zu $f$ äquivalente disjunktive Normalform $d$.

Hierzu kennen wir nun zwei komplementäre Methoden:

1. Ausmultiplizieren: Wende auf $f$ Distributivität an bis zu einer DNF.
2. Wahrheitstabelle: Bestimme zum Junktor $J_f$ die kanonische DNF.

☺ Die gute Nachricht: Beide Methoden gelingen immer.
Unser Problem wird dadurch also gelöst… zumindest prinzipiell.

☹ Die schlechte Nachricht: Beide Methoden sind oft kostspielig.
Im schlimmsten Fall verursachen sie **exponentiellen Aufwand**:

1. Die kurze Formel $(x_1^0 \vee x_1^1) \wedge \cdots \wedge (x_n^0 \vee x_n^1)$ mit $n$ Klauseln wird zur langen DNF $\bigvee_{a \in \{0,1\}^n} \bigwedge_{i=1}^{n} x_i^{a_i}$ mit $2^n$ Klauseln.
2. Bei $n$ Variablen benötigt die Wahrheitstabelle $2^n$ Einträge.
   Für $n = 500$ Variablen sind das $2^{500} \approx 3.27 \cdot 10^{150}$ Einträge.

Exponentieller Aufwand ist nur für sehr kleine $n$ überhaupt durchführbar.
Wir suchen daher Methoden mit **polynomiellen Aufwand** $\leq \text{const} \cdot n^c$.

# Eines der sieben Millennium-Probleme: $\mathrm{P}$ vs $\mathrm{NP}$

Wir untersuchen $f \in \mathrm{ALF}_n = \mathscr{F}(\{\bot, \top\}, \{x_1, x_2, \ldots, x_n\}, \{\neg, \wedge, \vee\})$.

## Definition C1J: Erfüllbarkeitsproblem (*satisfiability*, SAT)

**Tautologieproblem**, TAU: Eingabe $f \in \mathrm{ALF}$. Ist $f$ eine Tautologie?
**Erfüllbarkeitsproblem**, SAT: Eingabe $f \in \mathrm{ALF}$. Ist $f$ erfüllbar?

Beide Fragen sind prinzipiell über die Wahrheitstabelle $J_f$ entscheidbar, dies erfordert jedoch exponentiellen Aufwand, im schlimmsten Fall $\kappa 2^n$.

Beide Probleme sind äquivalent: Genau dann ist $f$ eine Tautologie, wenn die Negation $\neg f$ nicht erfüllbar ist. Meist betrachtet man daher nur SAT.

## Problem C1K: Gilt $\mathrm{P} = \mathrm{NP}$?

Erlaubt das Erfüllbarkeitsproblem eine Lösung in polynomieller Zeit?

Das ist eine der größten ungelösten Fragen der Komplexitätstheorie. Es ist eines der sieben Millennium-Probleme mit einem Preisgeld von 1Mio Dollar, siehe `de.wikipedia.org/wiki/Millennium-Probleme`.

☺ Zum Kontrast: Gauß B2C hat polynomiellen Aufwand, nur $\sim n^3$.

# Eines der sieben Millennium-Probleme: $\mathrm{P}$ vs $\mathrm{NP}$

Das Erfüllbarkeitsproblem ist keineswegs isoliert, sondern typisch.

**Prüfen vs Finden:** Dieses Problem illustriert ein Grundprinzip:

- Es ist oft leicht, für eine vorgelegte Lösung die Probe zu machen.
- Es ist meist viel schwerer, überhaupt eine Lösung zu finden.

Wir sehen dies hier ganz konkret für aussagenlogische Formeln $f$.

Für jede Belegung $\beta : \{0,1\}^n \to \{0,1\}$ können wir leicht $\beta(f)$ auswerten: Definition C1E ist ein Algorithmus in $\kappa(f)$ Schritten, linear in der Länge. Ein **Beleg für die Erfüllbarkeit** ist also in polynomieller Zeit prüfbar.

Einen **Beleg zu finden**, benötigt jedoch exponentielle Zeit $\kappa 2^n$ mit dem simplen Algorithmus, der die gesamte Wahrheitstabelle $J_f$ durchgeht. Die dringende Frage ist: Gelingt auch das Finden in polynomieller Zeit?

Lösungen des Erfüllbarkeitsproblems werden genutzt zum Design von Schaltkreisen, in automatischen Beweisen und künstlicher Intelligenz. Heuristische Verfahren lösen (gutartige) Fälle mit tausenden Variablen. Ein allgemeines, polynomielles Verfahren ist jedoch nicht bekannt.

# Schlussregeln: neue wahre Aussagen aus alten!

Eine **Schlussregel** erlaubt uns, aus bereits bewiesenen Aussagen neue Aussagen abzuleiten. Solche Regeln der „Textverarbeitung“ dienen uns zum strukturierten Aufbau mathematischer Beweise.

| | |
|---|---|
| $p \wedge q$ | Wir beweisen $p \wedge q$. |
| $q$ | Wir schließen $q$. |

| | |
|---|---|
| $p$ | Wir beweisen $p$. |
| $p \vee q$ | Wir schließen $p \vee q$. |

Ein **Beweis** eines Satzes entsteht durch schrittweise Schlussfolgerung, als ein logisch schlüssiger Weg von der Voraussetzung zur Behauptung.

| | |
|---|---|
| $p$ | Wir beweisen $p$. |
| $q$ | Wir beweisen $q$. |
| $p \wedge q$ | Wir schließen $p \wedge q$. |

| | |
|---|---|
| $p \vee q$ | Wir beweisen $p \vee q$. |
| $\neg p$ | Wir beweisen $\neg p$. |
| $q$ | Wir schließen $q$. |

Die ersten beiden oben gezeigten Schlussregeln entsprechen den Tautologien $p \wedge q \Rightarrow q$ und $p \Rightarrow p \vee q$. Die dritte Schlussregel zeigt, wie wir $p \wedge q$ beweisen, also als Folgerung ableiten. Die vierte Schlussregel zeigt, wie wir $p \vee q$ nutzen, also als Voraussetzung einsetzen können.

# Schlussregeln und Beweisverfahren

Schlussregeln entsprechen Tautologien, sie sind aber keine Aussagen, sondern Regeln für Beweise: Sie verarbeiten Aussagen, sie sind Vorlagen für Argumente, sie erklären, wie wir Beweise führen.

Die hier gezeigte Darstellung als Tabelle ist dekorativ und übersichtlich. Links steht die formale Schreibweise, rechts die umgangssprachliche Interpretation. Diese Regeln zeigen, wie wir die Aussagen $p \wedge q$ und $p \vee q$ *nutzen*, d.h. als Voraussetzung einsetzen, und auch, wie wir sie *beweisen*, d.h. als Folgerung ableiten. sie formulieren praktische Handlungsanweisungen, wie wir Beweise führen: Zunächst ich in der Vorlesung, dann Sie in den Übungen. Ich erkläre Ihnen die wichtigsten *Beweismuster*, damit Sie diese kennen, verstehen, anwenden lernen.

Diese Begriffe scheinen zunächst sperrig. Lohnt sich der Aufwand? Ja! Wir unterscheiden zwischen der *Behauptung* einer Aussage und dem *Beweis* einer Aussage. Dazu haben wir zunächst geklärt, wie Aussagen aufgebaut sind; wir können damit bereits Aussagen aussprechen und aufschreiben. Wir wollen nun klären, wie wir Aussagen beweisen.

# Die Schnittregel: Modus Ponens

Die folgende Implikation ist eine Tautologie, also allgemeingültig:

$$\big(p \wedge (p \Rightarrow q)\big) \Rightarrow q$$

Wir vereinbaren die **Schnittregel**, lat. **Modus Ponens**:

| | |
|---|---|
| $p \Rightarrow q$ | Wir beweisen die Aussage $p \Rightarrow q$. |
| $p$ | Wir beweisen die Aussage $p$. |
| $q$ | Wir schließen die Aussage $q$. |

**Beispiel:** Wenn es regnet, dann ist die Straße nass.
Jetzt regnet es. Daraus folgt: Die Straße ist nass.

☺ Die Schnittregel ist die einfachste und wichtigste Schlussregel, denn alle weiteren ergeben sich hieraus mit Hilfe von Tautologien:

## Definition C2A: Schlussregeln der Aussagenlogik

Alle Schlussregeln der Aussagenlogik entstehen
aus den Tautologien mit Hilfe der Schnittregel.

# Die Schnittregel: Modus Ponens

Die zentrale Aufgabe der mathematischen Logik ist es,
die Gesetze des logischen Schließens zu untersuchen.

Die Schnittregel heißt genauer *Modus ponendo ponens* (lat. ‘das zu Setzende setzend’), *Abtrennungsregel* oder *Implikationsbeseitigung*.

Sie ist die einfachste und wichtigste Schlussregel, alle weiteren unserer Schlussregeln ergeben sich hieraus mit Hilfe von Tautologien.

 Dieses Vorgehen stellt sicher, dass wir aus gegebenen wahren Aussagen weitere wahre Aussagen ableiten. Bei korrekter Anwendung der Schlussregeln können wir niemals eine falsche Aussage ableiten. Die Schlussregeln sind narrensicher, vornehm sagt man *konsistent*.

 Die Schlussregeln sagen uns genau, welche Beweisschritte wir als logische Schlüsse akzeptieren und welche nicht. Hingegen geben sie uns keinerlei Hinweis, welche die erlaubten Schritte wir in einem Beweis gehen sollen. Das ist eine Frage der Kreativität und der Erfahrung!

 Ich führe im Folgenden einige der wichtigsten Beweisformen aus. Aus Kapitel A und B kennen Sie schon wichtige, konkrete Beispiele!

# Beweis durch Kettenschluss

Die folgende Implikation ist eine Tautologie, genannt **Transitivität**:

$$\big((p \Rightarrow q) \wedge (q \Rightarrow r)\big) \quad \Rightarrow \quad (p \Rightarrow r)$$

Dank Schnittregel folgt hieraus der **Kettenschluss:**

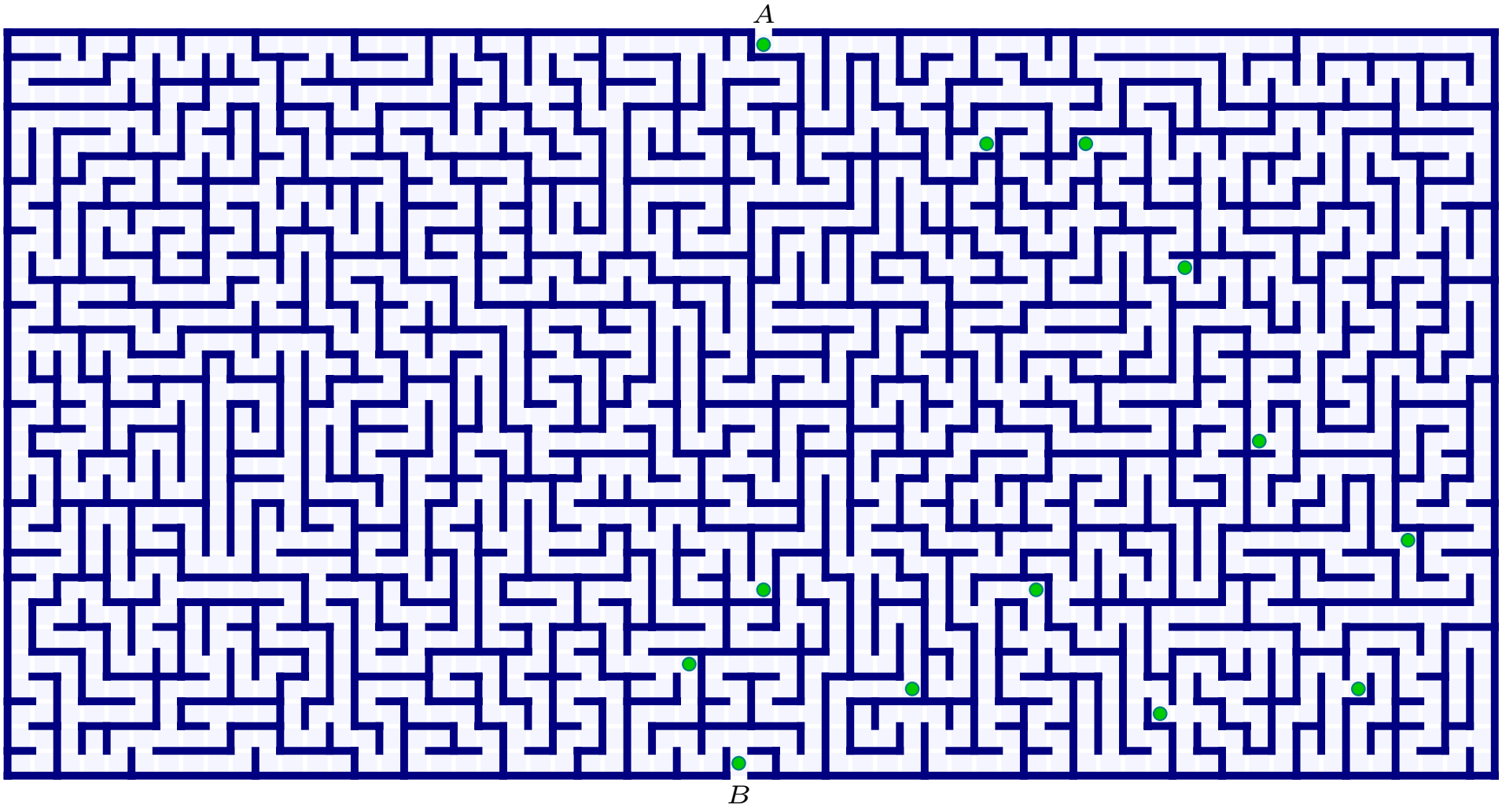
| | |
|---|---|
| $p \Rightarrow q$ | Wir beweisen die Aussage $p \Rightarrow q$. |
| $q \Rightarrow r$ | Wir beweisen die Aussage $q \Rightarrow r$. |
| $p \Rightarrow r$ | Wir schließen die Aussage $p \Rightarrow r$. |

**Beispiel:** Wenn es regnet, dann ist die Straße nass.
Wenn die Straße nass ist, dann besteht Schleudergefahr.
Daraus folgt: Wenn es regnet, dann besteht Schleudergefahr.

 Das ist eine nützliche **Beweisstrategie**: Um $p \Rightarrow r$ zu beweisen, führen wir Zwischenschritte ein und zeigen $p \Rightarrow q_1 \Rightarrow \cdots \Rightarrow q_n \Rightarrow r$.
Das unterteilt einen komplizierten Beweis in leichtere Schritte.

# Beweis durch Kettenschluss

Ein Beweis ist eine Kette von logischen Schlüssen: Ausgehend von der Voraussetzung A wird schrittweise die Folgerung B geschlossen. Zwischenschritte helfen bei der Exploration und der Konsolidierung.



# Wie detailliert muss ein Beweis sein?

Der Vergleich *Beweis – Methode – Weg* ist anschaulich und treffend!

Beweise in einem Lehrbuch für Studienanfänger sind recht ausführlich, für ein Expertenpublikum werden Beweise deutlich knapper formuliert. Was also ist ein Beweis genau? Wie detailliert ausgeführt muss er sein? Wie groß dürfen die logischen Sprünge maximal sein? Hierzu sind zwei Antworten möglich: formal dogmatisch oder sozial pragmatisch.

**Dogmatische Antwort:** In einem vollständig formalisierten Beweis ist jeder Schritt die Anwendung einer Schlussregel. Wir beginnen mit einer Liste von wahren Aussagen (Axiome, Voraussetzungen) und erweitern diese schrittweise durch logisches Schließen, jeweils mit Angabe der verwendeten Schlussregel. Am Ende steht die ersehnte Behauptung.

Im obigen Bild ist das der vollständig ausgeführte Lösungsweg, etwa als eine lange Folge von kleinen Beweisschritten, jeder davon ist elementar. Die Richtigkeit kann ein Computer mechanisch prüfen (*proof checker*). Für menschliche Leser ist die mechanische Prüfung sehr mühsam und wenig lehrreich, sie vermittelt meist keine Idee, Vision oder Inspiration.

# Wie detailliert muss ein Beweis sein?

**Pragmatische Antwort:** Traditionell schreiben wir Beweise nicht für Maschinen, sondern für Menschen. Es gibt immer mehr Ausnahmen, etwa in der Programmierung, aber denken wir an diese Vorlesung.

Für ein menschliches Gegenüber ist es üblich, nicht alle elementaren Schritte auszuführen, sondern den Beweisgang allein durch geeignete Zwischenpunkte abzustecken. Das ist effizienter, sowohl für den Sender als auch für den Empfänger. Die Zwischenpunkte sollen eng genug sein, sodass der Empfänger den Weg dazwischen selbst rekonstruieren kann.

Das rechte Maß, ob detailliert ausgeführt oder nur grob skizziert, hängt somit vom Empfänger ab! Beweise in Lehrbüchern sind recht detailliert ausgeführt, Artikel in Fachzeitschriften sind meist knapper formuliert und die Beweise nur grob skizziert. Das verschiebt die Beweislast vom Sender zum Empfänger. Die richtige Balance ist eine Kunst!

**Beispiel:** In dieser Vorlesung bemühe ich mich, alle entscheidenden Zwischenschritte anzugeben. Routinierte Rechnungen hingegen führe ich meist nicht aus, sondern übertrage sie Ihnen. Das ist effizienter.

# Beweis durch Fallunterscheidung

Ein Beweis durch **Fallunterscheidung** verläuft wie folgt:

| | |
|---|---|
| $p \Rightarrow p_1 \vee \ldots \vee p_n$ | Wir zerlegen $p$ in mehrere Fälle |
| $p_1 \Rightarrow q$ | Wir beweisen jeden Fall einzeln. |
| $\ldots$ | Also jeden Fall… |
| $p_n \Rightarrow q$ | … wirklich jeden! |
| $p \Rightarrow q$ | Wir schließen $p \Rightarrow q$. |

**Beispiel:** Wir wollen die folgende Aussage beweisen:
$q =$ (Es gibt irrationale Zahlen $x, y \in \mathbb{R} \setminus \mathbb{Q}$, sodass $x^y$ rational ist.)

**Beweis:** Wir betrachten die Zahlen $a = \sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ und $b = a^a$.
Es gilt $p_1 =$ ($b$ ist rational) oder $p_2 =$ ($b$ ist irrational).

- $p_1 \Rightarrow q$: Ist $b$ rational, so gilt Aussage $q$ dank $(x, y) = (a, a)$.
  Nachrechnen: $a^a = b \in \mathbb{Q}$.
- $p_2 \Rightarrow q$: Ist $b$ irrational, so gilt Aussage $q$ dank $(x, y) = (b, a)$.
  Nachrechnen: $b^a = (a^a)^a = a^{a^2} = a^2 = 2 \in \mathbb{Q}$.

Wir schließen: Die Behauptung $q$ ist wahr. QED

# Beweis durch Fallunterscheidung

 Beweisstrategie: Wir zeigen zunächst $p \Rightarrow p_1 \vee p_2 \vee \ldots \vee p_n$.
Dies ist eine **vollständige Fallunterscheidung** zur Voraussetzung $p$.
Die Wahl und geeignete Formulierung dieser Fälle erfordert Kreativität, ihre Vollständigkeit erfordert Sorgfalt. Die Fälle dürfen sich durchaus überlappen, aber sie müssen alles abdecken! Dann zeigen wir einzeln $p_1 \Rightarrow q$, $p_2 \Rightarrow q$, …, $p_n \Rightarrow q$; diese kleineren Beweise gelingen leichter.

Unser Beispiel beweist die Existenzaussage $q$, aber können Sie explizit eine Lösung nennen? Nein, das können Sie nicht: Sie wissen nicht, welcher Fall wirklich eintritt. Dieser Beweis ist nicht konstruktiv!

Das Problem versteckt sich hier in der harmlosen Oder-Aussage $p_1 \vee p_2$.
Klassisch ist diese immer wahr, dank ausgeschlossenem Dritten C1F.
Konstruktiv wissen wir aber nicht, welcher der beiden Fälle eintritt, also welches der Paare $(a, a)$ oder $(b, a)$ wirklich eine Lösung ist.

Der Beweis nutzt korrekt unsere Schlussregeln, und er ist vollständig.
Konstruktiv zu arbeiten kostet mehr Mühe, bringt aber auch mehr Ertrag.

 Der Satz von Gelfond–Schneider zeigt die Transzendenz von $\sqrt{2}^{\sqrt{2}}$.

# Äquivalenz als gegenseitige Implikation

Folgende Äquivalenz ist eine Tautologie, also allgemeingültig:

$$(p \Leftrightarrow q) \quad \Leftrightarrow \quad ((p \Rightarrow q) \wedge (q \Rightarrow p))$$

Dank Schnittregel können wir Äquivalenz zur Implikation abschwächen:

$$\frac{p \Leftrightarrow q}{p \Rightarrow q} \qquad \frac{p \Leftrightarrow q}{q \Rightarrow p}$$

Umgekehrt folgt die **Äquivalenz durch gegenseitige Implikation:**

$$\frac{\begin{array}{l} p \Rightarrow q \\ q \Rightarrow p \end{array}}{p \Leftrightarrow q}$$

Wir beweisen: $p$ impliziert $q$.
Wir beweisen: $q$ impliziert $p$.
Wir schließen: $p$ und $q$ sind äquivalent.

**Beispiel:** Für alle $x \in \mathbb{R}$ gilt die Äquivalenz $(x^2 = x) \Leftrightarrow (x \in \{0, 1\})$.

**Beweis:** „$\Leftarrow$“: Für $x = 0$ gilt $x^2 = x$, für $x = 1$ ebenso. (Lösungen prüfen)
„$\Rightarrow$“: Aus $x^2 = x$ folgt $x^2 - x = 0$, und daraus $x(x - 1) = 0$. Hieraus folgt $x = 0$ oder $x = 1$, also $x \in \{0, 1\}$ wie behauptet. (Alle Lösungen finden)

# Äquivalenz als gegenseitige Implikation

☺ Damit ist die Äquivalenz bewiesen. . . . In diesem einfachen Beispiel gelingt dies auch ebenso leicht direkt mit einer Folge von Äquivalenzen.

**Übung:** Die Implikation „$\Leftarrow$“ gilt in jedem Ring $(R, +, 0, \cdot, 1)$.
Die Umkehrung „$\Rightarrow$“ gilt zum Beispiel im Ring $\mathbb{Z}_6$ nicht mehr!

$$\text{Für alle } x \in \mathbb{Z}_6 \text{ gilt:} \quad (x^2 = x) \Leftrightarrow (x \in \{0, 1, 3, 4\})$$

Dies illustriert, dass sich beide Implikationen verschieden verhalten.
Auch deshalb lohnt es sich, sie getrennt zu untersuchen.

☺ Die Zerlegung in zwei Implikationen ist vor allem dann wichtig, wenn beide Implikationen verschiedene, unabhängige Wege gehen.

Diese Trennung zerlegt den Beweis in zwei leichtere Hälften.
Diese sind unabhängig, das erleichtert oft unsere Argumentation.

Zum Beweis einer Äquivalenz $p \Leftrightarrow q$ nutzen wir daher fast immer die Zerlegung in die beiden Implikationen $p \Rightarrow q$ und $q \Rightarrow p$.

☺ Für Implikationen haben wir maßgeschneiderte Beweistechniken, etwa die Kontraposition oder den indirekten Beweis durch Widerspruch.

# Implikation und Kontraposition

Die Schnittregel **Modus ponens** besagt:

| | | |
|---|---|---|
| $p \Rightarrow q$ | Wir beweisen $p \Rightarrow q$: | „Wenn's regnet, ist die Straße nass.“ |
| $p$ | Wir beweisen $p$: | „Es regnet.“ |
| $q$ | Wir schließen $q$: | „Die Straße ist nass.“ |

Die gültige Umkehrung dieser Regel heißt **Modus tollens**:

| | | |
|---|---|---|
| $p \Rightarrow q$ | Wir beweisen $p \Rightarrow q$: | „Wenn's regnet, ist die Straße nass.“ |
| $\neg q$ | Wir widerlegen $q$: | „Die Straße ist nicht nass.“ |
| $\neg p$ | Wir schließen $\neg p$: | „Es regnet nicht.“ |

Dies entspricht der **Kontraposition**:

$$\frac{p \Rightarrow q}{\neg q \Rightarrow \neg p} \qquad \frac{\neg q \Rightarrow \neg p}{p \Rightarrow q}$$

Modus ponens, Modus tollens und Kontraposition sind überall nützlich!
Sie haben jedoch böse Stiefbrüder und -schwestern: die **Trugschlüsse**.
Diese sollen sie weder akzeptieren noch selbst produzieren.

# Implikation und Kontraposition

**Aufgabe:** Sie verfügen über ein aktuelles Stuttgarter Telefonbuch, nicht als elektronische Datenbank, sondern ausgedruckt auf Papier.

Beweisen oder widerlegen Sie folgende Aussage: „Wenn die Nummer mit `456` beginnt, dann beginnt der zugehörige Name nicht mit `Sto`."

Wie würden Sie dies prüfen? naiv-ungeschickt? geschickt-effizient?

**Lösung:** Eine direkte Prüfung geht *alle* Paare $(\text{Name}, \text{Nummer})$ durch und prüft jeweils die Aussage $(\text{Nummer} = \texttt{456*}) \Rightarrow (\text{Name} \neq \texttt{Sto*})$.

Äquivalent ist die Kontraposition $(\text{Name} = \texttt{Sto*}) \Rightarrow (\text{Nummer} \neq \texttt{456*})$. Es genügt dazu, *nur* die kurze Liste dieser Namen durchzugehen.

Im vorliegenden Szenario ist die zweite Frage leichter zu beantworten als die erste, da das Telefonbuch schon nach Namen sortiert vorliegt!

☺ Das ist der eigentliche Nutzen der Kontraposition. Beide Aussagen, $p \Rightarrow q$ und $\neg q \Rightarrow \neg q$, sind logisch äquivalent. In der Praxis kommt es jedoch häufig vor, dass eine leichter zugänglich ist als die andere.

☺ Logik nützt nicht nur in Beweisen, sondern ebenso in vielen Abläufen wie Datenbankanfragen oder allgemein in der Programmierung.

# Implikation und Kontraposition

**Aufgabe:** Für jede ganze Zahl $a \in \mathbb{Z}$ gilt $(2 \mid a) \Leftrightarrow (2 \mid a^2)$.

**Lösung:** Wir beweisen die Äquivalenz durch die beiden Implikationen.
Wir zeigen $(2 \mid a) \Rightarrow (2 \mid a^2)$ direkt: Ist $a = 2c$ gerade, so auch $a^2 = 4c^2$.
Wir zeigen $(2 \mid a) \Leftarrow (2 \mid a^2)$ durch die Kontraposition $(2 \nmid a) \Rightarrow (2 \nmid a^2)$:
Aus $2 \nmid a$ folgt $a = 2c + 1$ mit $c \in \mathbb{Z}$. Es gilt $a^2 = 4c^2 + 4c + 1$, also $2 \nmid a^2$.

**Aufgabe:** Für jede ganze Zahl $a \in \mathbb{Z}$ gilt $(3 \mid a) \Leftrightarrow (3 \mid a^2)$.

**Lösung:** Euklidische Division ergibt $a = 3c + r$ mit $c \in \mathbb{Z}$ und $r \in \mathbb{Z}_3$.

$$\begin{aligned}
a = 3c &\Rightarrow a^2 = 9c^2 &&= 3(3c^2) \\
a = 3c + 1 &\Rightarrow a^2 = 9c^2 + 6c + 1 &&= 3(3c^2 + 2c) + 1 \\
a = 3c + 2 &\Rightarrow a^2 = 9c^2 + 12c + 4 &&= 3(3c^2 + 4c + 1) + 1
\end{aligned}$$

Das zeigt $(3 \mid a) \Rightarrow (3 \mid a^2)$ direkt und umgekehrt $(3 \mid a) \Leftarrow (3 \mid a^2)$ per Kontraposition. Noch genauer gilt sogar: Aus $3 \nmid a$ folgt $a^2 \operatorname{rem} 3 = 1$.

# Implikation und Kontraposition

**Aufgabe:** Prüfen Sie die Äquivalenz $(p \mid a) \Leftrightarrow (p \mid a^2)$ für $p$ prim.

**Lösung:** „$\Rightarrow$“: Für jede ganze Zahl $p \in \mathbb{Z}$ gilt: Aus $p \mid a$ folgt $p \mid a^2$.
Ausführlich: $p \mid a$ bedeutet $pq = a$ für ein $q \in \mathbb{Z}$, also gilt $p(qa) = a^2$.

„$\Leftarrow$“: Ist $p$ prim, so folgt aus $p \mid a \cdot a$ stets $p \mid a$ (siehe Definition A2K).

Alternative: $\mathbb{Z}_p$ ist ein Körper, aus $a \operatorname{rem} p \neq 0$ folgt also $a^2 \operatorname{rem} p \neq 0$.
Diese Rechnung beweist somit die Kontraposition $(p \nmid a) \Rightarrow (p \nmid a^2)$.

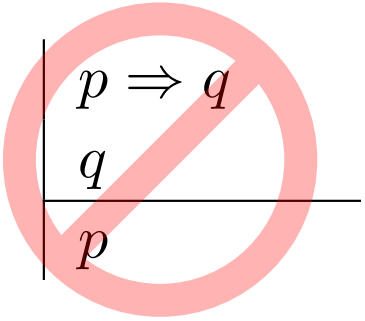
**Aufgabe:** Prüfen Sie ebenso $(4 \mid a) \overset{?}{\Leftrightarrow} (4 \mid a^2)$ und $(6 \mid a) \overset{?}{\Leftrightarrow} (6 \mid a^2)$.

**Lösung:** Es gilt „$(4 \mid a) \Rightarrow (4 \mid a^2)$“, aber nicht „$(4 \mid a) \Leftarrow (4 \mid a^2)$“.
Ein Gegenbeispiel ist $a = 2$: Es gilt $4 \mid 2^2$, aber $4 \nmid 2$.

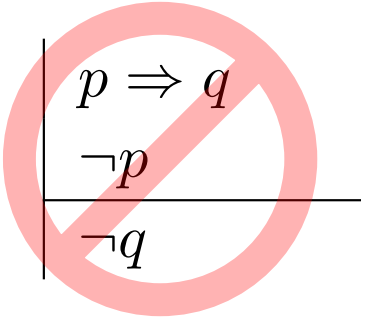
Es gilt „$(6 \mid a) \Rightarrow (6 \mid a^2)$“ und zudem „$(6 \mid a) \Leftarrow (6 \mid a^2)$“.
Dies folgt aus dem Fundamentalsatz der Arithmetik (A2J).

Alternative: Im Ring $\mathbb{Z}_6$ berechnen wir die Quadratabbildung $a \mapsto a^2$ gemäß $0 \mapsto 0$, $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 3$, $4 \mapsto 4$, $5 \mapsto 1$. Diese Rechnung zeigt $(6 \mid a) \Rightarrow (6 \mid a^2)$ und zudem die Umkehrung $(6 \nmid a) \Rightarrow (6 \nmid a^2)$.

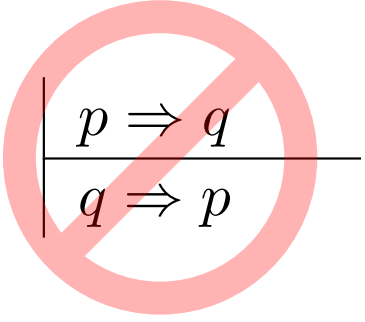
# Warnung vor Trugschlüssen!



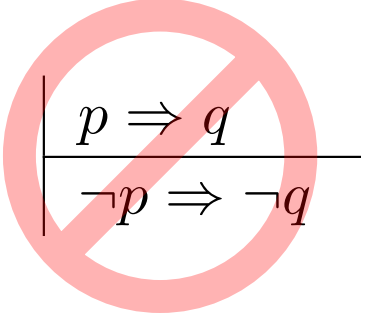

„Am Ende der Vorlesung trinke ich immer Wasser.“
„Ich trinke jetzt einen Schluck Wasser.“
„Also ist die Vorlesung zu Ende.“




„Wenn Sie alles wissen, dann bestehen Sie mit Eins.“
„Sie wissen aber noch nicht alles.“
„Also bestehen Sie nicht mit Eins.“




„Wenn ich Logik verstehe, dann bin ich glücklich.“
„Also, wenn ich glücklich bin, verstehe ich Logik.“




„Wenn Freitag ist, dann tanze ich.“
„Also, wenn nicht Freitag ist, dann tanze ich nicht.“

# Warnung vor Trugschlüssen!

Zur Illustration habe ich hier übertrieben einfache Beispiele gewählt, die besonders anschaulich und klar sind: *logisch* und *inhaltlich* falsch.

Das perfide Problem mit Trugschlüssen ist:

- Sie liefern nicht immer *wahre* Aussagen,
  deshalb sind sie als Schlussregeln ungeeignet.
- Sie liefern aber auch nicht immer *falsche* Aussagen,
  deshalb sind sie so verlockend und nicht leicht zu entlarven.

Das erklärt und betont noch einmal unsere Definition C2A: Wir wollen Schlussregeln, die aus wahren Aussagen nur wahre Aussagen ableiten. Diese Sicherheit garantieren wir durch die Vorlage von Tautologien!

