Grundlagen Theoretischer Informatik I

SoSe 2011 in Trier

Henning Fernau
Universität Trier
fernau@uni-trier.de

Grundlagen Theoretischer Informatik I Gesamtübersicht

- Organisatorisches; Einführung
- Logik & Beweisverfahren
- Mengenlehre
- algebraische Strukturen
- reguläre Sprachen

aus den letzten Vorlesungen

Abriss der Logik: Aussagenlogik und Prädikatenlogik

. . . und heute . . .

Zusammenhang mit Beweisverfahren

Was wollen wir beweisen ?

Die zu beweisende Aussage ist oft von der Form $\mathrm{p} \Rightarrow \mathrm{q}$.

Hinweis: Manchmal ist p nicht ausdrücklich angegeben.

Ohne jedwede Annahmen kann man aber nichts beweisen (wollen).

p ist dann (implizit) z.B. durch *Grundannahmen* (*Axiome*) gegeben.

Es "hilft" auch manchmal die Tautologie $\mathrm{q} \equiv (\mathrm{t} \Rightarrow \mathrm{q})$.

Manchmal sind auch *Äquivalenzaussagen* zu zeigen: $\mathrm{p} \iff \mathrm{q}$:
Hierzu verwendet man meist die Tautologie $(\mathrm{p} \iff \mathrm{q}) \equiv ((\mathrm{p} \Rightarrow \mathrm{q}) \wedge (\mathrm{q} \Rightarrow \mathrm{p}))$.

Einfachste Beweise für $p \Rightarrow q$ (interessant für “Induktionsanfänge”)

Inhaltsleerer Beweis: Wir zeigen: p ist stets falsch.
Betrachte Aussageformen $p(n) := (n > 1)$ und $q(n) := (n^3 > n)$.
$p(0) \to q(0)$ durch inhaltsleeren Beweis.

Trivialer Beweis: Wir zeigen: q ist wahr, unabhängig von p.
Betrachte $p := (0 < a \leq b)$ und $q(n) := (a^n \leq b^n)$.
$\rightsquigarrow q(0) = (a^0 \leq b^0) = (1 \leq 1)$ ✓

Anwendung: Beweisverfahren — Direkter Beweis

Die zu beweisende Aussage ist von der Form $\mathrm{p} \Rightarrow \mathrm{q}$.

Erinnerung: Eine Implikation ist nur dann falsch, wenn p wahr ist und q falsch.

$\rightsquigarrow$ zu untersuchender Fall (Annahme): p ist wahr.

Aus dieser Annahme muss jetzt gefolgert werden, dass q wahr ist.

Dann ist nämlich die Implikation wahr.

Der Beweis selbst hat oft die Form von Schlussketten, auf die dann der *modus ponens* angewendet wird.

Es seien a, b ganze Zahlen. a heißt durch b *teilbar* gdw. b *teilt* a, gdw. b ist *Teiler* von a, i.Z. $b \mid a$, gdw. es gibt eine ganze Zahl k mit $a = b \cdot k$.

Direkter Beweis — Ein einfaches Beispiel

Es sei a eine ganze Zahl. $(6 \mid a) \Rightarrow (3 \mid a)$.

Schlusskette:

$$\begin{aligned}(6 \mid a) \quad &\Rightarrow (\exists k(a = 6k)) \quad \Rightarrow (\exists k(a = (3 \cdot 2) \cdot k)) \Rightarrow (\exists k(a = 3 \cdot (2 \cdot k))) \\ &\Rightarrow (\exists k'(a = 3k')) \quad \Rightarrow (3 \mid a).\end{aligned}$$

Warum sind die einzelnen Schritte richtig ?
Wie schreibt man einen Beweis in Prosa auf ?

Direkter Beweis —

Ein weiteres Beispiel aus der *Zahlentheorie* (Restklassenarithmetik)

Lemma: Gilt $t \mid n$ und $t \mid m$, so auch $t \mid (n + m)$.

