Zusatz: Einführung in die Mathematischen Beweistechniken

Quick-Start Informatik
Theoretischer Teil
WS 11/12

Jens Keppeler

7. Oktober 2011

Das folgende Zusatzskript, sowie die dazugehörigen Folien orientieren sich an:

Mathematische Grundlagen der Informatik (Mathematisches Denken und Beweisen, Eine Einführung)
Christoph Meinel, Martin Mundhenk
Vieweg + Teubner Verlag
Kapitel 6

Die Mathematik befasst sich mit *Definitionen, Sätze, Lemma, ...*.

- *Definitionen* legen bestimmte Sachverhalte und/oder Notationen fest. Zum Beispiel:

  Definition 1 *Seien a und b natürliche Zahlen. $a + b$ beschreibt die Addition der natürlichen Zahlen a und b.*

- *Sätze, Lemma, ...* sind Aussagen, die aus den verschiedensten Definitionen folgen können. Um nachzuweisen, dass diese Aussagen stimmen, müssen wir einen mathematischen Beweis durchführen. Beispiel:

  Lemma 2 (Binomische Formel) $(a + b)^2 = a^2 + 2ab + b^2$

  Beweis: $(a+b)^2 = (a+b)\cdot(a+b) = a^2 + a\cdot b + a\cdot b + b^2 = a^2 + 2a\cdot b + b^2$

In der Informatik kämpfen wir ebenfalls mit mathematischen Strukturen, über die wir Aussagen treffen möchten. Beispielsweise über einen Algorithmus bzw. über einen Programmcode. Wichtig ist zum Beispiel der Nachweis über die Korrektheit der Algorithmen in der Flugzeugsteuerung und der Medizintechnik. In diesen Bereichen gab es in der Vergangenheit aufgrund von Programmierfehlern bzw. Fehlern in Algorithmen mehrere Unfälle. Wir benötigen daher in der Informatik die mathematischen Beweistechniken, um eine eindeutige Antwort auf die Gültigkeit unserer Feststellungen/Aussagen zu finden. (Macht mein Algorithmus [bzw. Programm] das was er soll? Läuft mein Algorithmus so schnell wie er sollte?). Die mathematischen Beweistechniken bilden daher eine wichtige Grundlage. In diesem Kapitel geben wir einen kurzen Einblick über das Führen/Gestalten von Beweisen.

1 Direkter Beweis

Mathematische Aussagen haben häufig die Form "Wenn... dann..." (Aussagenlogisch: $p \to q$). Dabei nennen wir p die Voraussetzung und q die Folgerung.

Beispiel 3 *Betrachte die Aussage: Wenn eine Zahl durch 10 teilbar ist, dann ist sie auch durch 5 teilbar.*

Wir teilen dann unser p und q auf:

p : Eine Zahl ist durch 10 teilbar

q : Eine Zahl ist durch 5 teilbar

Nun müssen wir, um zu zeigen, dass die Beispielaussage gilt, die Implikation $p \to q$ nachweisen. Wir betrachten dazu die Wertetabelle:

p	q	$p \to q$
0	0	1
0	1	1
1	0	0
1	1	1

In der Tabelle sehen wir: Wenn p falsch ist, dann kann daraus folgen, dass q wahr oder falsch ist, es gilt dann immer $p \to q$. Wenn p wahr ist, dann muss unbedingt auch q wahr sein, damit $p \to q$ wahr ist. Wir müssen daher zeigen, wenn p wahr ist, dann muss auch q wahr sein.

Wir sehen also:

- *In der dritten Zeile:* Wenn unsere Voraussetzung richtig ist ($p = 1$) und die die Folgerung falsch ist ($q = 0$), dann ist unsere aufgestellte Behauptung falsch.
- *In der vierten Zeile:* Wenn unsere Voraussetzung richtig ist ($p = 1$) und die die Folgerung richtig ist ($q = 1$), dann ist unsere aufgestellte Behauptung richtig.

Für unseren Beweis müssen wir noch klären, was "Teilbarkeit" überhaupt bedeutet. Daher definieren wir:

Definition 4 (Teilbarkeit) *Eine Zahl a ist durch b teilbar, wenn es eine ganze Zahl k gibt mit $a = b \cdot k$*

Beispiel 5 70 *ist duch* 10 *teilbar, da* $70 = 10 \cdot k$ *für* $k = 7$.

