Formale Grundlagen der Informatik

SoSe 2008 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Formale Grundlagen der Informatik

Gesamtübersicht

1. Rechnen: Gesetze und Regeln
2. Zählen und Würfeln: Kombinatorik und Wahrscheinlichkeitsrechnung
3. Modellieren und Formalisieren: Keine Angst vor Formalismen
4. Warum stimmt das eigentlich ? Beweisverfahren
5. Herangehen an Aufgaben aus Informatik und Mathematik

Organisatorisches

Vorlesung Montag 8.15 bis 11.30 im HS 11 (mit Pause)
an den folgenden Tagen: 8.45 bis 12.00 (mit Pause)
12-14 Uhr: Gelegenheit zur Gruppenarbeit zu ausgewählten Übungen
parallel dazu: 13.30-14.15 **Sprechstunde**: Wir fünf sind im 4.OG für Sie da.
(Große) Übung 14-16 Uhr, d.h.: 14.15-15.45 (Gulan, Raible, Bakman, Schlecht) im H 406
Am Abend überdenken Sie bitte den Stoff; sie erhalten auch Gelegenheit zu weiteren Übungen.
An den folgenden Tagen stehen Ihnen Studierende (Bakman, Schlecht) von 8.00 bis 8.45 im H 406 für Fragen hier zur Verfügung. Dann werden auch die Übungen vom letzten Abend angesprochen. **(Kleine) Übung; Sprechstunde**
(Weitere Unterrichtsformen: praktische Übungen, Seminare)

Beweisverfahren—Warum stimmt das eigentlich ?

Es gibt verschiedene Arten der Beweisführung:
direkte Beweise
indirekte Beweise / Beweise durch Widerspruch
konstruktive / algorithmische Beweise (sehr informatisch)
nicht-konstruktive Beweise (siehe Chomp)
Induktionsbeweise

Für alle diese Beweise haben Sie in der Schule Beispiele kennengelernt.

Für die Informatik ist Beweisen wichtig insbesondere im Zusammenhang mit der Korrektheit von Programmen und ihrer Laufzeit.

Korrektheit von Programmstücken—ein einfaches Beispiel:

`swap(x,y)` soll die Werte der beiden Variablen `x` und `y` vertauschen.
Dies Verhalten wurde beim Sortieralgorithmus verwendet.
Oft gibt es `swap` nicht als elementaren Befehl.
$\rightsquigarrow$ `swap` muss erst durch eine Folge einfacherer *Zuweisungen* simuliert werden,
unter Zuhilfenahme einer *Hilfsvariablen* `h`:

```
h:=x; x:=y; y:=h
```

Warum arbeitet das Programmstück korrekt als Implementierung von `swap` ?
Betrachten wir einen direkten Beweis hierfür:
Eingangs gilt: `x` enthalte den Wert a und `y` enthalte den Wert b; der Wert von `h` ist beliebig.
Nach dem ersten Befehl enthält mit `x` auch `h` den Wert a, die übrigen Werte sind unverändert.
Nach dem zweiten Befehl enthält `h` den Wert a, während `x` und `y` den Wert b besitzen.
Am Ende enthalten `y` und auch `h` den Wert a, während `x` den Wert b enthält.
Tatsächlich sind also die Inhalte von `x` und `y` vertauscht worden.

Eine Aufgabe: Überprüfung der Korrektheit von Programmen
Frage: Was berechnet das folgende Programmstück (in Pseudo-Code) ?

1. Lies ganze Zahlen v, x, y, z ein.

2. Setze $u := v \cdot x$. (u ist eine Hilfsvariable für ganze Zahlen.)

3. Setze $u := (u + y) \cdot x$.

4. Setze $u := u + z^2$.

5. Gib u aus.

Beweisverfahren—Warum stimmt das eigentlich ?

Es gibt verschiedene Arten der Beweisführung:
Die voranstehende Argumentation mit *Vorbedingungen* und *Nachbedingungen* ist ein Beispiel für einen direkten Beweis.

Das Schema dieses Beweisverfahrens ist:
Ausgangslage: Es gibt eine Menge W von wahren Aussagen und eine Aussage $\mathfrak{a}$, die zu zeigen ist.
Schrittweise wird nun W erweitert:
Man argumentiert, warum aus den Aussagen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \in W$ die (neue) Aussage $\mathfrak{a}'$ folgt, die nunmehr in W aufgenommen werden kann.
Diese Argumentationsweise bricht ab, sobald $\mathfrak{a}$ in W aufgenommen werden konnte.