Beweis: 1. $(t \mid n) \Rightarrow (\exists k_n (n = t \cdot k_n))$.
2. $(t \mid m) \Rightarrow (\exists k_m (m = t \cdot k_m))$.
Aus 1. und 2. folgt:

$$n + m = t \cdot k_n + t \cdot k_m = t(k_n + k_m)$$

$\rightsquigarrow \exists k((n + m) = t \cdot k)$ (wähle $k = k_n + k_m$)

$\rightsquigarrow t \mid (n + m)$.

Analog: Lemma: Gilt $t \mid n$ und $t \mid m$, so auch $t \mid (n - m)$.

Zum Umgang mit Quantoren

Viele mathematische Aussagen haben die Gestalt von *Allaussagen*:

$$\forall x(p(x) \Rightarrow q(x)) \qquad (*)$$

Man beweist sie, indem man die Aussage $p(a) \Rightarrow q(a)$ für jedes a aus dem zugrundeliegenden Universum beweist.

Das liefert folgende Beweisstruktur:

1. Wähle a beliebig aus dem Universum.
2. Beweise die Implikation $p(a) \Rightarrow q(a)$.
3. Da a beliebig gewählt werden kann, folgt $(*)$.

Daher liefert der vorige Beweis die Aussage: $\forall x \in \mathbb{Z}((6 \mid x) \Rightarrow (3 \mid x))$.

direkter Beweis mit Allquantor

Lemma: (Einsteiler) $\forall t \in \mathbb{N}(t \mid 1 \implies t = 1)$.

Beweis: Wähle $t \in \mathbb{N}$ beliebig.

$t \mid 1 \rightsquigarrow \exists k(1 = tk) \rightsquigarrow \exists k(1/t = k)$

$\rightsquigarrow$ (Universum!) $t = 1$

Zum Umgang mit Quantoren

Manche mathematische Aussagen haben die Gestalt von *Existenzaussagen*:

$$[p \implies](\exists x(q(x)))$$

Solche Aussagen lassen sich oft *konstruktiv* beweisen.

Eine natürliche Zahl n heißt *zusammengesetzt* gdw. $\exists t \in \mathbb{N}((1 < t < n) \wedge (t|n))$.

Satz: Zu jeder natürlichen Zahl n gibt es n aufeinander folgende zusammengesetzte Zahlen.

Etwas formaler: $\forall n(\exists k(\forall i \in \{1, \ldots, n\}(\text{zusammengesetzt}(k + i))))$.

Beweis: Sei n beliebig. Wähle $k = (n + 1)! + 1$. $\rightsquigarrow \forall i \in \{1, \ldots, n\}((i + 1) \mid (k + i))$.
(Denn $(i + 1) \mid (k - 1)$ und $(i + 1) \mid (i + 1)$, s. vorvoriges Lemma.)

Zum Umgang mit Quantoren

Manche mathematische Aussagen haben die Gestalt von *Existenzaussagen*:

$$\exists x(p(x) \Rightarrow q(x)) \qquad (*)$$

Man beweist sie, indem man die Aussage $p(a) \Rightarrow q(a)$ für *irgendein geeignet gewähltes* a aus dem zugrundeliegenden Universum beweist.

Das liefert folgende Beweisstruktur:

1. Wähle a geeignet aus dem Universum.
2. Beweise die Implikation $p(a) \Rightarrow q(a)$.
3. Da a speziell gewählt wurde, folgt $(*)$.

Beweis durch Umkehrschluss (Kontraposition)

Erinnerung: Tautologie $(p \Rightarrow q) \equiv (\neg q \Rightarrow \neg p)$

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. $2 \mid a$.

Beweis: 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.

Hinweis: Verallgemeinerung: Ist t kein Teiler von a^2, so auch nicht von a.

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

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Lemma: Für jede natürliche Zahl t und jede natürliche Zahl n gilt: Wenn $t \geq 2$ und wenn t ein Teiler von n ist, dann ist t kein Teiler von $n+1$.