Beispiel 6 *Sei a durch 10 teilbar. Dann hat a die Form $a = 10 \cdot k$ für eine ganze Zahl k.*

Wir nehmen nun unsere Aussage p und formen diese Schritt für Schritt um.

p Eine Zahl ist durch 10 teilbar

a_1 $a = 10 \cdot k$ für eine ganze Zahl k (Definition der Teilbarkeit)

a_2 $a = 2 \cdot 5 \cdot k$ für eine ganze Zahl k $(10 = 2 \cdot 5)$

a_3 $a = 5 \cdot k'$ für eine ganze Zahl k' $(k' = 2 \cdot k)$

q Eine Zahl ist durch 5 teilbar (Definition der Teilbarkeit)

Wir beobachten die Implikationsfolge $p \to a_1 \to a_2 \to a_3 \to q$, also $(p \to q)$. Nun verpacken wir unseren Beweis in einen schönen mathematischen Text:

Lemma 7 *Wenn eine Zahl durch 10 teilbar ist, dann ist sie auch durch 5 teilbar*

Beweis:
Sei a eine Zahl, die durch 10 teilbar ist. Dann hat a die Form $a = 10 \cdot k$ (nach Def der Teilbarkeit) für eine ganze Zahl k. Durch Umformen erhalten wir $a = 10 \cdot k = 5 \cdot 2 \cdot k = 5 \cdot k'$ für eine ganze Zahl k'. Nach der Definition der Teilbarkeit ist die Zahl a auch durch 5 teilbar.

□

2 Beweis durch Kontraposition

Nicht immer ist es einfach $p \to q$ direkt nachzuweisen. Daher überlegen wir uns:

Wir betrachten nun ein Spiel. Wir haben eine Menge von Karten. Auf der Vorderseite ist jeweils eine Farbe Blau oder Gelb, und auf der Rückseite befindet sich jeweils eine Zahl. Für alle Karten soll nun gelten:

Wenn eine Karte vorne blau ist, dann ist die Zahl auf der Rückseite gerade.

Wenn wir nun eine Karte ziehen, und auf der Rückseite dieser Karte befindet sich eine ungerade Zahl, welche Farbe wird sie dann haben?

Natürlich gelb. Wir formalisieren nun unseren Sachverhalt aussagenlogisch:

p Die Karte ist vorne blau

q Auf der Karte befindet sich eine gerade Zahl

Unsere Tatsache: "Wenn eine Karte vorne blau ist, dann ist die Zahl auf der Rückseite gerade", wäre aussagenlogisch formalisiert: $(p \to q)$. Wir betrachten nun die Negationen von p und q:

$\neg p$ Die Karte ist vorne gelb

$\neg q$ Auf der Karte befindet sich eine ungerade Zahl

Wir haben nun gesagt: "Wenn sich auf der Rückseite eine ungerade Zahl befindet, dann ist die Karte vorne gelb", daher gilt dann: $(\neg q \to \neg p)$. Wir betrachten unsere Wertetabelle:

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

Fazit: $(p \to q) \equiv (\neg q \to \neg p)$, da die Spalteneinträge von $(p \to q)$ und $(\neg q \to \neg p)$ übereinstimmen.

Wir können also $\neg q \to \neg p$ anstatt $p \to q$ nachweisen. Diese Beweistechnik nennen wir "Beweis durch Kontraposition".

