Proof theory and modal logic

Sonia Marin

supervised by: **Lutz Straßburger** and Dale Miller
Parsifal, INRIA

January 14, 2015

Inria-LIX PhD seminar

Proof theory

What is a mathematical proof?

What is proof theory about?

- build a deductive system for a logic and formalize the proofs of its theorems
- study the structure of the proofs, their computational behavior, ...
- construct the proofs in the most efficient way

A deductive system for classical logic

atomic propositions combined with connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$, ...

Axioms

ax.1 $A \rightarrow (B \rightarrow A)$

ax.2 $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

ax.3 $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

Rules

mp $\dfrac{A \quad A \rightarrow B}{B}$ modus ponens

A Hilbert-style proof of $p \to p$

1. ax.2: $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to (B \to C)) \to ((p \to B) \to (p \to C))$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to (B \to C)) \to ((p \to B) \to (p \to C))$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to C)) \to ((p \to (q \to p)) \to (p \to C))$

A Hilbert-style proof of $p \rightarrow p$

1. ax.2: $(p \rightarrow ((q \rightarrow p) \rightarrow C)) \rightarrow ((p \rightarrow (q \rightarrow p)) \rightarrow (p \rightarrow C))$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $A \to (B \to A)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to (B \to p)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to (B \to p)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to ((q \to p) \to p)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to ((q \to p) \to p)$
3. mp: $(p \to (q \to p)) \to (p \to p)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to ((q \to p) \to p)$
3. mp: $(p \to (q \to p)) \to (p \to p)$
4. ax.1: $p \to (q \to p)$

A Hilbert-style proof of $p \to p$

1. ax.2: $(p \to ((q \to p) \to p)) \to ((p \to (q \to p)) \to (p \to p))$
2. ax.1: $p \to ((q \to p) \to p)$
3. mp: $(p \to (q \to p)) \to (p \to p)$
4. ax.1: $p \to (q \to p)$
5. mp: $p \to p$

Sequent calculus

Sequents

$$A_1, \ldots, A_m \vdash B_1, \ldots, B_n$$

$$A_1 \wedge \ldots \wedge A_m \rightarrow B_1 \vee \ldots \vee B_n$$

Axioms

sequents of the form: $A \vdash A$

Rules

inference rules of the form: $\dfrac{S_1}{S}$ or $\dfrac{S_1 \quad S_2}{S}$

A sequent system for classical logic

LK

$$ax \; \frac{}{A \vdash A} \qquad cut \; \frac{\Gamma \vdash \Delta, A \quad A, \Gamma \vdash \Delta}{\Gamma \vdash \Delta}$$

$$\neg_l \; \frac{\Gamma \vdash A, \Delta}{\Gamma, \neg A \vdash \Delta} \qquad \neg_r \; \frac{\Gamma, A \vdash \Delta}{\Gamma \vdash \Delta, \neg A} \qquad \to_l \; \frac{\Gamma \vdash \Delta, A \quad \Gamma, B \vdash \Delta}{\Gamma, A \to B \vdash \Delta} \qquad \to_r \; \frac{\Gamma, A \vdash \Delta, B}{\Gamma \vdash \Delta A \to B}$$

$$\wedge_l \; \frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_1 \wedge A_2 \vdash \Delta} \qquad \wedge_r \; \frac{\Gamma, \vdash \Delta, A \quad \Gamma \vdash \Delta, B}{\Gamma \vdash \Delta, A \wedge B} \qquad \vee_l \; \frac{\Gamma, A \vdash \Delta \quad \Gamma, B \vdash \Delta}{\Gamma, A \vee B} \qquad \vee_r \; \frac{\Gamma, A_i \vdash \Delta}{\Gamma, A_1 \vee A_2 \vdash \Delta}$$

$$w_l \; \frac{\Gamma \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad w_r \; \frac{\Gamma \vdash \Delta}{\Gamma \vdash \Delta, A} \qquad c_l \; \frac{\Gamma, A, A \vdash \Delta}{\Gamma, A \vdash \Delta} \qquad c_r \; \frac{\Gamma \vdash \Delta, A, A}{\Gamma \vdash \Delta, A}$$

A sequent proof of $(p \to q) \to p \vdash p$

$$\to_l \frac{\Gamma \vdash A, \Delta \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta}$$

$$\frac{\vdash p \to q, p \quad p \vdash p}{(p \to q) \to p \vdash p}$$

Proof tree

Sequent rules used

A sequent proof of $(p \to q) \to p \vdash p$

$$\dfrac{\dfrac{p \vdash q, p}{\vdash p \to q, p} \quad p \vdash p}{(p \to q) \to p \vdash p}$$