Beweis: Unsere Aussage lautet formal (mit Universum $\mathbb{N}$):

$$\forall n \forall t((t \geq 2) \wedge (t \mid n)) \implies \neg(t \mid n+1).$$

Dies ist logisch äquivalent zu:

$$\forall n \forall t(t \geq 2) \implies ((t \mid n)) \implies \neg(t \mid n+1)).$$

Wähle t, n beliebig mit $t \geq 2$. Führe einen Widerspruchsbeweis für die verbleibende Implikation.

$\rightsquigarrow$ Nimm an: $(t \mid n) \wedge (t \mid n+1)$.

$\rightsquigarrow$ $t \mid (n+1) - n \rightsquigarrow$ (Lemma Restklassenarithmetik) $t \mid 1$

$\rightsquigarrow$ (Universum ! und Lemma Einsteiler) $t = 1$ Widerspruch !

Beweis durch Widerspruch (indirekter Beweis, reductio ad absurdum)

Allgemeine Hinweise

Erinnerung: Tautologie $(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow f)$; klassisches Falsum: $r \wedge \neg r$

Ist p nicht (explizit) vorhanden, setzen wir $p = t$; um q zu beweisen, zeigen wir daher $\neg q \Rightarrow f$.

Wir können einen Beweis durch Kontraposition als Widerspruchsbeweis lesen: Haben wir $\neg q \Rightarrow \neg p$ gezeigt, so gilt auch:

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

In obiger Beweisfigur haben wir also $r = p$.
Umgekehrt ist ein Widerspruchsbeweis der Form $\neg q \Rightarrow f$ auch ein Umkehrschluss der Implikation $(t \Rightarrow q) \equiv q$.

Der Satz von Euklid

Satz: Es gibt unendlich viele Primzahlen.

Wie können wir diese Aussage formal aufschreiben ?

$\mathbb{N}$: Menge der natürlichen Zahlen
$\mathbb{P} \subseteq \mathbb{N} \setminus \{0, 1\}$: Menge der *Primzahlen*
$p \in \mathbb{P} \iff \forall q \in \mathbb{N}(q|p \implies (q = 1 \vee q = p))$.

Der Satz von Euklid lässt sich also wie folgt notieren (mit Universum $\mathbb{N}$):

Der Satz von Euklid — ein *nicht-konstruktiv*er Existenzbeweis für $\forall n \exists p((n < p) \wedge p \in \mathbb{P})$.

Die Negation lautet daher: $\exists n \forall p((n \geq p) \vee p \notin \mathbb{P})$.
Diese Aussage ist äquivalent zu:

$$\exists n \forall p(p \in \mathbb{P} \implies (p \leq n)).$$

Beweis: M.a.W.: Es gäbe dann eine größte Primzahl p_k, d.h.: $\mathbb{P} = \{p_1, \ldots, p_k\}$.
Setze $b := p_1 \cdot \cdots \cdot p_k + 1$.
Da $b > p_k$, gilt $b \notin \mathbb{P}$. $\rightsquigarrow \exists 1 < t < b(t \mid b)$.
Wir können annehmen, dass $t \in \mathbb{P}$ (Warum ? s.u.).
Nach vorigem Lemma ist t kein Teiler von $b - 1 = p_1 \cdot \cdots \cdot p_k$.
$\rightsquigarrow t \notin \mathbb{P}$. Widerspruch !

Fallunterscheidungen

Erinnerung: Tautologie $p \equiv (q \implies p) \wedge (\neg q \implies p)$.

$\rightsquigarrow$ Fallunterscheidung: 1. q ist wahr; 2. q ist falsch.

Lemma: Sei $a \in \mathbb{Z}$.
a^2 geteilt durch vier lässt entweder den Rest Eins oder den Rest Null.

Beweis: 1. Fall: a ist gerade. $\rightsquigarrow \exists k(a = 2k)$. $\rightsquigarrow a^2 = (2k)^2 = 4k^2$. $\rightsquigarrow 4 \mid a^2$.

2. Fall: a ist ungerade. $\rightsquigarrow \exists k(a = 2k + 1)$. $\rightsquigarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$. $\rightsquigarrow 4 \mid (a^2 - 1)$.