Beispiel 8 *Wenn a^2 ungerade ist, dann ist a ungerade*

Wir betrachten unsere Aussagen:

p a^2 ist eine ungerade Zahl

q a ist eine ungerade Zahl

und deren Negationen:

$\neg p$ a^2 ist eine gerade Zahl

$\neg q$ a ist eine gerade Zahl

Wir betrachten nun wieder unsere Aussagenfolge:

$\neg q$ a ist eine gerade Zahl

a_1 a ist durch 2 teilbar (Jede gerade Zahl ist durch 2 teilbar)

a_2 $a = 2 \cdot k$ für eine ganze Zahl k (Definition der Teilbarkeit)

a_3 $a^2 = 2^2 \cdot k^2$ für eine ganze Zahl k (quadrieren)

a_4 $a^2 = 2 \cdot k'$ für eine ganze Zahl k' $(k' = 2 \cdot k^2)$

a_5 a^2 ist durch 2 teilbar (Definition der Teilbarkeit)

$\neg p$ a^2 ist eine gerade Zahl (Definition einer geraden Zahl)

Wir haben also $\neg q \to \neg p$ und somit auch $p \to q$ gezeigt. Kompakt geschrieben:

Lemma 9 *Wenn a^2 ungerade ist, dann ist a ungerade.*

Beweis: Beweis durch Kontraposition
Wir nehmen an, dass a gerade ist. Dann ist a durch 2 teilbar und hat nach Definition der Teilbarkeit die Form $a = 2 \cdot k$ für eine ganze Zahl k. Durch Quadrieren erhalten wir $a^2 = 2^2 \cdot k^2 = 2 \cdot 2 \cdot k^2 = 2 \cdot k'$ mit $k' = 2 \cdot k^2$ für ganze Zahlen k und k'. Somit ist a^2 durch 2 teilbar und somit gerade.

□

Anmerkung: Wenn wir versuchen würden unser Beispiel auf direktem Wege zu lösen, dann wäre dies sehr viel schwerer, da wir von Anfang an ein a^2 hätten und wir uns schwierig auf das a beziehen können. Es ist daher wichitg, die richtige Beweistechnik zu wählen, um sich viel Arbeit zu ersparen.

3 Beweis durch Widerspruch

Wiederum gibt es Fälle, bei denen der direkte Beweis und der Beweis durch Kontraposition nicht geeignet ist. Wir fordern daher eine dritte Beweistechnik, den Beweis durch Widerspruch:
Einführendes Beispiel: Supermärkte haben im Allgemeinen folgende Regel zu befolgen:

Wenn sie Alkohol an ihre Kunden verkaufen, dann müssen die Kunden ≥ 18 Jahre alt sein

Die Polizei führt des öfteren Kontrollen auf Supermärkte durch, um die obige Aussage zu überprüfen. Dabei beauftragen diese Jugendliche, die jünger als 18 Jahre alt sind, in den Supermarkt zu gehen, um Alkohol zu kaufen. Was muss nun passieren, damit die obige Aussage stimmt? Sie dürfen den Alkohol **nicht** verkaufen, dann hat der Supermarkt seinen Test bestanden. Wir halten aussagenlogisch fest:

p Der Supermarkt verkauft Alkohol an ihre Kunden

q Die Kunden sind ≥ 18 Jahre alt

$\neg q$ Die Kunden sind jünger als 18 Jahre

$(p \to q)$ Wenn Sie Alkohol an ihre Kunden verkaufen, dann müssen die Kunden $\geq$ 18 Jahre alt sein

Die Polizei beauftragt Jugendliche Alkohol zu kaufen und diese Jugendliche sind jünger als 18 Jahre. Wir erhalten: $(p \wedge \neg q)$. Wenn unter diesen Umständen der Supermarkt kein Alkohol verkäuft, (Also wenn wir eine Falschaussage f haben, die unsere Behauptung widerlegt), dann erhalten wir insgesamt: $((p \wedge \neg q) \to f)$. Wir beweisen also $p \to q$ indem wir $((p \wedge \neg q) \to f)$ zeigen, also $(p \wedge \neg q)$ zu einer Falschaussage bzw. Widerspruch führen. (Unsere Falschaussage f liegt in unserem Beispiel darin, dass wir annehmen dass der Supermarkt den Alkohol verkaufen wird, dies aber nicht tut) Den Beweis für die Gültigkeit werden wir in einer Übung führen. Wir nennen diese Beweistechnik *Beweis durch Widerspruch.*

Beispiel 10 *Wenn a und b gerade natürliche Zahlen sind, dann ist auch deren Produkt $a \cdot b$ gerade.*

Wir teilen unsere Aussage in Teilaussagen auf:

p a und b sind gerade natürliche Zahlen

q $a \cdot b$ ist gerade

$\neg q$ $a \cdot b$ ist ungerade

Wir wenden nun $((p \wedge \neg q) \to f)$ an, wobei wir auf eine falsche Aussage f treffen müssen.

