Beweistechniken

Vorlesungsskript zur Übung *Beweistechniken*

Teil des Moduls *Entwurf und Analyse von Algorithmen für angewandte Informatik*

Prof. Dr. Markus Nebel

6. Oktober 2013

Inhaltsverzeichnis

1 Was ist ein Beweis?

Nachfolgend wollen wir die wesentlichen Techniken zum Führen eines mathematischen Beweises wiederholen. Dieser Abschnitt kann dabei keinesfalls das intensive Studium dieser Techniken ersetzen, er soll jedoch eine Hilfestellung bieten, um das entsprechende Wissen aufzufrischen. Wir wollen dabei damit beginnen, uns vor Augen zu führen, was ein Beweis überhaupt ist:

> *Ein Beweis ist eine Folge von Aussagen, von denen jede logisch aus den bisherigen folgt (siehe Ableitungsbegriff der Kalküle). Dabei starten wir mit „Dingen", die wir als gültig (wahr) annehmen (siehe Axiome der Kalküle).*

Als Konsequenz hat ein Beweis drei Teile, einen *Anfang*, eine *Mitte* und ein *Ende*. Der Anfang enthält dabei jene Dinge, die wir als wahr annehmen wollen, wobei die Definitionen der Objekte über die wir sprechen oder aber über sie bewiesene Aussagen dazu gehören. Die Mitte wird aus jenen Aussagen gebildet, die wir jeweils logisch aus dem zuvor gesagten folgern. Das Ende ist die Aussage, die wir beweisen möchten.

Beispiel 1: *Rechenregel in Ringen*

Es sei $(R, +, \cdot)$ ein beliebiger *Ring*[1]. Unter Verwendung der Ring-Axiome wollen wir zeigen, dass

$$(\forall a, b, c \in R)(a \cdot (b - c) = a \cdot b - a \cdot c)$$

gilt. Dabei sei $(\forall x \in R)(0 \cdot x = x \cdot 0 = 0)$ für 0 das neutrale Element bzgl. $\cdot$ gegeben.

Anfang: Wir machen uns klar, was uns die Ring-Axiome liefern (*Assoziativität*, *Kommutativität*, *Distributivität*, *neutrale Elemente*, *Inverse*). Des Weiteren vergegenwärtigen wir uns die Definition von $a - b := a + (-b)$, d. h. die Subtraktion entspricht der Addition des (bzgl. $+$) inversen Elementes. Wir nehmen als gegeben an (da z. B. an anderer Stelle bewiesen), dass $0 \cdot x = x \cdot 0 = 0$.

Mitte:

$a \cdot (b - c)$	$=$	$a \cdot (b + (-c))$	Definition
	$=$	$a \cdot b + a \cdot (-c)$	Distributivität
$a \cdot c + a \cdot (-c)$	$=$	$a \cdot (c + (-c))$	Distributivität
	$=$	$a \cdot 0$	Inverses bzgl. $+$
	$=$	0	gegeben
$\Rightarrow a \cdot (-c)$	$=$	$-(a \cdot c)$	additives Inverses (Definition)
$\Rightarrow a \cdot b + a \cdot (-c)$	$=$	$a \cdot b - (a \cdot c)$	

Damit folgt mit dem oben gezeigten $a \cdot (b - c) = a \cdot b + a \cdot (-c)$ nun:

Ende: $a \cdot (b - c) = a \cdot b - (a \cdot c) = a \cdot b - a \cdot c$. □

(Man mache sich die Bedeutung der letzten Gleichheit klar!)

[1] Für die Definition von Ringen, siehe `https://de.wikipedia.org/wiki/Ringtheorie#Ring`.

Beispiel 2: *Injektivität*

Seien f und g Funktionen mit $A \overset{f}{\mapsto} B \overset{g}{\mapsto} C$. Wir zeigen, dass aus der Injektivität von f und g auch die Injektivität von $g \circ f$ folgt.

Anfang: Definition der Injektivität; Definition $(g \circ f)(x) = g(f(x))$; Annahme f, g injektiv (d. h. $(\forall x, x' \in A)(f(x) = f(x') \Rightarrow x = x')$ und $(\forall x, x' \in B)(g(x) = g(x') \Rightarrow x = x')$.

Mitte:

$(g \circ f)(x) = (g \circ f)(x')$	$\Rightarrow$	$g(f(x)) = f(f(x'))$	Definition
	$\Rightarrow$	$f(x) = f(x')$	g injektiv
	$\Rightarrow$	$x = x'$	f injektiv

Ende: Also $g \circ f$ injektiv, was zu beweisen war. □

Ist man erst einmal geübt im Führen von Beweisen, ist es nicht mehr erforderlich, diese strenge Strukturierung einzuhalten und insbesondere im Anfangs-Teil alle Details zusammenzutragen, die in den Beweis einfließen könn(t)en. Es hilft jedoch insbesondere dem Ungeübten typische Fehler beim Beweisen zu vermeiden, die da sind:

- falsche Annahmen treffen;
- zu starke Annahmen treffen;
- Definitionen fehlerhaft anwenden oder die Verwendung der falschen Definitionen.

Aber auch

- zu große Schritte machen (so dass eine Aussage nicht offensichtlich aus den vorherigen folgt und man dabei insbesondere unzulässige Schritte unternimmt);
- *"Handwaving"* („Es muss doch irgendwie so sein, wie denn auch sonst?!"); eine solche Argumentation ist kein Beweis;
- inkorrekte Logik verwenden, insbesondere die Negation einer Aussage falsch zu bestimmen.

Die Beispiele in diesem Skript halten sich penibel an die Aufteilung in Anfang, Mitte und Ende und sind recht detailliert ausformuliert. Damit sollen sie einerseits das jeweilige Beweisschema klar herausstellen, sollen aber andererseits auch als Leitschnur dienen, welcher Detailgrad in der zugehörigen Übung „Beweistechniken" angemessen ist.

2 Beweistechniken und -schemata

Für die Ausgestaltung eines Beweises stehen verschiedenste Techniken zur Verfügung. In den folgenden Abschnitten werden die gängigen dieser Beweisschemata, sortiert nach der Art der zu beweisenden Aussage, vorgestellt. Diese Schablonen bilden das Grundgerüst, mit dem sich komplexe Aussagen in einfachere Teilaussagen zerlegen lassen.

Zwar gilt es anschließend immer noch, dieses grobe Gerüst mit „Leben“ zu füllen: den eigentlichen, anwendungsspezifischen Schlussfolgerungen. Doch gelingt es mit den richtigen Techniken oft, eine Aussage soweit aufzugliedern, dass die Beweise der einzelnen Teilaussagen leicht(er) gelingen. Insbesondere weniger geübte „Beweiser“ profitieren davon, dass ein solches Gerüst die logische Grobstruktur eines Beweises festzurrt und somit hilft, Zirkelschlüsse und ähnliche Fehler zu vermeiden.