Direkte Beweise und Korrektheit von Programmstücken

Korrektheitsbeweise für einfache Programmstücke passen wie folgt in diese Beweisstruktur:
Anfangs enthält W Aussagen über Variablenbelegungen vor dem Durchlauf des Programmstücks, etwa von der Form:
"Unmittelbar vor der Abarbeitung der Zeile 1 enthält die Variable x den Wert 2."
Aus Aussagen der Form: "Unmittelbar vor der Abarbeitung der Zeile i gilt: ..." (Vorbedingungen) werden nun, durch Nachvollziehen des Befehls auf der Zeile i, Aussagen der Form "Unmittelbar vor der Abarbeitung der Zeile $\mathrm{i}+1$ gilt: ..." gewonnen (Nachbedingungen).
Unter der Annahme, das Programm enthalte eine letzte Zeile n mit dem "leeren Befehl" **end** sollten nun die Aussagen (oder einige der Aussagen) der Form "Unmittelbar vor der Abarbeitung der Zeile n gilt: ..." den Aussagen entsprechen, die man eigentlich über das Programmstück als Nachbedingungen insgesamt beweisen will.

Direkter Beweis—ein einfaches Beispiel

Behauptung: Das Quadrat jeder geraden natürlichen Zahl n ist gerade.

Beweis: Es sei n eine gerade natürliche Zahl.
Da n gerade, lässt sich n eindeutig als $n = 2k$ darstellen; hierbei ist k ist eine natürliche Zahl.
Darauf folgert man (mit Kommutativ- und Assoziativgesetzen):

$$n^2 = (2 \cdot k)^2 = 2 \cdot (2k^2)$$

Da $2k^2$ mit k eine natürliche Zahl ist, ist n^2 daher das Doppelte einer natürlichen Zahl und damit gerade.

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Grundidee: Folgt aus einer Aussage p etwas offensichtlich Falsches, so muss das Gegenteil, formal $\neg\mathrm{p}$, richtig sein.

Wie beim direkten Beweis können wir dabei (evtl. hypothetisch) eine Menge wahrer oder als wahr angenommener Aussagen W nach und nach erweitern, bis wir gezwungen wären, sowohl die Wahrheit von q als auch die Wahrheit der Verneinung $\neg\mathrm{q}$ einzuräumen.

Der indirekte Beweis—ein logisches Beispiel

Satz: $(\mathrm{p} \Rightarrow \mathrm{q})$ ist logisch äquivalent zu $(\neg\mathrm{q} \Rightarrow \neg\mathrm{p})$.

Beweis: Es seien p und q irgendwelche logischen Aussagen, denen mithin entweder der Wahrheitswert **wahr** oder **falsch** zukommt.
Wir zeigen: Gilt $\mathrm{p} \Rightarrow \mathrm{q}$, so folgt $(\neg\mathrm{q} \Rightarrow \neg\mathrm{p})$.
Wahre Aussagen sind mithin $W = \{\mathrm{p} \Rightarrow \mathrm{q}, \neg\mathrm{q}\}$ und wir müssen zeigen, dass (durch Erweiterung von W) schließlich $\neg\mathrm{p}$ in W liegt.
Nehmen wir einmal an, p wäre wahr. Wegen $\mathrm{p} \Rightarrow \mathrm{q}$ wäre dann aber auch q wahr, im Widerspruch zu $\neg\mathrm{q} \in W$. also ist unsere Annahme falsch, d.h., p ist falsch, also $\neg\mathrm{p}$ kann in W aufgenommen werden.

Die umgekehrte Richtung sieht man genauso.

Der vorige Satz ist die Grundlage für:
Beweis durch Umkehrschluss (Kontraposition)

Lemma: Ist eine Quadratzahl ungerade, so auch ihre Wurzel.

Was bedeutet dieser Satz ? Ausführliche Schreibweise:

Es sei a *eine natürliche Zahl.*
Wenn a^2 *eine ungerade Zahl ist, dann ist* a *ungerade.*

Wir haben also die Aussage(forme)n:
$p(a) := (a^2$ ist ungerade$)$ und $q(a) := (a$ ist ungerade$)$.
Unser Satz lautet also: $\forall a \in \mathbb{N}(p(a) \Rightarrow q(a))$.