## ♦ Definition C2A: Schlussregeln der Aussagenlogik

Alle Schlussregeln der Aussagenlogik entstehen
aus den Tautologien mit Hilfe der Schnittregel.

Genau das sind unsere Schlussregeln, nicht mehr und nicht weniger. Alles andere sind Trugschlüsse und potentiell gefährlich.

# Warnung vor Trugschlüssen!

**Aufgabe:** Überprüfen Sie, ob der folgende Schluss logisch gültig ist:

Wenn Herr K. ein Konservativer ist,
dann ist er für die Privatisierung.

Herr K. ist für die Privatisierung.

---

Herr K. ist ein Konservativer.

**Lösung:** Dies ist eine Instanz des folgenden Musters:

$$\frac{p \Rightarrow q \qquad q}{p}$$

Die Formel $(p \Rightarrow q) \wedge q \Rightarrow p$ ist jedoch keine Tautologie:

| $p$ | $q$ | $s = (p \Rightarrow q)$ | $t = (s \wedge q)$ | $t \Rightarrow p$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 |

# Warnung vor Trugschlüssen!

Der angegebene Schluss ist logisch ungültig, er ist ein Trugschluss!
Aus den vorliegenden Prämissen können wir nicht logisch schließen, dass Herr K. ein Konservativer ist. Anschaulich ist das vollkommen klar: Auch manche Nicht-Konservative können für die Privatisierung sein.

So weit so klar. Es gibt allerdings ein mögliches Missverständnis:
Der Schluss ist zwar logisch ungültig, die fälschlicherweise abgeleitete Aussage kann aber trotzdem wahr sein. Auch durch falsche Argumente und Schlüsse kann man (zufällig) auf eine wahre Aussage kommen.

Nehmen wir einmal an, auf anderen Wegen erfahren wir, dass Herr K. tatsächlich ein Konservativer ist, etwa durch seine eigene Aussage.
„Habe ich doch gleich gewusst, dass Herr K. ein Konservativer ist;
er ist ja auch für die Privatisierung, da war mir schon alles klar.“

⚠ Es kommt nicht auf die (hier zufällig richtige) Behauptung an, sondern auf die nachvollziehbare, logisch korrekte Begründung!
Das wird außerhalb der Mathematik oft sträflich missachtet.
Ehren Sie Ihr logisches Handwerk, schließen Sie richtig!

# Beweis durch Widerspruch

Schließlich kommen wir zum berühmt-berüchtigten, aber nützlichen **Beweis durch Widerspruch**, lat. **Reductio ad absurdum**:

$$\frac{(p \wedge \neg q) \Rightarrow \bot}{p \Rightarrow q}$$

Wir führen $p$ und $\neg q$ zum Widerspruch.
Wir schließen $p \Rightarrow q$.

♦ **Satz A1F: Irrationalität von $\sqrt{2}$, Euklid ca. 300 v.Chr.**

Es gibt keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$.

**Beweis:** Angenommen, es gäbe $r \in \mathbb{Q}$ mit $r^2 = 2$.
Rational bedeutet $r = a/b$ mit $a, b \in \mathbb{Z}$ und $b \neq 0$.
Zudem sei der Bruch $a/b$ vollständig gekürzt.
Aus der Gleichung $(a/b)^2 = 2$ folgt $a^2 = 2b^2$.
Daher ist $a^2$ gerade, also auch $a$, das heißt $a = 2\overline{a}$ mit $\overline{a} \in \mathbb{Z}$.
Einsetzen in $a^2 = 2b^2$ ergibt $4\overline{a}^2 = 2b^2$, also $2\overline{a}^2 = b^2$.
Daher ist $b^2$ gerade, also auch $b$, das heißt $b = 2\overline{b}$ mit $\overline{b} \in \mathbb{Z}$.
Somit ließe sich $a/b = \overline{a}/\overline{b}$ weiter kürzen. Das ist ein Widerspruch!
Also gibt es keine rationale Zahl $r \in \mathbb{Q}$ mit der Eigenschaft $r^2 = 2$. QED

# Beweis durch Widerspruch

Diese trickreich-raffinierte Beweisform heißt auch **indirekter Beweis**. Erfahrungsgemäß bereitet sie anfänglich am meisten Kopfzerbrechen. Formal folgt sie aus Schnittregel und Kontraposition:

$$\begin{aligned} ((p \wedge \neg q) \Rightarrow \bot) &\Leftrightarrow (\top \Rightarrow (\neg p \vee q)) \\ &\Leftrightarrow (\neg p \vee q) \\ &\Leftrightarrow (p \Rightarrow q) \end{aligned}$$

In Worten: Um $p \Rightarrow q$ zu beweisen, nehmen wir $p \wedge \neg q$ an und leiten einen Widerspruch ab. Also können $p$ und $\neg q$ nicht gleichzeitig gelten. Daraus schließen wir: Wenn $p$ gilt, dann muss auch $q$ gelten.

Das klassische Beispiel eines Widerspruchsbeweises ist, wie oben ausgeführt, die Irrationalität von $\sqrt{2}$: Keine rationale Zahl $r \in \mathbb{Q}$ erfüllt die Gleichung $r^2 = 2$. Wir formulieren und beweisen dies indirekt so:

Hier ist $p$ die Voraussetzung $r \in \mathbb{Q}$, und $q$ ist die Folgerung $r^2 \neq 2$. Zum Beweis nehmen wir $p$ und $\neg q$ an, also $r \in \mathbb{Q}$ und $r^2 = 2$, und führen dies zum Widerspruch. Dies zeigt $(p \wedge \neg q) \Rightarrow \bot$. Wir schließen $p \Rightarrow q$.

# Es gibt unendliche viele Primzahlen: durch Widerspruch

## Satz C2B: Unendlichkeit der Primzahlmenge

In den natürlichen Zahlen $\mathbb{N}_{\geq 1}$ gibt es unendlich viele Primzahlen.

Manchmal wird dies durch Widerspruch bewiesen, das ist möglich:

**Beweis durch Widerspruch „nach Euklid“:** Angenommen, es gäbe nur endlich viele Primzahlen $2 = p_1 < p_2 < \cdots < p_n$. Wir untersuchen $q = p_1 \cdot p_2 \cdots p_n + 1$. Keine der Primzahlen $p_i$ teilt $q$. Also ist $q$ prim. Wegen $q > p_n$ ist $q$ eine weitere Primzahl. Widerspruch! QED

**Fragen:** M Ist dieser Beweis gültig? I Können Sie damit arbeiten? L Was entgegnen Sie dem folgenden, bitter enttäuschten Vorwurf?

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$$

Ja, der Beweis ist logisch korrekt, doch eher schlechter Stil:

- Historisch falsch: So hat Euklid den Satz nicht bewiesen!
- Didaktisch unklug: Der Beweis provoziert Missverständnisse!
- Algorithmisch nutzlos: Es gelingt besser direkt und konstruktiv!

# Es gibt unendliche viele Primzahlen: konstruktiver Beweis

Zu $n \in \mathbb{N}_{\geq 2}$ sei $\mathrm{lpf}(n) := \min\{\, p \in \mathbb{N}_{\geq 2} \mid p \mid n \,\}$ der kleinste Faktor $\geq 2$.
Dies ist eine Primzahl, da $\geq 2$ und unzerlegbar: $\mathrm{lpf} =$ least prime factor.

## Satz C2c: Unendlichkeit der Primzahlmenge, konstruktiv

In den natürlichen Zahlen $\mathbb{N}_{\geq 1}$ gibt es unendlich viele Primzahlen:
Zu Primzahlen $p_1, p_2, \ldots, p_n$ ist $\mathrm{lpf}(p_1 \cdot p_2 \cdots p_n + 1)$ eine weitere.

**Beweis:** Wir haben $p = p_1 \cdot p_2 \cdots p_n \geq 1$ und $q = p + 1 \geq 2$. Dazu sei $q_1 = \mathrm{lpf}(q)$ der kleinste Primfaktor. Wir zeigen $q_1 \notin \{p_1, p_2, \ldots, p_n\}$:
Es gilt $q \operatorname{rem} q_1 = 0$ und $q \operatorname{rem} p_i = 1$, also $q_1 \neq p_i$. QED

☺ Dieser Beweis gefällt mir wesentlich besser. Er liefert objektiv mehr:

**Algorithmus:** Zu jeder Menge $M = \{\, p_1, p_2, \ldots, p_n \,\}$ von Primzahlen erhalten wir die echt größere Menge $M' = M \cup \{\, \mathrm{lpf}(p_1 p_2 \cdots p_n + 1) \,\}$.

Beispiel: $\{\} \mapsto \{2\} \mapsto \{2,3\} \mapsto \{2,3,7\} \mapsto \{2,3,7,43\} \mapsto \{2,3,7,13,43\} \mapsto \{2,3,7,13,43,53\} \mapsto \ldots$ Dies können wir beliebig lange fortführen!

M So entsteht die **Euklid–Mullin–Folge**, siehe `oeis.org/A000945`.

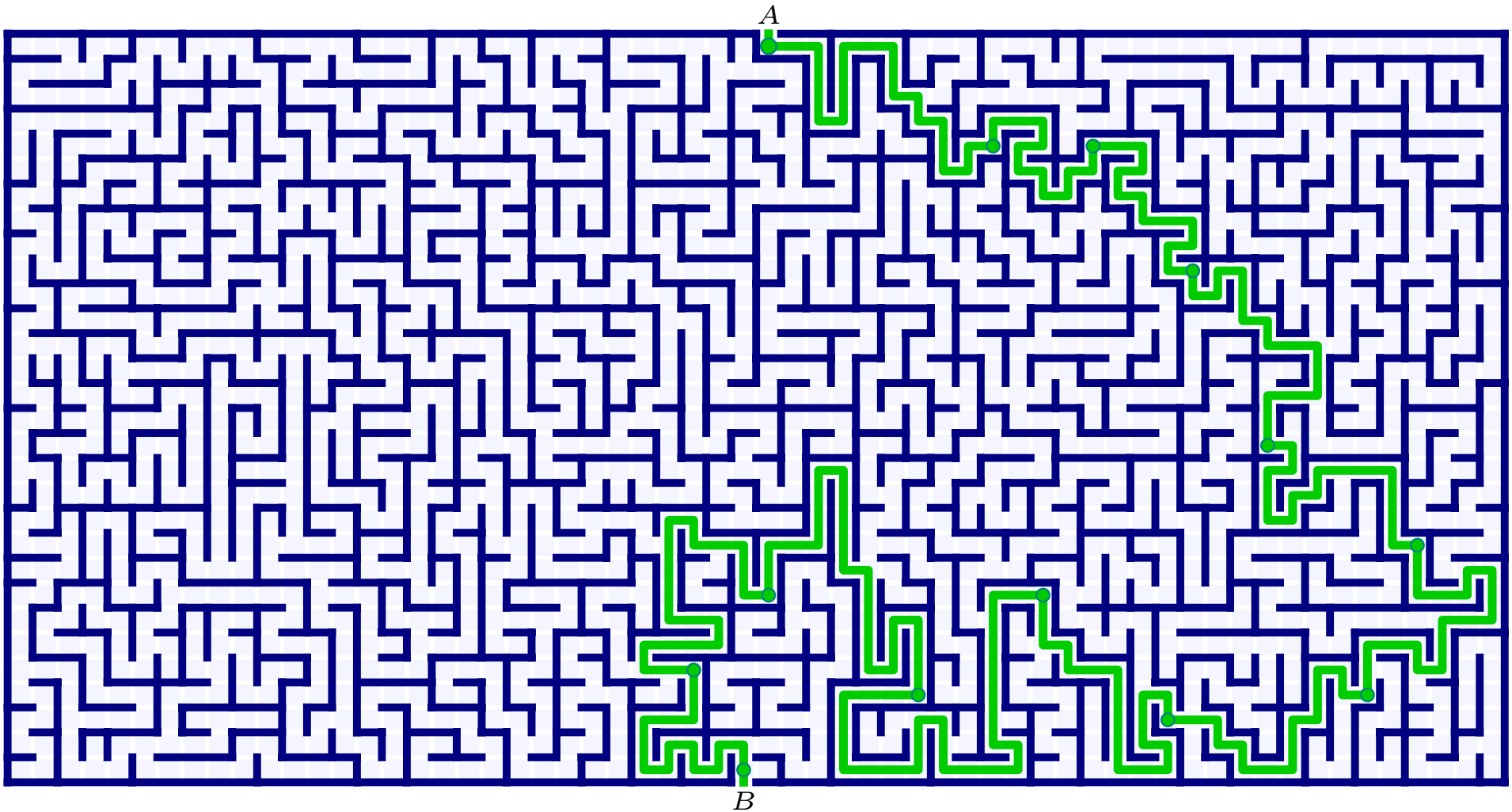
I Die effiziente Suche nach großen Primzahlen ist ein eigenes Gebiet.

# Ein Beweis ist eine Abfolge logischer Schlüsse.

| Satz | Beh | Voraussetzung |
|---|---|---|
| | | Folgerung |
| | Beweis | |

| Algo | Spez | Eingabe |
|---|---|---|
| | | Ausgabe |
| | Methode | |

| Lösung | Prob | Start |
|---|---|---|
| | | Ziel |
| | Weg | |



# Ein Beweis ist eine Abfolge logischer Schlüsse.

Ein Satz besteht immer aus zwei Teilen: Erstens seiner Behauptung „Wenn A, dann B“, also einer Voraussetzung A und einer Folgerung B. Zweitens aus einem Beweis, also einer Kette von logischen Schlüssen: Ausgehend von der Voraussetzung A wird die Folgerung B geschlossen.

Auch ein Algorithmus hat immer zwei Teile: Erstens seine Spezifikation, sie präzisiert die geforderte Eingabe und die zugesicherte Ausgabe. Zweitens eine Methode, also eine Kette von elementaren Operationen: Ausgehend von der Eingabe A wird die Ausgabe B produziert.

Ganz allgemein verläuft so die Lösung jedes Problems, etwa das Finden eines Weges in einem Labyrinth: Das Problem besteht aus der Angabe von Start und Ziel. Der Weg führt schrittweise vom Start zum Ziel. Diese graphische Analogie ist erstaunlich präzise und treffsicher.

Zwecks Aufgabenteilung werden Behauptung und Beweis getrennt, ebenso Spezifikation und Methode, allgemein Problem und Lösung. Insbesondere kann es auch mehrere mögliche Beweise / Methoden / Lösungen geben, oder noch keine/r ist bekannt und wird gesucht.

# Beweisen = Berechnen = Lösen

**Wie lösen Sie ein mathematisches Problem?** George Pólya erklärt hierzu in seinem Buch *How to solve it* die folgenden vier Phasen:

1. Zuerst müssen Sie das vorliegende Problem verstehen:
   Was ist das Ziel? Wo liegt der Start?
2. Anschließend machen Sie sich einen Plan:
   Was sind mögliche Wege vom Start zum Ziel?
3. Führen Sie Ihren Plan sorgfältig aus:
   Führt Ihr vermuteter Weg vom Start zum Ziel?
4. Schließlich schauen Sie zurück:
   Was lässt sich vereinfachen oder verbessern?

Das Suchen eines Weges ist meist kein geradliniger Prozess, sondern eher ein verzweigtes Erkunden und planvolles Probieren. Dazu benötigen Sie Kreativität und Sorgfalt, Geduld und Erfahrung! Es lässt sich erlernen, und dies erfordert vor allem viel eigene Übung.

Probleme zu lösen lernen Sie nur, indem Sie selbst Probleme lösen.

# Intuition oder Präzision? Beides!

Anschauung und Intuition sind überall nützlich, auch in der Mathematik. Sie bieten Motivation und Orientierung sowie schnelle Kommunikation.

Präzision und Formalisierung sind Markenzeichen mathematischer Sorgfalt; sie bieten Sicherheit, Vollständigkeit und dauerhafte Gültigkeit.

Für mathematische Arbeit benötigen Sie beides, Intuition und Präzision.

Idealerweise erkläre ich Ihnen beides. Das ist allerdings aufwändig.

Manchmal genügt die Anschauung: Ich nenne die Idee, Sie führen sie aus (und nutzen dabei Ihre bisherigen Fähigkeiten zur Formalisierung).

Manchmal genügt die Formalisierung: Ich führe sie aus, Sie fassen sie zusammen (und entwickeln dabei Ihre Anschauung und Intuition).

Auf dem Weg von der Idee / Vermutung zum Satz / Beweis wird die erste Formulierung meist präzisiert, manchmal auch angepasst und korrigiert. In der Ausführung (Rechnung, Beweis) stellt sich nämlich häufig heraus, dass zunächst Sonderfälle oder Einschränkungen vergessen wurden.

# Aussageformen aka Prädikate

**Beispiel:** Über den natürlichen Zahlen $\mathbb{N}$ betrachten wir die Ausdrücke

$$\begin{aligned} p(x) &:\Leftrightarrow (5 \leq x) \wedge (x < 10), \\ q(x,y) &:\Leftrightarrow x^2 = y. \end{aligned}$$

Hier ist $p$ zunächst noch keine Aussage, also weder wahr noch falsch, sondern eine **Aussageform** oder ein **Prädikat** für natürliche Zahlen.

Erst durch Einsetzen einer natürlichen Zahl $n \in \mathbb{N}$ wird die Aussageform $p$ zur Aussage $p(n)$; diese Aussage kann nun wahr oder falsch sein.

**Beispiele:** Die Aussage $p(9)$ ist wahr, doch $p(10)$ ist falsch.
Die Aussage $q(2,4)$ ist wahr, doch die Aussage $q(4,2)$ ist falsch.
Hingegen ist $q(x,4)$ eine Aussageform in der noch freien Variablen $x$.

## Definition C3A: Aussageform aka Prädikat

Ein **Prädikat** $p(x,y,\dots)$ in den Variablen $x,y,\dots$ ist ein Ausdruck, der zu einer Aussage wird durch Spezialisieren $(x,y,\dots) \mapsto (\alpha,\beta,\dots)$ der Variablen $x,y,\dots$ zu konkreten Objekten $\alpha,\beta,\dots$ im Diskursuniversum.

# Aussageformen aka Prädikate

Wir nennen hierbei das Prädikat $p(x)$ **einstellig**, wenn es nur eine freie Variable $x$ enthält. Ebenso definieren wir **zweistellige Prädikate** $q(x, y)$ oder **dreistellige Prädikate** $r(x, y, z)$ etc. Ein **nullstelliges Prädikat** $p$ ist ganz einfach eine Aussage, denn es hängt von keiner Variablen ab.

Wie schon bei Aussagen (C1A) lassen wir bei Prädikaten (C3A) vorerst offen, wie genau diese Ausdrücke aufgebaut sind. Zunächst nutzen wir naiv die Umgangssprache; je nach Anwendung präzisieren wir dann die verwendete Sprache (Syntax), im obigen Beispiel $(\mathbb{N}, +, \cdot, \leq)$.

Dabei muss unzweifelhaft klar sein, über welche Objekte wir sprechen! Typische Beispiele sind die natürlichen Zahlen $\mathbb{N}$, die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$, die komplexen Zahlen $\mathbb{C}$ … oder ganz allgemein über eine beliebige Menge $\Omega$ von Objekten.

Dies nennen wir das **Diskursuniversum**, engl. *universe of discourse*. Es umfasst jeweils alle Objekte, über die wir gerade sprechen wollen.

# Aussageformen aka Prädikate

⚠ Zu jeder Variablen $x$ müssen wir festlegen, welche Menge $\Omega_x$ sie durchläuft, also welche Ersetzungen $x \mapsto \alpha \in \Omega_x$ vorgesehen sind.

**Beispiel:** Wir betrachten weiterhin die obigen Prädikate.

$$\begin{aligned} p(x) &:\Leftrightarrow (5 \leq x) \wedge (x < 10) \\ q(x,y) &:\Leftrightarrow x^2 = y \end{aligned}$$

Diese können wir als Prädikate für natürliche Zahlen nutzen, das heißt, wir können $x, y$ durch natürliche Zahlen ersetzen.

Alternativ können wir $p$ und $q$ als Prädikate für ganze, rationale oder reelle Zahlen nutzen: Durch Ersetzen von $x, y$ durch reelle Zahlen $\alpha, \beta \in \mathbb{R}$ erhalten wir eine Aussage; diese kann wahr oder falsch sein. Für komplexe Zahlen $x \in \mathbb{C} \setminus \mathbb{R}$ hat $p$ keinen Sinn mehr, $q$ jedoch schon.

Hingegen hat es überhaupt keinen Sinn, für $x, y$ Farben einzusetzen, oder Personennamen oder MP3-Dateien oder Python-Programme; auch für diese Daten sind Prädikate denkbar, aber $p, q$ gehören nicht dazu.

# Aussageformen aka Prädikate

Wir arbeiten über dem Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ der ganzen Zahlen; implizit ist dabei auch die Vergleichsoperation $=$ eingeschlossen.

**Aufgabe:** Formulieren Sie das Prädikat $d(a, c)$ für „$a$ teilt $c$ in $\mathbb{Z}$“ und das Prädikat $u(a)$ für „$a$ ist unzerlegbar in $\mathbb{Z}$“ mit den Daten $(\mathbb{Z}, +, 0, \cdot, 1, =)$.

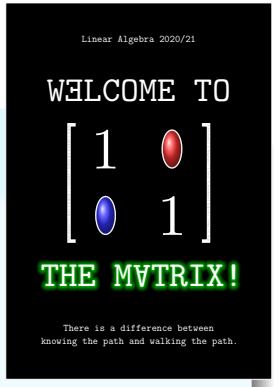
**Lösung:** Wir nutzen die Umgangssprache, denn erst die folgende Definition C3B bietet uns eine hilfreiche formale Ausdrucksweise.

$$\begin{aligned} d(a,c) &= (\text{Es existiert } b \in \mathbb{Z}, \text{ sodass } a \cdot b = c \text{ gilt.}) \\ u(a) \quad &= (\text{Für alle } b, c \in \mathbb{Z} \text{ gilt:} \\ &\qquad \text{Aus } a = b \cdot c \text{ folgt entweder } b = \pm 1 \text{ oder } c = \pm 1.) \end{aligned}$$

Die Quantoren „es existiert“ und „für alle“ benötigen wir sehr häufig. Daher lohnt es sich, hierfür eine bequeme und präzise Schreibweise einzuführen und die zugehörigen Rechenregeln genau zu untersuchen. Genau das ist unser Ziel in diesem Abschnitt zu Quantoren.

# Existenz- und Allquantor

In der Mathematik nutzen wir häufig **Quantoren**. Diese helfen, komplizierte Sachverhalte präzise und effizient auszudrücken.




## Definition C3B: Existenz- und Allquantor

Aus jedem Prädikat $p(x)$ erhalten wir folgende Aussagen:

| Aussage | Bedeutung | Name |
|---|---|---|
| $(\forall x : p(x))$ | Für jedes $x$ gilt die Aussage $p(x)$. | Allquantor |
| $(\exists x : p(x))$ | Für mindestens ein $x$ gilt $p(x)$. | Existenzquantor |

In diesen Aussagen ist die Variable $x$ nicht mehr frei sondern gebunden; sie kann nun nicht mehr durch ein konkretes Objekt $\alpha$ ersetzt werden. Sie kann jedoch überall durch eine neue Variable $y$ ersetzt werden: $\forall x : p(x)$ und $\forall y : p(y)$ sind äquivalent, ebenso $\exists x : p(x)$ und $\exists y : p(y)$.

Ist $q(x, y, \dots)$ ein Prädikat in mehreren Variablen $x, y, \dots$, so wird in $\forall x : q(x, y, \dots)$ und $\exists x : q(x, y, \dots)$ nur die Variable $x$ gebunden: Wir erhalten Aussageformen in den verbleibenden Variablen $y, \dots$.

# Existenz- und Allquantor

Sprechen wir nur über endlich viele Objekte $\Omega = \{a_1, a_2, \ldots, a_n\}$, so gilt:

$$\begin{aligned} \forall x \in \Omega : p(x) \quad &\Leftrightarrow \quad p(a_1) \wedge p(a_2) \wedge \ldots \wedge p(a_n) \\ \exists x \in \Omega : p(x) \quad &\Leftrightarrow \quad p(a_1) \vee p(a_2) \vee \ldots \vee p(a_n) \end{aligned}$$

In der Literatur finden Sie daher auch folgende Schreibweisen:

$$\bigwedge_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigwedge_{x \in \Omega} p(x) \quad \text{für} \quad \forall x \in \Omega : p(x)$$

$$\bigvee_{i=1}^{n} p(a_i) \quad \text{oder allgemein} \quad \bigvee_{x \in \Omega} p(x) \quad \text{für} \quad \exists x \in \Omega : p(x)$$

Wir nutzen die Wahrheitswerte $0 =$ falsch oder $1 =$ wahr, wobei $0 < 1$.
Damit erklären wir zu Quantoren die Wahrheitswerte wie folgt:

$$\begin{aligned} \langle\, \forall x : p(x) \,\rangle \;&:=\; \min_{x \in \Omega} \langle\, p(x) \,\rangle \quad \in \{0, 1\} \\ \langle\, \exists x : p(x) \,\rangle \;&:=\; \max_{x \in \Omega} \langle\, p(x) \,\rangle \quad \in \{0, 1\} \end{aligned}$$

Die explizite Angabe der Menge $\Omega$ ist redundant, aber sehr hilfreich.

# Existenz- und Allquantor

**Beispiel:** Wir arbeiten im Ring $(\mathbb{Z}, +, 0, \cdot, 1)$ der ganzen Zahlen.
Formulieren Sie teilbar, invertierbar, unzerlegbar und prim im Ring $\mathbb{Z}$ sowie Euklids Lemma (1) umgangssprachlich und (2) mit Quantoren.

$$
\begin{aligned}
a \mid c \quad &:\Leftrightarrow \quad (\exists b\,(a \cdot b = c)) \\
&\Leftrightarrow \quad \exists b \,:\, a \cdot b = c \\
\text{invertierbar}(a) \quad &:\Leftrightarrow \quad \exists b \,:\, a \cdot b = 1 \\
&\Leftrightarrow \quad a \mid 1 \\
\text{unzerlegbar}(a) \quad &:\Leftrightarrow \quad (\forall b\,(\forall c\,((a = b \cdot c) \Rightarrow ((b \mid 1)\ \dot\vee\ (c \mid 1))))) \\
&\Leftrightarrow \quad \forall b, c \,:\, a = b \cdot c \;\Rightarrow\; b \mid 1 \ \dot\vee\ c \mid 1 \\
\text{prim}(a) \quad &:\Leftrightarrow \quad \neg(a \mid 1) \wedge (\forall b\,(\forall c\,((a \mid b \cdot c) \Rightarrow ((a \mid b) \vee (a \mid c))))) \\
&\Leftrightarrow \quad a \nmid 1 \ \wedge\ \forall b, c \,:\, a \mid b \cdot c \;\Rightarrow\; a \mid b \vee a \mid c
\end{aligned}
$$

Euklids Lemma über $\mathbb{Z}$ sagt $\forall a : \text{prim}(a) \Leftrightarrow (a = 0 \ \dot\vee\ \text{unzerlegbar}(a))$.

Wir dürfen Klammern weglassen, solange die Bedeutung klar bleibt.
Das Trennzeichen ‘:’ dient der besseren Lesbarkeit und darf entfallen.
Die Abkürzung $\forall x, y$ steht für $\forall x\,\forall y$. Ebenso steht $\exists x, y$ kurz für $\exists x\,\exists y$.

# Existenz- und Allquantor

Um Klammern zu sparen nutzen wir „Potenz vor Punkt vor Strich“.
Bei logischen Operatoren vereinbaren wir entsprechend die Rangfolge
Negation vor Konjunktion vor Disjunktion vor Implikation vor Äquivalenz.

**Aufgabe:** Prüfen Sie anhand obiger Definitionen sorgfältig nach,
ob die Zahl $a = 0, 1, 2$ in $\mathbb{Z}$ unzerlegbar bzw. prim ist. Das hilft!

**Lösung:** Wir setzen $a = 0, 1, 2$ in diese beiden Prädikate ein:

$$\begin{array}{lll}
\mathrm{unzerlegbar}(0) & \Leftrightarrow\ \forall b, c : 0 = b \cdot c \ \Rightarrow\ b \mid 1 \ \dot\vee\ c \mid 1 & \text{falsch (0)} \\
\mathrm{prim}(0) & \Leftrightarrow\ 0 \nmid 1 \ \wedge\ \forall b, c : 0 \mid b \cdot c \ \Rightarrow\ 0 \mid b \vee 0 \mid c & \text{wahr} \\
 & & \\
\mathrm{unzerlegbar}(1) & \Leftrightarrow\ \forall b, c : 1 = b \cdot c \ \Rightarrow\ b \mid 1 \ \dot\vee\ c \mid 1 & \text{falsch (1)} \\
\mathrm{prim}(1) & \Leftrightarrow\ 1 \nmid 1 \ \wedge\ \forall b, c : 1 \mid b \cdot c \ \Rightarrow\ 1 \mid b \vee 1 \mid c & \text{falsch (1')} \\
 & & \\
\mathrm{unzerlegbar}(2) & \Leftrightarrow\ \forall b, c : 2 = b \cdot c \ \Rightarrow\ b \mid 1 \ \dot\vee\ c \mid 1 & \text{wahr} \\
\mathrm{prim}(2) & \Leftrightarrow\ 2 \nmid 1 \ \wedge\ \forall b, c : 2 \mid b \cdot c \ \Rightarrow\ 2 \mid b \vee 2 \mid c & \text{wahr}
\end{array}$$

Beweis durch Gegenbeispiel: (0) $(b, c) = (0, 0)$ und (1) $(b, c) = (1, 1)$.
(1') Die Forderung $a \nmid 1$ schließt alle invertierbaren Elemente aus.

# Beweisverfahren für Existenz- und Allquantor

Quantoren erhalten ihre Bedeutung durch die folgenden Schlussregeln.
Für den Allquantor $\forall$ nutzen wir **Spezialisieren** und **Verallgemeinern**:

| | |
|---|---|
| $\forall x : p(x)$ | $p(\alpha)$ für jedes $\alpha$ / für alle $\alpha$ |
| $p(\alpha)$ für jedes $\alpha$ (beliebig gewählt) | $\forall x : p(x)$ |

Für den Existenzquantor $\exists$ nutzen wir **Auswählen** und **Konstruieren**:

| | |
|---|---|
| $\exists x : p(x)$ | $p(\alpha)$ für (mindestens) ein $\alpha$ |
| $p(\alpha)$ für ein $\alpha$ (geeignet gewählt) | $\exists x : p(x)$ |

Das präzisiert die Bedeutung von „für alle“ und „es existiert“.

Links steht jeweils, wie wir eine quantifizierte Aussage *nutzen*,
also als Voraussetzung einsetzen und daraus Folgerungen ziehen.

Rechts steht, wie wir die quantifizierte Aussage *beweisen*,
also als eine Folgerung aus gegebenem Wissen ableiten.

# Rechenregeln für Existenz- und Allquantor

Die Reihenfolge der Quantoren ist wesentlich! Beispiel $p(a,b) = (a < b)$:

$$\forall a : \exists b : a < b \quad \text{also ausgeschrieben} \quad \forall a \underbrace{(\exists b\,(a < b))}_{q(a)}$$

$$\exists b : \forall a : a < b \quad \text{also ausgeschrieben} \quad \exists b \underbrace{(\forall a\,(a < b))}_{r(b)}$$

In $(\mathbb{Z}, <)$ ist die erste Aussage wahr, die zweite jedoch falsch!
Allquantoren vertauschen untereinander, ebenso Existenzquantoren:

$$\forall x : \forall y : p(x,y) \quad \Leftrightarrow \quad \forall y : \forall x : p(x,y)$$
$$\exists x : \exists y : p(x,y) \quad \Leftrightarrow \quad \exists y : \exists x : p(x,y)$$

Wenn wir einen Allquantor über einen Existenzquantor nach vorne ziehen, so bleibt die Aussage wahr, wird dabei aber schwächer:

$$\exists x : \forall y : p(x,y) \quad \underset{\not\Leftarrow}{\Longrightarrow} \quad \forall y : \exists x : p(x,y)$$

Beispiel $p(x,y) =$ „$x$ ist Mutter von $y$“: Zu jedem Menschen existiert eine Mutter, aber es existiert keine Mutter zu allen Menschen gemeinsam.

# Rechenregeln für Existenz- und Allquantor

Wir kennen die beiden Regeln von **De Morgan** (C135, endlicher Fall):

$$\neg(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \quad \Leftrightarrow \quad (\neg p_1) \vee (\neg p_2) \vee \cdots \vee (\neg p_n)$$
$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \quad \Leftrightarrow \quad (\neg p_1) \wedge (\neg p_2) \wedge \cdots \wedge (\neg p_n)$$

Allgemein gelten die Regeln von **De Morgan für Quantoren**:

$$\neg(\forall x : p(x)) \quad \Leftrightarrow \quad \exists x : (\neg p(x))$$
$$\neg(\exists x : p(x)) \quad \Leftrightarrow \quad \forall x : (\neg p(x))$$

Um eine Allaussage $\forall x : p(x)$ zu *beweisen*, müssen wir $p(\alpha)$ für jedes $\alpha$ nachweisen. Um sie zu *widerlegen*, genügt ein einziges Gegenbeispiel; das ist genau die Aussage der ersten Regel von De Morgan.