2.1 Implikationen

Viele Behauptungen haben die Form

$$A \Rightarrow B \qquad \text{bzw.} \qquad A_1 \wedge A_2 \wedge \cdots \wedge A_k \Rightarrow B.$$

Dabei ist A manchmal nicht ausdrücklich angegeben, sondern liegt implizit vor (siehe etwa die Ring-Axiome in Beispiel 1 von oben). Beachten Sie, dass eine Implikation $A \Rightarrow B$ gültig sein kann, auch wenn B niemals gilt:

„Wenn die Erde eine Scheibe ist, dann fallen die Schiffe am Rand hinunter.“

Diese Aussage ist als solche korrekt – nur hat sie keinerlei „praktische“ Konsequenzen, da wir ja wissen, dass die Erde eben keine Scheibe ist und somit der „dann“-Teil *nie* zum tragen kommen wird. Formal ist $A \Rightarrow B$ gleichbedeutend zu $B \vee \neg A$.

Ein häufiger Fehler im Umgang mit Implikationen besteht darin, sie mit *Äquivalenzen* zu verwechseln (Äquivalenzen sind Thema von Abschnitt 2.2). Das kann man sich an folgendem, klassischen Alltagsbeispiel klarmachen:

„Wenn es regnet, dann wird die Straße nass.“

(Wir ignorieren hier mal Tunnels, Überdachungen etc.)
Bei dieser Implikation gilt die *Umkehrung* nicht:

„Wenn die Straße nass wird, dann regnet es.“

Schließlich kann auch ein übereifriger Gartenbesitzer mit seinem Rasensprenger die Straße nass werden lassen, ohne dadurch Regenwetter heraufzubeschwören. Hier ist also die Äquivalenz

„Genau dann, wenn es regnet, wird die Straße nass.“

nicht richtig, obwohl der „wenn-dann“-Teil erfüllt ist.

Um $A \Rightarrow B$ zu beweisen, können wir auf die im Folgenden vorgestellten Techniken zurückgreifen. Diese elementaren Beweisschemata sind deutlich allgemeiner anwendbar, als es vielleicht im ersten Moment ersichtlich ist, denn viele Formen von Aussagen lassen sich auf Implikationen zurückführen.

2.1.1 Direkter Beweis

Hier zeigen wir B unter der Annahme A, indem wir logische Folgerungen aus B ableiten, bis wir bei A angekommen sind.

Beispiel 3: *Quadrate ungerader Zahlen*

Wir zeigen: Das Quadrat einer ungeraden Zahl $n \in \mathbb{N}_0$ ist wieder eine ungerade Zahl.

Anfang: Definition ungerade (n ungerade gdw. $(\exists k \in \mathbb{Z})(n = 2k - 1)$); Definition Quadrat; Abgeschlossenheit von $\mathbb{Z}$ bzgl. $+$ und $\cdot$.

Mitte: n ungerade $\Rightarrow$ es gibt ein $k \in \mathbb{Z}$ mit $n = 2k - 1$.
Dann gilt: $n^2 = (2k-1)^2 = 4k^2 - 4k - 1 = 2 \cdot \underbrace{\big(2k(k-1)\big)}_{=:k' \in \mathbb{Z}} - 1$

Ende: Also ist auch $n^2 = 2k' - 1$ ungerade. □

Die Beispiele 1 und 2 von oben sind ebenfalls direkte Beweise.

Manchmal bestehen die logischen Schlüsse auch schlicht aus arithmetischen Termumformungen oder Äquivalenzumformungen von Gleichungen. In diesem Fall spricht man lapidar von einem *Beweis durch Nachrechnen*.

Erfahrungsgemäß verleitet die einfache formal-logische Struktur eines solchen Beweises dazu, wesentliche Argumente in der „Rechnung“ zu verstecken, was mitunter zu falschen Schlüssen führt. Man sollte daher stets alle wesentlichen Zwischenergebnisse der Rechnung aufschreiben und nötigenfalls kenntlich machen, nach welcher Rechenregel ein Zwischenergebnis folgt (wie in der Rechnung von Beispiel 1).

Beispiel 4: *Lineare homogene Differentialgleichung erster Ordnung*

Wir zeigen: $f(x) = e^{-\int g(x)\,dx}$ ist eine Lösung der Differentialgleichung

$$f'(x) + g(x)f(x) = 0\,. \tag{1}$$

Anfang: (Rechen) Regeln der Analysis: Fundamentalsatz, Kettenregel

Mitte: Wir zeigen die Behauptung durch Nachrechnen.

$$\begin{aligned} f'(x) + g(x)f(x) &= e^{-\int_0^x g(s)\,ds} \cdot \left(-\frac{d}{dx}\int_0^x g(s)\,ds\right) + g(x)e^{-\int_0^x g(s)\,ds} \\ &= e^{-\int_0^x g(s)\,ds}\big(g(x) - g(x)\big) \\ &= 0 \end{aligned}$$

Ende: $f(x) = e^{-\int g(x)\,dx}$ ist eine Lösung von (1). □

(Eine analoge Rechnung zeigt, dass für $C \in \mathbb{R}$ auch $Ce^{-\int g(x)\,dx}$ eine Lösung ist.)

2.1.2 Indirekter Beweis (auch *Beweis durch Kontraposition*)

Wir zeigen $\neg A$ unter der Annahme $\neg B$, d. h. wir zeigen $\neg B \Rightarrow \neg A$ direkt, was logisch äquivalent zu $A \Rightarrow B$ ist.

Beispiel 5: *Gerade Quadratzahlen*

Wir zeigen: n^2 gerade $\Rightarrow n$ gerade.

Anfang: Kontraposition, Aussage aus Beispiel 3

Mitte: Die Kontraposition der zu zeigenden Aussage lautet:

$$n \text{ nicht gerade} \Rightarrow n^2 \text{ nicht gerade.}$$

Da nun jede natürliche Zahl n entweder gerade oder ungerade ist, ist die Kontraposition genau die Aussage aus Beispiel 3. Zusammen mit dem dortigen Beweis haben wir also indirekt gezeigt:

Ende: n^2 gerade $\Rightarrow n$ gerade. □

2.1.3 Beweis durch Widerspruch (auch *reductio ad absurdum*)

Wir zeigen, dass die Annahme $A \wedge \neg B$ zu einem logischen Widerspruch führen muss. Formal-logisch betrachtet ist das ein Spezialfall des indirekten Beweises, nämlich für die Aussage *wahr* $\Rightarrow (A \Rightarrow B)$, deren Kontraposition $\neg B \wedge A \Rightarrow$ *falsch* lautet.

Reductio ad absurdum wird besonders gerne verwendet, wenn A implizit gegeben ist (siehe Beispiel 6 unten). Dann ist lediglich (unter Verwendung der allgemeinen Voraussetzung A) aus $\neg B$ ein Widerspruch herzuleiten.