Proof tree

$$\to_l \ \dfrac{\Gamma \vdash A, \Delta \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta}$$

$$\to_r \ \dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}$$

Sequent rules used

A sequent proof of $(p \to q) \to p \vdash p$

$$
\dfrac{\dfrac{\dfrac{p \vdash p}{p \vdash q, p}}{\vdash p \to q, p} \quad p \vdash p}{(p \to q) \to p \vdash p}
$$

Proof tree

$$
\to_l \dfrac{\Gamma \vdash A, \Delta \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta}
$$

$$
\to_r \dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}
$$

$$
\mathsf{w}_r \dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}
$$

Sequent rules used

A sequent proof of $(p \to q) \to p \vdash p$

$$\dfrac{\dfrac{\dfrac{\color{red}{p \vdash p}}{p \vdash q, p}}{\vdash p \to q, p} \quad \color{red}{p \vdash p}}{(p \to q) \to p \vdash p}$$

Proof tree

$$\to_l \; \dfrac{\Gamma \vdash A, \Delta \quad B, \Gamma \vdash \Delta}{\Gamma, A \to B \vdash \Delta}$$

$$\to_r \; \dfrac{\Gamma, A \vdash B, \Delta}{\Gamma \vdash A \to B, \Delta}$$

$$\mathsf{w}_r \; \dfrac{\Gamma \vdash \Delta}{\Gamma \vdash A, \Delta}$$

Sequent rules used

Modal logic

or modal logics . . .

Epistemic logics, deontic logics, temporal logics, provability logics

Modal logic

or modal logics ...

Epistemic logics, deontic logics, temporal logics, provability logics

atomic propositions combined with connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\Box$, $\Diamond$

Modal logic

or modal logics . . .

Epistemic logics, deontic logics, temporal logics, provability logics

atomic propositions combined with connectives: $\neg$, $\wedge$, $\vee$, $\rightarrow$, $\Box$, $\Diamond$

Axioms

ax.1 $A \rightarrow (B \rightarrow A)$

ax.2 $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

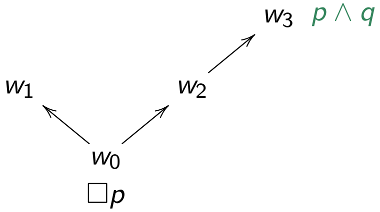
ax.3 $(\neg A \rightarrow \neg B) \rightarrow (B \rightarrow A)$

k $\Box(A \rightarrow B) \rightarrow (\Box A \rightarrow \Box B)$

Kripke semantics

$w \Vdash A \wedge B$ iff $w \Vdash A$ and $w \Vdash B$

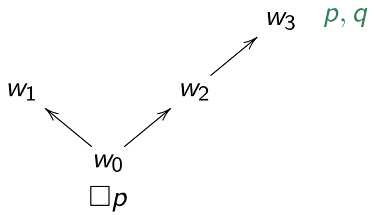
$w \Vdash \Box A$ iff for all $v \in W$ such that $wRv : v \Vdash A$



Kripke semantics

$w \Vdash A \wedge B$ iff $w \Vdash A$ and $w \Vdash B$

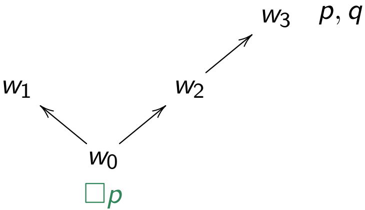
$w \Vdash \Box A$ iff for all $v \in W$ such that $wRv : v \Vdash A$



Kripke semantics

$$w \Vdash A \wedge B \text{ iff } w \Vdash A \text{ and } w \Vdash B$$

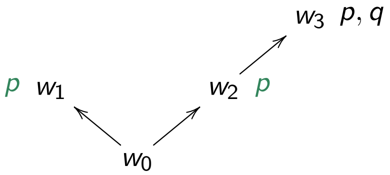
$$w \Vdash \Box A \text{ iff for all } v \in W \text{ such that } wRv : v \Vdash A$$



Kripke semantics

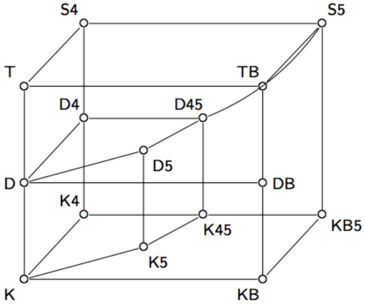
$w \Vdash A \wedge B$ iff $w \Vdash A$ and $w \Vdash B$

$w \Vdash \Box A$ iff for all $v \in W$ such that $wRv : v \Vdash A$



And more axioms . . .