Kontraposition $\rightsquigarrow \forall a \in \mathbb{N}(\neg q(a) \Rightarrow \neg p(a))$.

Beweis durch Umkehrschluss (Kontraposition) (Forts. des Bsp.)

Zu zeigen ist also: *Es sei* a *eine natürliche Zahl.*
Wenn a *keine ungerade Zahl ist, dann ist* a^2 *nicht ungerade.*
Dies ist offensichtlich eine komplizierte Formulierung für:
Ist a gerade, so auch a^2.
Eine Zahl a heißt *gerade* gdw. $2 \mid a$ (2 ist Teiler von a).

Beweis: (nochmal formalisierter aufgeschrieben)
a gerade $\Rightarrow (\exists k(a = 2k)) \Rightarrow (\exists k(a \cdot a = (2k) \cdot a)) \Rightarrow (\exists k(a^2 = 2 \cdot (ka))) \Rightarrow a^2$ gerade.

Satz: Eine Quadratzahl ist genau dann gerade, wenn ihre Wurzel gerade ist.

Aufgabe: Beweisen Sie diesen Satz ! Was ist noch zu zeigen, wenn wir die obigen Aussagen benutzen dürfen ? Welche “Beweisfigur” haben Sie verwendet ?

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Grundidee: Folgt aus einer Aussage p etwas offensichtlich Falsches, so muss das Gegenteil, formal $\neg p$, richtig sein.

Satz: $\sqrt{2}$ ist irrational.

Beweis: Wir führen die Annahme, $x = \sqrt{2}$ wäre rational, zum Widerspruch.

x rational $\rightsquigarrow$ es gibt *teilerfremde* $a, b \in \mathbb{Z} : x = a/b$.

$\rightsquigarrow 2 = x^2 = a^2/b^2 \rightsquigarrow 2b^2 = a^2$

$\rightsquigarrow a^2$ ist gerade $\rightsquigarrow a$ ist gerade (s. obiger Satz)

$\rightsquigarrow a = 2c$ für eine ganze Zahl $c \rightsquigarrow 2b^2 = 4c^2$

$\rightsquigarrow b^2 = 2c^2 \rightsquigarrow b^2$ ist gerade $\rightsquigarrow b$ ist gerade

Also: 2 ist Teiler von a und von b, im Widerspruch zur Wahl von a und b.

Peano-Axiome: ein klassisches Beispiel einer *rekursiven Definition*

axiomatische Definition der Menge der natürlichen Zahlen $\mathbb{N}$ durch Giuseppe Peano (1889)
eigentlich von Richard Dedekind in “Was sind und was sollen die Zahlen ?” (1888)
1. 0 ist eine natürliche Zahl.
2. Zu jeder natürlichen Zahl n gibt es genau einen Nachfolger n', der ebenfalls eine natürliche Zahl ist.
3. Es gibt keine natürliche Zahl, deren Nachfolger 0 ist.
4. Zwei verschiedene natürliche Zahlen n und m besitzen stets verschiedene Nachfolger n' und m'.
5. Enthält eine Menge X die Zahl 0 und mit jeder natürlichen Zahl n auch stets deren Nachfolger n', so enthält X bereits alle natürlichen Zahlen. *Induktionsaxiom*
(Ist X dabei selbst eine Teilmenge der natürlichen Zahlen, dann ist $X = \mathbb{N}$.)

Peano verwendet dabei die Begriffe 0, Zahl und *Nachfolger*.

Wie sehen natürliche Zahlen aus ? (nach Dedekind / Peano)

$0, 0', 0'', 0''', 0'''', \ldots$

Es ist jedoch bequemer, bei der gewohnten Schreibweise zu bleiben:

$0, 1, 2, 3, 4, \ldots$

Diese ist überdies deutlich kürzer als die rekursiv definierte.

Rekursion versus Induktion

Induktiv können wir "der Reihe nach" die definierten Objekte auflisten.

Den umgekehrten Weg geht die Rekursion: n' ist eine natürliche Zahl, wenn n eine ist, und das ist der Fall, wenn entweder $n = 0$ gilt oder aber n von der Form m' ist...