Beispiel 6: *Irrationalität von* $\sqrt{2}$

Wir zeigen: $\sqrt{2} \notin \mathbb{Q}$.

Anfang: Definition Teiler, Definition ggT, Definition rationale Zahl, n^2 gerade $\Rightarrow n$ gerade (Beispiel 5).

Mitte: *Annahme:* $\sqrt{2} \in \mathbb{Q}$.

Dann gäbe es $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit $\text{ggT}(p, q) = 1$, sodass $\frac{p}{q} = \sqrt{2}$.
Multiplizieren mit q und Quadrieren beider Seiten lieferte daraus $p^2 = 2q^2$ und mit $q^2 \in \mathbb{N}$ gälte folglich $2 \mid p^2$. Nach Beispiel 5 müsste dann auch p eine gerade Zahl sein, es gäbe also ein $k \in \mathbb{N}$ mit $p = 2k$.
Einsetzen in $p^2 = 2q^2$ lieferte $2^2k^2 = 2q^2$, also $2k^2 = q^2$. Mit dem gleichen Argument wie oben folgte daraus $2 \mid q$. Damit wäre 2 ein Teiler von sowohl p, als auch q, was $\text{ggT}(p, q) \geq 2$ bedeutete. Nach Definition wurden p und q aber so gewählt, dass $\text{ggT}(p, q) = 1$, d. h. wir hätten einen Widerspruch abgeleitet. Damit kann die Annahme $\sqrt{2} \in \mathbb{Q}$ nicht korrekt sein und es folgt per *reductio ad absurdum*:

Ende: $\sqrt{2}$ ist irrational. □

Auch wenn es grammatisch die präzisere Form ist, wird in längeren Beweisen der in Beispiel 6 verwendete Konjunktiv oft fallen gelassen.

2.1.4 Vollständige Fallunterscheidung

Für Aussagen der Form $A_1 \vee \cdots \vee A_k \Rightarrow B$ bietet sich das Beweisschema der vollständigen Fallunterscheidung an. Formal „zerlegt“ man dazu die Implikation in k einzelne Implikationen

$$A_1 \Rightarrow B,\ A_2 \Rightarrow B,\ \ldots,\ A_k \Rightarrow B,$$

die zusammen die Gesamtbehauptung ergeben. Im typischen Anwendungsfall ist die Prämisse der Implikation noch nicht explizit als Disjunktion gegeben, sondern muss erst „künstlich“ in diese Form gebracht werden. Formal verwendet man dabei die Äquivalenz

$$A \quad \Leftrightarrow \quad (A \wedge C) \ \vee \ (A \wedge \neg C)\,,$$

bzw. ihre allgemeinere Form

$$A \quad \Leftrightarrow \quad (A \wedge C_1) \ \vee \ (A \wedge C_2) \ \vee \ \cdots \ \vee \ (A \wedge C_k) \ \vee \ (A \wedge \neg C_1 \wedge \cdots \wedge \neg C_k)\,.$$

Essentiell dabei ist die *Vollständigkeit* der Fallunterscheidung: *Es muss nachgewiesen werden, dass immer (mindestens) einer der Fälle greift.* In der formalen Version oben ist das durch den letzten Term erzwungen; dieser *„Sonst“-Fall* umfasst alles, was in keinen der vorangehenden Fälle passt. Hat man keinen expliziten „Sonst“-Fall angegeben, muss man also beweisen, dass $C_1 \vee \cdots \vee C_k$ immer gilt.

Beispiel 7: *Größer durch Quadrieren*

Wir zeigen: Für $x \in \mathbb{R} \setminus (0,1)$ gilt $x^2 \geq x$.

Anfang: Rechenregeln in $\mathbb{R}$

Mitte: Sei $x \in \mathbb{R} \setminus (0,1)$ gegeben. Wir unterscheiden die Fälle:

$x \leq 0$	In diesem Fall gilt $x^2 \geq 0 \geq x$.
sonst	Dann muss x positiv sein; da $x \notin (0,1)$ ist also $x \geq 1$. Dann ist aber $x^2 \geq 1 \cdot x = x$.

In beiden Fällen folgt $x^2 \geq x$ und weitere Fälle sind nicht möglich, also gilt:

Ende: Für $x \in \mathbb{R} \setminus (0,1)$ ist $x^2 \geq x$.

2.2 Äquivalenzen

Die (logische) *Äquivalenz* $A \Leftrightarrow B$ zweier Aussagen A und B ist gleichbedeutend mit der Konjunktion der beidseitigen Implikationen:

$$A \Rightarrow B \ \wedge \ A \Leftarrow B\,.$$

Man teilt also den Beweis in zwei Teile auf und zeigt die beiden Implikationen nacheinander mit einem der Verfahren aus Abschnitt 2.1.

Beispiel 8: *Antisymmetrie der Teilbarkeitsrelation*

Wir zeigen für $n, m \in \mathbb{N}_0$: $n \mid m \wedge m \mid n \Leftrightarrow n = m$

Anfang: Definition Teilbarkeit

Mitte: Wir zeigen die beiden Implikationen getrennt:

„$\Leftarrow$“ Wir zeigen $n = m \Rightarrow n \mid m \wedge m \mid n$ direkt.
Sei also $n = m$. Jede Zahl ist Teiler ihrer selbst, folglich gilt $n \mid n$.

„$\Rightarrow$“ Wir zeigen $n \mid m \wedge m \mid n \Rightarrow n = m$ durch Kontraposition,
d. h. wir zeigen $n \neq m \Rightarrow n \nmid m \vee m \nmid n$.
Sei also $n \neq m$. Dann ist eine der beiden Zahlen größer; o. B. d. A. nehmen wir an $n > m$. Wir unterscheiden die folgenden Fälle:

$m = 0$ Da $n > m = 0$ ist, gilt $0 = m \nmid n$.

$m > 0$ Dann kann n kein Teiler von m sein, denn für jedes $k \in \mathbb{N}$, $k > 0$, gilt $nk > m$, also insbesondere $nk \neq m$. Außerdem ist nach Annahme $n0 = 0 \neq m$. Damit ist nach Definition $n \nmid m$.

Da nur diese Fälle möglich sind und in allen Fällen $n \nmid m \vee m \nmid n$ gilt, ist die Implikation bewiesen.

Damit sind beide Richtungen nachgewiesen und es gilt:

Ende: $n \mid m \wedge m \mid n \Leftrightarrow n = m$. □

2.3 Inklusionsbeziehung und Gleichheit von Mengen

Nach Definition ist $A \subseteq B$ gleichbedeutend mit $x \in A \Rightarrow x \in B$. Damit sind Aussagen über Teilmengenbeziehungen ein Spezialfall der Implikation. Die Gleichheit $A = B$ zweier Mengen A und B ist wiederum definiert als $A \subseteq B \wedge B \subseteq A$ und lässt sich damit genauso handhaben wie eine logische Äquivalenz: Wir zeigen die beiden Inklusionen/Implikationen nacheinander.