- d: $\Box A \to \Diamond A$
- t: $A \to \Diamond A$
- b: $A \to \Box\Diamond A$
- 4: $\Diamond\Diamond A \to \Diamond A$
- 5: $\Diamond A \to \Box\Diamond A$



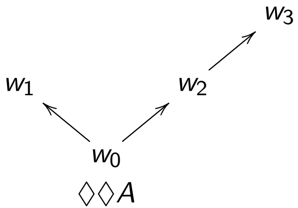
And even more axioms . . .

Name	Axiom	Frame condition
K	$\Box(A \to B) \to (\Box A \to \Box B)$	N/A
T	$\Box A \to A$	reflexive: $w\,R\,w$
4	$\Box A \to \Box\Box A$	transitive: $w\,R\,v \wedge v\,R\,u \Rightarrow w\,R\,u$
	$\Box\Box A \to \Box A$	dense: $w\,R\,u \Rightarrow \exists v\,(w\,R\,v \wedge v\,R\,u)$
D	$\Box A \to \Diamond A$ or $\Diamond\top$	serial: $\forall w\,\exists v\,(w\,R\,v)$
B	$A \to \Box\Diamond A$	symmetric : $w\,R\,v \Rightarrow v\,R\,w$
5	$\Diamond A \to \Box\Diamond A$	Euclidean: $w\,R\,u \wedge w\,R\,v \Rightarrow u\,R\,v$
GL	$\Box(\Box A \to A) \to \Box A$	R transitive, R^{-1} well-founded
Grz	$\Box(\Box(A \to \Box A) \to A) \to A$	R reflexive and transitive, R^{-1}–Id well-founded
H	$\Box(\Box A \to B) \vee \Box(\Box B \to A)$	$w\,R\,u \wedge w\,R\,v \Rightarrow u\,R\,v \vee v\,R\,u$
M	$\Box\Diamond A \to \Diamond\Box A$	(a complicated second-order property)
G	$\Diamond\Box A \to \Box\Diamond A$	convergent: $w\,R\,u \wedge w\,R\,v \Rightarrow \exists x\,(u\,R\,x \wedge v\,R\,x)$
	$A \to \Box A$	$w\,R\,v \Rightarrow w = v$
	$\Diamond A \to \Box A$	partial function: $w\,R\,u \wedge w\,R\,v \Rightarrow u = v$
	$\Diamond A \leftrightarrow \Box A$	function: $\forall w\,\exists! u\,w\,R\,u$
	$\Box A$ or $\Box\bot$	empty: $\forall w\,\forall u\,\neg(w\,R\,u)$

Modal axioms/Frame conditions

$$4\colon \Diamond\Diamond A \to \Diamond A$$

$$\text{transitivity: } \forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \to wRu$$

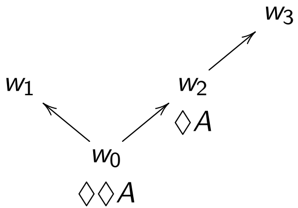


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

$$4\colon \Diamond\Diamond A \to \Diamond A$$

transitivity: $\forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \to wRu$

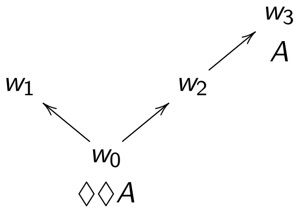


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

$$4 \colon \Diamond\Diamond A \to \Diamond A$$

$$\text{transitivity: } \forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \to wRu$$

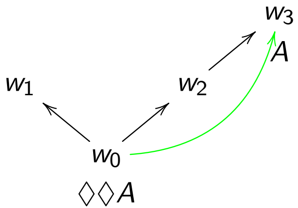


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

$$4\colon \Diamond\Diamond A \to \Diamond A$$

transitivity: $\forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \to wRu$

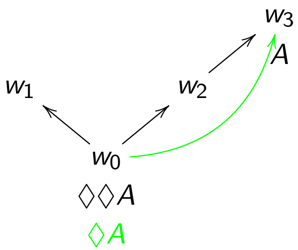


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

$$4\colon \Diamond\Diamond A \rightarrow \Diamond A$$

transitivity: $\forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \rightarrow wRu$

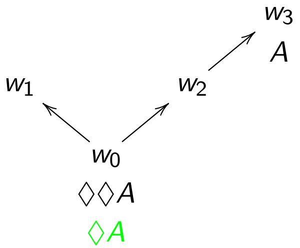


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

$$4\colon \Diamond\Diamond A \to \Diamond A$$

transitivity: $\forall w.\, \forall v.\, \forall u.\; wRv \wedge vRu \to wRu$

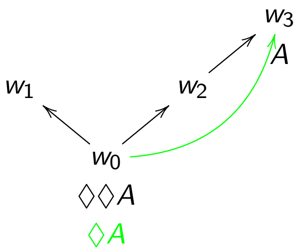


$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

Modal axioms/Frame conditions

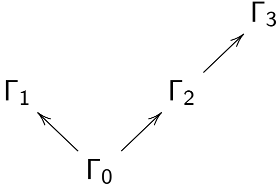
$$4\colon \Diamond\Diamond A \to \Diamond A$$

