Beweisen ohne Sorgen

Teil (A): Was wir mit Beweisen *nicht* meinen

(aus: Armin P. Barth, „Logik? – Logisch!“ Teil 2, in VSMP Bulletin, Nr. 112, Febr. 2010, pp. 21 – 31)

Abraham Lincoln sagte einmal: *It is true that you may fool all the people some of the time; you can even fool some of the people all the time; but you can't fool all of the people all the time*.

Es lässt sich leicht einsehen, dass die Aussagenlogik nicht stark genug ist, um diese Aussage zu formalisieren. Sie stellt nur plumpe Aussagen zur Verfügung. Damit lässt sich aber nicht ausdrücken, dass es *einige* Menschen gibt, die zu *allen* Zeitpunkten für dumm verkauft werden können. Wir brauchen, wollen wir anspruchsvollere Aussagen formalisieren, eine bessere Logik. Wir benötigen zum Beispiel Variablen *x* und *t*, die aus der Menge aller Menschen respektive aus der Menge aller Zeiten schöpfen. Und wir benötigen ein Prädikat (eine Relation) $P(x)$, das erfüllt ist, wenn x eine Person bedeutet, und weiter ein Prädikat $Z(t)$, das erfüllt ist, wenn *t* eine Zeit bedeutet, und schliesslich ein zweistelliges Prädikat $D(x,t)$, das erfüllt ist, wenn Person *x* zur Zeit *t* für dumm verkauft wird. Dann kann der erste Satz des Lincoln-Zitates so formalisiert werden:

$$\forall x\big(P(x)\rightarrow\exists t\big(Z(t)\wedge D(x,t)\big)\big)$$

Dabei steht $\forall$ für „für alle“ und $\exists$ für „es existiert ein“. Erst mit diesen zusätzlichen Elementen wird die logische Sprache stark genug, um die meisten Aussagen ausdrücken zu können, denen Mathematiker bei ihrem alltäglichen Tun begegnen. Wir sehen uns daher veranlasst, im Folgenden den syntaktischen Aufbau der viel reichhaltigeren Sprache der *Prädikatenlogik* aufzubauen.

formale Sprache

Gegenüber der Aussagenlogik muss hier der Zeichensatz natürlich erweitert werden. Wir beschränken uns wiederum auf ein Minimum an Symbolen:

Der Zeichensatz	$\neg$	$\wedge$	$\forall$	$=$	( )	'
	nicht	und	für alle	gleich	Klammern	Apostroph

Wiederum benutzen wir auch andere Zeichen gerne und zwar als Abkürzungen:

$\Phi\vee\Psi$	als Abkürzung für	$\neg\big(\neg\Phi\wedge\neg\Psi\big)$
$\Phi\rightarrow\Psi$	als Abkürzung für	$\neg\Phi\vee\Psi$
$\Phi\leftrightarrow\Psi$	als Abkürzung für	$\big(\Phi\rightarrow\Psi\big)\wedge\big(\Psi\rightarrow\Phi\big)$
$\exists xP(x)$	als Abkürzung für	$\neg\forall x\big(\neg P(x)\big)$
$x\neq y$	als Abkürzung für	$\neg\big(x=y\big)$

Zudem benötigen wir Variablen als Platzhalter für Individuen, Prädikate als Eigenschaften von Individuen und Funktionen, die Individuen neue Individuen zuweisen. Genauer:

- Wir führen eine Menge *Var* von *Variablen* ein, die wir mit x, x', x'',... oder – im Sinne einer Abkürzung – mit $x, y, z,...$ (oder auch indiziert) bezeichnen.
- Wir führen eine endliche Menge *Präd* von *Prädikaten* ein. *Präd* enthält also Prädikate $P_i(...)$, wobei i eine endliche Indexmenge I durchläuft und eine Stellenzahlfunktion $\lambda: I \to \mathbb{N}$ jedem Prädikat seine Stellenzahl $\lambda(i)$ zuordnet.
- Wir führen weiter eine endliche Menge *Funk* von *Funktionen* ein. *Funk* enthält also Funktionen $f_j(...)$, wobei *j* eine endliche Indexmenge *J* durchläuft und eine Stellenzahlfunktion $\mu: J \to \mathbb{N}$ jeder Funktion ihre Stellenzahl $\mu(j)$ zuordnet.
- 0-stellige Funktionen wollen wir *Konstanten* nennen, und wir notieren sie so: c_k, wobei k eine Indexmenge *K* durchläuft.