Beispiel 9: *Vielfache von 6*

Wir zeigen die Mengengleichheit $M_1 = M_2$ für

$$M_1 = \left\{6k \;\middle|\; k \in \mathbb{N}_0\right\} \qquad \text{und} \qquad M_2 = \left\{n \in \mathbb{N}_0 \;\middle|\; 2 \mid n \wedge 3 \mid n\right\}.$$

Anfang: Definition Teilbarkeit; n, m ungerade $\Rightarrow nm$ ungerade

Mitte: Wir zeigen die beiden Inklusionen getrennt.

„$\subseteq$“ $M_1 \subseteq M_2$ ist gleichbedeutend mit $x \in M_1 \Rightarrow x \in M_2$, was wir direkt zeigen.
Sei also $x = 6k$ für ein $k \in \mathbb{N}_0$. Mit $k_1 = 3k$ und $k_2 = 2k$ gilt dann $x = 2k_1$ und $x = 3k_2$, d. h. $2 \mid x$ und $3 \mid x$. Somit ist auch $x \in M_2$.

„$\supseteq$“ $M_1 \supseteq M_2$ ist gleichbedeutend mit $x \in M_1 \Leftarrow x \in M_2$. Das zeigen wir direkt.
Sei x gegeben mit $2 \mid x$ und $3 \mid x$. Das heißt $x = 3\ell$ für ein $\ell \in \mathbb{N}_0$. Da das Produkt zweier ungerader Zahlen wieder ungerade ist, x aber eine gerade Zahl ist, muss ℓ auch eine gerade Zahl sein: $\ell = 2k$ für ein $k \in \mathbb{N}_0$. Wir haben also gezeigt, dass es ein k gibt mit $x = 6k$, d. h. $x \in M_1$.

Beide Inklusionen sind nachgewiesen, folglich gilt die Mengengleichheit

Ende: $M_1 = M_2$. □

2.4 Existenzaussagen

Die Existenz eines Objektes mit einer entsprechenden Eigenschaft zeigt man oft *konstruktiv*, d. h. durch die Benennung eines Weges, wie man zu dem behaupteten Objekt gelangt.

Beispiel 10: *Große Zahlen*

Wir zeigen: $(\exists n \in \mathbb{N})(n \geq 17)$
$18 \in \mathbb{N}$ und $18 \geq 17$. □

Beispiel 10 ist natürlich ein extrem einfacher Fall. Eine realistischere Anwendung des konstruktiven Existenzbeweises erweitert die Syntax von Loop-Programmen:

Beispiel 11: *Simulation von If durch Loop*

Wir zeigen: Es gibt ein Loop-Programm, das äquivalent ist zu

`If` $x = 0$ `Then` A `End`

wobei A ein beliebiges Loop-Programm ist.

Anfang: Definition Syntax und Semantik Loop-Programme

Mitte: Ein mögliches Loop-Programm sieht wie folgt aus:

$y := 1$;
`Loop` x `Do` $y := 0$;
`Loop` y `Do` A `End`

Die beiden Programme sind äquivalent, da die erste Loop-Schleife y genau dann auf 0 setzt, wenn $x \neq 0$. In diesem Fall wird der Rumpf der darauffolgenden Schleife gar nicht ausgeführt. Ist aber $x = 0$, so verbleibt y auf 1 und A wird (einmal) ausgeführt.

Somit ist gezeigt:

Ende: Es gibt ein äquivalentes Loop-Programm zu `If` $x = 0$ `Then` A `End`.

Reductio ad absurdum ist auch hier anwendbar: Man führt dann die Annahme $\neg(\exists x : E(x)) \equiv \forall x : \neg E(x)$ zu einem Widerspruch führt. Dazu kann man die Methoden für allquantifizierte Formeln anwenden, die wir in Abschnitt 2.5 besprechen.

2.4.1 Existenz und Eindeutigkeit

Möchte man zeigen, dass es *genau* ein $x \in D$ mit einer speziellen Eigenschaft E gibt, so zeigt man:

(1) $(\exists x_0 \in D)\big(E(x_0)\big)$. (Es gibt *mindestens* ein Element.)

(2a) $(\forall x \in D \setminus \{x_0\})\big(\neg E(x)\big)$. (Es gibt kein weiteres Element.)

oder

(2b) $(\forall x \in D)(\forall y \in D)\big(E(x) \wedge E(y) \Rightarrow x = y\big)$. (Alle „$E$-Elemente“ sind gleich.)

Eine Variante sind Aussagen, für die die Nicht-Existenz $\neg(\exists x : E(x))$ eines Objektes mit Eigenschaft E bewiesen werden soll. Hier kann man die Annahme der Existenz zu einem Widerspruch führen.

2.4.2 Das Schubfachprinzip

Als „Schubfachprinzip“ (oder auch „Taubenschlagprinzip“, nach dem englischen Begriff *pigeonhole principle*) bezeichnet man ein elementares, aber nicht-konstruktives Argument für den Beweis der Existenz eines Elements mit bestimmten Eigenschaften. Formal sei uns eine Menge M von Objekten und eine Partition der Menge M in k *disjunkte* Teilmengen gegeben:

$$M = \bigcup_{i=1}^{k} S_i, \qquad \text{mit} \qquad S_i \cap S_j = \emptyset \text{ für } i \neq j$$

Ist nun die Anzahl $m = |M|$ verschiedener Objekte größer als die Anzahl k der Partitionen (die Schubfächer), so muss es ein Schubfach S_j geben, das mindestens $|S_j| \geq 2$ Elemente enthält. Die Korrektheit dieses Arguments folgt direkt aus einem Vergleich der Kardinalitäten von M und $\bigcup S_i$.

Beispiel 12: *Haarspaltereien*

Wir zeigen: Es gibt in Berlin zwei Menschen, die *genau* gleich viele Haare auf dem Kopf haben.

Anfang: Einwohner Berlins: über 3 000 000,
Kopfhaare eines Menschen: weniger als 1 000 000

Mitte: Partitionieren wir die Einwohner Berlins nach der Anzahl ihrer Kopfhaare, so haben wir über 3 000 000 Menschen auf höchstens 1 000 000 Schubfächer verteilt. Nach dem Schubfachprinzip gilt also:

Ende: Es gibt zwei Menschen in Berlin, die gleich viele Haare auf dem Kopf haben.

2.5 Allquantifizierte Aussagen

Hier geht es darum, Eigenschaften für *alle* Objekte einer bestimmten Art zu beweisen. Formal schreiben wir die Aussage, dass die Eigenschaft A_x für alle Objekte x einer Menge D erfüllt ist, als

$$(\forall x \in D)(A_x) \ .$$

Für viele Eigenschaften eignen sich Induktionsbeweise (Abschnitte 2.5.2 – 2.5.4), oft bietet sich aber auch ein indirekter Beweis ein. Will man Aussagen mit Allquantoren direkt beweisen, so kann eine Fallunterscheidung (z. B. positive und negative Zahlen) hilfreich sein.