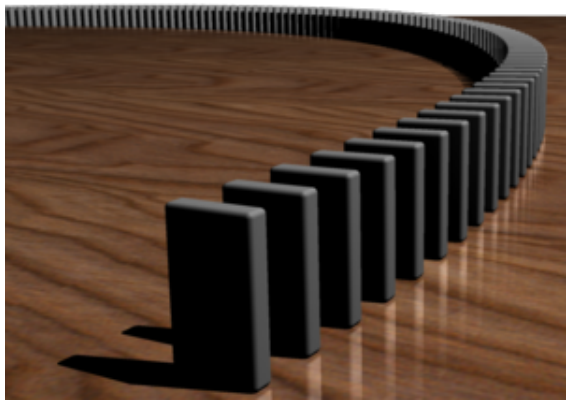
Grundgedanke der mathematischen Induktion

Es sei $p(n)$ eine Aussageform, die von $n \in \mathbb{N}$ abhängt.
Mathematische Induktion ist eine Beweistechnik, die auf dem Induktionsaxiom fußt und schematisch wie folgt arbeitet.

1. *Induktionsanfang* (IA) (auch *Anker* genannt): Zeige $p(0)$.
2. *Induktionsschritt* (IS) Es wird gezeigt, dass für alle $n \in \mathbb{N}$ gilt: Aus $p(n)$ folgt $p(n+1)$.
$p(n)$ heißt hier auch *Induktionsannahme* oder *Induktionsvoraussetzung* (IV).

Nach dem Prinzip der mathematischen Induktion folgt hieraus:
Für alle natürlichen Zahlen n gilt: $p(n)$.

Induktion veranschaulicht: Der Dominoeffekt:



Die Aufstellung gewährleistet:
Wenn der k-te Dominostein in der Reihe fällt, so auch der $k+1$-te.

Jetzt fällt der erste Dominostein.

Folgerung: Schließlich werden alle Steine umgefallen sein.

Ein gutes Einführungskapitel, das auch wieder unsere Bemerkungen zu den Fibonacci-Zahlen ergänzt, finden Sie hier.

Induktion am Beispiel.

Satz: $\forall n \in \mathbb{N}(n^2 = \sum_{i=1}^{n}(2i-1))$.

Beweis: IA: Die "leere Summe" ist gleich Null, d.h., die Behauptung gilt für $n = 0$.
IS: Angenommen, die Aussage gilt für n. Dann rechnen wir:

$$\begin{aligned}
(n+1)^2 &= n^2 + 2n + 1 && \text{binomischer Lehrsatz} \\
&= (\sum_{i=1}^{n}(2i-1)) + 2n + 1 && \text{IV} \\
&= \sum_{i=1}^{n+1}(2i-1)
\end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die Behauptung.

Summenregel I

Satz: Sind A und B disjunkte endliche Mengen, so gilt:

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

Beweis: Die Aussage ist trivial für $|B| = 0$, also $B = \emptyset$.

Die Aussage ist ebenso klar für $|B| = 1$, also $B = \{a\}$ für ein $a \notin A$. (*)

Im IS nehmen wir an, die Aussage würde für alle B mit $|B| \leq n$ gelten.

Betrachte ein B mit $|B| = n + 1$. Also ist $B \neq \emptyset$.

Wähle $b \in B$ willkürlich, aber fest. Auf $B' = B \setminus \{b\}$ lässt sich die IV anwenden.

$\rightsquigarrow |A \cup B'| = |A| + |B'|$.

Wegen (*) gilt $|A \cup B| = |(A \cup B') \cup \{b\}| = |A| + (|B'| + 1) = |A| + |B' \cup \{b\}| = |A| + |B|$. $\rightsquigarrow$ Beh.

Summenregel II (allgemein)

Satz: Sei $k \in \mathbb{N}$ und $A_1, \ldots, A_k$ seien endliche, paarweise disjunkte Mengen. Dann gilt:

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

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

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

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

Ein weiteres Beispiel: Money, Money, Money, ...

Satz: Jeder Cent-Betrag ≥ 4 Cent kann unter ausschließlicher Verwendung von 2- und 5-Cent-Münzen bezahlt werden.

Beweis: Klar für 4 Cent.