Die Existenzaussage $\exists x : p(x)$ beweisen wir, indem wir ein $\alpha$ vorweisen, das $p(\alpha)$ erfüllt. Die Negation $\neg\exists x : p(x)$ besagt, kein $\alpha$ erfüllt $p(\alpha)$; das ist äquivalent zu $\forall x : \neg p(x)$, also alle $\alpha$ erfüllen nicht $p(\alpha)$.

# Rechenregeln für Existenz- und Allquantor

Ebenso verallgemeinern sich die Distributivgesetze (C135):

$$\begin{aligned}(\forall x : p(x)) \vee q &\quad\Leftrightarrow\quad \forall x : (p(x) \vee q)\\ (\exists x : p(x)) \wedge q &\quad\Leftrightarrow\quad \exists x : (p(x) \wedge q)\end{aligned}$$

Hier helfen die Klammern zur Präzisierung. Weiterhin gilt:

$$\begin{aligned}(\forall x : p(x)) \wedge q &\quad\Leftrightarrow\quad \forall x : (p(x) \wedge q)\\ (\exists x : p(x)) \vee q &\quad\Leftrightarrow\quad \exists x : (p(x) \vee q)\end{aligned}$$

Ebenso verhalten sich Quantoren bezüglich Implikationen:

$$\begin{aligned}(\forall x : (p \Rightarrow q(x))) &\quad\Leftrightarrow\quad (p \Rightarrow (\forall x : q(x)))\\ (\exists x : (p \Rightarrow q(x))) &\quad\Leftrightarrow\quad (p \Rightarrow (\exists x : q(x)))\\ (\forall x : (p(x) \Rightarrow q)) &\quad\Leftrightarrow\quad ((\exists x : p(x)) \Rightarrow q)\\ (\exists x : (p(x) \Rightarrow q)) &\quad\Leftrightarrow\quad ((\forall x : p(x)) \Rightarrow q)\end{aligned}$$

Das folgt aus den obigen Regeln dank $(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$. Wir nutzen diese Regeln insbesondere zum **Beweis durch Fallunterscheidung**.

# Existenz und Eindeutigkeit: Definition

## Definition C3c: Existenz und Eindeutigkeit als Quantor

Für $\exists x$ sagen wir zur Betonung auch „Es existiert *mindestens* ein $x$“.

$$\exists^{\geq 1} x : p(x) \quad :\Leftrightarrow \quad \exists x : p(x)$$

Wir definieren den Quantor „Es existiert *höchstens* ein $x$“ wie folgt:

$$\exists^{\leq 1} x : p(x) \quad :\Leftrightarrow \quad (\forall x, y : (p(x) \land p(y)) \Rightarrow (x = y))$$

Wir definieren den Quantor „Es existiert *genau* ein $x$“ wie folgt:

$$\exists! \, x : p(x) \quad :\Leftrightarrow \quad (\exists x : p(x)) \land (\forall x, y : (p(x) \land p(y)) \Rightarrow (x = y))$$

Manche Autoren schreiben statt $\exists! \, x$ daher suggestiv $\exists^{=1} x$.

**Beispiele:**

| Aussage | über $\mathbb{Q}$ | über $\mathbb{R}_{\geq 0}$ | über $\mathbb{R}$ |
|---|---|---|---|
| $\exists^{\geq 1} x : x^2 = 2$ | falsch | wahr | wahr |
| $\exists^{\leq 1} x : x^2 = 2$ | wahr | wahr | falsch |
| $\exists^{=1} x : x^2 = 2$ | falsch | wahr | falsch |

# Existenz und Eindeutigkeit: ein Beispiel

**Aufgabe:** Sei $(M, \cdot, 1)$ ein Monoid. Formulieren Sie mit Quantoren:
(1) $\mathrm{Inv}(a)$: „Das Element $a \in M$ ist im Monoid $(M, \cdot, 1)$ invertierbar."
(2) $\mathrm{Lös}(a)$: „Für jedes $b \in M$ ist $a \cdot x = b$ in $M$ eindeutig lösbar."
(3) Beweisen Sie schließlich: $\forall a \in M : (\mathrm{Inv}(a) \Rightarrow \mathrm{Lös}(a))$

**Lösung:** Diese Prädikate lauten in Quantorenschreibweise:

$$\text{(1)} \quad \mathrm{Inv}(a) \quad :\Leftrightarrow \quad \exists a' \in M \,:\, a \cdot a' = 1 \,\wedge\, a' \cdot a = 1$$

$$\text{(2)} \quad \mathrm{Lös}(a) \quad :\Leftrightarrow \quad \forall b \in M \;\; \exists! x \in M \,:\, a \cdot x = b$$

(3) Vorgelegt seien $a, a' \in M$ mit $a \cdot a' = 1$ und $a' \cdot a = 1$. Sei $b \in M$.

(3a) Existenz: Das Element $x := a' \cdot b$ erfüllt $a \cdot x = b$, denn

$$a \cdot x \overset{\text{Def}}{=} a \cdot (a' \cdot b) \overset{\text{Ass}}{=} (a \cdot a') \cdot b \overset{\text{rInv}}{=} 1 \cdot b \overset{\text{lNtr}}{=} b.$$

(3b) Eindeutigkeit: Für $x, y \in M$ gelte $a \cdot x = b$ und $a \cdot y = b$. Dann folgt:

$$x \overset{\text{lNtr}}{=} 1 \cdot x \overset{\text{lInv}}{=} (a' \cdot a) \cdot x \overset{\text{Ass}}{=} a' \cdot (a \cdot x)$$
$$\overset{\text{Vor}}{=} a' \cdot (a \cdot y) \overset{\text{Ass}}{=} (a' \cdot a) \cdot y \overset{\text{lInv}}{=} 1 \cdot y \overset{\text{lNtr}}{=} y.$$

# Existenz und Eindeutigkeit: weitere Beispiele

Die Frage der Existenz und Eindeutigkeit begegnet uns sehr häufig in der Mathematik, und eigentlich auch sonst überall bei der Lösung von relevanten Problemen. Sie kennen bereits erste wichtige Beispiele:

**Division mit Rest** (A2A). Zu je zwei ganzen Zahlen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}^*$ existiert genau ein Paar $q, r \in \mathbb{Z}$ mit $a = bq + r$ und $0 \leq r < |b|$.

**Zifferndarstellung** (A2B). Zu jeder natürlichen Zahl $n \in \mathbb{N}$ existiert genau eine Zifferndarstellung $x \in \mathbb{Z}_B^{(\mathbb{N})}$ zur Basis $B \in \mathbb{N}_{\geq 2}$.

**Fundamentalsatz der Arithmetik** (A2J). Zu jeder natürlichen Zahl $a \in \mathbb{N}_{\geq 1}$ existiert genau eine Primfaktorzerlegung, also eine Familie von Primzahlen $p_1 \leq p_2 \leq \cdots \leq p_n$ in $\mathbb{N}$ mit der Eigenschaft $a = p_1 p_2 \cdots p_n$.

**Invertierbarkeit von Matrizen** (B2D). Sei $A \in \mathbb{K}^{n \times n}$ invertierbar und $b \in \mathbb{K}^n$. Zur Gleichung $Ax = b$ existiert genau eine Lösung $x \in \mathbb{K}^n$.

**Lagrange–Interpolation** (B3A). Durch beliebige Datenpunkte $(x_0, y_0), \ldots, (x_n, y_n) \in \mathbb{K}^2$ verläuft genau ein Polynom $P \in \mathbb{K}[X]_{\leq n}$.

**Minimum-Maximum-Prinzip** (B3B). Zu jedem Spielbrett $\Omega \subset \mathbb{Z}^2$ und beliebigen Randdaten existiert genau eine Gewinnerwartung $u : \Omega \to \mathbb{R}$.

# Existenz und Eindeutigkeit: typisches Alltagsbeispiel

**Beispiel:** Ein Beispiel aus dem Alltag, nach einer wahren Begebenheit: „Zum Wandern treffen wir uns früh um 8 Uhr am Parkplatz im Wald.“

Dahinter stecken zwei wichtige Annahmen / Forderungen / Probleme:

1. Es gibt tatsächlich einen Parkplatz im Wald
2. . . . und er ist eindeutig; alle meinen denselben.

Andernfalls ist die Verabredung schlecht formuliert und wird scheitern.
Existenz und Eindeutigkeit sind meist die unabdingbare Grundlage!

Praktisch gesehen schließen sich noch zwei weitere Probleme an:

3. Wir finden effektiv einen Weg zu dem (!) Parkplatz im Wald
4. . . . und zwar ausreichend effizient, schnell genug bis 8 Uhr.

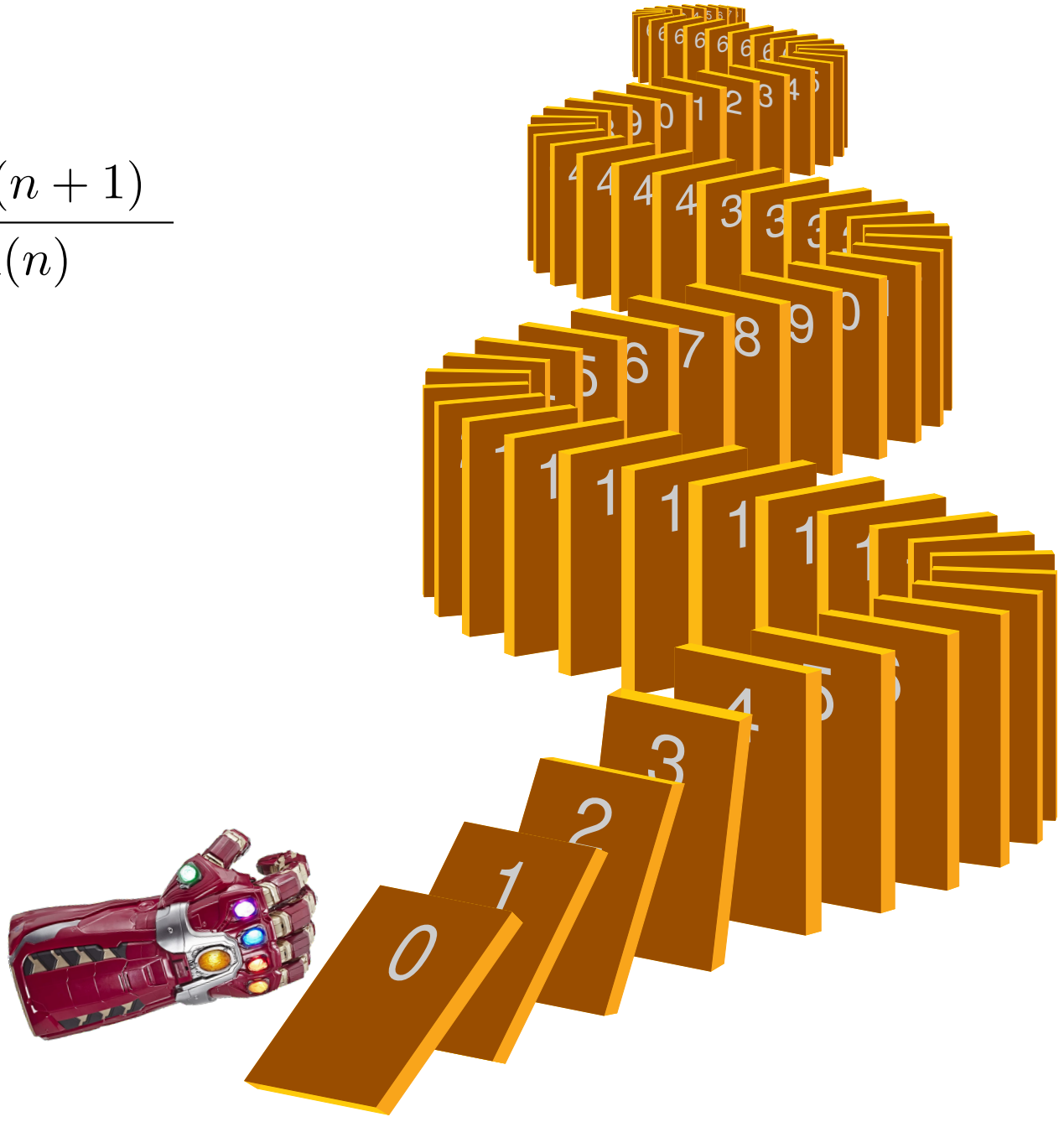
 Genauso verhält es sich nahezu immer beim Lösen von Problemen, insbesondere in der Mathematik, aber erstaunlich oft auch überall sonst:

Das gestellte Problem sollte idealerweise genau eine Lösung haben, wir wollen diese effektiv herstellen und zudem möglichst effizient.

Welche der obigen Probleme können Sie lösen? effektiv oder effizient?

# Vollständige Induktion: the road to infinity!

$$\frac{A(0) \qquad A(n) \Rightarrow A(n+1)}{\forall n \in \mathbb{N} : A(n)}$$



# Vollständige Induktion: the road to infinity!

Sie wollen für jede natürliche Zahl $n \in \mathbb{N}$ die Aussage $A(n)$ beweisen.
Das ist insgesamt eine unendliche Familie $(A(n))_{n\in\mathbb{N}}$ von Aussagen!
Ist das überhaupt möglich? Wie können Sie das jemals erreichen?

☹ Sie haben, wie jeder Mensch, natürlich nur endlich viel Zeit!
Es gibt demgegenüber aber unendlich viele natürliche Zahlen.

Sie können nicht selbst hingehen und alles einzeln prüfen,
das ist zu weit, zu viel, zu lang, Sie würden damit nie fertig.

Sie benötigen eine Maschine, die das effizient für Sie erledigt.
Die vollständige Induktion leistet genau das, klar und effizient!

☺ Per Induktion beweisen Sie die Aussage $A(n)$ für jedes $n \in \mathbb{N}$:

| | |
|---|---|
| $A(0)$ | Induktionsanfang: Sie beweisen die Aussage $A(0)$. |
| $A(n) \Rightarrow A(n+1)$ | Induktionsschritt: Sie beweisen $A(n) \Rightarrow A(n+1)$. |
| $\forall n \in \mathbb{N} : A(n)$ | Induktionsschluss: die Allaussage $\forall n \in \mathbb{N} : A(n)$. |

Der Induktionsschritt ist die Implikation $A(n) \Rightarrow A(n+1)$, dabei ist $A(n)$
die (Induktions)Voraussetzung und $A(n+1)$ die (Induktions)Folgerung.

# Vollständige Induktion: the road to infinity!

## Satz C4A: Prinzip der vollständigen Induktion, erste Fassung

Sei $(A(n))_{n\in\mathbb{N}}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N} : A(n)$$

(2) Es gilt der Induktionsanfang $A(0)$ und für jedes $n \in \mathbb{N}$
zudem der Induktionsschritt $A(n) \Rightarrow A(n+1)$, kurz:

$$A(0) \ \wedge \ \forall n \in \mathbb{N} : [\, A(n) \Rightarrow A(n+1) \,]$$

**Beweis:** Die Implikation „(1) $\Rightarrow$ (2)“ ist klar, genauer sogar trivial.
Die Implikation „(2) $\Rightarrow$ (1)“ ist Teil der Dedekind–Peano–Axiome (A1B):
Vorgelegt sei $E \subseteq \mathbb{N}$, hier die Erfüllungsmenge $E = \{\, n \in \mathbb{N} \mid A(n) \,\}$
aller natürlichen Zahlen $n \in \mathbb{N}$, für die die Aussage $A(n)$ wahr ist.
Gilt $0 \in E$ und für jedes $n \in E$ auch $(n+1) \in E$, so folgt $E = \mathbb{N}$. QED

# Vollständige Induktion: the road to infinity!

Unter **Induktion** verstehen wir fast immer die **vollständige Induktion**. Andere Gebiete nutzen vor allem die unvollständige Induktion, also den Schluss von speziellen Beispielen auf das (vermutete) Allgemeine; als Gegenstück schließt die Deduktion vom Allgemeinen auf das Spezielle.

Die Physik zum Beispiel nutzt Induktion zur Erstellung von Hypothesen, diese werden experimentell getestet, entweder *erhärtet* oder *widerlegt*, jedoch prinzipiell niemals vollständig *bewiesen*. Die Deduktion leitet umgekehrt Vorhersagen ab, auch diese werden experimentell getestet.

Das Prinzip der vollständigen Induktion ist an sich nichts Schwieriges, es ist als Fundament in die Definition der natürlichen Zahlen eingebaut.

Zur Erinnerung an Satz A1B über $(\mathbb{N}, 0, s)$: Die Nachfolgerabbildung $s : \mathbb{N} \to \mathbb{N} : n \mapsto n + 1$ erfüllt die **Dedekind–Peano–Axiome**:

- D0: Null ist kein Nachfolger: $0 \notin s(\mathbb{N})$, also $\forall n \in \mathbb{N} : n + 1 \neq 0$.
- D1: Die Abbildung $s$ ist injektiv: $\forall p, q \in \mathbb{N} : p \neq q \Rightarrow p + 1 \neq q + 1$.
- D2: Prinzip der **vollständigen Induktion**: Vorgelegt sei $E \subseteq \mathbb{N}$ mit $0 \in E$, und für jedes $n \in E$ gilt $n + 1 \in E$. Dann gilt bereits $E = \mathbb{N}$.

# Ein klassisches Beispiel: der kleine Gauß

**Aufgabe:** Wir suchen eine geschlossene Formel für die Summe

$$S(n) \;:=\; \sum_{k=1}^{n} k \;=\; 1+2+\cdots+n.$$

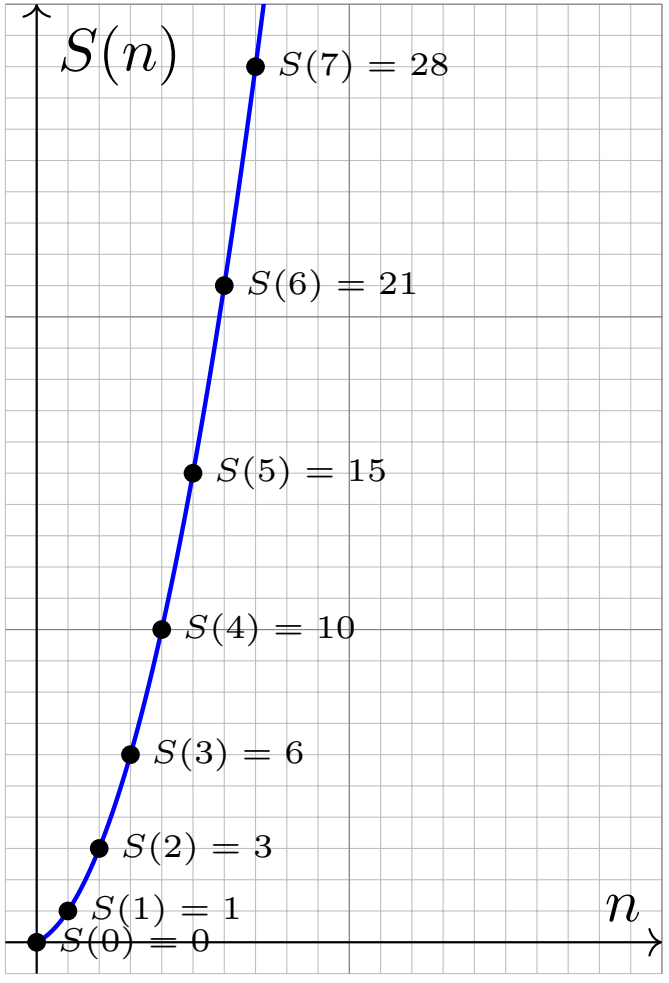
Wie können Sie das Problem angehen?

1. Berechnen Sie kleine Beispiele.
2. Formulieren Sie eine Vermutung.
3. Beweisen Sie Ihre Vermutung!

**Lösung:** (1) Für kleine Werte $n = 0, 1, 2, \ldots$ finden wir die Werte $S(n)$ in der Graphik.

(2) Das sieht aus wie eine Parabel!
Durch diese Datenpunkte verläuft $F(x) = x(x+1)/2$, siehe B101.

(3) Beweis durch Induktion!



# Ein klassisches Beispiel: der kleine Gauß

Wir summieren die Terme $f(k) = k$ für $k = 1, 2, 3, \ldots$ und vergleichen

die Summe $S(n) := \sum_{k=1}^{n} f(k)$ mit der Formel $F(n) := \frac{n(n+1)}{2}$.

**Behauptung:** Für alle $n \in \mathbb{N}$ gilt die Aussage $A(n) : S(n) = F(n)$.

**Beweis:** Wir beweisen die Behauptung durch vollständige Induktion.

**Induktionsanfang:** Wir finden $S(0) = 0$ und $F(0) = 0$, also gilt $A(0)$.

**Induktionsschritt $A(n) \Rightarrow A(n+1)$:** Sei $n \in \mathbb{N}$. Wir setzen $A(n)$ voraus und folgern daraus die Aussage $A(n+1)$, also $S(n+1) = F(n+1)$:

$$
\begin{aligned}
S(n+1) &\overset{\text{Def}}{=} S(n) + f(n+1) \\
&\overset{\text{IV}}{=} F(n) + (n+1) \\
&\overset{\text{Def}}{=} \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\
&\overset{\mathbb{Q}}{=} \frac{(n+2)(n+1)}{2} \qquad \overset{\text{Def}}{=} F(n+1)
\end{aligned}
$$

# Ein klassisches Beispiel: der kleine Gauß

Wie *finden* wir die geschlossene Formel für die Summe $S(n) = \sum_{k=1}^{n} k$?

Speziell wenn wir schon wissen oder zumindest vermuten,
dass $S(n)$ eine Polynomfunktion vom Grad $\leq 2$ ist?

Dann genügt es, drei Punkte auszuwerten,
etwa $S(0) = 0$ und $S(1) = 1$ und $S(2) = 3$.

Dies liefert die Polynomfunktion $S(n) = n(n+1)/2$, siehe B101.
Diese Vermutung können wir anschließend per Induktion beweisen!

☺ Die Induktion sagt uns, wie wir eine Vermutung *beweisen* können.
Sie sagt uns jedoch nicht, wie wir mögliche Vermutungen *finden* können.

☺ Die Induktion ist ein Standardverfahren und oft einfache Routine.
Alternativ gelingen manchmal auch kreativere, noch schönere Beweise.

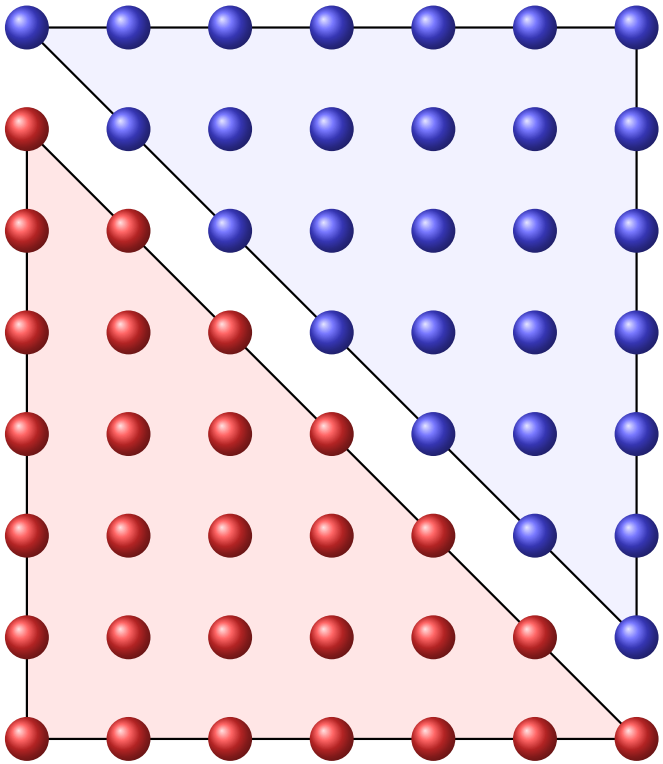
☺ Der folgende Beweis ist geometrisch-anschaulich und genial-einfach.
Auch dieses Argument kann und will ich Ihnen nicht vorenthalten.

☺ In diesem Falle muss ich doch zugeben: Unsere erste bescheidene
Induktion schießt mit Kanonen auf Spatzen, hier auf den kleinen Gauß.

# Ein klassisches Beispiel: der kleine Gauß

Wie *finden* wir die geschlossene Formel für die Summe $S(n) = \sum_{k=1}^{n} k$?
Hier ein geometrischer Beweis, als Bild ganz ohne Worte:

$$1 + 2 + 3 + \quad \ldots \quad + n =: S(n)$$



$$2S(n) = n(n+1)$$

*C'est par la logique que l'on prouve, et par l'intuition que l'on découvre.*
[Mit der Logik beweisen wir, mit der Intuition entdecken wir.]
Henri Poincaré (1854–1912)

# Induktion: Mehr ist leichter. Weniger ist schwer.

**Aufgabe:** (1) Finden und beweisen Sie eine geschlossene Formel für

$$s_n := \sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{n(n+1)}.$$

(2) Eine genauere Aussage ist hier leichter zu beweisen! Zeigen Sie

$$A(n) : s_n = 1 - 1/(n+1).$$

**Beweis:** (2) Induktionsanfang: Wir haben $s_0 = 0$, also gilt $A(0)$.
Induktionsschritt $A(n) \Rightarrow A(n+1)$: Sei $n \in \mathbb{N}$ eine natürliche Zahl.
Wir setzen $A(n)$ voraus und folgern daraus die Aussage $A(n+1)$:

$$\begin{aligned} s_{n+1} &\overset{\text{Def}}{=} s_n + \frac{1}{(n+1)(n+2)} \overset{\text{IV}}{=} 1 - \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} \\ &\overset{\mathbb{Q}}{=} 1 - \frac{n+2}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)} \overset{\mathbb{Q}}{=} 1 - \frac{1}{n+2} \end{aligned}$$

☺ Der Induktionsbeweis für (2) gelingt erfreulich leicht und routiniert.
Induktion ist ein Standardverfahren, im Idealfall ganz einfach und direkt.

# Induktion: Teleskopsummen sind genial-einfach

(1) Eine geschlossene Formel zu *finden* erfordert Kreativität!

☺ Der Term $\frac{1}{k(k+1)} = \frac{1}{k} - \frac{1}{k+1}$ führt zu folgender **Teleskopsumme**:

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \cdots + \left(\frac{1}{n} - \frac{1}{n+1}\right) = 1 - \frac{1}{n+1}$$

Die Induktion ist eine sehr nützliche und mächtige Beweistechnik:

☺ Vorgegeben sei eine geeignete Aussageform $(A(n))_{n\in\mathbb{N}}$.
In günstigen Fällen erhalten wir per Induktion $\forall n \in \mathbb{N} : A(n)$.

☺ Induktionsbeweise können schwierig sein, doch Induktion hilft:
Wir arbeiten systematisch, strukturiert, routiniert: Standardverfahren!

Die Induktion löst leider nicht alle Probleme! Inventor's paradox:

☹ Die Methode der Induktion sagt uns nicht, wie wir $A(n)_{n\in\mathbb{N}}$ finden.
Das hängt ab von unseren Zielen, Wünschen, Ideen, Ambitionen, ...

☹ Selbst wenn das globale Ziel $\forall n \in \mathbb{N} : A(n)$ klar ist, erfordert es manchmal Geschick, es in geeignete Zwischenschritte zu zerlegen.

# Induktion mit Start in $m \in \mathbb{N}$

## Satz C4B: Prinzip der vollständigen Induktion, zweite Fassung

Sei $A(n)_{n \geq m}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}_{\geq m}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}_{\geq m}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N}_{\geq m} \,:\, A(n)$$

(2) Es gilt $A(m)$, und $A(n)$ impliziert $A(n+1)$ für jedes $n \in \mathbb{N}_{\geq m}$, kurz:

$$A(m) \;\wedge\; \forall n \in \mathbb{N}_{\geq m} \,:\, \big[\, A(n) \Rightarrow A(n+1) \,\big]$$

Indexverschiebung: Die zweite Fassung ist äquivalent zur ersten für

$$B(n) = A(m+n).$$

Für den Startwert $m = 0$ ist die zweite Fassung identisch zur ersten.
Für einen beliebigen Startwert $m \in \mathbb{N}$ ist die zweite meist bequemer.
Beide Sichtweisen sind nützlich, daher führe ich sie hier explizit aus.

# Induktion: Mehr ist leichter. Weniger ist schwer.

**Aufgabe:** (1) Beweisen Sie für alle $n \in \mathbb{N}$ die obere Schranke

$$s_n := \sum_{k=1}^{n} \frac{1}{k^2} = \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \quad < \quad 2.$$

☹ Der direkte Versuch per Induktion schlägt hier leider fehl!

(2) Eine stärkere Aussage ist hier leichter zu beweisen! Zeigen Sie

$$A(n) \ : \ s_n \leq 2 - 1/n \quad \text{für alle } n \in \mathbb{N}_{\geq 1}.$$

☺ Bei Induktion gilt oft: Mehr ist leichter. Weniger ist schwer.

**Beweis:** (2) Induktionsanfang: $s_1 = 1 \leq 2 - 1/1$. Induktionsschritt:

$$s_n = s_{n-1} + \frac{1}{n^2} \leq 2 - \frac{1}{n-1} + \frac{1}{n^2} < 2 - \frac{n}{n(n-1)} + \frac{1}{n(n-1)} = 2 - \frac{1}{n}$$

**Alternative:** (1) Für alle $k \geq 2$ gilt $1/k^2 < 1/k(k-1) = 1/(k-1) - 1/k$.
(2) Daraus folgt $\sum_{k=2}^{n} 1/k^2 < 1 - 1/n$ dank Teleskopsumme wie oben.

# Inventor's paradox nach George Pólya

Wir stehen staunend vor einem einfachen doch trickreichen Beweis:
Die *stärkere* Aussage ist *einfacher* zu beweisen. Wie kann das sein?

Das ist bei vollständiger Induktion ein häufiges, ja typisches Phänomen!
George Pólya nannte es das **inventor's paradox**:

*The typical proposition $A$ accessible to proof by mathematical induction has an infinity of cases $A_0, A_1, A_2, \ldots, A_n, \ldots$. The case $A_0$ is often easy; at any rate, $A_0$ has to be handled by specific means. Once $A_0$ is established, we have to prove $A_{n+1}$ assuming $A_n$.*

***A proposition $A'$ stronger than $A$ may be easier to prove than $A$.***

*In fact, let $A'$ consist of the cases $A'_0, A'_1, A'_2, \ldots, A'_n, \ldots$. In passing from $A$ to $A'$ we make the burden of the proof heavier: we have to prove the stronger $A'_{n+1}$ instead of $A_{n+1}$. Yet we make also the support of the proof stronger: we may use the more informative $A'_n$ instead of $A_n$.*


Grundprinzip: Ihre Investition von heute ist Ihr Ertrag von morgen!

# Inventor's paradox nach George Pólya

*In general, in trying to devise a proof by mathematical induction,*
*you may fail for two opposite reasons.*
*You may fail because you try to prove too much:*
*your $A_{n+1}$ is too heavy a burden.*
*Yet you may also fail because you try to prove too little:*
*your $A_n$ is too weak a support.*

***You have to balance the statement of your theorem***
***so that the support is just enough for the burden.***

George Pólya, 1887–1985, *Mathematics and plausible reasoning, vol. I, Induction and analogy in mathematics*, 1954, p. 119

Wenn Sie eigenständig Induktionsbeweise führen, müssen Sie also

1. die Behauptung $A(n)_{n\geq m}$ geeignet formulieren und ausbalancieren
2. und damit anschließend den Induktionsbeweis sorgfältig ausführen.

Viele Übungsaufgaben verlangen nur (2), das ist leichter, aber künstlich.
Aufgabe (1) erfordert verzweigtes Erkunden und planvolles Probieren.

# Induktion: starke Fassung

## Satz C4C: Prinzip der vollständigen Induktion, starke Fassung

Sei $A(n)_{n\geq m}$ eine Familie von Aussagen $A(n)$ indiziert durch $n \in \mathbb{N}_{\geq m}$. Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in \mathbb{N}_{\geq m}$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in \mathbb{N}_{\geq m} \,:\, A(n)$$

(2) Es gilt $A(m)$ und $A(m) \wedge \cdots \wedge A(n) \Rightarrow A(n+1)$ für jedes $n \in \mathbb{N}_{\geq m}$:

$$A(m) \;\wedge\; \forall n \in \mathbb{N}_{\geq m} \,:\, \big[\, A(m) \wedge \cdots \wedge A(n) \Rightarrow A(n+1) \,\big]$$

Das ist äquivalent zur einfachen Induktion C4B für die starke Aussage

$$B(n) = A(m) \wedge \cdots \wedge A(n).$$

Wir haben nämlich den Anfang $B(m) = A(m)$ und den Induktionsschritt $B(n) \Leftrightarrow A(m) \wedge \cdots \wedge A(n) \Rightarrow A(m) \wedge \cdots \wedge A(n) \wedge A(n+1) \Leftrightarrow B(n+1)$.
Die starke Induktion ist eine bequeme Umformulierung der Induktion.
Beide Sichtweisen sind nützlich, daher führe ich sie hier explizit aus.