$p \wedge \neg q$: a und b sind gerade natürliche Zahlen und $a \cdot b$ ist ungerade

a_1 : a ist gerade und $b = 2 \cdot k$ für eine natürliche Zahl k und $a \cdot b$ ist ungerade

a_2 : a ist gerade und $a \cdot b = 2 \cdot k \cdot a$ für eine natürliche Zahl k und $a \cdot b$ ist ungerade

a_3 : a ist gerade und $a \cdot b = 2 \cdot k'$ für eine natürliche Zahl k' und $a \cdot b$ ist ungerade mit $k' = k \cdot a$.

f : a ist gerade und $a \cdot b$ ist gerade und $a \cdot b$ ist ungerade

Die Aussage f ist offensichtlich falsch, da $a \cdot b$ entweder gerade oder ungerade sein kann.

Lemma 11 *Wenn a und b gerade natürliche Zahlen sind, dann ist auch $a \cdot b$ gerade.*

Beweis:
Beweis durch Widerspruch
Angenommen zwei natürliche Zahlen a und b sind gerade und $a \cdot b$ ist ungerade. Dann hat b die Form $b = 2 \cdot k$ für eine natürliche Zahl k nach Definition der Teilbarkeit . Multipliziert man diesen Ausdruck mit a, dann ergibt dies $a \cdot b = 2 \cdot k \cdot a$. Wir definieren $k' = k \cdot a$, so dass wir $a \cdot b = 2 \cdot k'$ erhalten. Dabei ist k' eine natürliche Zahl. Somit ist $a \cdot b$ gerade. **Widerspruch**

□

4 Äquivalenzbeweis

Oftmals haben Aussagen die Form $p \leftrightarrow q$. Diese werden in der Mathematik durch "Genau dann, wenn..." ausgedrückt.

Beispiel 12 *Genau dann, wenn a gerade ist, ist auch a^2 gerade.*

Wir betrachten unsere Wertetabelle:

p	q	$p \leftrightarrow q$	$p \rightarrow q$	$q \rightarrow p$	$(p \rightarrow q) \wedge (q \rightarrow p)$
0	0	1	1	1	1
0	1	0	1	0	0
1	0	0	0	1	0
1	1	1	1	1	1

Wir sehen, dass die dritte Spalte mit der letzten übereinstimmt. Somit können wir $p \leftrightarrow q$ mit $(p \rightarrow q) \wedge (q \rightarrow p)$ ersetzen.
In unserem Beispiel wäre das:

p : a ist gerade

q : a^2 ist gerade

$p \rightarrow q$: "Wenn a gerade ist, dann ist auch a^2 gerade"

$q \rightarrow p$: "Wenn a^2 gerade ist, dann ist auch a gerade"

Beweis:
$\Rightarrow$ siehe Übung
$\Leftarrow$ siehe Beweis Lemma ...

Es gibt in der Informatik noch weitere wichtige Beweistechniken:

- Beweis durch vollständige Induktion (für natürliche Zahlen)
- Beweis atomarer Aussagen
- Beweis mit Fallunterscheidung
- ...

Beweise lernt ihr am Besten durch ÜBEN, ÜBEN und ÜBEN (i.d.R. werdet ihr wöchentlich mit mindestens einer Beweisaufgabe konfrontiert).
Tipps zum Beweisen:

- Es ist zu achten, dass keine Gedankensprünge in dem Beweis enthalten sind. Jede Folgerung, die man trifft, sollte klar sein
- Eine Angabe der Beweistechnik am Anfang hilft dem Leser dem Beweis zu folgen
- Beweise sollen möglichst präzise und genau sein, sodass der Leser die Gedankengänge vollständig nachvollziehen kann
- Eine Kennzeichnung am Ende eines Beweises (z.B. durch *qed* oder $\square$), auch wenn es dem Schreiber klar erscheint, ist für den Leser hilfreich
- Am Ende von längeren Beweisen ist ein kurzer Satz, was ihr gezeigt habt, hilfreich