Angenommen, wir wissen, wie $n > 4$ Cent bezahlt werden können, nämlich mit n_2 2-Cent-Münzen und mit n_5 5-Cent-Münzen. $\rightsquigarrow n = 2n_2 + 5n_5$.

Da $n > 4$, gilt $n_2 \geq 2$ oder $n_5 \geq 1$ (klar ?).

Wir geben jetzt zwei Regeln an, mit denen wir $n + 1$ Cent mit n_2' 2-Cent-Münzen und mit n_5' 5-Cent-Münzen bezahlen können:

Gilt $n_2 \geq 2$, so setze $n_2' := n_2 - 2$ und $n_5' := n_5 + 1$.

Andernfalls gilt $n_5 \geq 1$. $\rightsquigarrow$ Setze $n_2' = n_2 + 3$, $n_5' := n_5 - 1$.

Probe: $n + 1 = 2n_2 + 5n_5 + 1 = 2(n_2 - 2) + 5(n_5 + 1) = 2(n_2 + 3) + 5(n_5 - 1)$.

Die Behauptung folgt (wie genau ?) mit mathematischer Induktion.

Programmtexte als Formalismen—ein Weg zur Informatik

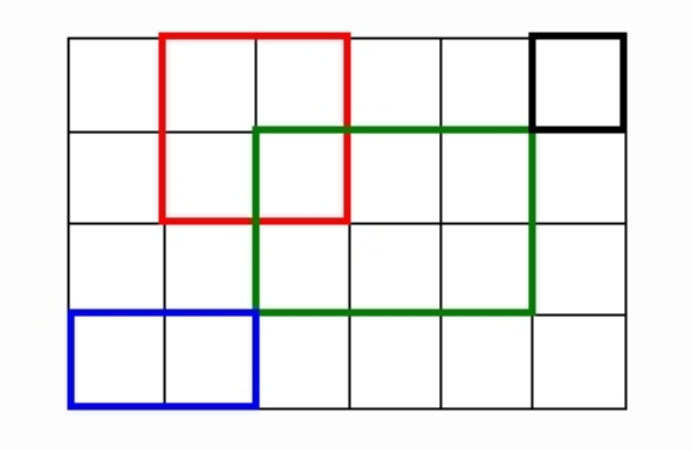
```
procedure BS(A)
//Die Eingabe A ist eine Liste zu sortierender Gegenstände
  for each i from 1 to length(A) do:
       for each j from length(A) downto i + 1 do:
         if A[ j ] < A[ j-1 ] then
           swap( A[ j ], A[ j-1 ] )
         end if
//A[j-1] ist ein kleinstes Element von A[j-1],...,A[length(A)]
       end for
//A[i] ist ein kleinstes Element von A[i],...,A[length(A)]
//Die Liste A[1],..,A[i] ist aufsteigend sortiert
  end for
end procedure
```

Programmtexte als Formalismen—ein Weg zur Informatik

```
procedure BS(A)
//Die Eingabe A ist eine Liste von n zu sortierenden Gegenständen
  for each i from 1 to n do:
       for each j from n downto i + 1 do:
         if A[ j ] < A[ j-1 ] then
           swap( A[ j ], A[ j-1 ] )
         end if
       end for
//swap wird höchstens n−i mal ausgeführt
  end for
//(Die äußere Schleife wird n mal ausgeführt.)
//Also wird swap insgesamt höchstens (n−1)+(n−2)+···+1 = n(n−1)/2 mal ausgeführt
end procedure
```

Aufgabe: Welche Teile müssten Sie noch beweisen ?!
Wie könnte man das Programm noch vereinfachen aufgrund Ihrer / unserer Betrachtungen ?

Nochmals etwas Geometrie auf Schachrechtecken...



Beweise: In einem rechteckigen Gitter mit x Spalten und y Zeilen lassen sich, auf den Gitterlinien zeichnend,

$$1/2 \cdot x \cdot (x+1) \cdot 1/2 \cdot y \cdot (y+1)$$

verschiedene Rechtecke einzeichnen. Quelle

Definition: Ich kürze obige Formel im Folgenden mit $R(x,y)$ ab.

Damit das Gitter einen Sinn macht, müssen x und y größer 0 sein.

Nochmals etwas Geometrie auf Schachrechtecken...