# Induktion: starke Fassung

**Beispiel:** Zum Fundamentalsatz der Arithmetik zeigen wir für $n \in \mathbb{N}_{\geq 1}$:

$A(n)$ : Die natürliche Zahl $n$ ist ein Produkt unzerlegbarer Faktoren.

Für „Produkt unzerlegbarer Faktoren in $\mathbb{N}$“ sage ich kurz UProdukt.

**Beweis:** Wir führen Induktion über $n$ in der starken Fassung C4c.

**Induktionsanfang:** Es gilt $A(1)$: Die Zahl $1$ ist das leere UProdukt.

**Induktionsschritt:** Sei $n \in \mathbb{N}_{\geq 1}$. Wir setzen $A(1) \wedge \cdots \wedge A(n)$ voraus.
Wir untersuchen $a = n + 1$. Hierzu unterscheiden wir zwei Fälle:

- Entweder $a$ ist unzerlegbar: Dann ist $a$ ein UProdukt der Länge $1$.
- Oder $a$ ist zerlegbar gemäß $a = b \cdot c$ mit $b, c \geq 2$. Somit gilt $b, c \leq n$. Nach Voraussetzung sind $b$ und $c$ UProdukte, somit auch $a = b \cdot c$.

Per Induktion schließen wir $A(n)$ für jede natürliche Zahl $n \in \mathbb{N}_{\geq 1}$. QED

 Bitte wiederholen Sie den Fundamentalsatz der Arithmetik A2j.
Die Eindeutigkeit ist schwieriger, noch interessanter und nützlicher!
Der Fundamentalsatz ist sehr wichtig und hilfreich, zudem bieten Ihnen die dort genutzten Beweistechniken lebendiges Anschauungsmaterial.

# Induktion: einheitliche Fassung

Wir können die Induktion auch ohne Induktionsanfang formulieren!

## Satz C4D: vollständige Induktion, einheitliche Fassung

Sei $A(n)_{n\in M}$ eine Familie von Aussagen indiziert durch $n \in M \subseteq \mathbb{N}$.
Dann sind die folgenden beiden Aussagen zueinander äquivalent:

(1) Für jede natürliche Zahl $n \in M$ gilt die Aussage $A(n)$, kurz:

$$\forall n \in M \,:\, A(n)$$

(2) Für jede natürliche Zahl $n \in M$ gilt die Aussage:

$$\big[\, \forall k \in M_{<n} \,:\, A(k) \,\big] \;\Rightarrow\; A(n)$$

**Beweis:** Das ist äquivalent zur starken Induktion C4C: Die Implikation „(1) $\Rightarrow$ (2)“ ist ist klar, genauer sogar trivial. Für „(2) $\Rightarrow$ (1)“ betrachten wir $M = \{\, n_0 < n_1 < n_2 < \ldots \,\}$. Dank (2) gilt $\top \Rightarrow A(n_0)$, also $A(n_0)$. Für jedes $i \in \mathbb{N}$ gilt $A(n_0) \wedge \cdots \wedge A(n_i) \Rightarrow A(n_{i+1})$. Wir schließen (1).

# Induktion: einheitliche Fassung

☺ Das ist elegant und effizient. Manche Beweise nutzen diese Form:
In Bedingung (2) ist der Induktionsanfang schon raffiniert eingebacken.

Das ist insbesondere dann eine willkommene Vereinfachung,
wenn der Induktionsanfang genauso verläuft wie der Schritt.

☹ In manchen Induktionsbeweisen ist der Anfang anders strukturiert
als der Schritt und erfordert daher sein eigenes, separates Argument.

Dann spaltet (2) wieder auf in Induktionsanfang und Induktionsschritt.
Nun gut, die einheitliche Form hat dann weder Vor- noch Nachteile.

☺ Die einheitliche Form C4D nützt auch für (große) endliche Mengen.
Auch hier ist eine Betrachtung aller Einzelfälle meist unwirtschaftlich,
der Induktionsbeweis hingegen spart Arbeit und schafft Klarheit.

☺ Die Formulierung C4D lässt sich noch wesentlich allgemeiner nutzen
für die „transfinite“ Induktion, statt über $M \subseteq \mathbb{N}$ über jede beliebige
wohlgeordnete Menge $(M, \leq)$, siehe F1T. Mehr hierzu in Kapitel F.

# Induktionsbeweise in der Linearen Algebra

Als Ausblick nenne ich exemplarisch einige Sätze, die wir im Verlauf der Linearen Algebra durch Induktion beweisen (in der Fassung rechts).

E1C Die Zykelzerlegung von Permutationen (C4C)
§E1.2 Der Zählsatz für endliche Mengen (C4C)
§E1.3 Dirichlets Schubfachprinzip (C4C)
§E2.1 Grundrechenarten für endliche Mengen (C4C)
E2I Teilmengen und Binomialkoeffizient (C4A)
E2K Zerlegungen und Stirling–Zahlen (C4A)
F1S Die natürlichen Zahlen sind wohlgeordnet. (C4A)
F2B Rekursionssatz von Dedekind (C4C)
F2M Aus der Bijektion $\mathbb{N}^2 \cong \mathbb{N}$ folgt $\mathbb{N}^n \cong \mathbb{N}$ (C4B)
F2P Aus der Bijektion $\mathbb{Q}^2 \cong \mathbb{Q}$ folgt $\mathbb{Q}^n \cong \mathbb{Q}$ (C4B)

Als Alternative entrolle ich manchmal den Induktionsbeweis zu einem expliziten Algorithmus, um die konkrete Konstruktion hervorzuheben. Das sind zwei Seiten einer Medaille: Die Korrektheit des angegebenen Algorithmus zeigen wir, indem wir dann den Induktionsbeweis führen.

# Induktionsbeweise in der Mathematik

Mit zunehmender Erfahrung verschmelzen die vier Formulierungen zu einem universellen „Prinzip der Induktion“; alle vier sind ja äquivalent.

Meist genügt dann eine Skizze, die Idee, der entscheidende Schritt, die detaillierte Ausformulierung ist anschließend eine routinierte Übung.

Je fortgeschrittener das Thema, desto kürzer sind die Routinebeweise, schließlich fallen sie weg zu Gunsten der wesentlichen neuen Ideen.

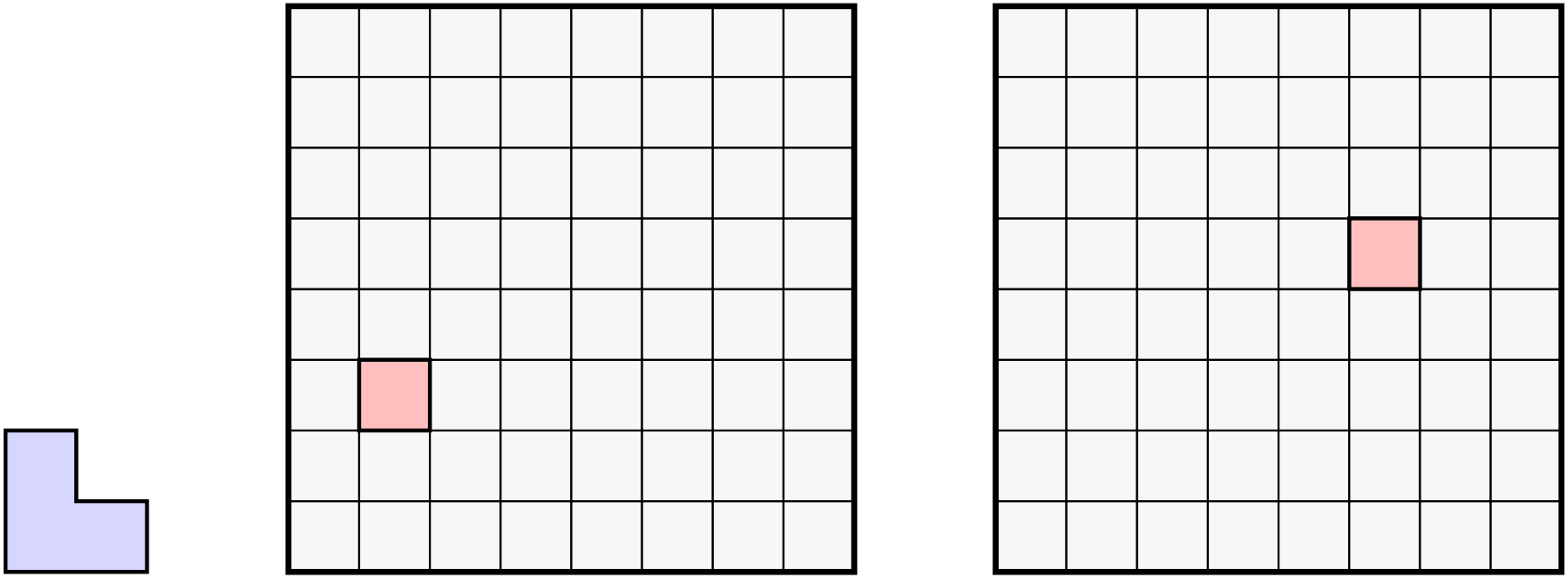
Ausführliche Beweise, insbesondere per Induktion, kosten viel Platz, den sparen wir später zu Gunsten der Lesbarkeit und der Übersicht.

Gelegentlich schreibe ich kurz „Dies folgt per Induktion über $n$“, und dies soll genügen, um daraus das vollständige Argument herzuleiten.

Daher müssen Sie alle Beweistechniken, insbesondere die Induktion, verinnerlichen, um damit Beweise prüfen und produzieren zu können.

 Bei aller Abkürzung: Den ausführlichen und genauen Beweis sollte man immer in der Hinterhand halten, um etwaige Zweifel zu klären. Das folgende schöne Beispiel illustriert dies eindrücklich.

# Induktion: Mehr ist leichter. Weniger ist schwer.



**Aufgabe:** (1) Wir betrachten ein Schachbrett, mit $8 \times 8$ Quadraten. Ein beliebiges dieser $64$ Quadrate wird rot markiert. Lassen sich die verbleibenden $63$ Quadrate mit L-Steinen zu je $3$ Quadraten abdecken?

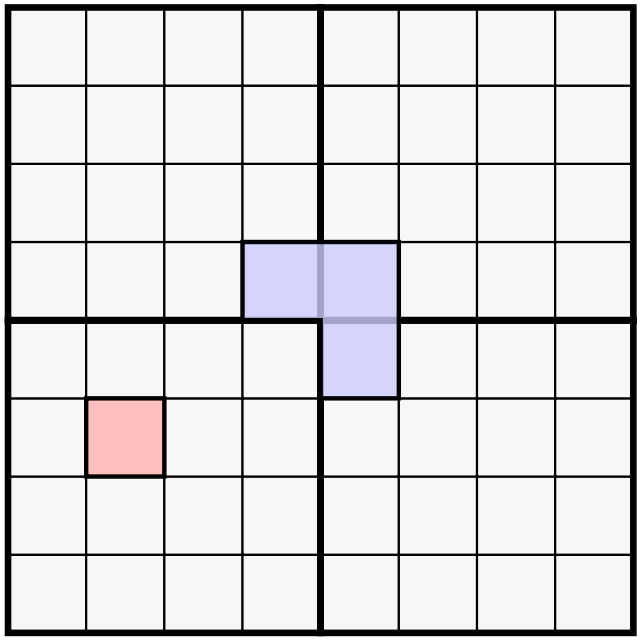
☹ In dieser allzu speziellen Form ist die Aufgabe recht schwierig. Mangels Struktur erkennen wir zunächst keinen Lösungsansatz.

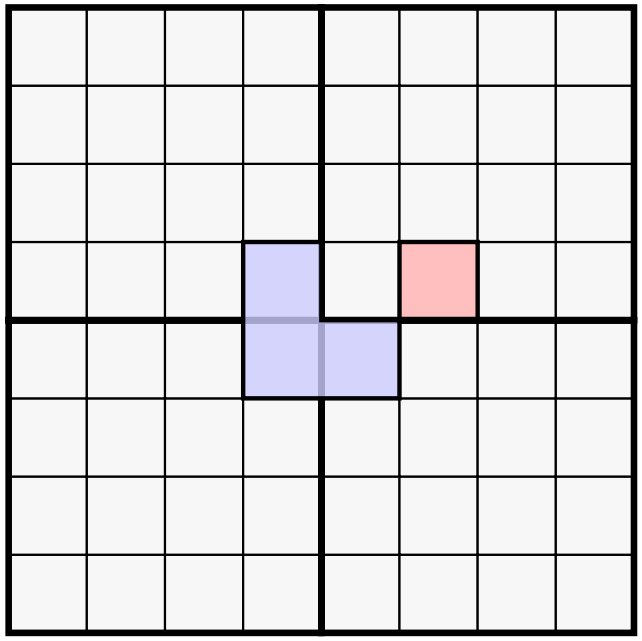
☺ Eine allgemeinere Frage ist hier viel leichter zu beantworten. . . Durch eine geschickte Induktion wird das Problem kinderleicht!

# Induktion: Mehr ist leichter. Weniger ist schwer.

(2) Lösen Sie das Problem für alle Spielbretter mit $2^n \times 2^n$ Quadraten.
Das klingt zunächst noch schwieriger, ist aber tatsächlich einfacher!

**Lösung:** Die geniale Idee als Bild ohne Worte:





**Übung:** Formulieren Sie dies sorgfältig als Induktion über $n \in \mathbb{N}$.
Ist die Idee erst einmal geboren, so ist die Ausführung recht leicht.

**Zusatz:** Formulieren und lösen Sie das dreidimensionale Puzzle.
Es wirkt zunächst noch komplizierter, gelingt aber ebenso leicht!

# Induktion: Beweisen ist leicht. Finden ist schwer.

**Scherzhafte Frage:** Wie lautet zu $g(x) = \mathrm{e}^x$ die $100$te Ableitung?

**Ernsthafte Frage:** Wie lautet zu $f(x) = x\,\mathrm{e}^x$ die $100$te Ableitung?

☺ Selbst wenn weder Frage noch Antwort von Induktion sprechen, kann es dennoch helfen, eine geeignete Induktion einzuführen!

**Anleitung:** (1) Berechnen Sie einige Ableitungen $f'$, $f''$, $f'''$, …
(2) Formulieren Sie eine Vermutung für die $n$te Ableitung $f^{(n)}$.
(3) Beweisen Sie Ihre Vermutung per Induktion über $n \in \mathbb{N}$.
(4) Spezialisieren Sie schließlich zu dem Fall $n = 100$.

**Lösung:** (1) Wir finden $f'(x) = (x+1)\,\mathrm{e}^x$, dann $f''(x) = (x+2)\,\mathrm{e}^x$, dann $f'''(x) = (x+3)\,\mathrm{e}^x$. (2) Wir vermuten daher $f^{(n)}(x) = (x+n)\,\mathrm{e}^x$.
(3) Der Beweis per Induktion ist nun leicht. Formulieren Sie dies aus!
(4) Speziell für $n = 100$ finden wir $f^{(100)}(x) = (x+100)\,\mathrm{e}^x$. Voilà!

☺ Meist läuft dieser Prozess weniger formell ab: Nach den ersten drei Beispielen wollen Sie vermutlich ausrufen „Ja, klar, und immer so weiter bis $100$.“ Dahinter steckt, wenn Sie ehrlich sind, eine Induktion!

# Induktion: Beweisen ist leicht. Finden ist schwer.

Die beiden vorigen und auch die nachfolgenden Aufgaben illustrieren ein wichtiges Prinzip: Liegt eine geeignet formulierte Vermutung erst einmal vor uns, so ist ihr Induktionsbeweis meist leicht: Rechnen! Das gilt selbstverständlich nicht immer, aber doch erstaunlich oft.

Ungleich schwieriger dagegen kann es sein, eine geeignete Vermutung überhaupt erst zu finden, zu formulieren und dabei auszubalancieren.

*Nicht im Beweis einer gegebenen Konstruktion,*
*sondern in der Erfindung der Konstruktion liegt*
*in den meisten Fällen die eigentliche Schwierigkeit.*
Hermann Weyl (1885–1955)

Lassen Sie sich nicht davon einlullen, dass viele Lehrbücher die ersten Induktionsaufgaben meist sehr stereotyp und allzu einfach formulieren. Das ist selbstverständlich sinnvoll und hilfreich für die ersten Schritte, aber kein realistisches Vorbild für selbständige mathematische Arbeit.

Induktion ist im Wesentlichen nicht stumpfsinniges, formales Rechnen, sondern eine filigrane Kunst. Probieren Sie es, Sie werden es erleben!

# Die Summe $1 + 3 + 5 + \cdots + (2n - 1)$

**Aufgabe:** Finden und beweisen Sie eine geschlossene Formel für die Summe $s_n$ der ersten $n$ ungeraden Zahlen:

$$s_n := \sum_{k=1}^{n} (2k - 1) = 1 + 3 + 5 + \cdots + (2n - 1)$$

(0) Berechnen Sie kleine Beispiele und formulieren Sie eine Vermutung.
Beweisen Sie Ihre Vermutung (1) per Induktion und (2) geometrisch.

**Lösung:** (0) Wir finden $s_0 = 0$, $s_1 = 1$, $s_2 = 4$, $s_3 = 9$, $s_4 = 16$, ....
Die naheliegende Vermutung ist daher: Es gilt $s_n = n^2$ für alle $n \in \mathbb{N}$.

(1) Wir beweisen die Aussage $A(n) : s_n = n^2$ per Induktion.
Für $n = 0$ gilt $s_0 = 0$, daher ist die Aussage $A(0) : s_0 = 0^2$ wahr.
Angenommen, es gilt $A(n) : s_n = n^2$. Damit zeigen wir nun $A(n+1)$:

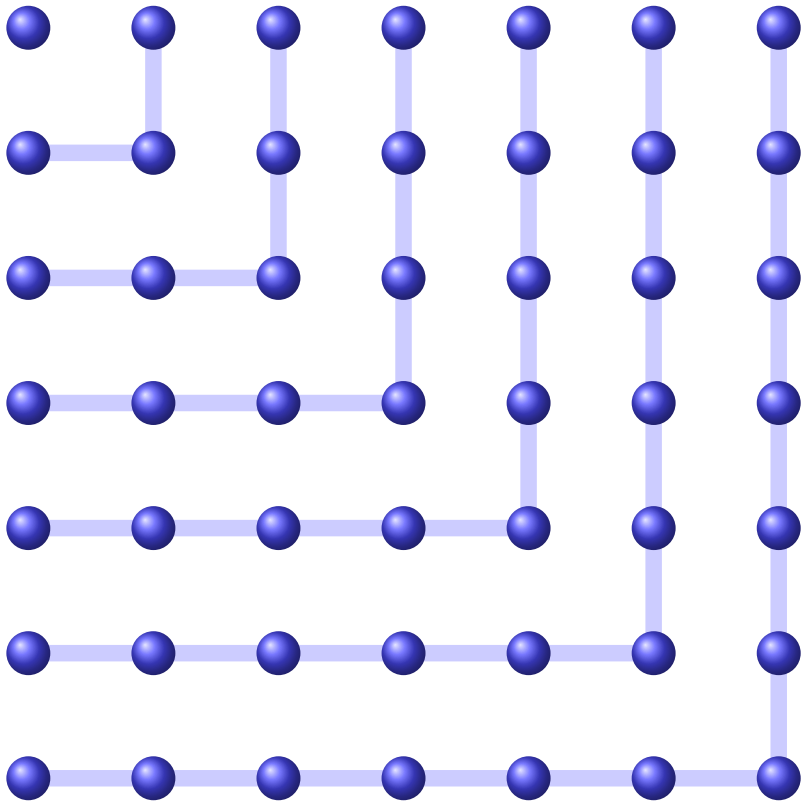
$$s_{n+1} \overset{\text{Def}}{=} s_n + (2n + 1) \overset{\text{IV}}{=} n^2 + 2n + 1 \overset{\mathbb{N}}{=} (n + 1)^2$$

Per vollständiger Induktion (Satz C4A) schließen wir daraus:
Für jede natürliche Zahl $n \in \mathbb{N}$ gilt die vermutete Gleichung $s_n = n^2$.

# Die Summe $1 + 3 + 5 + \cdots + (2n - 1)$

(2) Hier ein geometrischer Beweis, als Bild ganz ohne Worte:

$1 + 3 + 5 + \quad \ldots \quad + 2n{-}1 \quad =: s_n$



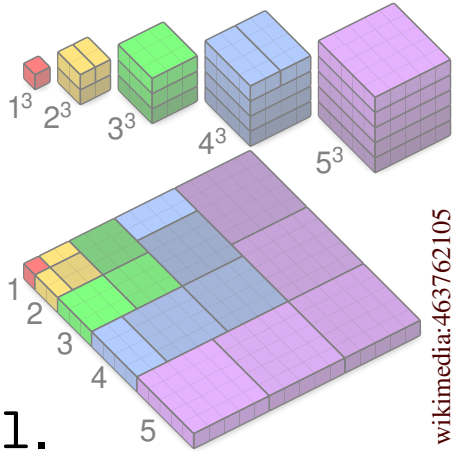
$s_n = n^2$

L Geometrische Beweise wie dieser oder zum kleinen Gauß (C408) sind wunderschönes Material für die Schule und bereits früh zugänglich. Sie bauen spielerisch eine Brücke zur algebraisch-formalen Induktion.

# Weitere Induktionsbeweise zu Summen

**Aufgabe:** Finden Sie die Summenformeln zu

$$\sum_{k=0}^{n-1} 1, \quad \sum_{k=0}^{n-1} k, \quad \sum_{k=0}^{n-1} k^2, \quad \sum_{k=0}^{n-1} k^3, \quad \dots$$




Siehe `de.wikipedia.org/wiki/Faulhabersche_Formel`.
Auch für $\sum_{k=0}^{n-1} k^3 = (\sum_{k=0}^{n-1} k)^2$ existiert ein geometrischer Beweis!

**Lösung:** Wir kennen bzw. finden bzw. vermuten die Summenformeln

$$\sum_{k=0}^{n-1} 1 = n, \qquad \sum_{k=0}^{n-1} k = \frac{n(n-1)}{2},$$

$$\sum_{k=0}^{n-1} k^2 = \frac{n(n-1)(2n-1)}{6}, \qquad \sum_{k=0}^{n-1} k^3 = \frac{n^2(n-1)^2}{4}.$$

**Übung:** Beweisen Sie diese Vermutungen nun durch Induktion über $n$.

Liegt eine solche Formel $\sum_{k=0}^{n-1} f(k) = [F]_0^n$ erst einmal (als Vermutung) vor, so gelingt der Beweis leicht durch folgende „diskrete Ableitung“.

# Hauptsatz zu Differenzen und Summen / HDS

## Satz C4E: Hauptsatz zu Differenzen und Summen / HDS

Für $f, F : \mathbb{Z} \to \mathbb{R}$ gelte $f(k) = F(k+1) - F(k)$ für alle $k \in \mathbb{Z}$.
Durch Summation erhalten wir hieraus die Teleskopsumme

$$\sum_{k=a}^{b-1} f(k) = \sum_{k=a}^{b-1} \big[F(k+1) - F(k)\big] = F(b) - F(a) =: \big[F\big]_a^b.$$

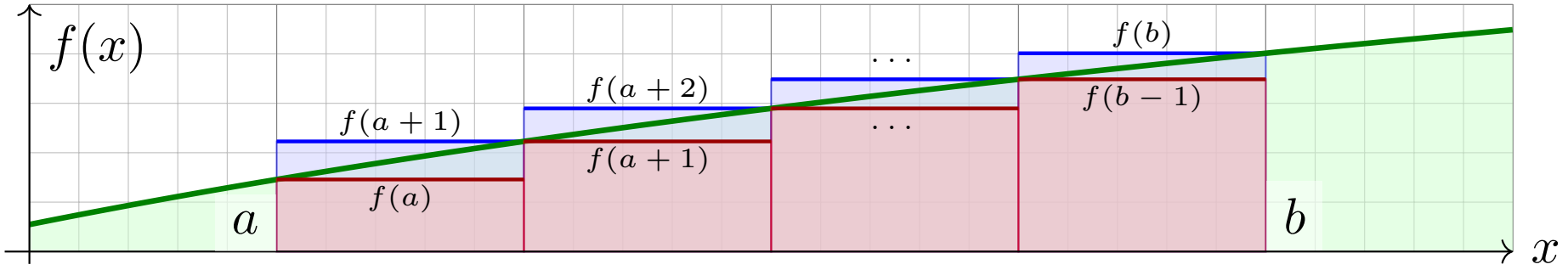
Beispiele sind $f(k) = 1$, $F(k) = k$ und $f(k) = k$, $F(k) = k(k-1)/2$ etc. wie oben angegeben. Man rechnet dies nun leicht / mechanisch nach.

Das ist das diskrete Analogon zum HDI / Hauptsatz der Differential- und Integralrechnung $\int_a^b f(x)\,\mathrm{d}x = [F]_a^b$ für $f, F : [a,b] \to \mathbb{R}$ stetig und $F' = f$.

In beiden Fällen ist Differenzieren leichter als Summieren / Integrieren, und der Hauptsatz schlägt die enorm nützliche Brücke zwischen beiden!

**Übung:** Beweisen Sie den obigen Satz per Induktion über $b$.
(Alles ist sehr leicht und steht eigentlich schon da.)

# Monotoner Vergleich von Summe und Integral




## Satz C4F: monotoner Vergleich von Reihe und Integral

Sei $f : \mathbb{R} \to \mathbb{R}$ monoton wachsend. Für alle $a \leq b$ in $\mathbb{Z}$ gilt dann:

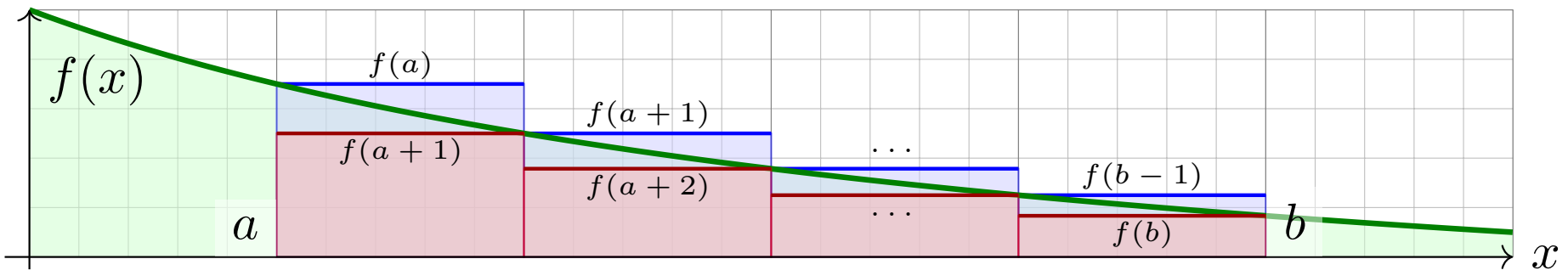
$$\sum_{k=a}^{b-1} f(k) \quad \leq \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \leq \quad \sum_{k=a+1}^{b} f(k)$$

Durch Umstellung ist dies äquivalent zu:

$$f(a) + \int_{x=a}^{b-1} f(x)\,\mathrm{d}x \quad \leq \quad \sum_{k=a}^{b-1} f(k) \quad \leq \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x$$

**Übung:** Beweisen Sie diesen Satz sorgsam per Induktion über $b$.

# Monotoner Vergleich von Summe und Integral




## Satz C4G: monotoner Vergleich von Integral und Reihe

Sei $f : \mathbb{R} \to \mathbb{R}$ monoton fallend. Für alle $a \leq b$ in $\mathbb{Z}$ gilt dann:

$$\sum_{k=a+1}^{b} f(k) \quad \leq \quad \int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \leq \quad \sum_{k=a}^{b-1} f(k)$$

Durch Umstellung ist dies äquivalent zu:

$$\int_{x=a}^{b} f(x)\,\mathrm{d}x \quad \leq \quad \sum_{k=a}^{b-1} f(k) \quad \leq \quad f(a) + \int_{x=a}^{b-1} f(x)\,\mathrm{d}x$$

**Übung:** Beweisen Sie diesen Satz sorgsam per Induktion über $b$.

# Die harmonische Reihe und der natürliche Logarithmus

☺ Für die vorigen beiden Übungen und die folgenden beiden Aufgaben benötigen Sie etwas Integration, wie Sie es in der Schule gelernt haben.

**Aufgabe:** Wir untersuchen die **harmonische Reihe**

$$H_n := \sum_{k=1}^{n} \frac{1}{k}.$$

(1) Schachteln Sie den Wert $H_n$ ein durch den Logarithmus $\ln(n)$.
(2) Folgern Sie das Konvergenzverhalten von $H_n$ für $n \to \infty$.
(3) Bei welchem Index $n$ überschreitet $H_n$ den Wert $1000$?

**Lösung:** (1) Für die Funktion $f(x) = 1/x$ erhalten wir dank Satz C4G:

$$\ln(n+1) \quad \leq \quad \sum_{k=1}^{n} \frac{1}{k} \quad \leq \quad 1 + \ln(n)$$

☺ Die harmonische Reihe wächst wie der natürliche Logarithmus!

(2) Insbesondere erhalten wir die Divergenz $\sum_{k=1}^{n} \frac{1}{k} \to \infty$ für $n \to \infty$.

(3) Bei $n \approx \mathrm{e}^{1000} \approx 2 \cdot 10^{434}$. Wir werden das also sicher nie erleben!

# Approximation einer Dirichlet–Reihe durch Integrale

**Aufgabe:** Berechnen Sie durch Summation näherungsweise den Wert

$$\zeta(3) := \sum_{k=1}^{\infty} \frac{1}{k^3} \quad \text{der Riemannschen Zeta–Funktion} \quad \zeta(s) = \sum_{k=1}^{\infty} \frac{1}{k^s}$$

bis auf einen Fehler $\leq \varepsilon = 0.5 \cdot 10^{-6}$, also sechs Nachkommastellen.
Wie kontrollieren Sie den Fehler? Wie weit müssen Sie summieren?

**Lösung:** Wir berechnen die endlichen Summen $s_n = \sum_{k=1}^{n} k^{-3}$ und wählen $n$ so, dass der Rest $\zeta(3) - s_n = \sum_{k=n+1}^{\infty} k^{-3}$ kleiner als $\varepsilon$ ist:

$$0 \;<\; \int_{x=n+1}^{\infty} x^{-3}\,\mathrm{d}x \;<\; \sum_{k=n+1}^{\infty} k^{-3} \;<\; \int_{x=n}^{\infty} x^{-3}\,\mathrm{d}x \;=\; \frac{1}{2n^2} \;\overset{!}{\leq}\; \varepsilon$$

Die Wahl $n = 1000$ garantiert einen Fehler $\leq 0.5 \cdot 10^{-6} = 0.0000005$.
Wir finden $s_{1000} = 1.20205640\ldots$, also $1.202055 < \zeta(3) < 1.202057$.

☺ Noch besser: $s_n + (n+1)^{-2}/2 \leq \zeta(3) \leq s_n + n^{-2}/2$, Fehler $\leq n^{-3}$.
Mit diesem raffinierten Trick genügt schon die Summation bis $n = 100$.

# Beispiel einer Klausuraufgabe (2020)

**Aufgabe:** Zeigen Sie per vollständiger Induktion, dass die folgende Aussage $A(n)$ für alle $n \in \mathbb{N}$ gilt.

$$A(n): \quad \text{Die Zahl } 5^{2n} - 2^n \text{ ist in } \mathbb{Z} \text{ durch } 23 \text{ teilbar.}$$

**Induktionsanfang:** Für $n = 0$ beweisen wir $A(0)$ direkt:

$$5^{2\cdot 0} - 2^0 = 1 - 1 = 0 = 23 \cdot 0.$$

**Induktionsschritt:** Sei $n \in \mathbb{N}$. Wir setzen voraus, dass $A(n)$ gilt, es existiert also $k \in \mathbb{Z}$ mit $5^{2n} - 2^n = 23k$, somit $5^{2n} = 2^n + 23k$. Daraus folgern wir nun die Behauptung $A(n+1)$:

$$\begin{aligned} 5^{2(n+1)} - 2^{n+1} &\overset{\mathbb{Z}}{=} 25 \cdot 5^{2n} - 2^{n+1} \\ &\overset{\text{IV}}{=} 25 \cdot (2^n + 23k) - 2 \cdot 2^n \\ &\overset{\mathbb{Z}}{=} 23 \cdot 2^n + 25 \cdot 23 \cdot k \qquad \overset{\mathbb{Z}}{=} 23(2^n + 25k) \end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 0$.
Per vollständiger Induktion folgt die Behauptung $A(n)$ für alle $n \in \mathbb{N}$.

# Beispiel einer Klausuraufgabe (2020)

☺ Die Induktion ist ein Standardverfahren und oft einfache Routine.
Für die vorliegende Aufgabe müssen Sie vor allem sorgfältig rechnen.

**Hinweis:** Wenn Sie diese Aufgabe selbst versuchen und aufmerksam betrachten, dann merken Sie: Es ist nicht immer offensichtlich, wo und wie Sie die Induktionsvoraussetzung nutzbringend einsetzen können. Hier hilft Ihnen letztlich Ihre Erfahrung. Übung macht die Meisterin!