Fallunterscheidungen: noch eine Anwendung in der Zahlentheorie

Lemma: Sei $a \in \mathbb{Z}$.
Ist a nicht durch drei teilbar, so lässt a^2 beim Teilen durch drei den Rest Eins.

Beweis: "a ist nicht durch drei teilbar." $\iff (3|(a-1)) \vee (3|(a-2))$.
"a^2 lässt beim Teilen durch drei den Rest Eins." $\iff 3|(a^2-1)$.

1. Fall: $(3|(a-1)), \rightsquigarrow \exists k(a = 3k+1). \rightsquigarrow$

$$a^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2+2k) + 1$$

$\rightsquigarrow 3|(a^2-1)$.

2. Fall: $(3|(a-2)), \rightsquigarrow \exists k(a = 3k+2). \rightsquigarrow$

$$a^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 3(3k^2+4k+1) + 1$$

$\rightsquigarrow 3|(a^2-1)$.

Fallunterscheidungen: Die allgemeine Sicht

Betrachte die Tautologie:

$$((p_1 \vee p_2 \vee \cdots \vee p_n) \implies q) \equiv [(p_1 \Rightarrow q) \wedge (p_2 \Rightarrow q) \wedge \cdots \wedge (p_n \Rightarrow q)]$$

Fallunterscheidungen können also mehr als zwei Fälle umfassen.

Beweise mit vielen Fallunterscheidungen sind aber in der Regel nicht sehr elegant (und eignen sich nicht für eine Grundvorlesung).

Das Schubfachprinzip von Dirichlet 

Falls man n Gegenstände auf m Fächer $(n > m > 0)$ verteilt, dann gibt es mindestens eine Menge, in der mehr als ein Objekt landet.

Beweis: Falls das Prinzip nicht stimmt, dann landet in jedem Schubfach höchstens ein Gegenstand.

Damit gibt es höchstens soviele Gegenstände wie Schubfächer.

$\rightsquigarrow$ Widerspruch zur Annahme, dass es mehr Gegenstände als Schubfächer gibt.

Schubfachprinzip: Eine spielerische Anwendung

In einer Gruppe von acht Leuten haben (mindestens) zwei am gleichen Wochentag Geburtstag.

$\mathfrak{n}$ Gegenstände: 8 Leute
$\mathfrak{m}$ Schubfächer: 7 Wochentage
Verteilung wird vorgenommen über die Geburtstage (aber das ist unwesentlich für das Prinzip)

Schubfachprinzip: Etwas mit Logik

Lemma: Es seien p_1, p_2, p_3 Aussagen. Unter ihnen gibt es zwei, die logisch äquivalent sind.

Beweis: n Gegenstände: 3 Aussagen

m Schubfächer: 2 Wahrheitswerte

Also kommt wenigstens zwei Aussagen derselbe Wahrheitswert zu.

Schubfachprinzip: Eine zahlentheoretische Anwendung

Satz: Jede Folge von n^2+1 verschiedenen Zahlen enthält eine monoton fallende oder eine monoton wachsende Unterfolge der Länge $n+1$.

Beispiel: ($n=3$) Die Folge $7,6,11,13,5,2,4,1,9,8$ enthält die fallende Folge $7,6,5,2,1$.

Beweis: Sei $a(1),\ldots,a(n^2+1)$ eine Zahlenfolge. Ordne $a(k)$ das Paar $(\sigma(k),\phi(k))$ zu mit:
$\sigma(k)$: Länge der längsten monoton steigenden Unterfolge, die bei $a(k)$ beginnt
$\phi(k)$: Länge der längsten monoton fallenden Unterfolge, die bei $a(k)$ beginnt

Wenn die Behauptung falsch wäre, so gölte $\forall k((\sigma(k)\leq n)\wedge(\phi(k)\leq n))$.
Schubfachprinzip $\rightsquigarrow$ es gibt $s<t$ mit $\sigma(s)=\sigma(t)$ und $\phi(s)=\phi(t)$.