Bei obigem Lincoln-Zitat etwa hatten wir keine Funktion, aber drei Prädikate benutzt, zwei einstellige und ein zweistelliges. Zum Aufbau einer formalen Sprache gehört es, dass man ganz präzise festlegt, was korrekt gebildete Terme, Formeln und Aussagen sind. Das wollen wir als nächstes in Angriff nehmen:

Definition: Alle Variablen und Konstanten sind *Terme*. Sind $\tau_1,...,\tau_{\mu(j)}$ schon Terme, so ist auch $f_j(\tau_1,...,\tau_{\mu(j)})$ ein Term. Nichts sonst ist ein Term. Mit *TM* bezeichnen wir die Menge aller Terme.

Es ist klar, dass wir damit genau unsere alltägliche Vorstellung von Termen realisiert haben. Immer neue Terme entstehen ja aus Variablen und Konstanten dadurch, dass man diese irgendwelchen Funktionen unterwirft und so neue Terme erzeugt. Auch bei der Definition von Formeln lassen wir uns wieder vom Alltag leiten:

Definition:

i. Sind σ und τ Terme, so ist $\sigma = \tau$ eine *Formel*.

ii. Sind $\tau_1,...,\tau_{\lambda(i)}$ Terme, so ist $P_i(\tau_1,...,\tau_{\lambda(i)})$ eine *Formel*.

Formeln vom Typ i. und ii. heissen *Primformeln*.

iii. Sind Φ und Ψ Formeln, so sind auch $\neg\Phi$, $\Phi \wedge \Psi$, $\Phi \vee \Psi$, $\Phi \to \Psi$, $\Phi \leftrightarrow \Psi$, $\exists x\Phi$ und $\forall x\Phi$ Formeln.

iv. Nichts sonst ist eine Formel.

Mit *FML* bezeichnen wir die Menge aller Formeln.

Zur Vereinfachung erlauben wir uns immer wieder Abkürzungen wie zum Beispiel $\forall x, y, z$ statt $\forall x \forall y \forall z$ oder $\exists x, y, z$ statt $\exists x \exists y \exists z$ oder $\tau_1 P_i \tau_2$ statt $P_i(\tau_1, \tau_2)$ usw. Wenn wir uns noch einmal das Lincoln-Zitat vor Augen führen, so fällt auf, dass sich das auch anders verstehen lässt. Unsere erste Formalisierung war ja

$$\forall x\big(P(x) \to \exists t\big(Z(t) \wedge D(x,t)\big)\big)$$

Der erste Satz des Zitates könnte aber – obwohl wenig wahrscheinlich – auch so verstanden werden, dass es einen speziellen Zeitpunkt gibt, an dem alle Menschen gleichzeitig für dumm verkauft werden können. Dann allerdings lautet die Formalisierung so:

$$\exists t\big(Z(t) \wedge \forall x\big(P(x) \to D(x,t)\big)\big)$$

Was immer Lincoln sagen wollte, beides sind Beispiele korrekt gebildeter Formeln der Prädikatenlogik.

Unser nächstes Ziel ist es, *Aussagen* zu definieren. Dazu lohnt sich ein Vorüberlegung: Die Formel (1) $x^2 + 7x + 5 = 0$ entspricht nicht unserer intuitiven Vorstellung einer Aussage, da sie nicht entweder wahr oder falsch ist. Der Wahrheitswert hängt von der Zahl ab, die wir in die Variable einzusetzen gedenken. Hingegen sind die Formeln (2) $\forall x, y\big(x^2 - y^2 = (x+y)\cdot(x-y)\big)$ und (3) $\forall x, y\big(x^2 + y^2 = (x+y)^2\big)$ Aussagen im intuitiven Sinn, (2) eine wahr und (3) eine falsche, falls wir an

den Individuenbereich $\mathbb{R}$ denken. Der Unterschied zwischen (1) und (2)&(3) liegt darin, dass in (1) die Variable *x* „frei“ (nämlich nicht an einen Quantor gebunden) vorkommt, während die Variablen in (2)&(3) „gebunden“ sind. Das macht die nächste Definition verständlich:

Definition: In den Formeln $\forall x(\Phi)$ und $\exists x(\Phi)$ heisst Φ *Wirkungsbereich* des Quantors $\forall$ bzw. $\exists$. Eine Variable *x* in der Formel Φ heisst *gebunden*, wenn sie sich im Wirkungsbereich eines Quantors $\forall x$ oder $\exists x$ befindet, sonst *frei*.
Eine *Aussage* ist eine Formel ohne freie Variablen. Mit *AUS* bezeichnen wir die Menge aller Aussagen.