**Alternative:** Sie können die gesamte Rechnung modulo $23$ ausführen. Diese nützliche Rechentechnik lernen Sie in Kapitel E ab Seite E341:

Auf $\mathbb{Z}$ nutzen wir die Kongruenz $a \equiv b \mod m$, hier für $m = 23$.
Es gilt $25 \equiv 2$. Damit wird die Induktion gänzlich überflüssig:

$$5^{2(n+1)} \overset{\mathbb{Z}}{=} 25^{n+1} \equiv 2^{n+1}$$

☺ Die Rechnung modulo $23$ ist einfacher, kürzer und klarer,
genau dazu führen wir diese wunderbare und nützliche Technik ein.
Beide Rechnungen tun dasselbe; gute Notation vereinfacht Ihre Arbeit.

# Eine zweite Induktion zur Teilbarkeit

**Aufgabe:** Zeigen Sie per vollständiger Induktion,
dass die folgende Aussage $A(n)$ für alle $n \in \mathbb{N}_{\geq 1}$ gilt.

$$A(n): \quad \text{Die Zahl } 3^{2n+4} - 2^{n-1} \text{ ist durch } 7 \text{ teilbar.}$$

**Induktionsanfang:** Für $n = 1$ beweisen wir $A(1)$ direkt:

$$3^{2\cdot 1+4} - 2^0 = 3^6 - 1 = 728 = 7 \cdot 104.$$

**Induktionsschritt:** Sei $n \in \mathbb{N}_{\geq 1}$. Wir setzen voraus, dass $A(n)$ gilt,
es existiert also $k \in \mathbb{Z}$ mit $3^{2n+4} - 2^{n-1} = 7k$, somit $3^{2n+4} = 7k + 2^{n-1}$.
Daraus folgern wir nun die Behauptung $A(n+1)$:

$$\begin{aligned} 3^{2(n+1)+4} - 2^n &\overset{\mathbb{Z}}{=} 3^{2n+4} \cdot 9 - 2^n \\ &\overset{\text{IV}}{=} (7k + 2^{n-1}) \cdot 9 - 2^n \\ &\overset{\mathbb{Z}}{=} 7k + 2^{n-1}(9-2) \qquad \overset{\mathbb{Z}}{=} 7(k + 2^{n-1}) \end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$.
Per vollständiger Induktion folgt die Behauptung $A(n)$ für alle $n \in \mathbb{N}_{\geq 1}$.

# Eine zweite Induktion zur Teilbarkeit

☺ Auch hier müssen Sie vor allem sorgfältig rechnen,
anfangs mit konkreten Zahlen in $\mathbb{Z}$, dann auch mit Variablen.

☺ Wenn Sie diesen Aufgabentyp zum ersten Mal selbst versuchen, ist es noch schwer. Wenn Sie die vorige Aufgabe schon gelöst haben, denn zahlt sich diese Erfahrung hier bereits aus: Übung macht die Meisterin!

**Alternative:** Sie können die gesamte Rechnung modulo $7$ ausführen.
Diese nützliche Rechentechnik lernen Sie in Kapitel E ab Seite E341:

Auf $\mathbb{Z}$ nutzen wir die Kongruenz $a \equiv b \mod m$, hier für $m = 7$.
Es gilt $9 \equiv 2$ und $2^3 = 8 \equiv 1$. Damit wird die Induktion überflüssig:

$$3^{2n+4} \overset{\mathbb{Z}}{=} 3^{2(n-1)+6} \overset{\mathbb{Z}}{=} 9^{n-1} \cdot 9^3 \equiv 2^{n-1} \cdot 2^3 \equiv 2^{n-1}$$

☺ Die Rechnung modulo $7$ ist einfacher, kürzer und klarer,
genau dazu führen wir diese wunderbare und nützliche Technik ein.
Beide Rechnungen tun dasselbe; gute Notation vereinfacht Ihre Arbeit.

# Beispiel einer Klausuraufgabe (2020)

**Aufgabe:** Zeigen Sie per vollständiger Induktion, dass die Aussage $A(n)$ für alle $n \in \mathbb{N}$ mit $n \geq 1$ gilt.

$$A(n): \quad \prod_{k=2}^{n} \left(1 - \frac{2}{k(k+1)}\right) = \frac{1}{3}\left(1 + \frac{2}{n}\right)$$

**Induktionsanfang:** Wir betrachten den ersten Fall $n = 1$.
Auf der linken Seite der Gleichung steht das leere Produkt

$$\prod_{k=2}^{1} \left(1 - \frac{2}{k(k+1)}\right) = 1.$$

Auf der rechten Seite der Gleichung steht

$$\frac{1}{3}\left(1 + \frac{2}{1}\right) = 1.$$

Also gilt die Behauptung $A(1)$.

# Beispiel einer Klausuraufgabe (2020)

**Induktionsschritt:** Sei $n \geq 1$. Wir setzen voraus, dass die Behauptung $A(n)$ gilt. Daraus folgern wir nun die nächste Behauptung $A(n+1)$:

$$\begin{aligned}
\prod_{k=2}^{n+1}\left(1-\frac{2}{k(k+1)}\right) &\overset{\text{Def}}{=} \left[\prod_{k=2}^{n}\left(1-\frac{2}{k(k+1)}\right)\right]\cdot\left(1-\frac{2}{(n+1)(n+2)}\right)\\
&\overset{\text{IV}}{=} \frac{1}{3}\left(1+\frac{2}{n}\right)\cdot\left(1-\frac{2}{(n+1)(n+2)}\right)\\
&\overset{\mathbb{Q}}{=} \frac{1}{3}\cdot\frac{n+2}{n}\cdot\frac{n^2+3n}{(n+1)\cdot(n+2)}\\
&\overset{\mathbb{Q}}{=} \frac{1}{3}\cdot\frac{n+3}{n+1} \overset{\mathbb{Q}}{=} \frac{1}{3}\left(1+\frac{2}{n+1}\right)
\end{aligned}$$

Das beweist den Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$.

Zur Betonung fasse ich zusammen: Aus dem Induktionsanfang $A(1)$ und dem Induktionsschritt $A(n) \Rightarrow A(n+1)$ für alle $n \geq 1$ folgt der **Induktionsschluss:** Die Behauptung $A(n)$ gilt für alle $n \geq 1$.

# Die Fibonacci–Folge

Die Fibonacci–Folge $(f_n)_{n\in\mathbb{N}}$ ist definiert durch die Startwerte $f_0 = 0$ und $f_1 = 1$ sowie die Rekursionsvorschrift $f_n = f_{n-1} + f_{n-2}$ für $n \in \mathbb{N}_{\geq 2}$. (Leonardo Fibonacci beschrieb damit im Jahr 1202 das Wachstum einer Kaninchenpopulation; in der Natur ist sie ein recht häufiges Muster.)

**Aufgabe:** (0) Vergleichen Sie $f_n$ und $2^{n-1}$ für kleine Werte von $n$.
(1) Formulieren Sie zu (0) eine Vermutung und beweisen Sie diese.
(2) Was ist für die Ungleichung $f_n \leq c^{n-1}$ die optimale Konstante $c$?

**Lösung:** (0) Für kleine Werte $n = 0, 1, 2, 3, \ldots$ finden wir

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | … |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_n$ | 0 | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | … |
| $2^{n-1}$ | $1/2$ | 1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | … |

Die naheliegende Vermutung ist daher $f_n \leq 2^{n-1}$ für alle $n \in \mathbb{N}$.
Dies beweisen wir nun per Induktion (1). Diese Ungleichung ist noch allzu verschwenderisch, daher verfeinern wir sie anschließend in (2).

# Die Fibonacci–Folge

(1) Wir beweisen die Aussage $A(n) : f_n \leq 2^{n-1}$ per Induktion über $n$.
Wir haben $f_0 = 0 < 2^{-1}$ und $f_1 = 1 = 2^0$, also gelten $A(0)$ und $A(1)$.
Angenommen, es gilt $A(n-1)$ und $A(n-2)$. Damit zeigen wir nun $A(n)$:

$$f_n \overset{\text{Def}}{=} f_{n-1} + f_{n-2} \overset{\text{IV}}{\leq} 2^{n-2} + 2^{n-3} < 2^{n-2} + 2^{n-2} = 2^{n-1}$$

Per vollständiger Induktion (C4c) gilt $f_n \leq 2^{n-1}$ für alle $n \in \mathbb{N}$.

(2) Wir wollen die induktive Ungleichung $A(n) : f_n \leq c^{n-1}$ optimieren.
Für jede Konstante $c \in \mathbb{R}_{>0}$ gilt zunächst $f_0 = 0 < c^{-1}$ und $f_1 = 1 = c^0$.
Angenommen, es gilt $A(n-1)$ und $A(n-2)$. Damit zeigen wir nun $A(n)$:

$$f_n \overset{\text{Def}}{=} f_{n-1} + f_{n-2} \overset{\text{IV}}{\leq} c^{n-2} + c^{n-3} = c^{n-3} \cdot (c+1) \overset{!}{\leq} c^{n-3} \cdot c^2$$

Wir suchen also $c \in \mathbb{R}_{>0}$ mit $1 + c \leq c^2$. Die kleinste solche Konstante ist die positive Lösung der quadratischen Gleichung $c^2 - c - 1 = 0$, also

$$\phi := (1 + \sqrt{5})/2.$$

Damit gelingt unsere Induktion und beweist $f_n \leq \phi^{n-1}$ für alle $n \in \mathbb{N}$.

# Die Fibonacci–Folge

Wir betrachten weiterhin die Fibonacci–Folge $(f_n)_{n\in\mathbb{N}}$, definiert durch $f_0 = 0$ und $f_1 = 1$ und die Rekursionsvorschrift $f_{n+2} = f_{n+1} + f_n$.

**Aufgabe:** Beweisen Sie für alle $n \in \mathbb{N}$ die **Binet–Formel**

$$A(n): \qquad f_n = \frac{\phi^n - \psi^n}{\phi - \psi}$$

wobei $\phi = \frac{1}{2}(1+\sqrt{5})$ und $\psi = \frac{1}{2}(1-\sqrt{5})$ die Nullstellen von $x^2 - x - 1$ sind. Explizit ausgeschrieben ergibt dies die phantastische Formel

$$f_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Ist zum Beweis die einfache oder die starke Induktion geschickter?

**Induktionsanfang:** Offensichtlich gelten $A(0)$ und $A(1)$:

$$\frac{\phi^n - \psi^n}{\phi - \psi} = \frac{1-1}{\phi - \psi} = 0, \qquad \frac{\phi^1 - \psi^1}{\phi - \psi} = \frac{\phi - \psi}{\phi - \psi} = 1$$

# Die Fibonacci–Folge

**Induktionsschritt:** Die einfache Induktion passt hier nicht direkt.
Wir nutzen die starke Induktion in der Form $A(n) \wedge A(n+1) \Rightarrow A(n+2)$.
Wir setzen also $A(n)$ und $A(n+1)$ voraus und folgern daraus $A(n+2)$:

$$f_{n+2} \overset{\text{Def}}{=} f_{n+1} + f_n \overset{\text{IV}}{=} \frac{\phi^{n+1} - \psi^{n+1}}{\phi - \psi} + \frac{\phi^n - \psi^n}{\phi - \psi}$$

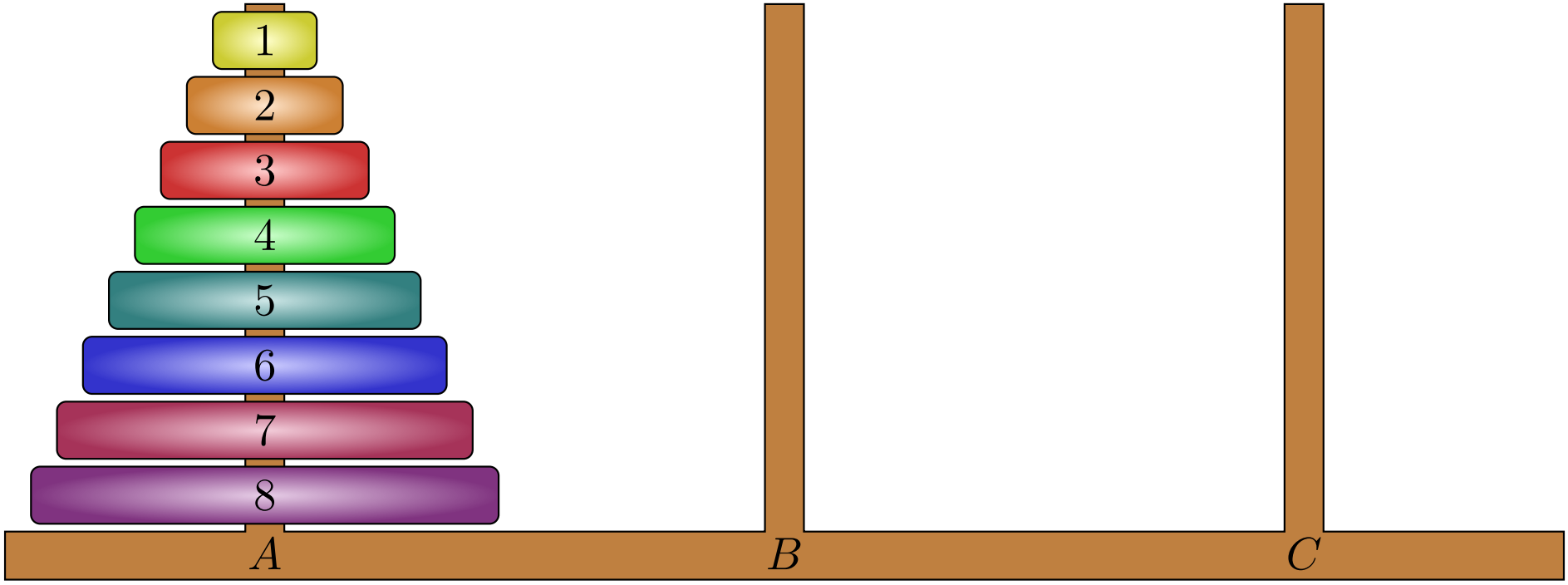
$$\overset{\mathbb{R}}{=} \frac{\phi^n(\phi+1) - \psi^n(\psi+1)}{\phi - \psi} \overset{\mathbb{R}}{=} \frac{\phi^n\phi^2 - \psi^n\psi^2}{\phi - \psi} \overset{\mathbb{R}}{=} \frac{\phi^{n+2} - \psi^{n+2}}{\phi - \psi}$$

Die Induktion ist ein Standardverfahren und oft einfache Routine.
Auch für diese Aufgabe müssen Sie vor allem sorgfältig rechnen.

Die Induktion sagt uns, wie wir die Gleichung *beweisen* können.
Sie sagt uns jedoch nicht, wie wir die Gleichung *finden* können.

**Übung:** Finden Sie die Binet–Formel mit folgender **Ansatzmethode**:
Für welche $x \in \mathbb{R}$ erfüllt $f_n = x^n$ die Rekursion $f_{n+2} = f_{n+1} + f_n$?
Gilt dies dann auch für jede Linearkombination $f_n = \lambda\phi^n + \mu\psi^n$?
Für welche Koeffizienten $\lambda, \mu$ gilt $f_0 = 0$ und $f_1 = 1$? (siehe M249)

# Die Türme von Hanoi




Das Spiel **die Türme von Hanoi** besteht aus drei Stäben $A, B, C$ und darauf die Scheiben $1, \ldots, n$ wachsender Größe. Zu jedem Zeitpunkt des Spiels sind die Scheiben auf jedem Stab der Größe nach geordnet.

Zu Beginn liegen alle Scheiben auf Stab $A$. Ziel des Spiels ist es, alle Scheiben von $A$ nach $C$ zu versetzen. Bei jedem Zug wird die oberste Scheibe von einem Stab auf einen anderen versetzt, vorausgesetzt, dass sich dort nicht schon eine kleinere Scheibe befindet.

# Die Türme von Hanoi

Als **Lösung** bezeichnen wir jede Folge legaler Züge,
die den Turm mit $n$ Scheiben von $A$ nach $C$ bewegt.

**Aufgabe:** Lösen Sie dieses Logik-Puzzle in vier Härtegraden:
$P_n$: Für den Turm der Höhe $n$ existiert (mind.) eine Lösung.
$Q_n$: ... der Länge $2^n - 1$. $R_n$: ... aber nicht mit weniger.
$S_n$: Es gibt genau eine kürzeste Lösung, mit $2^n - 1$ Zügen.

**Strategie:** Lösen Sie zunächst die kleinen Fälle $n = 0, 1, 2, 3, \ldots$.
Sie können hierzu Bücher oder Münzen geeigneter Größe stapeln.
Lösen Sie anschließend den allgemeinen Fall per Induktion über $n$.

I Es ist eine klassische Programmieraufgabe, die (!) optimale Lösung zu programmieren, etwa einfach-elegant als eine rekursive Funktion.

L Für die menschlich-manuelle Lösung, etwa für $n = 5$ Scheiben, ist eine iterative Formulierung leichter: Sehen Sie, wie dies geht?

Wenn Sie dies als wunderschöne Videos bewundern wollen, dann bei Grant Sanderson alias 3Blue1Brown, `youtu.be/2SUvWfNJSsM`, und Burkard Polster alias Mathologer, `youtu.be/MbonokcLbNo`.

# Die Türme von Hanoi

**Lösung:** Für den $0$–Turm sind die Aussagen $P_0, Q_0, R_0, S_0$ trivial.
Für den $1$–Turm sind die Aussagen $P_1, Q_1, R_1, S_1$ offensichtlich wahr.

$P_n \Rightarrow P_{n+1}$ und $Q_n \Rightarrow Q_{n+1}$: Dank $P_n$ versetzen wir den $n$–Turm von $A$ nach $B$ mit $2^n - 1$ Zügen. Wir versetzen die Scheibe $n+1$ von $A$ nach $C$ mit einem Zug. Dank $P_n$ versetzen wir den $n$–Turm von $B$ nach $C$ mit $2^n - 1$ Zügen. Insgesamt gelingt diese Lösung also mit $2^{n+1} - 1$ Zügen.

$R_n \Rightarrow R_{n+1}$: Die größte Schreibe $n+1$ wird mindestens einmal bewegt. Dank $R_n$ gehen dem ersten Mal mindestens $2^n - 1$ Züge voraus und ebenso folgen dem letzten Mal noch mindestens $2^n - 1$ weitere Züge. Insgesamt sind demnach mindestens $2^{n+1} - 1$ Züge notwendig.

Aus $Q_n$ und $R_n$ folgt: Jede optimale Lösung für den $n$–Turm hat genau die Länge $2^n - 1$ und bewegt die größte Scheibe genau einmal.

$S_n \Rightarrow S_{n+1}$: Jede kürzeste Lösung, der Länge $2^{n+1} - 1$, versetzt den $n$–Turm von $A$ nach $B$ mit $2^n - 1$ Zügen, dann die Scheibe $n+1$ von $A$ nach $C$ mit einem Zug, und schließlich den $n$–Turm von $B$ nach $C$ mit $2^n - 1$ Zügen. Dank $S_n$ gelingt dies auf genau eine Weise, also gilt $S_{n+1}$.

# Die Türme von Hanoi

Dieses Logikspiel wurde 1883 vom französischen Mathematiker Édouard Lucas erfunden. Es erfreut sich seither großer Beliebtheit und führt immer wieder zu überraschenden mathematischen Fragen.

Das Problem mit $3$ Stäben ist leicht. H.E. Dudeney fragte 1908 nach optimalen Lösungen bei $4$ Stäben. Seine Vermutung blieb über hundert Jahre lang offen und wurde erst 2014 bewiesen von Thierry Bousch: *La quatrième tour de Hanoï*, Bull. Belg. Math. Soc. 21 (2014) 895–912.

Allgemein für $k \geq 3$ Stäbe gibt es eine elegante, rekursive Lösung von J.S. Frame und B.M. Stewart (Amer. Math. Monthly, 1941). Im Falle $k = 3$ ist dies die eindeutige optimale Lösung mit $2^n - 1$ Zügen. Auch im Falle $k = 4$ ist die Frame–Stewart–Lösung optimal, wie Thierry Bousch zeigte. Für $k \geq 5$ hingegen ist die Optimalität weiterhin eine offene Vermutung.

📖 Mehr hierzu finden Sie im Buch von A.M. Hinz, S. Klavžar, C. Petr: *The Tower of Hanoi – Myths and Maths*, 2nd ed., Birkhäuser 2018.

🙂 Scheinbar einfache Probleme, selbst Kinderspiele, führen schnell zu tiefliegenden mathematischen Fragen – wenn wir nur genau hinsehen.

# PORC: Finde ein Muster! Dann beweise es per Induktion!

Wir definieren die Folge $a_1, a_2, a_3, \ldots \in \mathbb{N}$ rekursiv (dank Satz F2B) durch den Startwert $a_1 = 1$ und für alle $n \geq 2$ die Rekursionsvorschrift:

$$a_n = \begin{cases} a_{n-1} + n + 1 & \text{falls } d := \mathrm{ggT}(a_{n-1}, n) = 1, \\ a_{n-1}/d & \text{falls } d := \mathrm{ggT}(a_{n-1}, n) > 1. \end{cases}$$

**Aufgabe:** (0) Berechnen Sie (per Hand) die ersten zehn Folgenwerte.

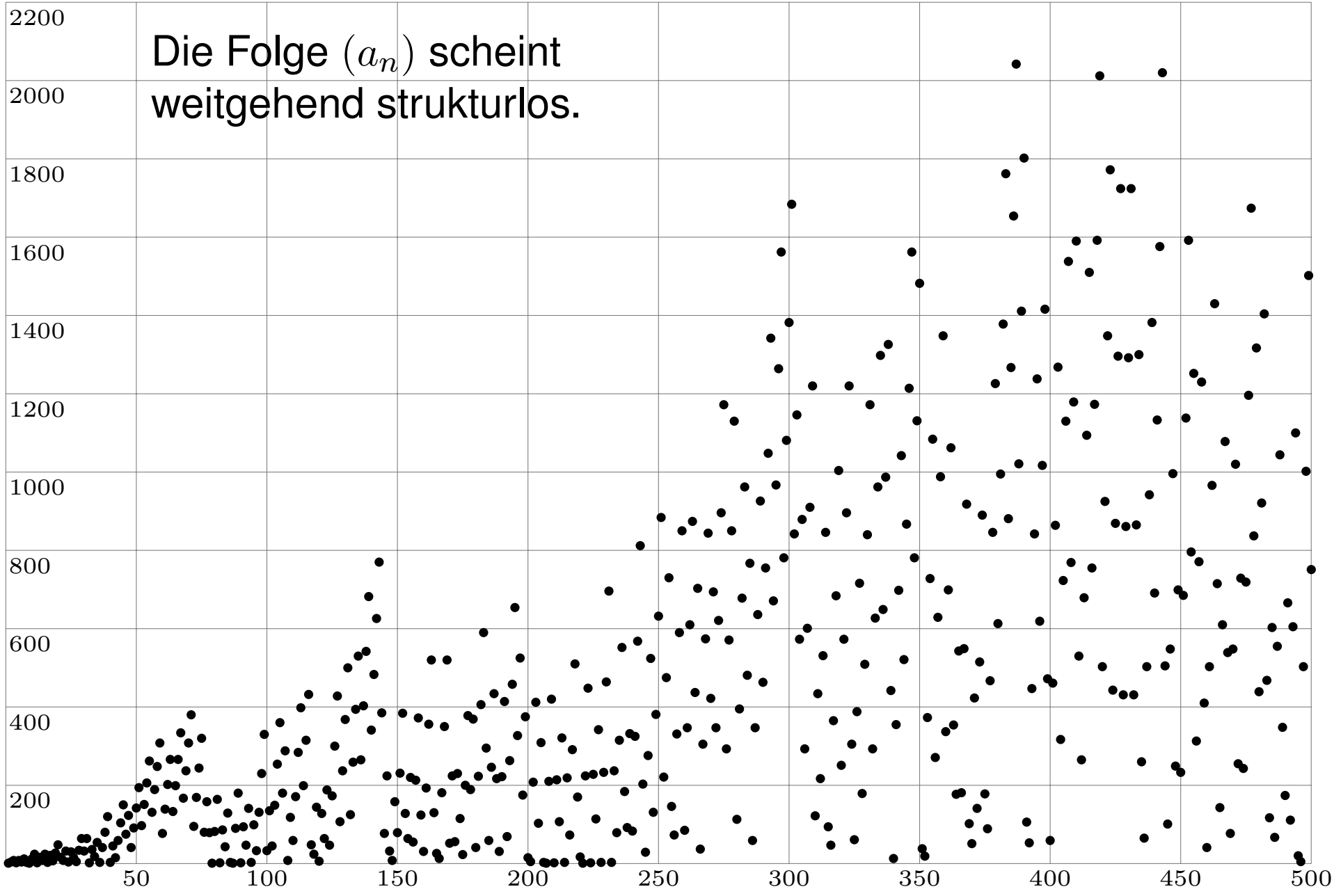
| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | 1 | 4 | 8 | 2 | 8 | 4 | 12 | 3 | 1 | 12 | 24 | 2 | 16 | 8 | 24 | 3 |

**Aufgabe:** Erlaubt die Zuordnung $n \mapsto a_n$ eine geschlossene Formel? Sobald Sie ein Muster erkennen, formulieren und beweisen Sie es!

(1) Plotten Sie (per Computer) die ersten $500$ Folgenwerte.
(2) Plotten Sie (per Computer) die ersten $1000$ Folgenwerte.

⚠ Das ist in der Realität die typische Situation: Die Aussage ist noch nicht vorformuliert, sondern muss erst gefunden werden: Dies gelingt durch **Exploration** und dann **Konsolidierung** in Form eines Beweises.

# PORC: Finde ein Muster! Dann beweise es per Induktion!



# PORC: Finde ein Muster! Dann beweise es per Induktion!

Um uns einen graphischen Überblick zu verschaffen, berechnen und plotten wir die ersten 500 Folgenwerte. Hier in Python und LaTeX/TikZ:

```
from math import gcd
a = 1; max = 500
for n in range(1, max):
    print(str(n) + '/' + str(a) + ', ', end='')
    d = gcd(a, n+1)
    if d > 1: a = a // d
    else:     a = a + n+2
print(str(max) + '/' + str(a))
```

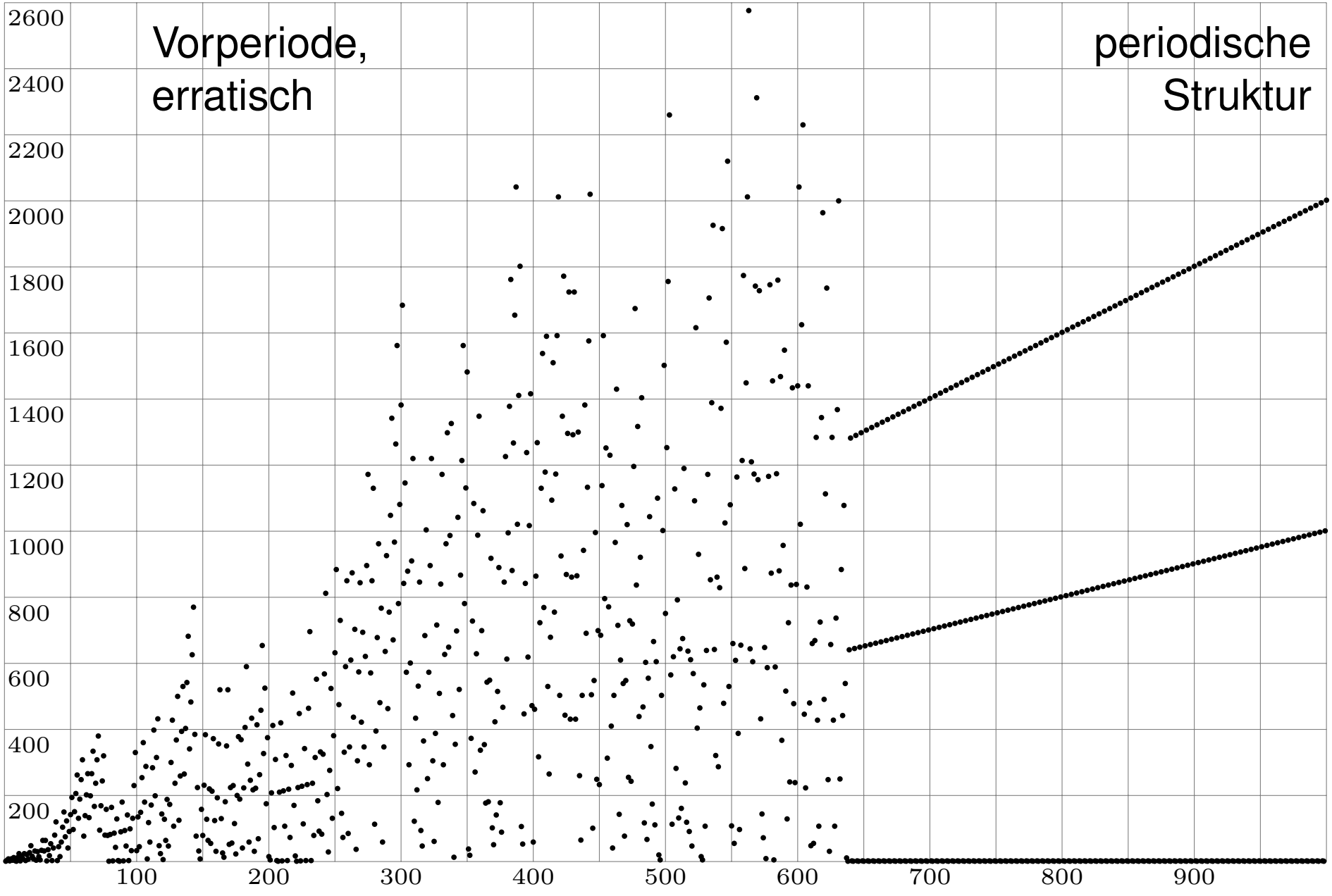
Dies berechnet und druckt die ersten $500$ Folgenwerte: `1/1, 2/4, 3/8, 4/2, 5/8, 6/4, 7/12, 8/3, 9/1, 10/12, 11/24, ..., 500/751`

Diese Liste von Koordinaten $(x, y)$ habe ich oben mit TikZ geplottet. Diese Daten sehen zunächst völlig strukturlos aus, doch dann...

Sehen Sie selbst! Bei $n = 638$ geschieht plötzlich ein Wunder...

# PORC: Finde ein Muster! Dann beweise es per Induktion!





# PORC: Finde ein Muster! Dann beweise es per Induktion!

**Lösung:** Die Folge $(a_n)_{n\in\mathbb{N}}$ scheint anfangs weitgehend strukturlos. Die Graphik bis $n = 500$ verschafft uns einen ersten groben Überblick. In der zweiten Graphik bis $n = 1000$ geschieht etwas Unerwartetes, ein Wunder: Die Folge wird plötzlich vollkommen regelmäßig.

Wie entsteht dieses Wunder? Der Wert $a_n = 1$ wird immer wieder angenommen, zunächst an den Stellen $n = 1, 9, 79, 87, 207, 221, 638$. Dies ist der erste *gerade* Index $n$ mit $a_n = 1$. Für alle $n \geq 638$ gilt dann:

$$a_n = \begin{cases} 1 & \text{für } n = 4k+2, \\ n+2 & \text{für } n = 4k+3, \\ 2n+2 & \text{für } n = 4k+4, \\ 2 & \text{für } n = 4k+5. \end{cases}$$

Für $n \geq 638$ ist $n \mapsto a_n$ *polynomial on residue classes*, kurz *PORC*.

**Aufgabe:** (3) Beweisen Sie diese Gleichungen per Induktion über $n$.

☺ Steht diese Aussage einmal vor Ihnen, so ist der Nachweis leicht: Als bewährtes Standardverfahren greift hier die vollständige Induktion!

# PORC: Finde ein Muster! Dann beweise es per Induktion!

**Lösung:** Wir beweisen die obige Behauptung per Induktion.

**Induktionsanfang:** Für $n = 638 = 4 \cdot 159 + 2$ gilt die Aussage $a_n = 1$.

⚠ Oft ist der Induktionsanfang leicht und der Induktionsschritt knifflig. Hier ist es umgekehrt: Der Induktionsanfang bei $n = 638$ erfordert die explizite Berechnung aller vorhergehenden Werte $a_1, a_2, a_3, \ldots, a_{638}$. Per Hand ist diese Rechnung zwar möglich, doch lang und monoton, recht mühselig und fehleranfällig. Zum Glück haben wir Computer!

**Induktionsschritt:** Wir wenden die Rekursionsvorschrift an:

$$a_n = \begin{cases} a_{n-1} + n + 1 & \text{falls } d := \operatorname{ggT}(a_{n-1}, n) = 1, \\ a_{n-1}/d & \text{falls } d := \operatorname{ggT}(a_{n-1}, n) > 1. \end{cases}$$

Sei nun $n > 638$. Wir nutzen die Induktionsvoraussetzung für $a_{n-1}$:
Für $n = 4k + 3$ gilt $a_{n-1} = 1$, daraus folgt $d = 1$ und $a_n = n + 2$.
Für $n = 4k + 4$ gilt $a_{n-1} = n + 1$, also $d = 1$ und $a_n = 2n + 2$.
Für $n = 4k + 5$ gilt $a_{n-1} = 2n$, also $d = n$ und somit $a_n = 2$.
Für $n = 4k + 2$ gilt $a_{n-1} = 2$, also $d = 2$ und somit $a_n = 1$.