1. Fall: $a(s)<a(t)$: Dann gibt es eine aufsteigende Folge der Länge $\sigma(t)+1$; betrachte $a(s)$ gefolgt von der bei $a(t)$ beginnenden steigenden Folge $\rightsquigarrow \sigma(s)\geq\sigma(t)+1$.
2. Fall: $a(s)>a(t)$ analoge Verlängerung der bei $a(s)$ beginnenden fallenden Folge.

$\lceil x \rceil$: kleinste ganze Zahl n mit $n \geq x$ (Aufrundefunktion; ceiling)

Das **Schubfachprinzip**: Eine Verallgemeinerung

Satz: Werden $n > k$ Gegenstände auf k Fächer verteilt, so gibt es mindestens ein Fach, das $\lceil \frac{n}{k} \rceil$ Gegenstände enthält.

Beweis: Wäre das nicht der Fall, so können die Fächer insgesamt nicht mehr als

$$k\left(\left\lceil \frac{n}{k} \right\rceil - 1\right) < k\left(\left(\frac{n}{k} + 1\right) - 1\right) = n$$

Gegenstände enthalten; Widerspruch !

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...

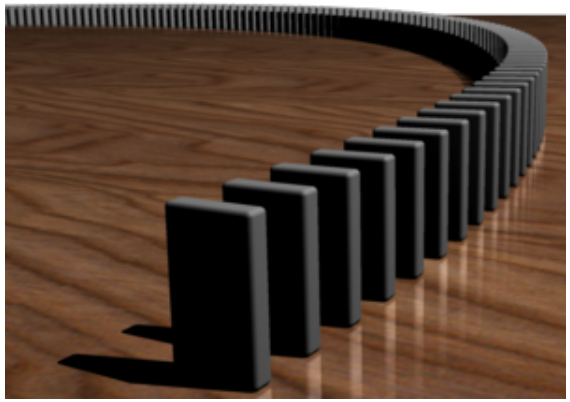
Grundgedanke der mathematischen Induktion

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: $p(n) \Rightarrow p(n+1)$.
$p(n)$ heißt hier auch *Induktionsannahme* oder *Induktionsvoraussetzung* (IV).

Nach dem Prinzip der mathematischen Induktion folgt hieraus: $\forall n(p(n))$.

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.

Induktion aus logischer Sicht.

Stimmt das Induktionsprinzip ?

$p(0)$ ist richtig wegen des Ankers.
$p(1)$ ist wahr, denn $p(0)$ ist wahr und $p(0) \Rightarrow p(1)$ ist Spezialfall des Induktionsschritts, also folgt $p(1)$ mit modus ponens.
$p(2)$ ist wahr, denn $p(1)$ ist wahr und $p(1) \Rightarrow p(2)$ ist Spezialfall des Induktionsschritts, also folgt $p(2)$ mit modus ponens.
...

Induktion aus logischer Sicht.

Angenommen, die Aussage $p(n)$ gölte nicht für alle natürlichen Zahlen n.
Dann gibt es eine kleinste Zahl n_0, für die sie falsch ist. Es gibt nun zwei Fälle:
1. $n_0 = 0$: Dies wird durch den Induktionsanfang ausgeschlossen.
2. $n_0 \neq 0$: Nach Voraussetzung ist n_0 die kleinste Zahl, für die $p(n)$ falsch ist, also ist $p(n_0 - 1)$ wahr.
Induktionsschritt $\rightsquigarrow p((n_0 - 1) + 1)$ ist wahr: Widerspruch.
Beide Fälle können also ausgeschlossen werden, damit ist die Aussage $p(n)$ für alle natürlichen Zahlen n wahr.

Bei diesem Argument wurde im magentafarbenen Teil implizit das harmlos erscheinende *Wohlordnungsaxiom* verwendet:
Jede nichtleere Teilmenge natürlicher Zahlen besitzt ein kleinstes Element.

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.

Induktion am Beispiel.

Satz: $\forall n \in \mathbb{N}(2^{n+1} - 1 = \sum_{i=0}^{n} 2^i)$.