In der Formel $\forall x(x<0 \to x<y) \wedge \exists z((0<z) \wedge (z<x))$ beispielsweise ist *x* in der linken Klammer gebunden und in der rechten frei, während *y* in der ganzen Formel frei und *z* in der ganze Formel gebunden ist. Insbesondere ist die Formel also keine Aussage.

Als nächstes führen wir noch zwei Konzepte ein, die wichtig sein werden: die *Substitution* und die *Sprache*.

Im mathematischen Alltag ist es überaus häufig, dass man für Variablen in Formeln irgendwelche Terme einsetzt; selbstredend ersetzt man dann jedes Vorkommen der Variablen durch denselben Term. Dieses Konzept wollen wir hier abbilden. Der Punkt ist, dass wir nur in eine freie Variable einsetzen sollten. Wir sollten unser Augenmerk überdies auf die Tatsache richten, dass bei der Substitution einer freien Variablen durch einen Term es durchaus passieren kann, dass eine im Term enthaltene Variable neu in den Wirkungsbereich eines Quantors gelangt. Ersetzen wir zum Beispiel in $\exists y(x<y)$ die freie Variable *x* durch einen Term, der *y* enthält, so gerät *y* in den Wirkungsbereich des Quantors. In der folgenden Definition tragen wir diesem Fall Rechnung:

Definition: Mit $\Phi(x|\tau)$ bezeichnen wir diejenige Formel, die man aus der Formel Φ erhält, wenn man jedes freie Vorkommen der Variablen *x* durch den Term τ ersetzt. Der Term τ heisst *frei für x in* Φ, falls durch diese Ersetzung keine Variable von τ in den Wirkungsbereich eines Quantors gerät.

Die oben eingeführten Begriffe der formalen Sprache hängen ganz wesentlich ab von den beiden Stellenzahlfunktionen $\lambda: I \to \mathbb{N}$ und $\mu: J \to \mathbb{N}$ sowie der Indexmenge *K* der Konstanten. In diesen „Dingen“ bündelt sich gewissermassen der reale Weltausschnitt, der durch die formale Sprache abgebildet werden soll. Da der gesamte Sprachaufbau vom Tripel (y, μ, K) abhängt, wollen wir dieses Tripel eine *Sprache* nennen:

Definition: Das Tripel $L := (\lambda, \mu, K)$ nennen wir *Sprache*. Wir schreiben $TM(L)$, $FML(L)$ und $AUS(L)$, um diese Abhängigkeit auszudrücken.

formale Beweise

Die Beschäftigung mit Logik ist darum so wichtig, weil sie jeglichem mathematischen Tun zu Grunde liegt. Wenn wir in irgendeiner mathematischen Theorie arbeiten, befolgen wir nebst den theoriespezifischen Sätzen und Axiomen immer auch die Regeln der Logik; die Logik ist die Begleiterin jeder anderen mathematischen Theorie. Die nun folgende Definition eines formalen Beweises muss dem Rechnung tragen, das heisst, unsere formale Sprache muss nebst den logischen Axiomen immer auch eine Menge von theoriespezifischen Formeln (das zu diesem Zeitpunkt bereits gesicherte Wissen der Theorie) bereitstellen. Formale Beweise basieren also letztlich auf logischen Axiomen, logischen Schlussregeln sowie dem Fundament der Theorie. Um die Axiome und Schlussregeln der Prädikatenlogik wollen wir uns nun zuerst kümmern.

Die logischen Axiome enthalten einerseits Axiome der Aussagenlogik und andererseits quantorenlogische Axiome. Bei der Aussagenlogik könnten wir uns für ein geeignetes Axiomensystem entscheiden, wir können uns das Leben aber auch erleichtern, wenn wir gleich alle Tautologien als Axiome zulassen. Dies wird ja durch die semantische Vollständigkeit der Aussagenlogik gerechtfertigt. Sollten wir bei irgendeinem Beweis eine aussagenlogische Tautologie verwenden, ist es praktisch,

diese als Axiom zur Verfügung zu haben, anstatt sie erst aus den Axiomen der Aussagenlogik herleiten zu müssen. Als Axiome unserer formalen Sprache wählen wir diese:

Logische Axiome	
Axiome der Aussagenlogik	Alle Tautologien
Quantorenlogische Axiome	(Q1) $\forall x\Phi(x)\to\Phi(\tau)$, falls τ frei für *x* in Φ ist. (Q2) $\forall x(\Phi\to\Psi)\to(\Phi\to\forall x\Psi)$, falls *x* nicht frei in Φ. (Q3) $\Phi(\tau)\to\exists x\Phi(x)$ (Q4) $\exists x\Phi(x)\to\neg\forall x\neg\Phi(x)$
Identitätslogische Axiome	(I1) $x=x$ (Reflexivität) (I2) $(x=y)\to(y=x)$ (Symmetrie) (I3) $(x=y)\wedge(y=z)\to(x=z)$ (Transitivität) (I4) $(x=y)\to(P_i(.....,x,.....)\to P_i(.....,y,.....))$ (I5) $(x=y)\to f_j(.....,x,.....)=f_j(.....,y,.....)$

Je ein Beispiel soll die ersten beiden quantorenlogischen Axiome illustrieren: Eine Anwendung von (Q1) ist etwa $\forall x(x^2\geq 0)\to(t^2\geq 0)$. Wenn ja für *alle* Individuen *x* die Ungleichung $x^2\geq 0$ gilt, so sicher auch für ein spezielles. Bei (Q2) ist es wichtig, dass *x* nicht frei in Φ vorkommt. Es darf entweder gar nicht oder nur gebunden erscheinen, da es sonst in der Konklusion plötzlich des Quantors entrissen ist. Die Formel $\forall y(\forall x(y>0\to x+y>x))\to\forall y(y>0\to\forall x(x+y>x))$ ist ein Beispiel einer Anwendung von (Q2).

All dies sind die logischen Axiome. Hat man irgendeine spezielle mathematische Theorie im Auge (Gruppentheorie, Arithmetik, Geometrie,...), die man mit Hilfe der Prädikatenlogik untersuchen will, so benötigt man natürlich weitere theoriespezifische Axiome und Sätze; die Menge dieser bezeichnen wir im Folgenden mit Σ.

Als Schlussregeln wollen wir hier wiederum die „Einsetzregel“ und den „modus ponens“ (wie schon in der Aussagenlogik) sowie die „Generalisierungsregel“ (GN) verwenden:

Einsetzregel	Φ $\Phi\to\Psi$ $-----(MP)$ Ψ	Φ $--(GN)$ $\forall x\Phi$
Schlussregeln der Prädikatenlogik		

Nun sind wir endlich in der Lage, ganz klar zu sagen, was ein Beweis ist:

Definition: Sei $\Psi\in FML(L)$. Ein *Beweis* von Ψ ist eine Folge $\Phi_0,\Phi_1,\Phi_2,...,\Phi_n,\Psi$ von Formeln, wobei jede Formel entweder ein logisches Axiom ist, aus Σ stammt oder aus einer bzw. zwei früheren Formeln durch Anwendung einer der Schlussregeln entstanden ist. Und wir schreiben: $\boxed{\Sigma\vdash\Psi}$.

Wenn beispielsweise $\Phi\wedge\Psi$ schon zu unseren gesicherten Erkenntnissen aus Σ gehört, dann ist diese Folge ein Beweis von Φ:

$$\Phi\wedge\Psi,\quad(\Phi\wedge\Psi)\to\Phi,\quad\Phi$$

Die erste Formel stammt ja aus Σ, die zweite ist eine Tautologie, und die dritte entsteht aus den beiden ersten durch MP. Wenn beispielsweise $\Phi\to\Psi$ und $\Psi\to\Xi$ schon zu unseren gesicherten Erkenntnissen aus Σ gehören, so ist diese Folge ein Beweis von $\Phi\to\Xi$:

$$\Phi \to \Psi, \quad (\Phi \to \Psi) \to ((\Psi \to \Xi) \to (\Phi \to \Xi)), \quad (\Psi \to \Xi) \to (\Phi \to \Xi), \quad \Psi \to \Xi, \quad \Phi \to \Xi$$

Die erste Formel entstammt Σ, die zweite ist eine Tautologie, die dritte entsteht durch MP, die vierte entstammt Σ, und die letzte entsteht wiederum durch MP.

Als eine weitere Illustration des formalen Beweisens betrachten wir noch den folgenden Satz:

Satz (Deduktionstheorem):

Sei $\Sigma \subset FML(L)$ und seien $\Phi, \Psi \in FML(L)$
Dann gilt:
$\Sigma \vdash (\Phi \to \Psi) \quad \Rightarrow \quad \Sigma \cup \{\Phi\} \vdash \Psi$
Die Umkehrung gilt auch, falls Φ eine Aussage ist.