# PORC: Finde ein Muster! Dann beweise es per Induktion!

Im Rückblick betrachtet ist die Struktur des Beweises klar und einfach:
Steht die zu beweisende Aussage erst einmal ausformuliert vor uns,
so führen wir, wie so oft, routiniert eine vollständige Induktion durch.
Hierzu genügt eine sorgsame Rechnung und Fallunterscheidung.

Und die Moral von der Geschicht? An dieser Aufgabe erkennen und
erfahren Sie einige wichtige Phänomene, die für die mathematische
Arbeit typisch sind, aber in Lehrbüchern meist unterrepräsentiert
und in Klausuren wenn überhaupt nur in Miniatur möglich:

☺ Oft ist noch keine Aussage vorformuliert, sondern mögliche Muster
müssen erst gefunden werden: (1) Diese **Exploration** erfordert meist
Ausprobieren, geschickt gewählte Beispiele, kritische Beobachtung, usw.
(2) Ist eine Beobachtung / Aussage / Vermutung bereits formuliert,
so suchen wir eine **Konsolidierung** in Form eines Beweises.

☺ Beide Phasen erfordern mathematisches Geschick und Kreativität!
In Ihren Hausaufgaben haben Sie Zeit für beides, bitte nutzen Sie dies.
Nur so können Sie mathematische Arbeit selbst erfahren und erlernen.

# PORC: Finde ein Muster! Dann beweise es per Induktion!

☺ Der Computer ist das Teleskop / Mikroskop der Mathematik.
Nutzen Sie seine Möglichkeiten und kennen Sie seine Limitationen.
Lernen Sie frühzeitig, dieses mächtige Hilfsmittel effizient anzuwenden!

Der Computer unterstützt Ihre Arbeit. Er nimmt Ihnen zwar nicht die Beobachtungen / Formulierungen / Beweise ab, aber er erledigt für Sie lästige Rechnungen, klaglos und zuverlässig. Dank der Ergebnisse dieser Rechnungen können Sie den Kern des Problems erfassen, Muster erkennen, Aussagen formulieren und anschließend beweisen!

☺ Wie im obigen Beispiel zeigen sich Muster oft erst auf großer Skala, die für Handrechnungen nur schwer oder gar nicht zugänglich ist.
Hierzu programmieren und nutzen Sie einen Computer!

Sie sehen dies eindrücklich im obigen Beispiel: Ohne die Graphiken hätten Sie das Muster nicht erkannt. Ohne die Berechnung von $a_{638}$ hätten Sie den Induktionsanfang nicht beweisen können.

Solche Weisheiten lernen Sie nur durch Erfahrung. Diese Erfahrung gewinnen Sie nur durch das eigenständige Lösen von Aufgaben.

# Welche Rolle spielt Logik im Alltag?

Mathematiker/innen wird gerne vorgeworfen, dass sie alles zu genau nehmen. Umgekehrt wird von ihnen verlässliche Präzision gefordert.

*Which one is it? You cannot have it both ways!*
*Everybody gangsta until the equations start lying.*

Zu Beginn des Kapitels habe ich einfache Alltagsbeispiele aufgeführt, für die präzise Formulierung und unbestechliche Logik wesentlich sind.

Für viele Anwendungen ist diese Klarheit wünschenswert, gar essentiell:
Wirtschaft und Verträge: Wurde fristgerecht geliefert / überwiesen?
Naturwissenschaft und Technik: Hat das Instrument angeschlagen?
Gesellschaft: Hat Kandidat $X$ die Wahl gewonnen? Sport: Gilt das Tor?

Im Rückblick auf dieses Kapitel komme ich auf dieses Spannungsfeld zwischen mathematischer Logik und alltäglichen Anwendungen zurück. Hierzu möchte ich Sie mit ein paar provokanten Beispielen konfrontieren und zum kritischen Nachdenken anregen. Es lohnt sich.

# Welche Rolle spielt Induktion im Alltag?

Ich frage offen: **Spielt Induktion im Alltag überhaupt eine Rolle?**
Für die formal ausgeführte, vollständige Induktion lautet die ehrliche Antwort wohl: fast nie! Doch bei genauerem Hinsehen erweist sich dann das Gegenteil: fast überall! Wie kann beides gleichzeitig wahr sein?

Diese **paradoxe Wahrnehmung** gilt für nahezu alle mathematischen Sätze und Techniken: Sie treten meist nicht als allgemeiner Sachverhalt in Erscheinung, sondern werfen lediglich einen Schatten in Form von konkreten Rechnungen und speziellen Anwendungen.

Für die mathematische Kennerin sind die logischen Grundlagen und dazu die mathematischen Werkzeuge klar und ihr Nutzen offensichtlich. Der mathematisch Unerfahrene jedoch verkennt jegliche Verbindung von Theorie und Anwendung und bestreitet vehement ihren Nutzen.

Der häufig wiedergekäute Vorwurf „Das ist reine Theorie ohne konkrete Anwendung“ ist daher meist keine Aussage über den mathematischen Gegenstand, sondern vielmehr ein Bekenntnis des Sprechers zu seiner eigenen Ignoranz. Bitte achten Sie in Zukunft bewusst darauf.

# Wo finden wir Induktion / Rekursion im Alltag?

Nun will ich meine kühnen Thesen mit konkreten Beispielen belegen.
Logik und Präzision treten besonders deutlich dort in Erscheinung,
wo es um etwas geht: bei strategischen Überlegungen, zum Beispiel
bei finanziellen Entscheidungen, oder etwas lockerer in Spielen.

Dabei verwenden wir ständig Induktion, ganz intuitiv und allgegenwärtig.
Es ist meist keine *vollständige* Induktion, diese ist auch gar nicht nötig,
für viele Anwendungen genügen endlich viele, gar wenige Schritte.
Sobald die Anzahl unübersichtlich wird, machen wir schnell Fehler.

Nichtsdestotrotz ist das Prinzip der Induktion hier klar und deutlich:
Wir zerlegen das gegebene Problem schrittweise in kleinere Probleme.
In Blickrichtung von klein zu groß spricht man von Induktion, umgekehrt
von groß zurück zu klein von Rekursion oder auch Rückwärtsinduktion.

Die folgenden erstaunlichen Beispiele stammen aus der Spieltheorie;
ihre Lösung ist elementar, erfordert aber etwas Geduld und Sorgfalt.
Sie illustrieren wunderbar, wie häufig uns (endliche) Induktion nützt.
Es lohnt sich also, diese Technik zu erlernen und anzuwenden.

# Wo finden wir Induktion / Rekursion im Alltag?

*Verstehen kann man das Leben nur rückwärts,*
*leben muss man es aber vorwärts.*
Søren Kierkegaard (1813–1855)

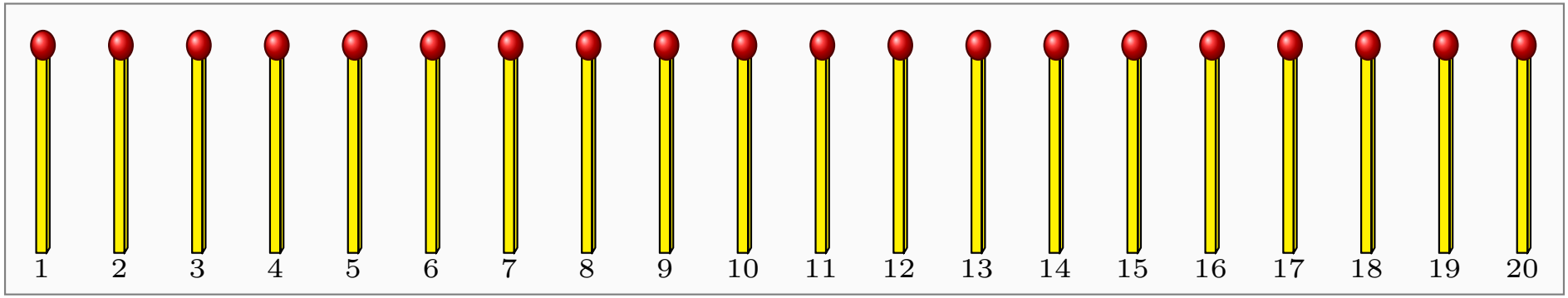
In den folgenden Beispielen wird die Induktion nicht formal ausgeführt; mit Ihren Kenntnissen können Sie das anschließend leicht nachholen. Stattdessen wird rekursiv argumentiert und damit informell gerechnet; hier wird Induktion *praktiziert*, und zwar meist etwas versteckt.

Richard Bellman (1920–1984) war ein US-amerikanischer Mathematiker. Er entwickelte 1953 die Kernidee der **Dynamischen Programmierung**. Das traditionelle Wort „Programmierung“ bedeutet dabei so viel wie „Planung“ oder „Optimierung“, hier rekursiv / induktiv angewendet.

Ökonomen bezeichnen die Dynamische Programmierung schlicht als **Rekursionsmethode**. Sie tritt bei zahlreichen Optimierungsproblemen natürlich auf und wird gerne und erfolgreich angewendet. Sie ist daher ein beliebtes Universalwerkzeug der Wirtschaftswissenschaften.

# Einzeiliges Nim und Rekursion / Induktion

Auf dem Tisch liegen anfangs $x \in \mathbb{N}$ Streichhölzer / Münzen / Steine.
Die Spieler ziehen abwechselnd, jeder entfernt ein oder zwei Hölzer.
Normalspiel / Misèrespiel: Wer nicht mehr ziehen kann, verliert / gewinnt.




Bevor Sie weiterlesen sollten Sie dieses Spiel einige Male durchspielen, am besten zu zweit. Folgen Sie Ihrer Neugier: Es macht Spaß!

Beobachten Sie dabei ihren Lernprozess vom *Whaaa?* bis zum *Aha!* Anfangs werden Sie vermutlich wenig Struktur erkennen. Mit Erfahrung ahnen Sie gewisse Regelmäßigkeiten. Diese können Sie in folgender Aufgabe ausarbeiten und schließlich die allgemeine Regel formulieren.

Am Ende steht ein mathematischer Satz als Extrakt Ihrer Erfahrungen. Diesen können Sie induktiv beweisen und zukünftig getrost anwenden!

# Einzeiliges Nim und Rekursion / Induktion

**Aufgabe:** (0) Schreiben Sie eine Funktion zur rekursiven Berechnung: Der Wert $0$ steht für eine Verlustposition und $1$ für eine Gewinnposition.

**Lösung:** (0a) Misèrespiel $\mu$: Wer nicht mehr ziehen kann, gewinnt.

```
1 def mu(x):
2     if x == 0: return 1   # Wer nicht mehr ziehen kann, gewinnt.
3     return 1 - min( mu(y) for y in range(max(0,x-2), x) )
```

(0b) Normalspiel $\nu$: Wer nicht mehr ziehen kann, verliert.

```
1 def nu(x):
2     if x == 0: return 0   # Wer nicht mehr ziehen kann, verliert.
3     return 1 - min( nu(y) for y in range(max(0,x-2), x) )
```

**Aufgabe:** Bestimmen Sie die Anzahl $f(x)$ der Funktionsaufrufe.

**Lösung:** Wir finden $f(0) = 0$ und $f(1) = 1$ sowie für alle $x \in \mathbb{N}_{\geq 2}$ rekursiv $f(x) = f(x-1) + f(x-2)$. Dies ist die Fibonacci–Folge!

⚠ Bei dieser naiven Methode wächst der Aufwand exponentiell mit $x$!

# Einzeiliges Nim und Rekursion / Induktion

**Aufgabe:** (1) Was sind Verlustpositionen? Was sind Gewinnzüge?

**Lösung:** (1) Wir berechnen rekursiv Gewinn $1$ und Verlust $0$ für das Misèrespiel $\mu$ bzw. das Normalspiel $\nu$ und erhalten folgende Tabelle:

| $x=$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\mu=$ | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| $\nu=$ | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 |

*Quidquid agis, prudenter agas et respice finem!*
[Was immer du tust, handele klug und bedenke das Ende!]

(2) Wie lautet die allgemeine Regel? Damit krönen wir unsere Analyse:

**Satz C5A: einzeiliges Nim mit Zugoptionen $S = \{1, 2, \ldots, n-1\}$**

Misèrespiel: Genau dann ist $x$ eine Verlustposition, wenn $x \bmod n = 1$.
Normalspiel: Genau dann ist $x$ eine Verlustposition, wenn $x \bmod n = 0$.

**Übung:** Beweisen Sie diesen Satz per Induktion über $x \in \mathbb{N}$.

# Einzeiliges Nim und Rekursion / Induktion

Der naiv-rekursive Algorithmus (0) benötigt exponentiellen Aufwand in $x$. Die Tabelle (1) berechnen wir ebenso rekursiv. Da wir jedoch die zuvor berechneten Ergebnisse speichern, ist der Aufwand nur noch linear in $x$. Das ist eine dramatische Verbesserung! Berechnen Sie so etwa $\nu(100)$.

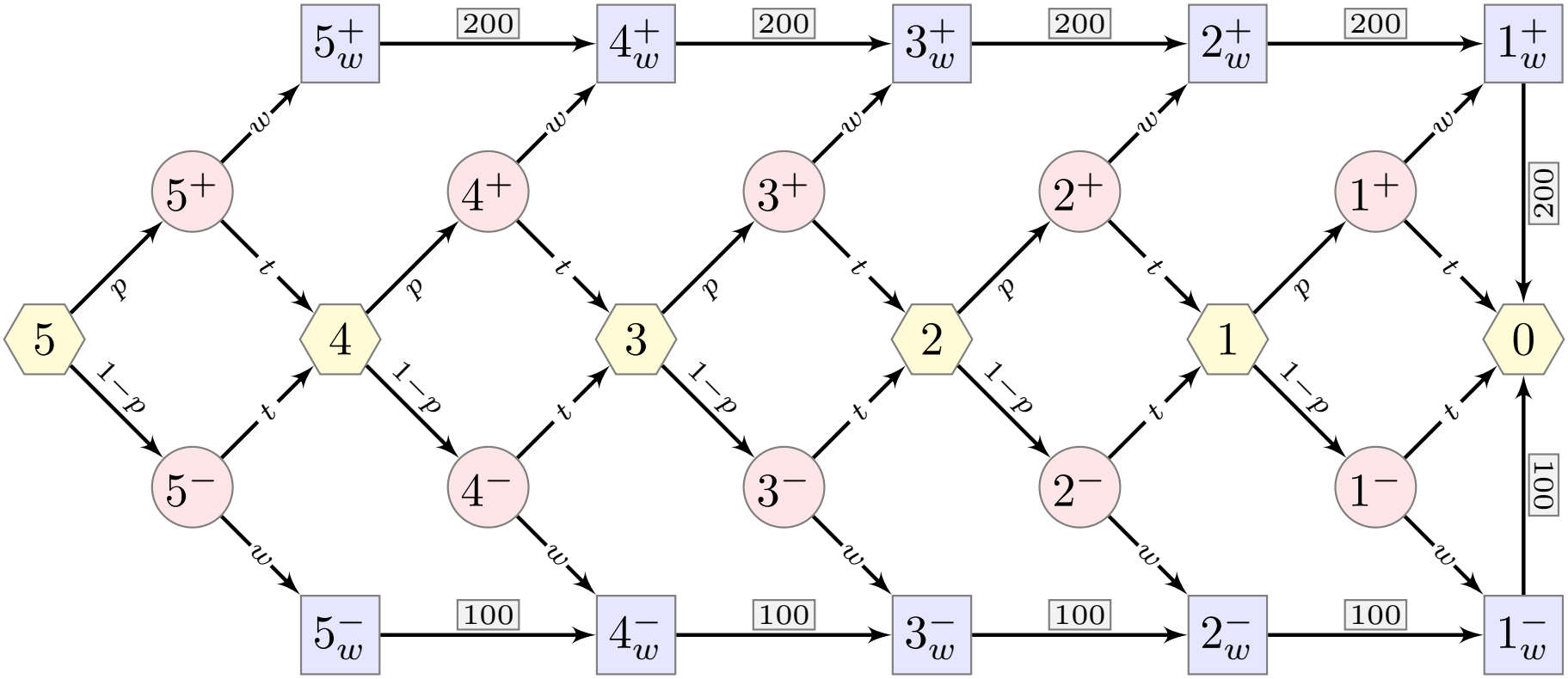
☹ Rekursion hat unter Anfänger/innen meist einen schlechten Ruf: Zuerst sind Denkweise und Progammiertechnik nicht leicht zu erlernen. Ist diese Hürde genommen, so folgt gleich die erste Ernüchterung: Naive Implementierung führt meist zu exponentiellem Aufwand.

☺ Rekursion entfaltet ihre wahre Kraft erst durch raffiniert-effiziente Implementierung: Die genial-einfache Idee hierzu heißt **Memoisation**, das geschickte Speichern der zuvor berechneten Zwischenergebnisse, von lat. **Memorandum**, kurz **Memo**, *das zu Erinnernde*.

☺ Im vorliegenden Falle vollendet Satz C5A unsere Lösung durch eine weitere dramatische Optimierung: Die Berechnung von $x \bmod n$ benötigt nur noch logarithmischen Aufwand, gemäß Ziffernzahl $\operatorname{len}(x) \sim \log_2(x)$. Sie ist zudem so einfach, dass wir sie im Kopf ausführen können!

# Optimierung durch Rekursion / Induktion

**Aufgabe:** Ihr Work&Travel endet in $5$ Wochen. Zu Beginn jeder Woche erhalten Sie ein Jobangebot: mit Wkt $p = 0.4$ ist es gut für $200$€, mit Wkt $1 - p = 0.6$ schlecht für $100$€. Wenn Sie es annehmen, bleiben Sie für die restliche Zeit dabei. Andernfalls reisen Sie eine Woche umher.




Wie viel können Sie erwarten? Ist $700$€ möglich? Geht mehr? optimal?

# Optimierung durch Rekursion / Induktion

Sie sehen hier den sorgsamen Übergang von der realen Fragestellung zu einem **mathematischen Modell**: Dies nennen wir **Modellierung**.

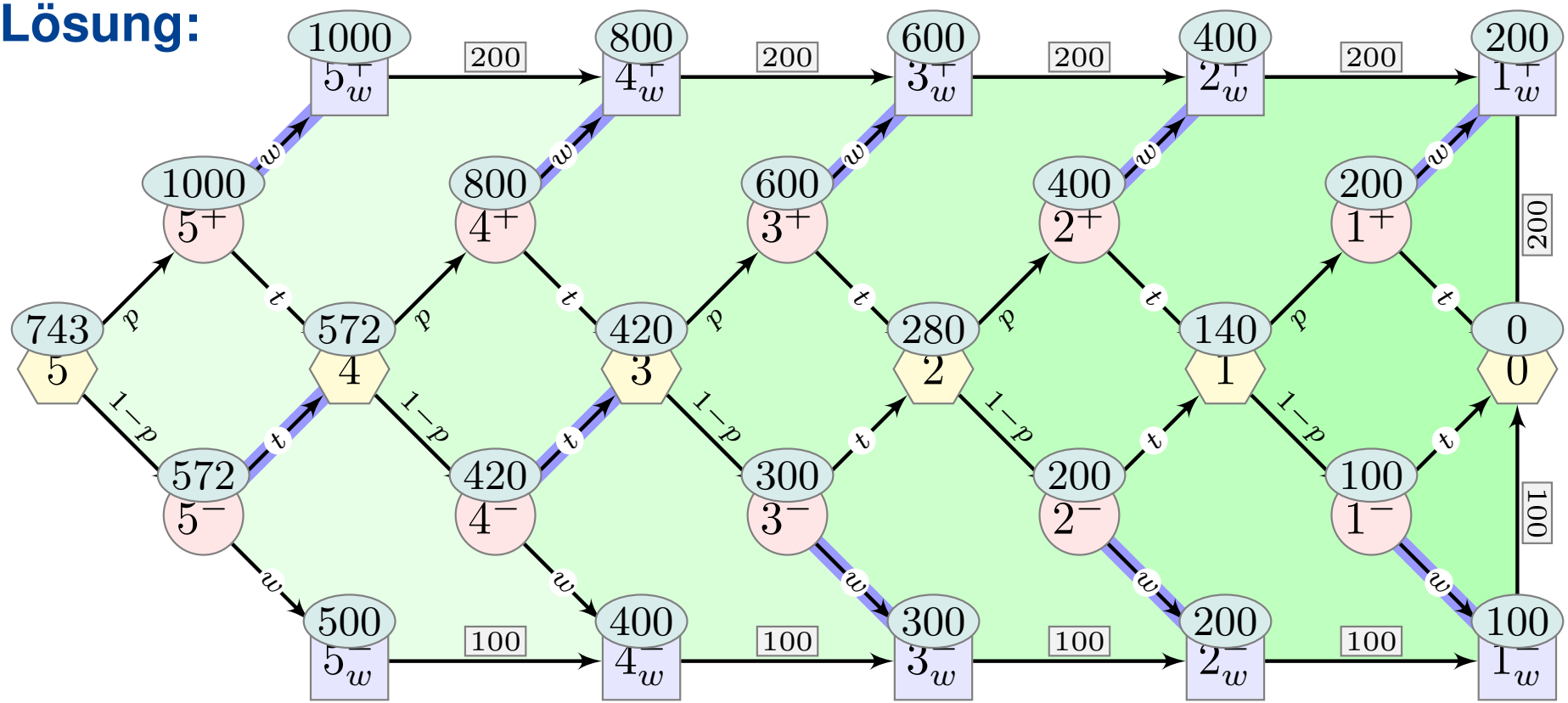
Meist gibt es mehrere mögliche Modelle zur gegebenen Fragestellung: Der umgangssprachliche Text ist wunderbar anschaulich und hoffentlich motivierend. Leider ist er in manchen Details noch nicht explizit, sondern appelliert an Weltwissen und Konventionen. Die Übersetzung in einen Graphen ist kurz und zudem präzise: Hier bleiben keine Fragen offen. Zum Beispiel: Reisen und Arbeiten kostet gleich viel Lebensunterhalt. Andernfalls codieren wir Reisekosten und Lebensunterhalt im Graphen.

Der hier gezeigte Graph ist ein **Markov–Graph**, denn er enthält neben den Spielzügen als möglichen Aktionen des Spielers realistischerweise auch Zufallszüge, auf die der Spieler keinen Einfluss hat. *That's life.*

In jeder der zehn Entscheidungssituationen $5^{\pm}, 4^{\pm}, 3^{\pm}, 2^{\pm}, 1^{\pm}$ muss eine Entscheidung für $w =$ work oder $t =$ travel getroffen werden. Es gibt also $2^{10} = 1024$ Strategien. Die optimale finden Sie durch Rekursion!

# Optimierung durch Rekursion / Induktion

**Lösung:**




In Worten: Einen guten Job nehmen Sie immer an, einen schlechten nur in den letzten $3$ Wochen. Bei $\geq 4$ Wochen lohnt sich noch abzuwarten.

Diese quantitative Analyse erfordert vor allem Sorgfalt und Geduld.
Die entscheidende Idee ist, vom Ende aus rekursiv vorzugehen.

☺ Gespielt wird vorwärts, optimiert wird rückwärts: per Induktion!

# Optimierung durch Rekursion / Induktion

 Wenn Sie diese Art von Problemstellung zum ersten Mal erkunden, sind Sie vermutlich versucht, in der Zeit wie üblich *vorwärts* zu denken.

 Wir lösen das Problem rekursiv, indem wir *rückwärts* argumentieren. Das führt zum Erfolg: Rekursives Denken ist zielgerichtetes Denken!

Das Thema Rekursion ist ebenso wichtig wie sagenumwoben.
Dazu gibt es zahlreiche Weisheiten, teils ernst, teils scherzhaft:

*Um Rekursion zu verstehen, muss man klein anfangen*
*und zunächst einmal Rekursion verstehen.*

Insbesondere in der Programmierung ist Rekursion allgegenwärtig.
Sie ist ein Universalwerkzeug zum Lösen komplexer Probleme.

*Recursion makes good programmers better*
*and bad programmers obvious.*

# Optimierung durch Rekursion / Induktion

**Übung:** Probieren Sie einige der anderen $1023$ Strategien aus.
Gibt es bessere? gleich gute? Die Sachlage erweist sich als knifflig!
Warum spreche ich dennoch kurzerhand von *der* optimalen Strategie?
Ist wenigstens die optimale Gewinnerwartung eindeutig / wohldefiniert?

**Übung:** Vorwärts gelesen scheinen nach den Entscheidungen $2^{\pm} \mapsto w$ alle folgenden Entscheidungen $\{3^{\pm}, 4^{\pm}\} \to \{w, t\}$ ganz überflüssig!
Warum müssen Sie sich dennoch ebenso genau damit befassen?
Sind diese Züge wichtig für das Spiel? oder für die Analyse?

Unser kunstvoller Graph hilft uns zunächst einmal zur Anschauung, aber dann auch ganz praktisch zur Organisation unserer Rechnung.
Die Rechnung kann automatisiert werden! **Topologische Sortierung** heißt in der Informatik jede geschickte Reihenfolge der Positionen, so dass jedes Teilproblem nur kleinere nutzt, die bereits berechnet wurden.

# Optimierung durch Rekursion / Induktion

**Übung:** Implementieren Sie die Rechnung in einer Tabellenkalkulation.
Sie finden eine einfache Lösung in der Datei `Work-and-Travel.ods`.

| | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **Work and Travel** | | Week -5 | | Week -4 | | Week -3 | | Week -2 | | Week -1 |
| 2 | | | 1000,00 | | 800,00 | | 600,00 | | 400,00 | | 200,00 |
| 3 | 0,400 | 1000,00 | 0,400 | 800,00 | 0,400 | 600,00 | 0,400 | 400,00 | 0,400 | 200,00 | |
| 4 | 743,20 | maximize | 572,00 | maximize | 420,00 | maximize | 280,00 | maximize | 140,00 | maximize | 0,00 |
| 5 | 0,600 | 572,00 | 0,600 | 420,00 | 0,600 | 300,00 | 0,600 | 200,00 | 0,600 | 100,00 | |
| 6 | | | 500,00 | | 400,00 | | 300,00 | | 200,00 | | 100,00 |

**Übung:** Variieren Sie die Konstanten, berechnen Sie weitere Beispiele.
Durch solche *Erfahrung* entwickeln Sie ein *Gefühl* für das Problem.

Verfeinerungen: (a) Mit Wkt $q^{\pm}$ wird Ihnen zu Wochenbeginn gekündigt.
(b) Reisen / Arbeiten kostet Geld, zur Vereinfachung einen festen Betrag.
(c) Sie benötigen mindestens $400$€, ansonsten maximieren Sie.
Das erweitert den Graphen, die Lösungsmethode bleibt gleich.

# Optimierung durch Rekursion / Induktion

 Der Mensch ist fähig, meist jedoch widerwillig, komplexe logische Zusammenhänge zu durchdringen, insbesondere Rekursion / Induktion.

**Thinking fast and slow** von Daniel Kahneman, Wirtschaftsnobelpreis 2002, unterscheidet zwei verschiedene Arbeitsweisen unseres Gehirns:

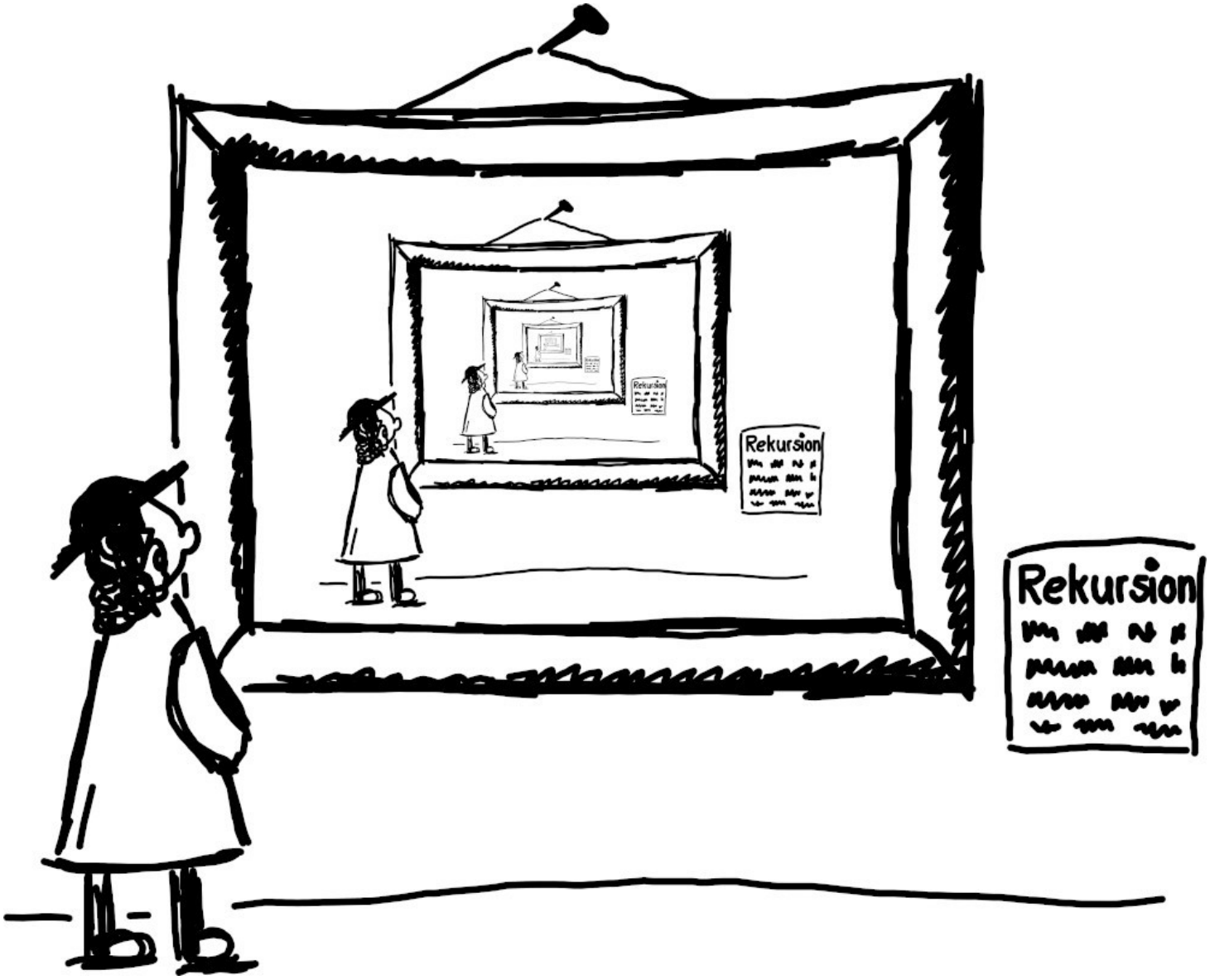
1. Schnell, automatisch, immer aktiv, emotional, stereotyp, unbewusst
2. Langsam, anstrengend, selten aktiv, logisch, berechnend, bewusst

Sie vertrauen oft Ihrem Instinkt, Bauchgefühl oder Erfahrung, insb. wenn Sie keine genaue Information haben oder keine Zeit, sie auszuwerten.

Ihr Verstand braucht wesentlich länger, um zu einem Urteil zu kommen. Das lohnt sich, wenn Sie die Muße haben und das Ziel wichtig genug ist.

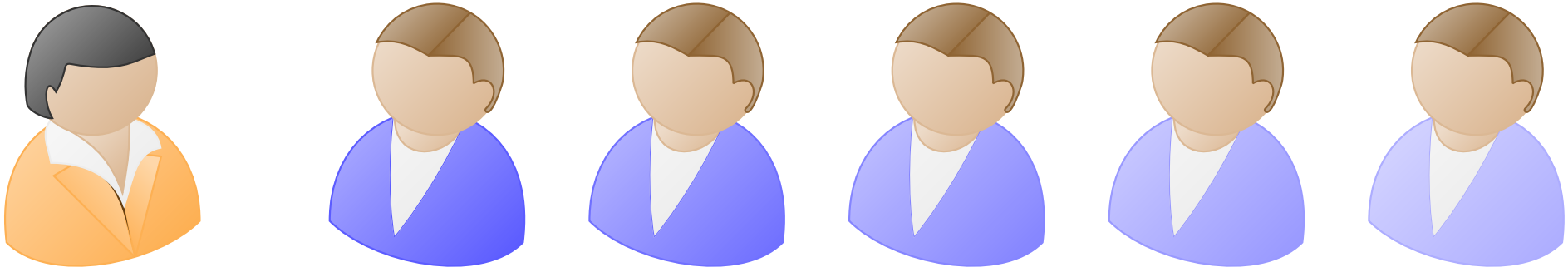
In Ihrem Mathematikstudium lernen Sie diese zweite Vorgehensweise. Dies hilft zu umsichtiger Analyse und vorausschauendem Handeln.

# Optimierung durch Rekursion / Induktion



# Optimale Partnerwahl: Looking for Mr. Right. . . or Mr. Almost

*Marriage problem: When to stop dating and start to get married?*



Alice $1$ $2$ $3$ $\ldots$ $n$

Alice begegnet im Laufe ihres Lebens $n$ potentiellen Ehemännern.
Bei Kandidat $k = 1, 2, 3, \ldots, n$ stellt sie die Eignung $X_k \in [0, 1]$ fest.

Er verliebt sich in die bezaubernde Alice, sie kann ihn nun heiraten oder zurückweisen. Diese Entscheidung ist in jedem Falle endgültig.