2.5.1 Beweise mit Variablen

In der Regel sind *freie Variablen* in einer (zu beweisenden) Aussage implizit *allquantifiziert*, d. h. der Nachweis ist für alle möglichen Werte für diese Variablen zu erbringen. In Beispiel 5 lautete die Behauptung etwa

$$n^2 \text{ gerade } \Rightarrow n \text{ gerade } .$$

Dabei geht die Menge „möglicher“ Werte aus dem Zusammenhang hervor (hier $D = \mathbb{N}_0$).

Viele (direkte) Beweise lassen sich dabei „generisch“ führen, indem man mit *„beliebig, aber fest“* gewählten Werten für die allquantifizierten Variablen arbeitet. Fast alle unserer bisherigen Beispiele waren Beweise mit Variablen, auch wenn wir sie nicht explizit so genannt hatten: In Beispiel 1 sind a, b und c *beliebige* Elemente aus dem Ring; f und g aus Beispiel 2 stehen für *beliebige* Funktionen; in Beispiel 3 zeigen wir eine Aussage über *alle* natürlichen Zahlen $n \in \mathbb{N}_0$; usw.

Solange man in einem Beweis keine speziellen Eigenschaften verwendet, die nur manche, aber nicht alle in Frage kommenden Elemente haben, kann man das geführte Argument wortwörtlich auf alle konkreten Elemente anwenden. (Nur theoretisch natürlich, denn wir beweisen ja i. d. R. Aussagen über *unendlichen* Grundmengen . . .)

Man kann diese Art von Beweisen als ein „Spiel“ formulieren, das wir dann in allen Eventualitäten gewinnen müssen, d. h. unser Beweis muss eine Gewinnstrategie sein:

1. Ein Gegner bestimmt die Werte aller allquantifizierten Variablen (innerhalb des gültigen Bereiches natürlich).

2. Wir liefern einen Beweis der Behauptung für diese *konkreten* Werte.

Über eine vollständige Fallunterscheidung können wir unsere Argumentation in Abhängigkeit der vom Gegner gewählten Werte führen (siehe Beispiel 7).

2.5.2 Vollständige Induktion

Diese Technik eignet sich, um Aussagen für alle $n \in \mathbb{N}_0$ zu beweisen, d. h. Aussagen der Form $(\forall n \in \mathbb{N}_0)(A_n)$, wobei A_n eine von n abhängige Aussage ist. Das Grundprinzip der vollständigen Induktion verlangt dabei, zwei Dinge zu zeigen:

Induktionsanfang (auch *Anker*)
Die Aussage A_n gilt für $n = 0$.
(bzw. für die kleinste natürliche Zahl, für die sie behauptet wurde).

Induktionsschritt
Gilt A_n für ein beliebiges, aber festes $n \in \mathbb{N}_0$ gilt, so gilt auch A_{n+1}.

Warum wird so eine Aussage für alle natürlichen Zahlen bewiesen? Hintergrund sind die *Peano-Axiome*, die die Menge der natürlichen Zahlen wie folgt definieren:

$0 \in \mathbb{N}_0$. *(Die Null ist eine natürliche Zahl.)*
$n \in \mathbb{N}_0 \Rightarrow n + 1 \in \mathbb{N}_0$.
(Der Nachfolger jeder natürlichen Zahl ist auch eine natürliche Zahl).

Man mache sich klar, warum so alle $n \in \mathbb{N}_0$ als natürliche Zahl identifiziert werden und überlege sich dann, warum entsprechend eine vollständige Induktion tatsächlich einen entsprechenden Beweis liefert.

Formal zeigt folgender Widerspruchsbeweis die Gültigkeit des Induktionsprinzips: Sei A_n eine Aussage, die für $n = 0$ erfüllt ist, und es gelte für alle $n \in \mathbb{N}_0$ die Implikation $A_n \Rightarrow A_{n+1}$. Angenommen es gälte trotzdem

$$\neg\big((\forall n \in \mathbb{N})(A_n)\big) \;\equiv\; (\exists n \in \mathbb{N})(\neg A_n)\;.$$

Von den potentiell vielen Zahlen n, für die (unter unserer Annahme) $\neg A_n$ gilt, sei m die kleinste (diese kleinste Zahl m existiert, weil die natürlichen Zahlen *wohl-geordnet* sind). Da A_0 gilt, muss $m \geq 1$ sein und folglich $m - 1 \in \mathbb{N}_0$. Da offensichtlich $m - 1 < m$ und m die kleinste Zahl, für die A_m *nicht* gilt, muss A_{m-1} wahr sein. Dann liefert aber die Implikation $A_{m-1} \Rightarrow A_m$ einen Widerspruch to $\neg A_m$. Folglich muss unsere Annahme falsch gewesen sein und A_n für alle $n \in \mathbb{N}$ gelten. □

In der Verwendung der vollständigen Induktion kann man sich immer auf diesen allgemeinen Beweis berufen, d. h. man muss dort nur noch A_0 und die Implikation $A_n \Rightarrow A_{n+1}$ nachweisen. Ein klassisches Beispiel demonstriert das Vorgehen:

Beispiel 13: *„Kleiner Gauß“*

Wir zeigen: Für alle $n \in \mathbb{N}_0$ gilt $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Anfang: Rechenregeln

Mitte: Wir zeigen die Aussage per vollständiger Induktion über n.

Induktionsanfang: $n = 0$:

$\sum_{i=1}^{0} i = 0 = \frac{0 \cdot 1}{2}$, d. h. die Aussage gilt für $n = 0$.

Induktionsvoraussetzung: Für ein festes $n \in \mathbb{N}$ gelte $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Induktionsschritt: Wir rechnen:

$$\begin{aligned}
\sum_{i=1}^{n+1} i \;&=\; n+1 \;+\; \sum_{i=1}^{n} i \\
&\underset{\text{IV}}{=}\; n+1 \;+\; \frac{n(n+1)}{2} \\
&=\; \frac{2(n+1) + n(n+1)}{2} \\
&=\; \frac{(n+1)\big((n+1)+1\big)}{2}
\end{aligned}$$

Die Aussage gilt unter der Induktionsvoraussetzung also auch für $n + 1$.

Damit ist gezeigt:

Ende: $(\forall n \in \mathbb{N}_0)\left(\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}\right)$. □

2.5.3 Allgemeine Induktion

Als Variante existiert die *allgemeine Induktion*, bei der man für den Induktionsschritt annimmt, dass die zu beweisende Aussage *für alle n' kleiner einem beliebigen, aber festen* $n \in \mathbb{N}$ gilt. Es ist natürlich weiterhin erlaubt, den Anfang bei einem $k \in \mathbb{N}_0$ statt bei 0 zu machen.