Wir wenden Induktion nach $z = x + y$ an, zeigen also, dass die Behauptung für $x + y = 2$ gilt (Induktionsanfang), und dass unter der Induktionsvoraussetzung

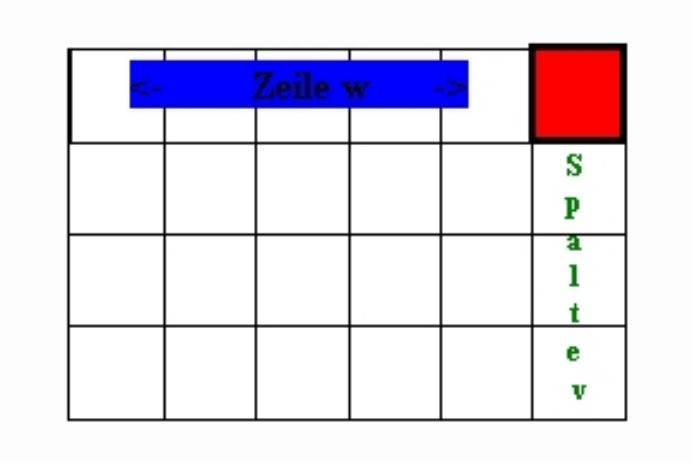
Anzahl Rechtecke in einem Gitter mit x Spalten und y Spalten $= R(x, y)$

der Induktionschritt auf $x + y + 1$ möglich ist.

Induktionsanfang: $x + y = 2 \rightsquigarrow$
Einziges mögliches Gitter besteht aus 1 Spalte und 1 Zeile.
Es ist $R(x, y) = 1$ und tatsächlich kann man nur ein Rechteck zeichnen.

Nochmals etwas Geometrie auf Schachrechtecken...

Induktionsschluss: Ein rechteckiges Gitter mit Spalten und Zeilen sei gegeben und die Summe der Anzahlen der Zeilen und Spalten sei gleich $x + y + 1$.
Wir wissen nicht, aus wievielen Zeilen und Spalten das Gitter besteht, wir kennen nur deren Summe. Damit wir aber formulieren und rechnen können, nennen wir die Anzahl der Spalten v und die Anzahl der Zeilen w.
Natürlich muss gelten $v > 0$ und $w > 0$ und nach Ansatz $v + w = x + y + 1$.
Wir stellen uns dieses Gitter aufgezeichnet vor und markieren das rechte obere Quadrat rot.
Die Spalten und Zeilen nummerieren wir von 1 bis v bzw. von 1 bis w, so dass das rote Quadrat in der Spalte v und in der Zeile w liegt.



Nochmals etwas Geometrie auf Schachrechtecken...

Die Anzahl der möglichen Rechtecke in diesem Gitter mit v Spalten und w Zeilen kann man nun disjunkt aufteilen in:

A = Menge der Rechtecke, die das rote Quadrat nicht enthalten.

B = Menge der Rechtecke, die das rote Quadrat enthalten.

Wir betrachten folgende Teilmengen der Menge A:

A_1 = Menge der Rechtecke ohne ein Quadrat aus der Spalte v

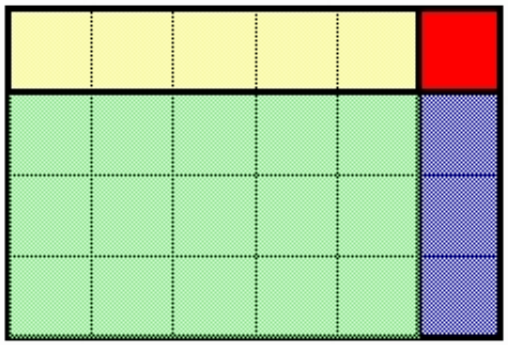
A_2 = Menge der Rechtecke ohne ein Quadrat aus der Zeile w

Weil es Rechtecke gibt, die weder ein Quadrat aus der Spalte v noch eines aus der Zeile w enthalten, ist das keine disjunkte Zerlegung.

Darum formulieren wir noch die Schnittmenge von A_1 und A_2

A_3 = Menge der Rechtecke ohne ein Quadrat aus der Zeile w und ohne ein Quadrat aus der Spalte v

Nochmals etwas Geometrie auf Schachrechtecken...