**Aufgabe:** Wie anspruchsvoll soll Alice sein? Was ist optimal?
Welche Eignung ihres Ehepartners kann Alice maximal erwarten?

Die Zufallsvariablen $X_1, \ldots, X_n$ seien unabhängig und gleichverteilt.
(Übung für Hartgesottene: Andere Verteilungen sind ebenso möglich.)

# Optimale Partnerwahl: Looking for Mr. Right. . . or Mr. Almost

**Lösung:** Alice ermittelt die optimale Strategie durch Rekursion wie folgt:
Sie heiratet den letzten Kandidaten $n$ auf jeden Fall. Erwartete Eignung:

$$\mu_n = \mathbf{E}(X_n) = 1/2$$

Sie heiratet Kandidat $n-1$, falls $X_{n-1} > \mu_n$. Erwartete Eignung:

$$\mu_{n-1} = \mathbf{E}(\max(X_{n-1}, \mu_n)) = 1/2 \cdot 1/2 + 1/2 \cdot 3/4 = 5/8$$

Sie heiratet Kandidat $n-2$, falls $X_{n-2} > \mu_{n-1}$. Erwartete Eignung:

$$\mu_{n-2} = \mathbf{E}(\max(X_{n-2}, \mu_{n-1})) = 5/8 \cdot 5/8 + 3/8 \cdot 13/16 = 89/128$$

 Alice' Ansprüche steigen, je mehr Kandidaten noch warten.
Ihre Ansprüche sinken, je weniger Kandidaten noch bleiben.

Das ist anschaulich klar und entspricht der Alltagserfahrung.
Nun können wir es begründen und genauer quantifizieren.

Vielleicht klingt das alles recht herzlos und übertrieben formal,
aber so ganz unrealistisch ist es dann auch wieder nicht!

# Optimale Partnerwahl: Looking for Mr. Right. . . or Mr. Almost

Für den folgenden Satz kehren wir die Nummerierung um:
Die „Rückwärtsinduktion“ ist eine ganz normale Induktion!

## Satz C5B: optimale Partnerwahl: Looking for Mr. Right

Alice optimiert die Partnerwahl wie folgt. Sie setzt $a_0 = 0$ und rekursiv

$$a_{n+1} = (1 + a_n^2)/2 \qquad \text{für alle } n \in \mathbb{N}.$$

Warten noch genau $n + 1$ Kandidaten, so heiratet Alice den nächsten Kandidaten genau dann, wenn seine Eignung größer als $a_n$ ist.

Mit dieser optimalen Strategie erwartet Alice die Eignung $a_{n+1}$.
Die Folge $(a_n)_{n\in\mathbb{N}}$ wächst streng monoton und konvergiert gegen $1$.

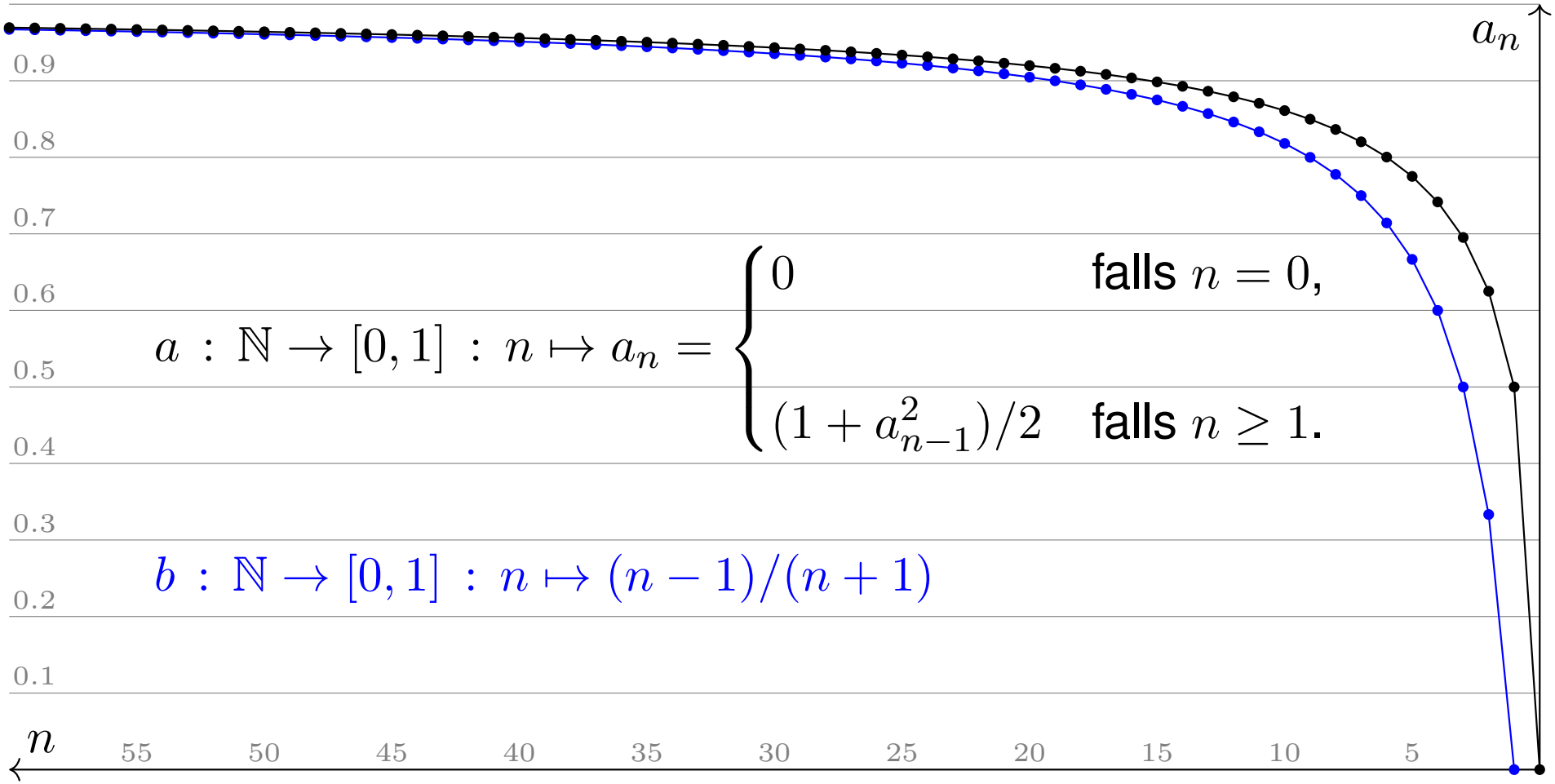
**Übung:** Beweisen Sie diesen Satz per Induktion über $n \in \mathbb{N}$.

☺ Die ungefähre Form der Kurve $n \mapsto a_n$ ist anschaulich plausibel.
Die genauen Werte können wir wie oben berechnen – und beweisen.

☺ Steht diese Aussage einmal vor Ihnen, so ist der Nachweis leicht:
Als bewährtes Standardverfahren greift hier die vollständige Induktion!

# Optimale Partnerwahl: Looking for Mr. Right. . . or Mr. Almost

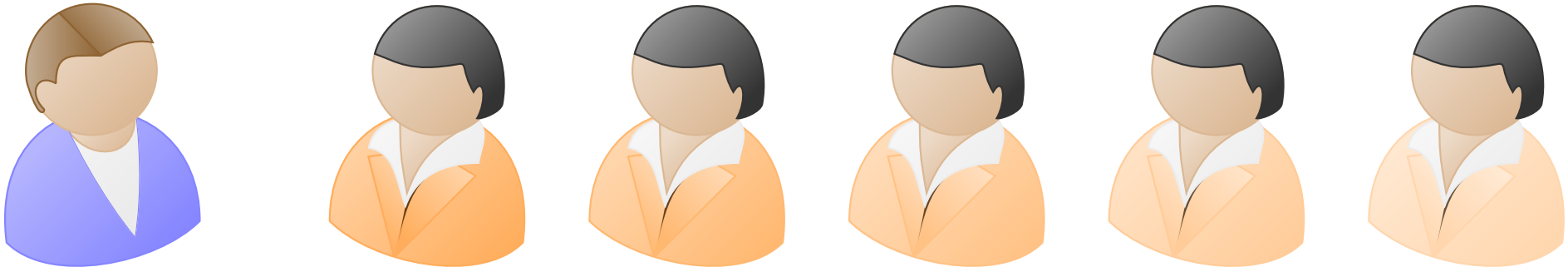
Alice' Erwartung bzw. Anspruch $a_n$ als Funktion der Kandidatenzahl $n$:




*Fun fact:* $b_n$ ist die Erwartung des *zweithöchsten* Wertes in $X_1, \ldots, X_n$.
Alice optimiert erfolgreich, doch es bleibt etwas Wehmut: Eines Tages begegnet ihr Mr. Right, doch sie ist schon mit Mr. Almost verheiratet.

# Optimales Stoppen: das Sekretärinnen-Problem

*Secretary problem: When to stop interviewing and start hiring?*



Bob $\quad 1 \quad 2 \quad 3 \quad \ldots \quad n$

Bob möchte eine Sekretärinnen einstellen. Dazu sind $n$ Bewerberinnen eingeladen, in zufälliger Reihenfolge. Bob sucht die beste Kandidatin, doch nur im Interview mit Kandidatin $k$ kann er feststellen, ob sie besser ist als alle vorigen. Er kann sie nun sofort einstellen oder ihr absagen. Diese Entscheidung ist in jedem Falle endgültig.

**Aufgabe:** Wie soll Bob vorgehen? Wie maximiert er seine Trefferwkt?

**Die $37\%$–Regel:** Interviewe zunächst $n/\mathrm{e}$ Kandidatinnen mit Absage; dann wähle die nächste Kandidatin, die besser ist als alle vorigen.
Das klingt verrückt? Es ist nachweislich die beste Strategie!

# Optimales Stoppen: der Bruss–Algorithmus

**Problem:** Sie bekommen $n$ Angebote zu Zeiten $t = 1, 2, 3, \ldots, n$.
Wir setzen $X_t = 1$, falls Angebot $t$ besser ist als alle vorigen $1, \ldots, t-1$.

Sie können solch ein Angebot entweder annehmen ($s =$ select $=$ stop)
oder dieses Angebot ein für alle Mal ablehnen ($r =$ reject $=$ resume).

Sie wollen unter allen Angeboten das beste auswählen,
also das letzte Angebot $t$ mit $X_t = 1$ annehmen.

**Beispiele:** Eine optimale Online-Auktion mit sofortiger Zu- oder Absage.
Den besten Gebrauchtwagen kaufen. Die beste Tankstelle entlang einer langen Straße auswählen. Die beste Sekretärin einstellen. Heiraten?

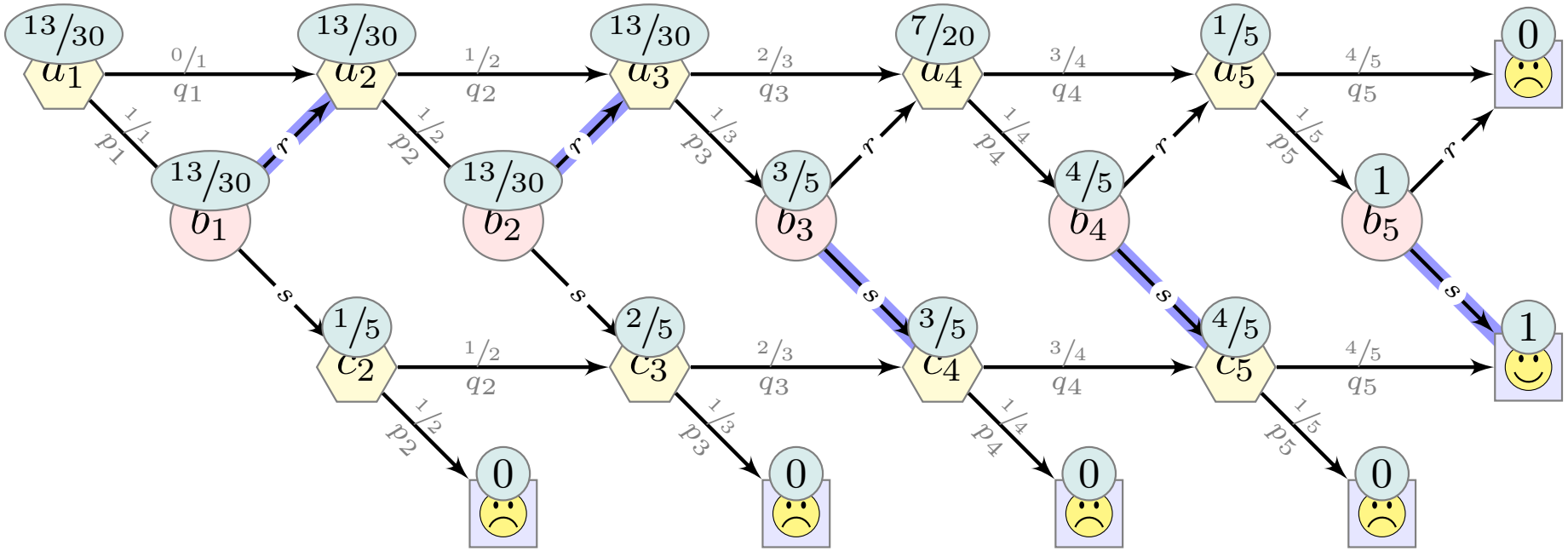
(a) Die Zufallsvariablen $X_1, X_2, \ldots, X_n$ seien unabhängig
mit den Wkten $\mathbf{P}(X_t{=}1) = p_t$ und $\mathbf{P}(X_t{=}0) = q_t = 1 - p_t$.

(b) Speziell betrachten wir $n$ unterschiedlich gute Angebote in zufälliger Reihenfolge, mit Gleichverteilung der $n!$ Anordnungen, also $p_t = 1/t$.

**Aufgabe:** (1) Formulieren Sie dieses Spiel als einen Markov–Graphen.
(2) Was ist die beste Strategie? (3) Was ist die optimale Erfolgswkt?

# Optimales Stoppen: der Bruss–Algorithmus

**Beispiel:** Wir untersuchen $n = 5$ mit $p_k = 1/k$ und $q_k = 1 - p_k$.




**Aufgabe:** Wie gelingt dies allgemein? Beweisen Sie folgenden Satz:

## Satz C5c: optimales Stoppen, Bruss 2000

Sei $s \in \{1, \ldots, n\}$ der größte Index mit $R_s := \sum_{k=s}^{n} p_k/q_k \geq 1$. Dann ist folgende Strategie optimal: Wähle das erste Angebot $k \geq s$ mit $X_k = 1$.

Die optimale Gewinnwkt ist dabei gleich $R_s Q_s$ mit $Q_s = q_s \cdots q_n$.

**Anwendung:** Für $p_k = 1/k$ gilt $s \gtrapprox n/\mathrm{e}$ und $R_s Q_s \gtrapprox 1/\mathrm{e} \gtrapprox 0.367$.

# Optimales Stoppen: der Bruss–Algorithmus

 Dieser Satz ist wunderbar effizient und sein Beweis ebenso elegant.
Der Algorithmus stammt aus dem wunderschönen Artikel von F.T. Bruss:
*Sum the odds to one and stop.* Ann. of Prob. 28 (2000) 1384–1391.

**Beweis:** Wir berechnen die Gewinnwkt $w$ in jedem Zustand $a_k, b_k, c_k$ bei optimaler Strategie. Wie immer gehen wir hierzu rekursiv vor:

Im Zustand $c_k$ ist die Gewinnwkt offensichtlich $w(c_k) = Q_k := q_k \cdots q_n$.
Wir setzen $R_k := p_k/q_k + \cdots + p_n/q_n$ und finden $s$ mit $R_s \geq 1 > R_{s+1}$.
Terminal, für $k = n+1$, gilt $w(c_k) = 1 = Q_k$ und $w(a_k) = 0 = R_k Q_k$.

(1) Im Falle $R_k < 1$ gilt $w(a_k) = R_k Q_k$ und $w(a_{k-1}) = R_{k-1} Q_{k-1}$:
Im Zustand $b_{k-1}$ wählen wir zwischen $w(a_k) = R_k Q_k$ und $w(c_k) = Q_k$.
Da wir $R_k < 1$ voraussetzen, entscheiden wir uns optimal für $c_k$.
Daraufhin gilt $w(a_{k-1}) = p_{k-1} Q_k + q_{k-1} R_k Q_k = R_{k-1} Q_{k-1}$.

(2) Im Falle $R_k \geq 1$ hingegen entscheiden wir uns optimal für $a_k$.
(Für $R_k = 1$ herrscht Indifferenz, die Wahl $c_k$ wäre genauso gut.)
Die Gewinnwkt ist dann $w(a_{k-1}) = w(a_k)$, wie oben gezeigt.
Für alle $k = 1, \ldots, s$ gilt daher $w(a_k) = w(a_s) = R_s Q_s$. QED

# Optimales Stoppen: der Bruss–Algorithmus

Die optimale Stoppzeit $s_n$ und die Gewinnwkt $w_n$ für $n = 1, \ldots, 40$:

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $s_n$ | 1 | 2 | 2 | 2 | 3 | 3 | 3 | 4 | 4 | 4 |
| $w_n$ | 1 | $1/2$ | $1/2$ | $11/24$ | $13/30$ | $77/180$ | $29/70$ | ... | ... | ... |
| $\approx$ | 1.000 | 0.500 | 0.500 | 0.458 | 0.433 | 0.428 | 0.414 | 0.410 | 0.406 | 0.399 |

| $n$ | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
|---|---|---|---|---|---|---|---|---|---|---|
| $s_n$ | 5 | 5 | 6 | 6 | 6 | 7 | 7 | 7 | 8 | 8 |
| $w_n$ | 0.398 | 0.396 | 0.392 | 0.392 | 0.389 | 0.388 | 0.387 | 0.385 | 0.385 | 0.384 |

| $n$ | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
|---|---|---|---|---|---|---|---|---|---|---|
| $s_n$ | 9 | 9 | 9 | 10 | 10 | 10 | 11 | 11 | 11 | 12 |
| $w_n$ | 0.383 | 0.383 | 0.382 | 0.381 | 0.381 | 0.380 | 0.380 | 0.379 | 0.379 | 0.379 |

| $n$ | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
|---|---|---|---|---|---|---|---|---|---|---|
| $s_n$ | 12 | 13 | 13 | 13 | 14 | 14 | 14 | 15 | 15 | 16 |
| $w_n$ | 0.378 | 0.378 | 0.378 | 0.377 | 0.377 | 0.377 | 0.376 | 0.376 | 0.376 | 0.376 |

# Optimales Stoppen: der Bruss–Algorithmus

**Übung:** Wählen Sie einen kleinen Wert $n$ und berechnen Sie das Paar $(s_n, w_n)$ von Hand. Vorbild: Der Fall $n = 5$ ist oben detailliert ausgeführt. Kontrolle: Für $n \leq 7$ finden Sie den exakten Wert $w_n$ in obiger Tabelle.

**Aufgabe:** Schreiben Sie ein Programm zur Berechnung von $(s_n, w_n)$. Kontrolle: Vergleichen Sie Ihre Werte mit der obigen Tabelle.

**Lösung:** In Python sieht eine mögliche Lösung wie folgt aus:

```
1 def bruss(n):
2     k = n; r = 0
3     while r < 1: k -= 1; r += 1/k
4     return k+1, r*k/n
```

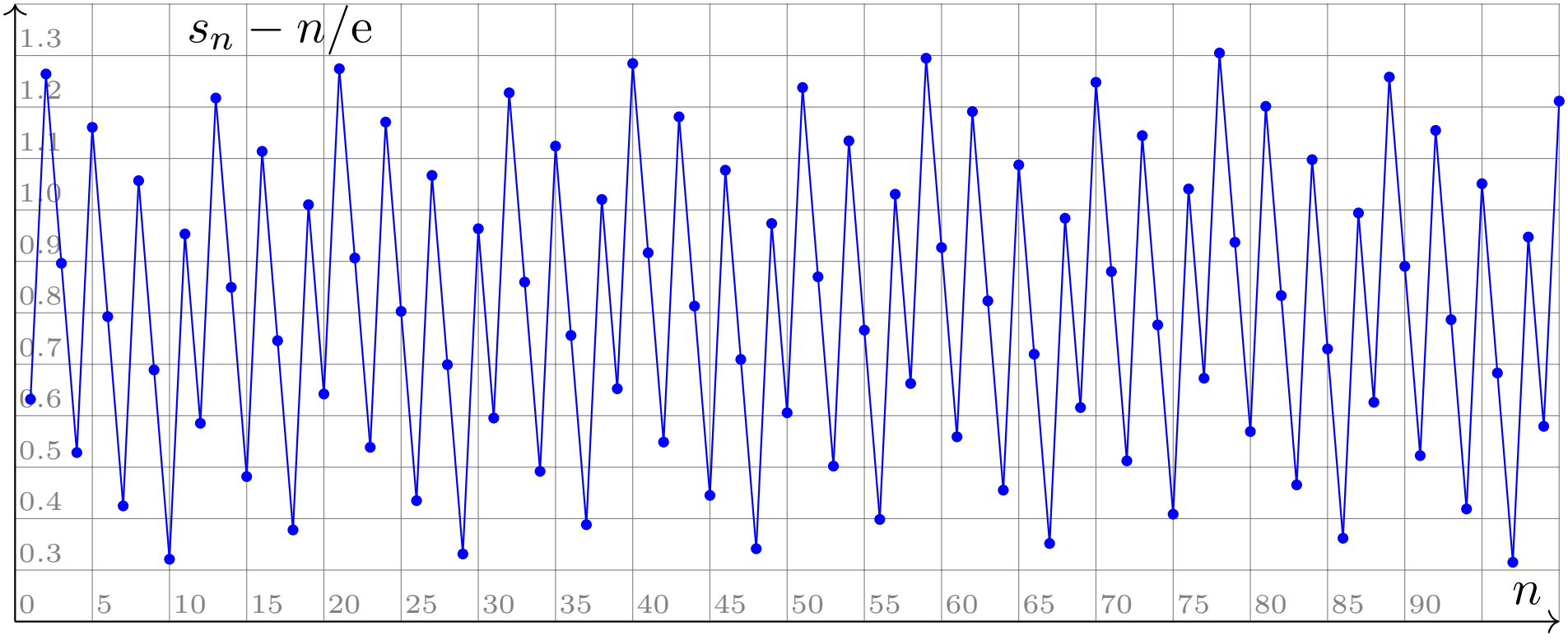
Der Aufruf `bruss(5)` liefert als Ergebnis das Wertepaar `3, 0.433`. Auf diese Weise wurden die Werte für die obige Tabelle berechnet.

☺ Die Korrektheit dieser Rechnung verdanken wir dem obigen Satz: Grundlagen / Theorie und Programmierung / Anwendung ergänzen sich!

# Optimales Stoppen: der Bruss–Algorithmus

**Aufgabe:** Vergleichen Sie die Stoppzeit $s_n$ mit der Faustformel $n/\mathrm{e}$.

**Lösung:** Die Berechnung übernimmt bequem unser obiges Programm.
Die folgende Graphik zeigt die Differenz $s_n - n/\mathrm{e}$ für $n = 1, \ldots, 100$:




Somit gilt $s_n = \lceil n/\mathrm{e} \rceil$ oder $s_n = \lceil n/\mathrm{e} \rceil + 1$, zumindest für alle $n \leq 100$.
Das bietet eine einfache, doch recht genaue Näherungsformel für $s_n$.

# Optimales Stoppen: der Bruss–Algorithmus

 Wenn Sie die logische Entwicklung dieser Aufgabe nachvollziehen, werden Sie ein interessantes Wechselspiel erkennen und verstehen:

- Wir beginnen mit einem **konkreten Beispiel**,
  nämlich der Analyse des Spiels für den Fall $n = 5$.
- Dadurch erkennen wir das **allgemeine Muster**
  und können dies anschließend als Satz C5C beweisen.
- Mit dem so gewonnenen Algorithmus können wir
  **weitere Beispiele** lösen und mehr Daten erschließen.
- Daran beobachten wir ein **genaueres Muster**.
  Dies wollen wir nun als Satz C5D beweisen!

Dieses Wechselspiel von theoretischen Grundlagen und praktischen Anwendungen, von mathematischen Sätze und numerischen Experimenten, ist durchaus typisch und überaus erfolgreich.

 So können wir uns langsam auf unbekanntes Terrain vortasten, Muster erkennen, Vermutungen formulieren und Ergebnisse beweisen.

# Optimales Stoppen: der Bruss–Algorithmus

Zu $n \in \mathbb{N}_{\geq 2}$ suchen wir die Stoppzeit $s_n$. Unsere numerischen Experimente lassen uns die folgende einfache Regel vermuten:

## Satz C5D: die $37\%$–Regel

Das Sekretärinnen-Problem wird durch folgende Faustformel gelöst:

(1) Für alle $n \in \mathbb{N}_{\geq 2}$ gilt $s_n = \lceil n/\mathrm{e} \rceil$ oder $s_n = \lceil n/\mathrm{e} \rceil + 1$, kurzum:

$$\boxed{s_n \;\approx\; n/\mathrm{e}}$$

(2) Die Gewinnerwkt ist $w_n = R_s Q_s$ mit $R_s \gtrapprox 1$ und $Q_s = (s-1)/n$, also:

$$\boxed{w_n \;\approx\; 1/\mathrm{e}}$$

Für $n \to \infty$ gilt $s_n/n \to 1/\mathrm{e}$ und $w_n \to 1/\mathrm{e}$. Als numerische Werte haben wir $\mathrm{e} \approx 2.718$ und $1/\mathrm{e} \approx 0.368$, daher der Name „$37\%$–Regel“.

**Aufgabe:** Beweisen Sie diese Näherungen. *Tipp:* Approximieren Sie hierzu die Summe durch ein Integral, $\sum_{k=s}^{n-1} \frac{1}{k} \gtrapprox \int_s^n \frac{1}{x}\,\mathrm{d}x = \ln(n/s)$.

# Optimales Stoppen: der Bruss–Algorithmus

**Lösung:** (1) Vorgegeben ist die natürliche Zahl $n \in \mathbb{N}_{\geq 2}$.
Wir suchen die Lösung $s \in \{1, \ldots, n\}$ zu folgender Ungleichung:

$$(*) \qquad \sum_{k=s+1}^{n} \frac{1}{k-1} \;<\; 1 \;\leq\; \sum_{k=s}^{n} \frac{1}{k-1}$$

Der Vergleich von Summe und Integral liefert hier:

$$\sum_{k=s}^{n-1} \frac{1}{k} \;\geq\; \int_{x=s}^{n} \frac{1}{x}\,\mathrm{d}x \;=\; \ln\Big(\frac{n}{s}\Big)$$

$$\sum_{k=s-1}^{n-1} \frac{1}{k} \;\leq\; \int_{x=s-2}^{n-1} \frac{1}{x}\,\mathrm{d}x \;=\; \ln\Big(\frac{n-1}{s-2}\Big)$$

Wir setzen dazu stillschweigend $s \geq 3$ voraus, also $n \geq 5$.
Die kleinen Fälle $n \leq 4$ lösen wir direkt, wie oben gezeigt.

# Optimales Stoppen: der Bruss–Algorithmus

Wir nutzen nun die Doppelungleichung $(*)$ und schließen:

$$\ln\Big(\frac{n}{s}\Big) < 1 \quad \Longrightarrow \quad s > n/\mathrm{e}$$

$$\ln\Big(\frac{n-1}{s-2}\Big) \geq 1 \quad \Longrightarrow \quad s \leq n/\mathrm{e} + 2 - 1/\mathrm{e}$$

Da $s$ eine ganze Zahl ist, folgt durch Auf/Abrunden:

$$\lceil n/\mathrm{e} \rceil \leq s \leq \lfloor n/\mathrm{e} + 2 - 1/\mathrm{e} \rfloor$$

Das bedeutet $s = \lceil n/\mathrm{e} \rceil$ oder $s = \lceil n/\mathrm{e} \rceil + 1$, oder zusammengefasst:

$$\boxed{s \in \lceil n/\mathrm{e} \rceil + \{0, 1\}}$$

Für große $n$ ist die kleine verbleibende Unsicherheit $\{0, 1\}$ unerheblich.
Für kleine $n$ können wir mühelos eine Tabelle anlegen, wie oben erklärt.
Allgemeiner Satz und numerische Rechnung ergänzen sich wunderbar!

# Optimales Stoppen: der Bruss–Algorithmus

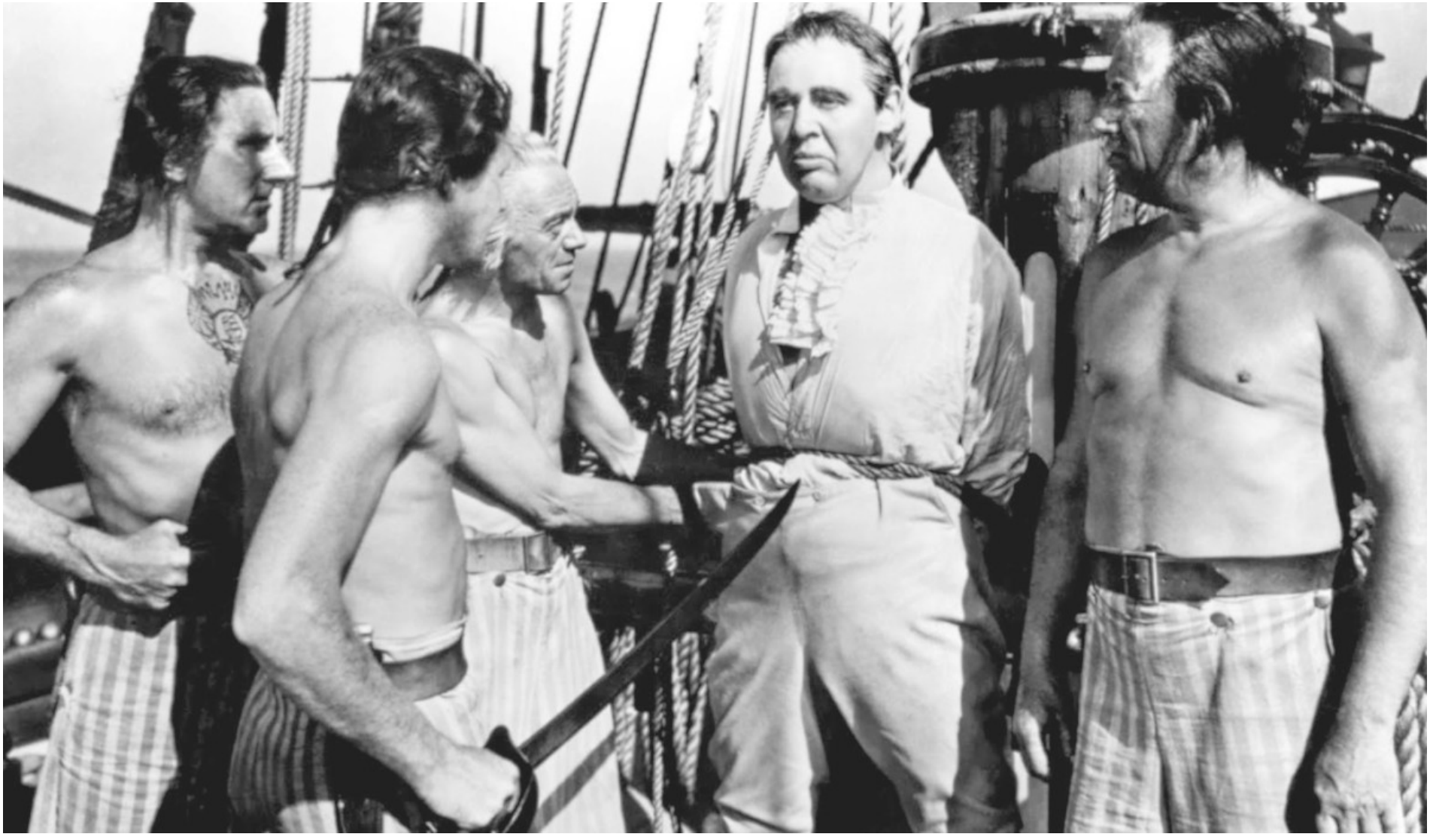
Damit ist das Sekretärinnen-Problem gelöst, theoretisch und praktisch. Es ist ein Paradebeispiel für die rekursive Lösung komplexer Probleme. In der schön konkreten Geschichte steckt abstrakt allgemeine Wahrheit. Solche Modelle werden tatsächlich genutzt für Online-Auktionen u.ä.

Das ist nur die Spitze des Eisbergs, damit beginnt erst das Abenteuer! Fragen des **optimalen Stoppens** finden sich nahezu überall in der Stochastik, insbesondere der Ökonomik und der Finanzmathematik, zum Beispiel beim Börsenhandel mit Aktien oder Optionen.

Die Frage lautet allgemein: Wie wählen wir den optimalen Zeitpunkt für eine Aktion? Unser Ziel ist es, den erwarteten Gewinn zu maximieren oder die erwarteten Kosten zu minimieren. Viele solche Probleme können rekursiv gelöst werden, so wie in unserem Beispiel.