Beachte, dass unser Korrektheitsbeweis des Induktionsprinzips aus dem letzten Abschnitt von dieser Verallgemeinerung völlig unberührt bleibt: Wenn m die kleinste Zahl ist, für die die Aussage nicht gilt, so muss die Aussage für *alle* kleineren Zahlen gelten. Damit ist die verallgemeinerte Implikation anwendbar und führt die Annahme, es gäbe Zahlen, für die Behauptung nicht gilt, genauso zum Widerspruch wie oben.

Beispiel 14: *Primteiler*

Wir zeigen: Jede natürliche Zahl $n \geq 2$ hat einen Primteiler, d. h. einen Teiler, der eine Primzahl ist.

Anfang: Definitionen Teiler, Primzahl

Mitte: Wir zeigen die Behauptung mit (allgemeiner) Induktion über n:

Induktionsanfang $n = 2$
2 ist selbst eine Primzahl und natürlich Teiler von sich selbst.

Induktionsvoraussetzung Angenommen, es gilt für ein festes $n \in \mathbb{N}$, dass alle $n' \in \mathbb{N}$ mit $2 \leq n' \leq n$ einen Primteiler haben.

Induktionsschritt Betrachte nun $n + 1$.
Wir machen eine vollständige Fallunterscheidung:

$n + 1$ prim	Dann ist $n + 1$ selbst der gesuchte Primteiler.
sonst	d. h. $n + 1$ ist nicht prim. Dann gibt es zwei nicht-triviale Teiler $2 \leq p, q \leq n$ mit $n + 1 = p \cdot q$. Nach Induktionsvoraussetzung hat nun $p \leq n$ einen Primteiler t, der natürlich auch ein Teiler von $n + 1 = q \cdot p$ ist. Damit hat auch $n + 1$ einen Primteiler.

Unter der (allgemeinen) Induktionsvoraussetzung hat also $n + 1$ in allen Fällen einen Primteiler.

Damit ist gezeigt:

Ende: $(\forall n \in \mathbb{N})(n \geq 2 \Rightarrow n$ hat Primteiler). □

2.5.4 Strukturelle Induktion

Die strukturelle Induktion ist eine Verallgemeinerung des Induktionsprinzips für allquantifizierte Aussagen über einer beliebigen *aufzählbaren* Menge. Konzeptionell führt man dann eine „gewöhnliche“ Induktion über die *Anzahl der Erzeugungsschritte* eines Elements, was Dank der Aufzählbarkeit der Menge kein Element auslässt.

Beispiel 15: *Basisoperationen boolescher Formeln*

Die Menge $\mathcal{F}$ boolescher Formeln über den Variablen $x_1, x_2, \ldots$ sei definiert als die kleinste Menge mit folgenden Eigenschaften:

(F1) Für $i \in \mathbb{N}$ ist $x_i \in \mathcal{F}$.

(F2) Für $\varphi \in \mathcal{F}$ ist auch $\neg(\varphi) \in \mathcal{F}$.

(F3) Für φ, $\psi \in \mathcal{F}$ ist auch $(\varphi \wedge \psi) \in \mathcal{F}$.

(F4) Für φ, $\psi \in \mathcal{F}$ ist auch $(\varphi \vee \psi) \in \mathcal{F}$.

Wir zeigen: Für jede boolesche Formel φ über den Operatoren $\wedge$, $\vee$ und $\neg$, existiert eine äquivalente Formel φ', die kein $\vee$ enthält.

Anfang: Definition boolescher Formeln, De Morgan $\neg(x \vee y) \equiv \neg x \wedge \neg y$

Mitte: Wir zeigen die Behauptung per struktureller Induktion, d. h. per allgemeiner Induktion über die Anzahl $n \in \mathbb{N}$ von Anwendungen der Eigenschaften (F1) bis (F4), die nötig sind, um eine Formel φ als Element von $\mathcal{F}$ zu identifizieren. (Beachte, dass für jedes Element in $\mathcal{F}$ durch die Klammerung ein eindeutiger *Erzeugungsprozess* entlang der Regeln (F1) bis (F4) gegeben ist.)

Induktionsanfang: $n = 1$: Wenn φ mit einer einzigen Regelanwendung erzeugt wurde, muss es die Regel (F1) gewesen sein und folgich $\varphi = x_i$ für ein $i \in \mathbb{N}$. Insbesondere enthält φ also kein $\vee$ und wir sind fertig.

Induktionsvoraussetzung: Für alle $1 \leq n' \leq n$ gilt: Ist φ in n' Schritten erzeugt worden, so gibt es eine äquivalente Formel φ', die kein $\vee$ enthält.

Induktionsschritt: Sei φ eine beliebige Formel, die in genau $n + 1 \geq 2$ Schritten erzeugt wurde. Dann muss im letzten Schritt der Erzeugung von φ eine der Regeln (F2), (F3) oder (F4) zum Tragen gekommen sein. Wir unterscheiden nach dieser letzten Regel:

(F2) d. h. $\varphi = \neg(\psi)$ für eine Formel ψ, die in n Schritten erzeugt wurde. Nach IV gibt es folglich eine äquivalente Formel $\psi' \equiv \psi$ ohne $\vee$. Mit $\varphi' = \neg(\psi') \equiv \varphi$ finden wir dann eine äquivalente Formel zu φ ebenfalls ohne $\vee$.

(F3) d. h. $\varphi = (\psi_1 \wedge \psi_2)$ für in n_1 bzw. n_2 Schritten erzeugte Formeln ψ_1 bzw. ψ_2, wobei $n_1, n_2 \leq n$. Nach IV gibt es $\psi_1' \equiv \psi_1$ und $\psi_2' \equiv \psi_2$ ohne $\vee$, woraus wir die Formel $\varphi' = (\psi_1' \wedge \psi_2') \equiv \varphi$ erhalten, die ebenfalls kein $\vee$ enthält.

(F4) d. h. $\varphi = (\psi_1 \vee \psi_2)$. Analog zu Fall (F3) gibt es $\psi_1' \equiv \psi_1$ und $\psi_2' \equiv \psi_2$ ohne $\vee$. Mit $\varphi' = \neg(\neg\psi_1' \wedge \neg\psi_2')$ haben wir eine Formel, die nach De Morgan und IV äquivalent zu φ ist und kein $\vee$ enthält.

In allen möglichen Fällen konnten wir unter der Induktionsvoraussetzung die Existenz einer äquivalenten Formel ohne $\vee$ nachweisen.

Damit ist gezeigt:

Ende: $(\forall \varphi \in \mathcal{F})(\exists \varphi' \in \mathcal{F})(\varphi \equiv \varphi' \wedge \varphi'$ enthält kein „$\vee$“).