Die Menge A_1 ist die Menge der Rechtecke in einem Gitter mit $v-1$ Spalten und w Zeilen (im grün und gelb markierten Teil des Gitters).
Die Menge A_2 ist die Menge der Rechtecke in einem Gitter mit v Spalten und $w-1$ Zeilen (im grün und blau markierten Teil des Gitters).
Die Menge A_3 ist die Menge der Rechtecke in einem Gitter mit $v-1$ Spalten und $w-1$ Zeilen. (im grün markierten Teil des Gitters)
Es gilt: $A_3 = A_1 \cap A_2$.
In allen Fällen ist die Summe der Anzahl der Spalten und Zeilen kleiner $v+w = x+y+1$.
Also gilt nach IV: $|A| = |A1| + |A2| - |A3| = R(v-1,w) + R(v,w-1) - R(v-1,w-1)$
Bis hierhin haben wir alle Rechtecke, die das rote Rechteck nicht enthalten, gezählt, bzw. wir haben eine rekursive Formel für die Berechnung dieser Rechtecke gefunden.

Nochmals etwas Geometrie auf Schachrechtecken...

Nun betrachten wir die Menge B genauer.
B ist die Menge der Rechecke, die das rote Quadrat enthalten. Gesucht ist $|\mathrm{B}|$.
Wenn das rote Quadrat in einem Rechteck enthalten ist, dann gehören 0 bis $v-1$ Quadrate der Zeile w und 0 bis $w-1$ Quadrate der Spalte v dazu.
Wir können alle Rechtecke zählen, wenn wir jeweils eine Anzahl von Quadraten aus der Spalte v wählen (w Möglicheiten von 0 bis $w-1$) und anschließend die Anzahl der Quadrate aus der Zeile w wählen von keines bis alle, also v Möglichkeiten.
$\rightsquigarrow$ Die Anzahl der Rechtecke mit dem roten Quadrat ist also gleich $w \cdot v = |\mathrm{B}|$.
Damit können wir die Gesamtzahl der Quadrate in einem Gitter mit v Spalten und w Ecken angeben als (mit $v+w = x+y+1$):
$|\mathrm{A}| + |\mathrm{B}| = \mathrm{R}(v-1, w) + \mathrm{R}(v, w-1) - \mathrm{R}(v-1, w-1) + v \cdot w$
Schreiben wir die durch $\mathrm{R}(,)$ gemeinten Formel hin: $|\mathrm{A}| + |\mathrm{B}| = 1/4 \cdot (v-1) \cdot v \cdot w \cdot (w+1) + 1/4 \cdot v \cdot (v+1) \cdot (w-1) \cdot w - 1/4 \cdot (v-1) \cdot v \cdot (w-1) \cdot w + v \cdot w$
Nun kann man durch Termumformungen die Gleichheit mit dem zu beweisenden Ausdruck
$\mathrm{R}(v, w) = 1/2 \cdot v \cdot (v+1) \cdot 1/2 \cdot w \cdot (w+1)$
zeigen. q.e.d.

Übungsaufgaben Beweisen Sie:

1. $\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$.

2. $1 + x + ... + x^{(n-1)} = \sum_{k=0}^{n-1} x^k = (1 - x^n)/(1 - x)$ für $x \neq 1$.

3. Informieren Sie sich über die “Türme von Hanoi”. Wie viele Züge müssen die Mönche (wenigstens) machen ?!

Jargon

Für gute Beweise sind gute Sprechweisen unerlässlich.
Jargon—mathematische Formalismen—und ihr Nutzen wurden auszugsweise bereits gestern erklärt.

Hier wird diese Galerie etwas erweitert:

1. Finden Sie geeignete Platzhalter / Variablen:

Schauen Sie sich daraufhin nochmals die bislang durchgeführten Aufgaben an. Nicht immer sind x, y, z die einzig mögliche Wahl ;-)

2. Benutzen Sie mathematische Sprechweisen / Fachvokabular (richtig) !

Dieses ist oft über Jahrhunderte entstanden und hat sich so bewährt. Das sehen Sie am besten,

wenn Sie mal versuchen, mathematische Orginalliteratur zu lesen, die älter als 150 Jahre ist. Das bereitet nicht nur Schwierigkeiten, weil damals viel auf Latein und Französisch geschrieben wurde...

Hilfreich sind verschiedenste Abkürzungen:

(a) logische Symbole: $\wedge$ UND; $\vee$ ODER AUCH; $\Longrightarrow$ IMPLIZIERT (daraus folgt; wenn..., dann); $\Longleftrightarrow$ GENAU DANN, WENN; ...