transitivity: $\forall w.\ \forall v.\ \forall u.\ wRv \wedge vRu \to wRu$



$w \Vdash \Diamond A$ iff there exists $v \in W$ such that wRv and $v \Vdash A$

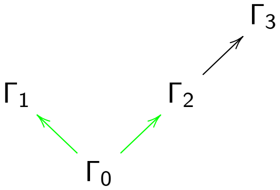
Nested sequents



root

Γ_0

Nested sequents

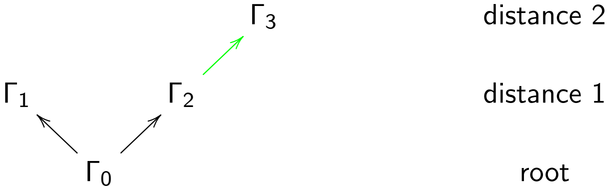


distance 1

root

$$\Gamma_0, [\Gamma_1], [\Gamma_2 \quad]$$

Nested sequents



$$\Gamma_0, [\Gamma_1], [\Gamma_2, [\Gamma_3]]$$

Nested sequent system for modal logic

NK+. . .

$$\mathsf{id}\ \frac{}{\Gamma\{a, \bar{a}\}} \qquad \vee\ \frac{\Gamma\{A, B\}}{\Gamma\{A \vee B\}} \qquad \wedge\ \frac{\Gamma\{A\} \quad \Gamma\{B\}}{\Gamma\{A \wedge B\}} \qquad \Box\ \frac{\Gamma\{[A]\}}{\Gamma\{\Box A\}} \qquad \Diamond\ \frac{\Gamma\{\Diamond A, [A, \Delta]\}}{\Gamma\{\Diamond A, [\Delta]\}}$$

$$\mathsf{d}^{\Diamond}\ \frac{\Gamma\{\Diamond A, [A]\}}{\Gamma\{\Diamond A\}} \qquad \mathsf{t}^{\Diamond}\ \frac{\Gamma\{\Diamond A, A\}}{\Gamma\{\Diamond A\}} \qquad \mathsf{b}^{\Diamond}\ \frac{\Gamma\{[\Delta, \Diamond A], A\}}{\Gamma\{[\Delta, \Diamond A]\}} \qquad 4^{\Diamond}\ \frac{\Gamma\{\Diamond A, [\Diamond A, \Delta]\}}{\Gamma\{\Diamond A, [\Delta]\}} \qquad 5^{\Diamond}\ \frac{\Gamma\{\Diamond A\}\{\Diamond A\}}{\Gamma\{\Diamond A\}\{\emptyset\}}$$

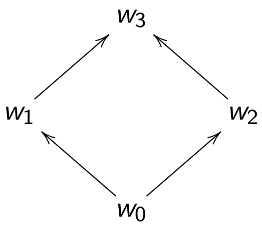
$$\mathsf{d}^{[]}\ \frac{\Gamma\{[\emptyset]\}}{\Gamma\{\emptyset\}} \qquad \mathsf{t}^{[]}\ \frac{\Gamma\{[\Delta]\}}{\Gamma\{\Delta\}} \qquad \mathsf{b}^{[]}\ \frac{\Gamma\{[\Sigma, [\Delta]]\}}{\Gamma\{[\Sigma], \Delta\}} \qquad 4^{[]}\ \frac{\Gamma\{[\Delta], [\Sigma]\}}{\Gamma\{[[\Delta], \Sigma]\}} \qquad 5^{[]}\ \frac{\Gamma\{[\Delta]\}\{\emptyset\}}{\Gamma\{\emptyset\}\{[\Delta]\}}$$

Future work

Scott-Lemmon axioms: (M.Fitting)

$$\Diamond^h \Box^i A \rightarrow \Box^j \Diamond^k A \text{ for } h, i, j, k \geq 0$$

ex: $\Diamond \Box A \rightarrow \Box \Diamond A$



Future work

Scott-Lemmon axioms: (M.Fitting)

$$\Diamond^h \Box^i A \to \Box^j \Diamond^k A \text{ for } h, i, j, k \geq 0$$

Frame properties: (O.Lahav)

$$\forall w_1 \ldots w_n \exists u \bigvee_{<S_R, S_=>} \left(\bigwedge_{i \in S_R} w_i R u \wedge \bigwedge_{i \in S_=} w_i = u \right)$$

$$\text{ex: } \forall w_1 . \forall w_2 . (w_1 R w_2 \vee w_2 R w_1)$$

$$w_1 \longrightarrow w_2 \quad \text{or} \quad w_1 \longleftarrow w_2$$