2.6 Aussagen mit geschachtelten Quantoren

Zuletzt sei angemerkt, dass Abhängigkeiten von Quantoren bestehen können. So können Existenzaussagen für alle x einer bestimmten Art A wie etwa in

$$(\forall x \in A)(\exists y \in B) : E(x, y)$$

getroffen werden. Dabei ist das y als dem jeweiligen x *zugeordnet* zu betrachten (gebunden). Dies kann man sich in einem Beweis zunutze machen, indem man beispielsweise zu jedem $x \in A$ ein entsprechendes $y \in B$ konstruktiv angibt, etwa durch die Angabe einer Funktion f, welche y aus x berechnet. Für dieses f ist dann $\forall x \in A : E(x, f(x))$ zu zeigen. Tatsächlich war Beispiel 15 bereits von dieser Form. Dort haben wir entlang der Struktur einer booleschen Formel φ eine äquivalente Formel φ' *konstruiert*.

Ein weiteres, wichtiges Beispiel für geschachtelte Quantoren ist die *Konvergenz* einer Zahlenfolge. Zur Erinnerung: Eine (reelle) Zahlenfolge $(a_n)_{n\in\mathbb{N}}$ konvergiert gegen eine Konstante $c \in \mathbb{R}$ wenn

$$(\forall \varepsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)(|a_n - c| < \varepsilon)$$

Beispiel 16: *Konvergenz der geometrischen Reihe*

Wir zeigen $\lim\limits_{n\to\infty} \sum\limits_{i=0}^{n} \left(\frac{1}{2}\right)^i = 2$.

Anfang: Definition Konvergenz, Geometrische Summe: $\sum_{i=0}^{n} c^i = \frac{1-c^{n+1}}{1-c}$

Mitte: Beweis durch Nachrechnen mit Variablen.

Sei $\varepsilon > 0$ beliebig, aber fest. Wir konstruieren ein n_0, das die Behauptung erfüllt. Die geschlossene Form für geometrische Summen ergibt $\sum_{i=0}^{n} \left(\frac{1}{2}\right)^i = 2 - \left(\frac{1}{2}\right)^n$, d. h. $|a_n - 2| = \left(\frac{1}{2}\right)^n$. Für $n \geq n_0 = \lfloor \log_{1/2}(\varepsilon) \rfloor + 1$ ist dann $\left(\frac{1}{2}\right)^n < \varepsilon$. (Exponenziere beide Seiten mit Basis $\frac{1}{2}$.)

Damit gilt also

$$(\forall \varepsilon > 0)(\exists n_0 \in \mathbb{N})(\forall n \geq n_0)\left(\left|\sum_{i=0}^{n} \left(\frac{1}{2}\right)^i - 2\right| < \varepsilon\right)$$

und folglich nach Definition

Ende: $\lim_{n\to\infty} \sum_{i=0}^{n} \left(\frac{1}{2}\right)^i = 2$. □

(Mit analogen Argumenten zeigt man für beliebiges $0 < c < 1$: $\lim\limits_{n\to\infty} \sum\limits_{i=0}^{n} c^i = \frac{1}{1-c}$.)

Andere und/oder tiefere Schachtelungen von Quantoren als in obigen Beispielen sind selten, kommen aber bisweilen vor (siehe etwa Pumping-Lemmata für Klassen formaler Sprachen). Das allgemeine Vorgehen lässt sich als eine Erweiterung des „Spiels“ aus Abschnitt 2.5.1 beschreiben:

- Von außen nach innen werden Werte für die quantifizierten Variablen vergeben.

- Bei einem Allquantor darf unser Gegner uns einen Wert für die Variable vorschreiben, mit dem wir dann zurechtkommen müssen.
- Bei einem Existenzquantor müssen wir – potentiell in Abhängigkeit bereits fixierter Variablenwerte – einen Wert konstruieren (oder indirekt seine Existenz nachweisen).
- Sind alle Quantoren abgearbeitet, müssen wir für die gewählten Variablenwerte eine gültigen Nachweis der Behauptung liefern.

3 Beweise in freier Wildbahn

Mit den Beweistechniken und -schemata, die Sie in den vorangehenden Abschnitten kennengelernt haben, sind Sie grundsätzlich gerüstet, die meisten Beweise, die Ihnen begegnen werden, zu verstehen und zu überprüfen. Die Schwierigkeit in der Praxis besteht dann oft darin, dass neue Beweise auf bereits bewiesenen Aussagen aufbauen und dass die vorgestellten Schemata in verschachtelter Weise verwendet werden.

Außerdem werden nicht immer alle Argumente explizit benannt und im Detail ausgeführt; insbesondere immer wiederkehrende Argumente werden oft „wegrationalisiert“. Davon sollte man sich aber nicht verleiten lassen, eine Schlussfolgerung blind zu schlucken, sondern sie solange verfeinern, bis ihre Gültigkeit offensichtlich wird (oder aber eine Lücke in der Argumentation gefunden ist!).

Zum Abschluss folgt hier ein längeres, detailliertes Beispiel, in dem einige der vorgestellten Schemata mehrfach verschachtelt verwendet werden.

Beispiel 17: *Sprache einer Grammatik*

Gegeben seien $\mathcal{L} = \{a\} \cdot \{b\}^* \cdot \{c, d\}$ sowie $G = (I, T, P, S)$ mit $I = \{S, B, C\}$, $T = \{a, b, c, d\}$ und

$$P = \left\{ \begin{array}{lcllcl} S & \to & aB, & C & \to & c, \\ B & \to & bB, & C & \to & d, \\ B & \to & C & & & \end{array} \right\}.$$

Behauptung: G erzeugt *genau* die Sprache $\mathcal{L}$.

Wir zeigen zuerst die folgende Hilfsbehauptung. Dazu seien

$$M_0 := \{S\}\,, \qquad M_1 := \{ab^nB | n \geq 0\}\,,$$
$$M_2 := \{ab^nC | n \geq 0\}\,, \qquad M_3 := \{ab^nc | n \geq 0\} \cup \{ab^nd | n \geq 0\} = \mathcal{L}\,.$$

Hilfsbehauptung: Für die Menge aller Satzformen $\vartheta(G)$ gilt

$$\vartheta(G) = M_0 \cup M_1 \cup M_2 \cup M_3 =: M\,.$$

$\vartheta(G) \subseteq M$ Die Menge aller Satzformen $\vartheta(G)$ ist (rekursiv) aufzählbar, da sie durch Anwenden der Regeln aus P entstehen. Daher können wir über alle $\beta \in \vartheta(G)$ durch eine *strukturelle Induktion* iterieren, in diesem Fall eine Induktion über die Anzahl N der Ableitungsschritte in G.

Induktionsanfang: Startsymbol ($N = 0$ Schritte)
$S \in M_0 \Rightarrow S \in M$. ✓

Induktionsvoraussetzung: Für die nicht-leere Teilmenge $T \subseteq \vartheta(G)$, die alle Satzformen umfasse, die sich in höchstens N Schritten ableiten lassen, gelte die Behauptung, d. h. $(\forall \beta \in T)\,(\beta \in M)$.