Der Beweis von "$\Rightarrow$" ist elementar: Angenommen, wir verfügen schon über einen Beweise von $\Phi \to \Psi$ aus Σ. Wir haben also eine Formelfolge vor uns, deren letztes Element $\Phi \to \Psi$ ist. Wir verlängern diesen Beweis einfach um Φ, Ψ (wobei wir den MP einsetzen), und schon haben wir einen Beweis von Ψ aus $\Sigma \cup \{\Phi\}$. Der Beweis der Umkehrung ist sehr viel trickreicher und kann etwa mit vollständiger Induktion nach der Länge des Beweises von Ψ aus $\Sigma \cup \{\Phi\}$ bewiesen werden.

Beispiel eines streng formalen Beweises für den Satz $\forall x\left(0 \le x \cdot x\right)$

1	$\forall x, y\left(x \le y \ \vee \ y \le x\right)$	Axiom der Totalordung
2	$\forall y\left(x \le y \ \vee \ y \le x\right)$	Quantorenlogisches Axiom aus 1
3	$\left(x \le 0 \ \vee \ 0 \le x\right)$	Quantorenlogisches Axiom aus 2
4	$\forall x, y\left(0 \le x \wedge 0 \le y \to 0 \le x \cdot y\right)$	Axiom der Totalordnung
5	$\forall y\left(0 \le x \wedge 0 \le y \to 0 \le x \cdot y\right)$	Quantorenlogisches Axiom aus 4
6	$\left(0 \le x \wedge 0 \le x \to 0 \le x \cdot x\right)$	Quantorenlogisches Axiom aus 5
7	$0 \le x \to 0 \le x \wedge 0 \le x$	Tautologie
8	$0 \le x \to 0 \le x \cdot x$	Kettenschluss
9	$\forall x, y, z\left(x \le y \to x + z \le y + z\right)$	Axiom der Totalordnung
10	$\forall y, z\left(x \le y \to x + z \le y + z\right)$	Quantorenlogisches Axiom aus 9
11	$\forall z\left(x \le 0 \to x + z \le 0 + z\right)$	Quantorenlogisches Axiom aus 10
12	$\left(x \le 0 \to x + \left(-x\right) \le 0 + \left(-x\right)\right)$	Quantorenlogisches Axiom aus 11
13	$\forall x, y\left(x + \left(-x\right) = 0 \wedge 0 + y = y\right)$	Axiom der Totalordnung
14	$\forall y\left(x + \left(-x\right) = 0 \wedge 0 + y = y\right)$	Quantorenlogisches Axiom aus 13
15	$\left(x + \left(-x\right) = 0 \wedge 0 + \left(-x\right) = -x\right)$	Quantorenlogisches Axiom aus 14
16	$x + \left(-x\right) = 0$	Schlussregel $\dfrac{\varphi \wedge \psi}{\varphi}$
17	$x + \left(-x\right) \le 0 + \left(-x\right) \to 0 \le 0 + \left(-x\right)$	Schlussregel aus 16
18	$x \le 0 \to 0 \le 0 + \left(-x\right)$	Kettenschluss, Zeilen 12, 17
19	$0 + \left(-x\right) = -x$	Schlussregel $\dfrac{\varphi \wedge \psi}{\psi}$ aus 15
20	$0 \le 0 + \left(-x\right) \to 0 \le -x$	Schlussregel aus 19
21	$x \le 0 \to 0 \le -x$	Kettenschluss, Zeilen 18,20
22	$\forall x\left(0 \le x \to 0 \le x \cdot x\right)$	Generalisierungsregel aus 8
23	$0 \le -x \to 0 \le \left(-x\right) \cdot \left(-x\right)$	Quantorenlogisches Axiom aus 22
24	$\forall x\left(\left(-x\right) \cdot \left(-x\right) = x \cdot x\right)$	Axiom der Totalordnung
25	$\left(-x\right) \cdot \left(-x\right) = x \cdot x$	Quantorenlogisches Axiom aus 24
26	$0 \le \left(-x\right) \cdot \left(-x\right) \to 0 \le x \cdot x$	Schlussregel aus 25
27	$0 \le -x \to 0 \le x \cdot x$	Kettenschluss, Zeilen 23, 26
28	$x \le 0 \to 0 \le x \cdot x$	Kettenschluss, Zeilen 21, 27
29	$\left(x \le 0 \vee 0 \le x\right) \to 0 \le x \cdot x$	Schlussregel $\dfrac{\varphi \to \sigma \quad \psi \to \sigma}{\left(\varphi \vee \psi\right) \to \sigma}$, Zeilen 8, 28
30	$0 \le x \cdot x$	Modus Ponens, Zeilen 3, 29
31	$\forall x\left(0 \le x \cdot x\right)$	Generalisierungsregel