Beweis: IA: Die Behauptung gilt für $n = 0$: $2^1 - 1 = 1 = 2^0$.
IS: Angenommen, die Aussage gilt für n. Dann rechnen wir:

$$\begin{aligned} 2^{n+2} - 1 &= 2^{n+1} + (2^{n+1} - 1) \\ &= 2^{n+1} + (\sum_{i=0}^{n} 2^i) \qquad \text{IV} \\ &= \sum_{i=0}^{n+1} 2^i \end{aligned}$$

Nach dem Prinzip der mathematischen Induktion folgt die Behauptung.

Induktion in der Anwendung: *Schleifeninvariante* $P(i, q) := (q = (i-1)^2)$.

1. Lies die natürliche Zahl n ein.

2. Setze $q := 0$ und $i := 1$.
   { $P(1, 0) = (0 = (1-1)^2)$ ✓ Induktionsanfang }

3. **Solange** $i \leq n$ **tue**:
   { IV: Es gilt $P(i, q)$, also $q = (i-1)^2$. }
   $q := q + 2i - 1$;
   $i := i + 1$
   { IS: Zu zeigen ist $P(i+1, q+2i-1) = (q + 2i - 1 = i^2)$ mit
   $i^2 = ((i-1)+1)^2 = (i-1)^2 + 2(i-1) + 1 = (i-1)^2 + 2i - 1 =^{IV} q + 2i - 1$. }

4. Gib q aus. { Bei Schleifenaustritt gilt: $i = n + 1. \rightsquigarrow q = n^2$ }

Induktion am Beispiel.

Satz: Jede natürliche Zahl ungleich Null kann als Produkt von Primzahlen geschrieben werden.

Beweis: IA: $n = 0$ inhaltsleer wahr. $n = 1$ stimmt (leeres Produkt)

IS: Angenommen, die Aussage gilt für n.

1. Fall: $n + 1$ ist Primzahl. Dann ist die Aussage trivialerweise richtig.

2. Fall: $n + 1$ ist keine Primzahl. Wegen $n > 0$ ist (da 1. Fall nicht zutrifft) $n + 1 \geq 4$ Produkt zweier Zahlen $(n + 1) = (k \cdot \ell)$ mit $2 \leq k, \ell < n$.

Nach IV lassen sich k, ℓ als Produkt von Primzahlen darstellen und mithin $n + 1$.

Nach dem Prinzip der vollständigen mathematischen Induktion folgt die Behauptung.

Hinweis: Dies vervollständigt unseren Beweis vom Satz von Euklid.

Das Prinzip der **vollständigen mathematischen Induktion** verallgemeinert das bislang Gesagte.
Der Induktionsschritt besteht nun aus dem Schluss

$$\forall n([p(0) \wedge p(1) \wedge \cdots \wedge p(n)] \Rightarrow p(n+1)).$$

Manchmal ist es hilfreich, bei Induktionsbeweisen “tiefer zurück” gehen zu dürfen, um den Induktionsschritt zu beweisen.

Ein abschließendes 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 oder 5 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 $n_5 \geq 1$ (leicht einsehbar durch Umkehrschluss).
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.

Strukturelle Induktion als vollständige mathematische Induktion

Erinnerung: Wir haben schon Beispiele für strukturelle Induktion über den rekursiven syntaktischen Aufbau aussagenlogischer Formeln gesehen.

Es ist also eine Aussage P für alle Formeln zu beweisen.

Ordne (im Beispiel) jeder Formel F die Anzahl $o(F)$ der Operatoren zu.
$P(o(F))$ sei die Aussage P, eingeschränkt auf alle Formeln mit höchstens $o(F)$ Operatoren.

$o(F) = 0$ gdw. F ist atomar $\leadsto$ Induktionsanker $P(0)$.
Die Induktionsannahme besagt nun: Es gelte die Aussage $P(n)$.
Im Induktionsschritt betrachten wir eine Formel F mit $n + 1$ Operatoren und betrachten (gemäß der rekursiven Formeldefinition) drei Unterfälle, z.B. $F = \neg G$ und bemerken, dass nach Induktionsannahme P für G gilt, da $o(G) = n$.