Diese Knobelaufgabe ist also nicht nur lehrreich für den Themenkreis Induktion / Rekursion / Rückwärtsinduktion, sondern zugleich ein erstes Anwendungsbeispiel, ein motivierender Startpunkt für die Optimierung, hier einer Stoppzeit, die weitreichende Anwendungen erschließt.

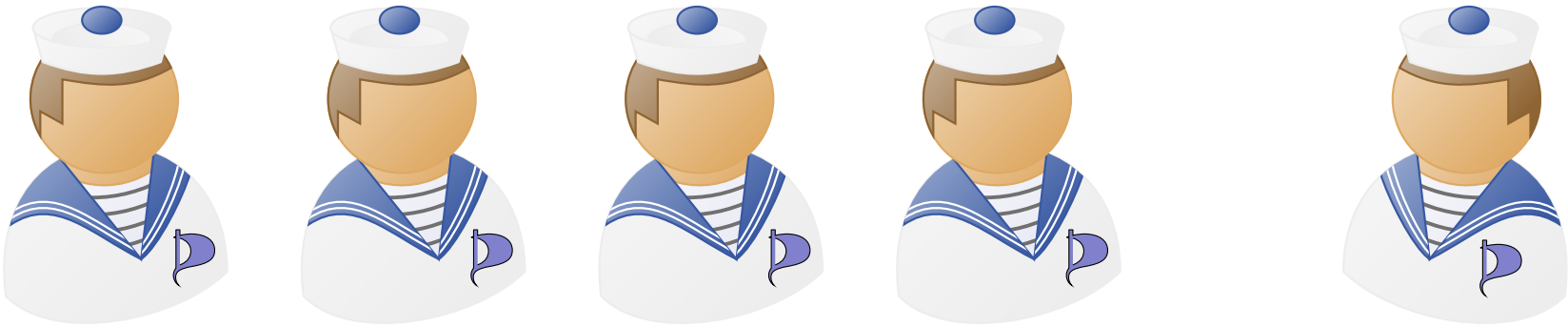
# Meuterei auf der Bounty (1935)



*Mutiny on the Bounty* mit Clark Gable und Charles Laughton unter der Regie von Frank Lloyd. Oscar 1936 als bester Film.

# Fünf gierige Piraten [*the pirate game*]

Fünf basisdemokratische Piraten $1, 2, 3, 4, 5$ teilen sich $100$ Dukaten.
(nach Ian Stewart: *A Puzzle for Pirates.* Scientific American 5/1999)




Der ranghöchste Pirat $5$ schlägt eine Zuteilung zur Abstimmung vor.
Stimmt mindestens die Hälfte dafür, so wird diese Zuteilung ausgeführt.
Bei Ablehnung wird der Vorschlagende über Bord ins Meer geworfen,
und die verbleibenden Piraten beginnen das Spiel von vorn.

Präzisierung: Ein Dukat ist unteilbar. Jeder Pirat will A: selbst überleben,
B: möglichst viel Gold, C: bei Indifferenz lieber andere ins Meer werfen,
D: lieber rangniedrige bestechen als ranghohe. Jeder Pirat ist rational.
Absprachen sind unmöglich, denn jeder misstraut jedem anderen und
würde Absprachen brechen. Diese Fakten sind gemeinsames Wissen.

# Fünf gierige Piraten [*the pirate game*]

Naiv könnte man vermuten, der ranghöchste Pirat muss um sein Leben fürchten und daher all sein Gold hergeben. Das Gegenteil ist der Fall!

**Aufgabe:** Lösen Sie das Piratenrätsel für $n = 5$, sowie für alle $n \in \mathbb{N}$.

**Lösung:** Wir nutzen Induktion über $n = 1, 2, 3, 4, 5, \ldots$ und finden:

| | 1 | 2 | 3 | 4 | 5 | … | 197 | 198 | 199 | 200 | 201 | 202 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 100 | ☠ | ☠ | ☠ | ☠ | … | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| $\mathscr{R}_1$ | 0 | 100 | ☠ | ☠ | ☠ | … | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| $\mathscr{R}_2$ | 1 | 0 | 99 | ☠ | ☠ | … | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| $\mathscr{R}_3$ | 0 | 1 | 0 | 99 | ☠ | … | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| $\mathscr{R}_4$ | 1 | 0 | 1 | 0 | 98 | … | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| ⋮ | | | | | | | | | | | | |
| $\mathscr{R}_{197}$ | 0 | 1 | 0 | 1 | 0 | … | 0 | 2 | ☠ | ☠ | ☠ | ☠ |
| $\mathscr{R}_{198}$ | 1 | 0 | 1 | 0 | 1 | … | 1 | 0 | 1 | ☠ | ☠ | ☠ |
| $\mathscr{R}_{199}$ | 0 | 1 | 0 | 1 | 0 | … | 0 | 1 | 0 | 1 | ☠ | ☠ |
| $\mathscr{R}_{200}$ | 1 | 0 | 1 | 0 | 1 | … | 1 | 0 | 1 | 0 | 0 | ☠ |
| $\mathscr{R}_{201}$ | 0 | 1 | 0 | 1 | 0 | … | 0 | 1 | 0 | 1 | 0 | 0 |

# Fünf gierige Piraten [*the pirate game*]

☺ Scharfsinn, Systematik & Induktion liefern die erstaunliche Antwort!
Wir nutzen die Prioritäten A–C und strenge Rationalität, insb. Egoismus ohne Kooperation. Real beobachtetes Verhalten kann davon abweichen.

⚠ Im Spiel mit $n \geq 201$ Piraten geht es nur noch ums Überleben!
Der Vorschlagende $n = 201, 202, 204, 208, \ldots$ kann überleben,
der Verschlagende $n = 203, 205, 206, 207, \ldots$ leider nicht.

Zur Analyse zerlegen wir $n = 200 + 2^k + r$ mit $k, r \in \mathbb{N}$ und $0 \leq r < 2^k$.

Im Falle $0 < r < 2^k$ geht Pirat $n$ über die Planke, egal was er vorschlägt:
Er kann nur $100$ Piraten bestechen. Dazu bekommt er alle $r$ Stimmen der Todgeweihten (inklusive seiner selbst). Das bleibt eine Minderheit.

Im Falle $r = 0$ überlebt Pirat $n = 200 + 2^k$ durch folgende Strategie:

- Falls $k$ gerade ist, gibt er allen Ungeraden $1, 3, \ldots, 199$ je ein Dukat.
- Falls $k$ ungerade ist, gibt er allen Geraden $2, 4, \ldots, 200$ je ein Dukat.

So bekommt er alle $100$ Stimmen der Bestochenen und zusätzlich noch alle $2^k - 2^{k-1} = 2^{k-1}$ Stimmen der Geretteten (inklusive seiner selbst).

☺ Prioritäten A–D lösen Indifferenzen und garantieren Eindeutigkeit.

# Ein Komitee zur Verbesserung der Hochschullehre

Die chronisch unterfinanzierte Hochschullehre soll mit einer Förderung von $50$ k€ exzellent werden. (Das ist aberwitzig, aber besser als nichts.) Ein Komitee von zwölf Professoren teilt die Fördersumme unter sich auf.


Der dienstälteste Professor $12$ legt eine Zuteilung zur Abstimmung vor. Bei Ablehnung wird der Vorschlagende als befangen ausgeschlossen, und die verbleibenden Professoren beginnen das Komiteespiel von vorn. Präzisierung: Ein k€ ist unteilbar. Weiter gelten obige Piratenregeln.

**Aufgabe:** Welcher Professor erhält wie viel von der Fördersumme?
Lösen Sie das Komiteespiel mit folgenden Abstimmungsregeln:
(1) Annahme erfordert mehr als die Hälfte der Stimmen.
(2) Annahme erfordert mindestens zwei Drittel der Stimmen.
(3) Annahme gilt erst bei höchstens einer Gegenstimme.

# Das Komiteespiel: mehr als die Hälfte

**Lösung:** (1) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

| $n$ | $q$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 50 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 2 | 2 | 50 | 0 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 3 | 2 | 0 | 1 | 49 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 4 | 3 | 1 | 2 | 0 | 47 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 5 | 3 | 2 | 0 | 1 | 0 | 47 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 6 | 4 | 0 | 1 | 2 | 1 | 0 | 46 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 7 | 4 | 1 | 2 | 0 | 0 | 1 | 0 | 46 | ☠ | ☠ | ☠ | ☠ | ☠ |
| 8 | 5 | 2 | 0 | 1 | 1 | 0 | 1 | 0 | 45 | ☠ | ☠ | ☠ | ☠ |
| 9 | 5 | 0 | 1 | 2 | 0 | 1 | 0 | 1 | 0 | 45 | ☠ | ☠ | ☠ |
| 10 | 6 | 1 | 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 44 | ☠ | ☠ |
| 11 | 6 | 2 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 44 | ☠ |
| 12 | 7 | 0 | 1 | 2 | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 43 |

Jeder Vorsitzende $n$ kann sich das Quorum $q = 1 + \lfloor n/2 \rfloor$ billig erkaufen und sich selbst den Löwenanteil des zu verteilenden Geldes sichern.

# Das Komiteespiel: mindestens zwei Drittel

**Lösung:** (2) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

| $n$ | $q$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 50 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 2 | 2 | 50 | 0 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 3 | 2 | 0 | 1 | 49 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 4 | 3 | 1 | 2 | 0 | 47 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 5 | 4 | 2 | 3 | 1 | 0 | 44 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 6 | 4 | 3 | 0 | 2 | 1 | 0 | 44 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 7 | 5 | 0 | 1 | 3 | 2 | 1 | 0 | 43 | ☠ | ☠ | ☠ | ☠ | ☠ |
| 8 | 6 | 1 | 2 | 0 | 3 | 2 | 1 | 0 | 41 | ☠ | ☠ | ☠ | ☠ |
| 9 | 6 | 2 | 3 | 1 | 0 | 0 | 2 | 1 | 0 | 41 | ☠ | ☠ | ☠ |
| 10 | 7 | 3 | 0 | 2 | 1 | 1 | 0 | 2 | 1 | 0 | 40 | ☠ | ☠ |
| 11 | 8 | 0 | 1 | 3 | 2 | 2 | 1 | 0 | 2 | 1 | 0 | 38 | ☠ |
| 12 | 8 | 1 | 2 | 0 | 3 | 0 | 2 | 1 | 0 | 2 | 1 | 0 | 38 |

Jeder Vorsitzende $n$ kann sich das Quorum $q = \lfloor 3n/2 \rfloor$ billig erkaufen und sich selbst den Löwenanteil des zu verteilenden Geldes sichern.

# Das Komiteespiel: höchstens eine Gegenstimme

**Lösung:** (3) Wir nutzen Induktion über $n = 1, 2, \ldots, 12$ und finden:

| $n$ | $q$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 50 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 2 | 1 | 0 | 50 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 3 | 2 | 1 | 0 | 49 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 4 | 3 | 2 | 1 | 0 | 47 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 5 | 4 | 3 | 2 | 1 | 0 | 44 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 6 | 5 | 4 | 3 | 2 | 1 | 0 | 40 | ☠ | ☠ | ☠ | ☠ | ☠ | ☠ |
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 35 | ☠ | ☠ | ☠ | ☠ | ☠ |
| 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 29 | ☠ | ☠ | ☠ | ☠ |
| 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 22 | ☠ | ☠ | ☠ |
| 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 14 | ☠ | ☠ |
| 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 | 5 | ☠ |
| 12 | 11 | 0 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 5 | 0 |

Professor $12$ kann sich nicht genug Unterstützung erkaufen. Professor $11$ hingegen bringt seinen Vorschlag mit überwältigender Mehrheit durch.

# Tanz der Vampire: Wissen und gemeinsames Wissen

In Transsylvanien treffen sich einmal jedes Jahr $100$ Vampire zum Tanz.
Anschließend verharren sie den Rest des Jahres schlafend in der Gruft.

Vampire altern nicht, sind untrüglich intelligent und vollkommen rational.
Jeder weiß dies. Auch dies weiß jeder. Selbst dies weiß jeder. Usw.

Jeder Vampir trägt ein Schandmal deutlich sichtbar auf seiner Stirn.
Dies weiß keiner von sich selbst, da Vampire kein Spiegelbild werfen.
Erführe er es, er suchte den Freitod im nächsten Sonnenaufgang.
(Diese Vampire verbrennen im Sonnenlicht. *Wear sunscreen!*)

Hingegen sieht jeder Vampir das Schandmal bei jedem anderen.
Jeder sieht es. Jeder weiß es. Auch dies weiß jeder. Usw. usw. usw.
Höfliche Rücksicht gebietet jedoch strenges Stillschweigen darüber.
(Tabuisierte Kommunikation der Vampire ist ihre große Schwäche.)

Im Jahr $2001$ platzt der Vampirjäger Professor Abronsius in das Fest:
„Mindestens einer von Euch trägt ein Schandmal!“ schreit er und flieht.
Die Vampire sehen keinen Grund, seiner Aussage zu widersprechen:
Er sagt ihnen nur, was ohnehin jeder heimlich weiß. Oder etwa nicht?

# Tanz der Vampire: Wissen und gemeinsames Wissen


Vampire werfen bekanntlich kein Spielbild.
Das führt zu komplizierten Verwicklungen.

**Aufgabe:** Was geschieht? Nichts? Plötzliche Erkenntnis? Wann?

**Lösung:** Nach dem Fest $2100$ sterben alle Vampire im Sonnenaufgang.
Führen Sie sorgfältig einen Beweis per Induktion: Was ist die Aussage?
Wie ist das möglich? Welche Neuigkeit hat der Professor verraten?

# Tanz der Vampire: Wissen und gemeinsames Wissen

Hier geht es um gemeinsames Wissen / *common knowledge*.
Nur weil eine Aussage wahr ist, weiß dies noch längst nicht jeder!
Nur weil es jeder weiß, ist es noch kein gemeinsames Wissen!

Die untrügliche Intelligenz der Vampire ist gemeinsames Wissen:
$\mathscr{R}_1$: Jeder Vampir ist untrüglich intelligent und vollkommen rational.
$\mathscr{R}_k$: Es gilt $\mathscr{R}_{k-1}$, und jeder Vampir weiß $\mathscr{R}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{R}_\infty$: Es gilt $\mathscr{R}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

Die Anzahl der Schandmale hingegen ist kein gemeinsames Wissen:
$\mathscr{S}_1$: Jeder ehrbare Vampir sieht alle $n$ Schandmale der anderen,
jeder Schandmalträger jedoch sieht genau $n-1$ Schandmale.
$\mathscr{S}_k$: Es gilt $\mathscr{S}_{k-1}$, und jeder Vampir weiß $\mathscr{S}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{S}_\infty$: Es gilt $\mathscr{S}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

Professor Abronsius' Aussage hingegen liefert stärkere Information:
$\mathscr{A}_1$: Jeder Vampir weiß, dass es mindestens ein Schandmal gibt.
$\mathscr{A}_k$: Es gilt $\mathscr{A}_{k-1}$, und jeder Vampir weiß $\mathscr{A}_{k-1}$. (Stufe $k \in \mathbb{N}_{\geq 2}$)
$\mathscr{A}_\infty$: Es gilt $\mathscr{A}_k$ für alle $k \in \mathbb{N}_{\geq 1}$. (gemeinsames Wissen)

# Tanz der Vampire: Wissen und gemeinsames Wissen

Es lohnt sich, diese berüchtigte Rätsel sorgfältig zu durchleuchten!
Wir nehmen hierzu an, genau $n$ Vampire tragen ein Schandmal,
und behaupten: Diese sterben am Morgen nach Fest $2000 + n$.

Im Falle $n = 1$ ahnt der Träger zunächst nichts vom Schandmal.
Durch Abronsius' Aussage erkennt er seine Schande und stirbt bei
Sonnenaufgang. (Wir nutzen die Voraussetzungen $\mathscr{A}_1$, $\mathscr{S}_1$ und $\mathscr{R}_1$.)

Im Falle $n = 2$ erwarten die beiden Träger den Freitod des anderen.
Beim Fest $2002$ treffen sie sich jedoch wieder, völlig unerwartet.
Dadurch erkennt jeder der beiden klar seine Schande und stirbt.
(Wir nutzen hierzu die Voraussetzungen $\mathscr{A}_2$, $\mathscr{S}_2$, $\mathscr{R}_2$ und den Fall $1$.)

Per Induktion gilt dieses Argument für jede natürliche Zahl $n \in \mathbb{N}_{\geq 2}$:
Jeder der $n$ Träger sieht genau $n - 1$ Schandmale und geht davon aus,
dass er keines trägt. Er erwartet daher den Freitod der $n - 1$ anderen
nach dem Fest $2000 + n-1$. Alle treffen sich jedoch beim Fest $2000 + n$
unerwartet wieder. Dadurch erkennt jeder zweifelsfrei seine Schande.
(Wir nutzen hierzu die Voraussetzungen $\mathscr{A}_n$, $\mathscr{S}_n$, $\mathscr{R}_n$ und den Fall $n - 1$.)

# Schmutzige Gesichter: eigenes und gegenseitiges Wissen

Hier ein berühmtes Logikrätsel aus der Folklore der Talmudschulen als Zentren jüdischer Gelehrsamkeit. (`de.wikipedia.org/wiki/Jeschiwa`)
Es handelt von eigenem Wissen und von gegenseitigem Wissen...

(1) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Na wohl der mit dem schmutzigen Gesicht!“ — „Falsch! Der Schmutzige sieht den Sauberen und denkt, sein Gesicht sei auch sauber. Der Saubere sieht den Schmutzigen und denkt, sein Gesicht sei auch schmutzig, also geht er sich waschen.“

(2) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Aber wir haben doch eben schon festgestellt: der mit dem sauberen Gesicht!“ — „Falsch: Beide gehen sich waschen. Überlege logisch: Der Saubere sieht den Schmutzigen und geht sich waschen. Der Schmutzige sieht das und versteht, dass sein Gesicht schmutzig ist, also geht auch er sich waschen.“

# Schmutzige Gesichter: eigenes und gegenseitiges Wissen

(3) Rabbi: „Zwei Männer klettern durch einen Kamin. Der eine kommt mit sauberem Gesicht heraus, der andere mit schmutzigem. Wer von beiden geht sich nun waschen?“ — Schüler: „Na, beide gehen sich waschen.“ — „Falsch: Keiner von beiden. Der Schmutzige sieht den Sauberen und geht sich nicht waschen. Der Saubere sieht das und versteht, dass sein Gesicht sauber ist, also geht auch er sich nicht waschen.“

(4) „Zwei Männer klettern durch einen Kamin. . . “ — „Ich weiß, keiner von beiden wird sich waschen.“ — „Falsch! Sage mir: Wie kann es sein, dass zwei Männer durch denselben Kamin klettern, und der eine macht sein Gesicht schmutzig, der andere aber nicht? Die ganze Frage ist unsinnig. Wenn du dein Leben dazu verwendest, sinnlose Fragen zu beantworten, werden auch alle deine Antworten sinnlos sein.“

**Aufgabe:** Wie lösen Sie den Widerspruch zwischen (2) und (3)?

**Lösung:** Zur Festlegung dieses Spiels fehlen uns noch Informationen: Wir benötigen die genaue Reihenfolge der Züge / Signale / Folgerungen! Erst zieht Spieler 1, dann Spieler 2 mit dem Wissen des vorigen Zuges.

# Schmutzige Gesichter: eigenes und gegenseitiges Wissen

Schmutzige Gesichter gibt es in vielen Rätseln, hier etwa in der Bahn:

Das Mathematische Forschungsinstitut Oberwolfach liegt wunderbar idyllisch mitten im Schwarzwald, etwa zweidrittelwegs von Stuttgart nach Freiburg. Im Zug zu unserem fiktiven Workshop „Mathematical Logic“ sitzen $12$ berühmte Logiker, manche davon mit schmutzigem Gesicht. Alle können sich gegenseitig sehen, es gibt jedoch keinen Spiegel, und diese überaus schüchternen Menschen reden nicht miteinander.

Der Schaffner erklärt der Gruppe höflich: „Mindestens zwei von Ihnen haben schmutzige Gesichter. Diese sollten schnellstmöglich aussteigen und sich waschen.“ An den nächsten Bahnhöfen $1, 2, 3, 4, 5$ passiert noch nichts. Erst am sechsten Bahnhof steigen einige der Passagiere aus, um sich das Gesicht zu waschen. Wie viele sind es?

**Aufgabe:** Lösen Sie dieses Logikrätsel. Präzisieren Sie alle hierzu nötigen Annahmen. Warum ist der Takt der Bahnhöfe wichtig?

**Lösung:** Genau sieben Personen haben ein schmutziges Gesicht. (Die Zahl $12$ ist hier vollkommen beliebig und überflüssig.)

# Schmutzige Gesichter: eigenes und gegenseitiges Wissen

Angenommen, es gibt genau $n \in \{2, 3, \ldots, 12\}$ schmutzige Gesichter.

Im Falle $n = 2$ wissen die beiden Betroffenen sofort Bescheid: Jeder der beiden sieht nur ein schmutziges Gesicht. Nach Aussage des Schaffners gibt es jedoch mindestens zwei. Daraus schließt jeder Betroffene richtig, das sein Gesicht schmutzig ist, und steigt am 1. Bahnhof aus.

Im Falle $n = 3$ sieht jeder Betroffene genau zwei schmutzige Gesichter und erwartet daher, dass diese am 1. Bahnhof aussteigen werden, wie zuvor im Fall $n = 2$ erklärt. Da dies jedoch nicht geschieht, folgert er richtig, das sein Gesicht schmutzig ist, und steigt am 2. Bahnhof aus.

Das Argument setzt sich per Induktion für alle $n$ fort. Dazu muss gelten: $\mathscr{R}_2$: Jeder kann richtig sehen und logisch schließen, wie oben erklärt. $\mathscr{R}_3$: Es gilt $\mathscr{R}_2$, und jeder weiß es. $\mathscr{R}_n$: Es gilt $\mathscr{R}_{n-1}$, und jeder weiß es.

Konkretes Beispiel: Alle Betroffenen steigen am sechsten Bahnhof aus. Demnach gibt es genau sieben Personen mit schmutzigem Gesicht.

Der vorgegebene Takt der Bahnhöfe ist wesentlich, damit allen klar ist, wann eine Aktion ausgeführt werden kann oder unterlassen wurde.

# Das Problem der Stuttgarter Mathematiker

Das folgende Rätsel stammt aus *Forschung und Lehre* (5/2019, S.503):

*An der Universität Stuttgart gibt es 17 Professoren (m/w) im Fachbereich Mathematik. Sie treffen sich einmal im Monat bei Sitzungen. Bei einer früheren Sitzung haben sie die Regel eingeführt, dass jeder Professor, der von einem Fehler in einer von ihm selbst publizierten Arbeit erfährt, sein Amt bei der nächsten Sitzung niederlegen muss. Noch nie ist ein Professor zurückgetreten. Das bedeutet aber nicht, dass keiner der Professoren je einen Fehler publiziert hat. Im Gegenteil, jeder Professor hat schon Fehler publiziert, und jeder andere hat das bemerkt. Man könnte auch so sagen: Jeder Professor weiß, dass jeder andere Professor schon Fehler gemacht hat, weiß aber nichts von eigenen Fehlern. Eines Tages besucht der Rektor der Universität den Fachbereich und hält eine kleine Ansprache, in der er einen denkwürdigen Satz spricht: „Ich muss Ihnen mitteilen, dass ein Professor unter Ihnen bemerkt hat, dass ein anderer Professor einen Fehler publiziert hat.“ Was passiert als Reaktion auf die Bekanntgabe des Rektors? […] Der Rektor sagt natürlich die Wahrheit. Und alle Professoren sind perfekte Logiker. Sowie absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler begangen hat. Zwei Alternativen möchte ich Ihnen anbieten: Antwort 1: […] Nichts passiert. Antwort 2: Recht lange passiert gar nichts. Aber dann, in der 17-ten Sitzung nach der Rede des Rektors treten alle 17 Professoren zurück.*

# Das Problem der Stuttgarter Mathematiker

Zur Antwort 2 wird folgende Erklärung geboten (F&L 5/2019, S.471):

*Was passiert, wenn es unter den 17 Professoren nur einen gäbe, der einen Fehler publiziert hat? Nennen wir ihn schwarzes Schaf. Da er von keinem schwarzen Schaf weiß, muss er aufgrund der Rede des Rektors schließen, dass er selbst ein schwarzes Schaf ist. Also muss er in der 1. Sitzung nach der Rede zurücktreten.*

*Wie ist es bei zwei schwarzen Schafen $A$ und $B$? Beide treten in der 1. Sitzung nicht zurück, da zwar jeder weiß, dass der andere ein schwarzes Schaf ist, aber nichts über sich selbst erschließen kann. Doch da $B$ in der 1. Sitzung nicht zurücktritt, muss $A$ schlussfolgern, dass er selbst ein schwarzes Schaf ist. Denn andernfalls hätte $B$ nach der Rede gewusst, dass er ein schwarzes Schaf ist und wäre in der 1. Sitzung zurückgetreten. Also muss $A$ in der 2. Sitzung zurücktreten. $B$ führt denselben Gedankengang durch, und auch er tritt in der 2. Sitzung zurück. […]*

*So kann man sich bis zur Situation mit 17 schwarzen Schafen vorarbeiten. Alle werden auf der 17. Sitzung zurücktreten. […] Der Rektor hat den Professoren doch Information vermittelt. Offensichtlich gibt es in einer Gruppe verschiedene Formen des Wissens. Jeder kann eine Tatsache $T$ wissen. Zusätzlich kann jeder wissen, dass jeder andere auch $T$ weiß. Ferner kann jeder wissen, dass jeder weiß, dass jeder $T$ weiß. Usw.*

# Das Problem der Stuttgarter Mathematiker

**Aufgabe:** Lesen Sie aufmerksam das obige Rätsel. Leider gingen bei der Übertragung dieses Rätselklassikers auf Stuttgarter Mathematiker wesentliche Voraussetzungen verloren. Ist Antwort 1 weiterhin möglich?

**Lösung:** Hier geht es um gemeinsames Wissen / *common knowledge*.
Nur weil eine Aussage wahr ist, weiß dies noch längst nicht jeder!
Nur weil es jeder weiß, ist es noch kein gemeinsames Wissen!

Die Antwort 2 nutzt Aussage $P$: *Alle Professoren sind perfekte Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat.* Die Gültigkeit der Aussage $P$ allein genügt jedoch nicht, es muss auch jeder wissen, dass $P$ gilt, usw. Denkbar wäre folgendes:

1. Nehmen wir an, jeder Professor ist ein perfekter Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat, doch mindestens ein Professor hält manch anderen für fehleranfällig. Die Aussage des Rektors, ein Professor habe eines anderen Fehler entdeckt, lässt ihn daher kalt, denn auf die Meinung dieses Kollegen gibt er nicht viel. Daher scheitert schon der Induktionsanfang.

# Das Problem der Stuttgarter Mathematiker

Zahlreiche weitere Varianten sind denkbar und in der hier angegebenen Formulierung des Rätsels nicht geklärt, weder bejaht noch verneint.

2. Nehmen wir weiterhin $P$ an: Jeder Professor ist ein perfekter Logiker und absolut fehlerfrei bei der Beurteilung, ob ein anderer einen Fehler publiziert hat. Zudem gelte $P'$: Jeder Professor weiß die Tatsache $P$. Jeder Professor glaubt also an die perfekte Urteilskraft jedes Kollegen. Er weiß allerdings nicht, ob die anderen dies ebenfalls glauben.

Hier gelingt noch der Induktionsanfang: Gibt es nur ein schwarzes Schaf, so erkennt es durch die Aussage des Rektors seinen eigenen Fehler.

Der Schluss von einem auf zwei schwarze Schafe hingegen misslingt. Die beiden schwarzen Schafe $A$ und $B$ treten in der 1. Sitzung nicht zurück. Kann $A$ nun schlussfolgern, dass er ein schwarzes Schaf ist? Leider nein: $A$ kann / muss befürchten, dass $B$ nicht an die perfekte Urteilskraft jedes Kollegen glaubt; die Aussage des Rektors ließe dann $B$ völlig kalt, da $B$ auf die Meinung seiner Kollegen nichts gibt. Daher scheitert hier der Induktionsschritt von $1$ auf $2$.

# Der unerwartete Abischerz: Wie ist das möglich?

Das folgende Paradox existiert in vielen Varianten, etwa als unerwartete Hinrichtung, `en.wikipedia.org/wiki/Unexpected_hanging_paradox`, Feueralarmübung oder Klassenarbeit, hier umgedreht als Abischerz.

*Darum wachet! Denn ihr wisst weder Tag noch Stunde.*
(Matthäus 25,13, Lutherbibel 2017)

Nach einer wahren Begebenheit: Die Abiturienten eines Gymnasiums planen ihren Abischerz. Aus Termingründen kommen dafür genau fünf Tage, Montag bis Freitag, in Frage. Die ängstliche Schulleiterin möchte den Termin wissen. Die Schüler verweigern dies mit der Begründung, der Abischerz müsse für die Lehrer vollkommen überraschend sein.

Die Schulleiterin denkt sich daher folgendes: „Der Abischerz kann sicher nicht am Freitag stattfinden, denn das ist der letzte mögliche Termin. Wäre bis Freitag Morgen nichts geschehen, dann wüssten wir, dass der Abischerz an diesem Tag stattfindet. Das wäre nicht überraschend.“

# Der unerwartete Abischerz: Wie ist das möglich?

Die Schulleiterin folgert sofort weiter: „Der Abischerz kann auch nicht am Donnerstag stattfinden. Freitag haben wir bereits ausgeschlossen. Wäre bis Donnerstag Morgen nichts geschehen, dann wüssten wir, dass der Abischerz an diesem Tag stattfindet. Das wäre nicht überraschend.“

Ebenso schließt die Schulleiterin Mittwoch, Dienstag und Montag aus und kommt zu dem Schluss: „Es wird gar kein Abischerz stattfinden.“ Alle Lehrer bewundern die logischen Ausführungen der Schulleiterin.

Die Abiturienten veranstalten ihren Abischerz am Mittwoch.
Wie vorhergesagt sind alle Lehrer vollkommen überrascht.

**Aufgabe:** Alle Argumente scheinen logisch. Was also geht schief?

**Lösungsidee:** Die Eigenschaft „vollkommen überraschend“ ist kritisch; sie ist nicht präzise definiert und wird daher unterschiedlich interpretiert. Weitere Probleme sind Selbstbezüglichkeit und evtl. Widersprüchlichkeit. Wie das Paradoxon aufzulösen ist, darüber wird anhaltend diskutiert; hierzu gibt es ungefähr so viele Lösungsvorschläge wie Autoren.

# Der unerwartete Abischerz: Wie ist das möglich?

*Es ist sehr wichtig, keine unbewiesenen Annahmen zu treffen,*
*aber noch wichtiger ist es, keine Worte zu benutzen,*
*hinter denen sich kein klarer Sinn verbirgt.*
(William Kingdon Clifford, 1845–1879)

**Lösung:** Wir können das Paradoxon auflösen, indem wir der vagen Formulierung „vollkommen überraschend“ einen präzisen Sinn geben. Hierzu betrachten wir wie zuvor verschiedene Stufen des Wissens:

$\mathscr{R}_0$: Der Abischerz findet höchstens an einem der fünf Tage Mo, Di, Mi, Do, Fr statt. Im Falle vertrödelter Planung gibt es keinen Abischerz.

$\mathscr{R}_1$: Es gilt $\mathscr{R}_0$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

$\mathscr{R}_2$: Es gilt $\mathscr{R}_1$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

$\mathscr{R}_n$: Es gilt $\mathscr{R}_{n-1}$, die Schulleiterin weiß dies, kann aber am Morgen des Abischerzes nicht sicher vorhersagen, dass er an diesem Tag stattfindet.

# Der unerwartete Abischerz: Wie ist das möglich?

Dank Aussage $\mathscr{R}_0$ kann die Schulleiterin den Termin des Abischerzes immerhin auf die fünf fraglichen Tage Mo, Di, Mi, Do, Fr eingrenzen.
Mit $\mathscr{R}_1$ kann sie Fr ausschließen, es bleiben nur Mo, Di, Mi, Do.
Mit $\mathscr{R}_2$ kann sie Fr, Do ausschließen, es bleiben nur Mo, Di, Mi.
Mit $\mathscr{R}_3$ kann sie Fr, Do, Mi ausschließen, es bleiben nur Mo, Di.
Mit $\mathscr{R}_4$ kann sie Fr, Do, Mi, Di ausschließen, es bleibt also nur Mo.
Mit $\mathscr{R}_5$ kann sie alle fünf Tage ausschließen: Es gibt keinen Abischerz.

Die Schulleiterin interpretiert die Aussage „vollkommen überraschend“ im stärksten Sinne als $\mathscr{R}_5$ oder noch höher. Aus dieser starken Annahme folgert sie zurecht, dass es dieses Jahr keinen Abischerz geben kann.

Die Abiturienten interpretieren „vollkommen überraschend“ nur als $\mathscr{R}_1$. Ihr Abischerz am Mittwoch ist so gesehen vollkommen überraschend.

⚠ Diese Beispiele zeigen eindringlich: In strategischen Situationen sind Wissen und Nichtwissen oft entscheidend, sowohl eigenes als auch gegenseitiges und gemeinsames. Eine sichere Analyse setzt präzise Formulierung voraus und erfordert mathematische Sorgfalt und Disziplin.