Quantoren: $\forall \mathfrak{x}$ FÜR ALLE $\mathfrak{x}$ GILT; $\exists \mathfrak{y}$ FÜR EIN $\mathfrak{y}$ GILT;

(b) Mengenschreibweise (das Cantorsche Paradies):

$\mathfrak{x} \in \mathcal{M}$: $\mathfrak{x}$ liegt in $\mathcal{M}$; $\mathcal{A} \cup \mathcal{B}$: Vereinigung; $\mathcal{A} \cap \mathcal{B}$: Schnitt, $\mathcal{A} \subseteq \mathcal{B}$: Mengeneinschluss / Inklusion; ...

(a) und (b) erscheinen gerne in Kombination:

Man verwendet gerne logische Ausdrücke, um Teilmengen zu beschreiben.

Man verwendet gerne Variablen aus verschiedenen Mengenbereichen: $\forall \mathfrak{x} \in \mathcal{M}$:

Tatsächlich sind viele Rechengesetze der Mengenlehre und Logik sich so ähnlich, dass die Theorie der Booleschen Algebren versucht, diese geeint darzustellen.

Jargon entschlüsseln

Eine *Folge* reeller Zahlen ist eine Funktion $F : \mathbb{N} \to \mathbb{R}$.

Wie heißt gewöhnlich die Folge F, wenn ihr die folgend beschriebene Eigenschaft (X) zukommt ?

(1) $\forall n \in \mathbb{N} : F(n) \geq F(n+1)$
(2) $\forall n \in \mathbb{N} : F(n) < F(n+1)$
(3) $\exists c \in \mathbb{R} \forall n \in \mathbb{N} : |F(n)| < c$
(4) $\exists c \in \mathbb{R} \forall e \in \mathbb{R}_{>0} \exists N \in \mathbb{N} \forall n \in \mathbb{N} (n \geq N \implies |F(n) - c| < e)$.
Wie heißt dann c gemeinhin ?

Etwas Zahlentheorie

Die *Zahlentheorie* beschäftigt sich im Wesentlichen mit den natürlichen Zahlen (oder auch den ganzen Zahlen) und ihren Eigenschaften.
Ihr Gegenstand ist Ihnen daher seit Ihrer Kindheit vertraut.

Für $a, b \in \mathbb{Z}$ heißt a *Teiler* von b (bwz. b *Vielfaches* von a) gdw. es ein $a' \in \mathbb{Z}$ mit $a \cdot a' = b$ gibt. Schreibweise: $a \mid b$: a teilt b

Beweisen Sie die folgenden Eigenschaften für beliebige ganze Zahlen a, b, c, d, e:

1. $a \mid a$ und $(-a) \mid a$.
2. $1 \mid a$ und $(-1) \mid a$.
3. $a \mid 0$; aus $0 \mid b$ folgt $b = 0$.
4. $((a \mid b) \wedge (b \mid a)) \Rightarrow ((a = b) \vee (a = -b))$.
5. $((a \mid b) \wedge (b \mid c)) \Rightarrow (a \mid c)$.
6. $((a \mid b) \wedge (a \mid c)) \Rightarrow (a \mid (db + ec))$.
7. $((a \mid b) \wedge (c \mid d)) \Rightarrow (ac \mid bd)$.

Noch mehr Zahlentheorie

Für $a \in \mathbb{Z}$ sei T_a die Menge aller positiven Teiler von a. Enthält T_p für eine natürliche Zahl p genau zwei Elemente, so heißt p *Primzahl*. Ist p Primzahl und gilt $p|n$, so heißt p *Primteiler* von n.

Beweisen Sie mit vollständiger Induktion:
Satz: Jede natürliche Zahl $n \geq 2$ besitzt mindestens einen Primteiler.
Hinweis: Verwenden Sie die Aussageform $A(n)$: "Jedes $k \in \mathbb{N}$ mit $2 \leq k \leq n$ besitzt einen Primteiler." und beweisen Sie $\forall n A(n)$ mit Induktion.

Führen Sie einen Widerspruchsbeweis unter Verwendung des voranstehenden Satzes für den berühmten Satz von Euklid: Es gibt unendlich viele Primzahlen.