Induktionsschritt: Sei $\beta \in T$ beliebig. Nach Induktionsvoraussetzung gilt dann einer der folgenden Fälle:

1. $\beta \in M_0 \Rightarrow \beta = S$.
   Dann kann nur die Regel $S \to aB$ angewendet werden; $\beta' = aB \in M_1$ (mit $n = 0$). Das bedeutet in diesem Fall sind auch alle Satzformen mit Ableitungen der Länge $N + 1$ in M.
2. $\beta \in M_1 \Rightarrow (\exists n \geq 0)\,(\beta = ab^nB)$.
   Hier können 2 Regeln angewendet werden
   - $B \to bB \Rightarrow \beta' = ab^nbB = ab^{n+1}B \in M_1$,
   - $B \to C \Rightarrow \beta' = ab^nC \in M_2$.

   Beide Ableitungen enden wieder mit Satzformen in M.
3. $\beta \in M_2 \Rightarrow (\exists n \geq 0)\,(\beta = ab^nC)$.
   Alle möglichen Regeln sind:
   - $C \to c \Rightarrow \beta' = ab^nc \in M_3$,
   - $C \to d \Rightarrow \beta' = ab^nd \in M_3$.
4. $\beta \in M_3 \Rightarrow (\exists n \geq 0)\,(\beta = ab^nc \vee \beta = ab^nd)$.
   Keine Ableitung mehr möglich.

Da es keine weiteren Möglichkeiten für $\beta \in M$ gibt, haben wir für jedes β', das sich in $N + 1$ Schritten erzeugen lässt, gezeigt, dass es in M enthalten ist. Nach dem Induktionsprinzip haben wir damit bewiesen, dass jede in G ableitbare Satzform in einer der Mengen M_0, M_1, M_2 oder M_3 liegt.

$\vartheta(G) \supseteq M$ Dieser zweite Teil der (Hilfs-) Behauptung lässt sich aufteilen: Für $\alpha \in M_0 \cup M_1 \cup M_2 \cup M_3$ beliebig, gibt es ein j mit $\alpha \in M_j$ und es reicht, für jede Menge einzeln zu zeigen, dass sie in $\vartheta(G)$ enthalten ist.

$j = 0$ $\alpha \in M_0 \Rightarrow \alpha = S \in \vartheta(G)$, denn jede Ableitung beginnt mit dem Startsymbol, womit S natürlich eine ableitbare Satzform ist.

$j = 1$ d. h. $M_1 \subseteq \vartheta(G)$: Das zeigt man mittels vollständiger Induktion über den Parameter n aus der Definition von M_1:

Induktionsanfang: $n = 0 \Rightarrow \alpha = aB$. Es ist $S \Rightarrow aB \in \vartheta(G)$. ✓

Induktionsvoraussetzung: Sei $ab^nB \in \vartheta(G)$.

Induktionsschritt: Nach Induktionsvoraussetzung existiert für ab^nB eine Ableitung in G, d. h. $S \overset{*}{\Rightarrow} ab^nB$. Mittels der Regel $B \to bB$ lässt sich diese fortsetzen:

$$S \overset{*}{\Rightarrow} ab^nB \Rightarrow ab^n\,bB = ab^{n+1}B.$$

Damit haben wir eine Ableitung für $ab^{n+1}B$ gefunden, also ist $ab^{n+1}B \in \vartheta(G)$.

$j = 2$ $\alpha \in M_2 \Rightarrow \alpha \in \vartheta(G)$:
Nach Definition ist $\alpha = ab^nC$ für ein $n \geq 0$. Wie gerade gezeigt, ist $ab^nB \in \vartheta(G)$ (mit dem gleichen n); es gibt also eine Ableitung

$$S \overset{*}{\Rightarrow} ab^nB$$

die sich mit $B \to C$ fortführen lässt:

$$S \overset{*}{\Rightarrow} ab^nB \Rightarrow ab^nC \;\Rightarrow\; ab^nC = \alpha \in \vartheta(G).$$

$j = 3$ $\alpha \in M_3 \Rightarrow \alpha \in \vartheta(G)$:
Analog zu eben heißt $\alpha \in M_3$: $(\exists n \geq 0)$ $(\alpha = ab^nc \vee \alpha = ab^nd)$. Wir verwenden wieder bereits Gezeigtes, nämlich dass es eine Ableitung

$$S \overset{*}{\Rightarrow} ab^nC$$

gibt, die wir nun auf zwei Arten vollenden können

$$S \overset{*}{\Rightarrow} ab^nC \Rightarrow ab^nc \qquad \text{mittels } C \to c,$$
$$S \overset{*}{\Rightarrow} ab^nC \Rightarrow ab^nd \qquad \text{mittels } C \to d.$$

Für alle möglichen $\alpha \in M_3$ haben wir also eine Ableitung in G gefunden.

Damit haben wir für alle Satzformen aus M gezeigt, dass sie in G ableitbar sind.

Insgesamt haben wir nun $\vartheta(G) = M$ bewiesen.
Aber warum hilft uns das mit unserer Hauptbehauptung $\mathcal{L}(G) = \mathcal{L}$?

$\mathcal{L}(G) \supseteq \mathcal{L}$ M_3 entspricht genau der Menge $\mathcal{L}$, somit gibt es für jedes Wort in $\mathcal{L}$ eine Ableitung in G.

$\mathcal{L}(G) \subseteq \mathcal{L}$ M_0, M_1 und M_2 enthalten nur Satzformen, die mindestens ein *Nichtterminal* enthalten, d. h. „unfertige“ Satzformen sind. Da die Menge $\vartheta(G)$ aber abgeschlossen ist bezüglich Ableitungen in G können alle diese unfertigen Satzformen bei weiterer Ableitung nur in terminalen Zeichenreihen aus $M_3 = \mathcal{L}$ münden. Es sind also nur Wörter aus $\mathcal{L}$ in G ableitbar.

Zusammen ergibt sich die Behauptung. □

3.1 Wie finde ich Beweise?

Für das eigenständige Führen von Beweisen ist die Kenntnis der gängigen Beweistechniken zwar sehr hilfreich (wenn nicht gar notwendig), aber mitnichten hinreichend. Auch hilft das Studieren fertiger, polierter Beweise wohl dabei, ein Bild davon zu bekommen, wie ein Beweis im Ergebnis aussehen soll; es reicht erfahrungsgemäß aber nicht aus, um Strategien zu entwickeln, wie man selbst neue Beweise findet.

Die einzige bekanntermaßen zuverlässige Methode ist *Übung*: Immer wieder eigene Argumente entwickeln, diese (möglichst) wasserdicht zu Papier bringen und Feedback dazu einholen. Reichlich Gelegenheit dazu haben Sie in der Übung „Beweistechniken“.