Logik und theoretische Informatik an der Universität Bern

Thomas Studer

Übersicht

- Über mich
- Institut für Informatik
- Informatik Olympiade
- Logik und theoretische Informatik

Thomas Studer

1992 – 2001
Studium der Informatik, Mathematik und Philosophie an der Uni Bern
Doktorat in Informatik

2001 – 2003
Software Engineer bei Crosspoint Informatik und Postfinance

seit 2003
Dozent für Informatik
Leiter der Forschungsgruppe für Logik und Theorie

seit 2019
Mitglied der kant. Maturitätskommission, Hauptexperte Informatik

Institut für Informatik

- 9 Forschungsgruppen
- ca. 70 wissenschaftliche Mitarbeiter/innen
- ca. 450 Studierende (Haupt- und Nebenfach Informatik)

Forschungsgruppen

David Bommes
Computer Graphics

Torsten Braun
Communication &
Distributed Systems

Christian Cachin
Cryptology &
Data Security

Paolo Favaro
Computer
Vision

Timo Kehrer
Software
Engineering

Thomas Studer
Logic & Theory

Matthias Stürmer
Digital Sustainability

Athina Tzovara
Computational Cognitive
Neurosscience

Kaspar Riesen
Pattern Recognition

Angebote

Bachelor Infotage

MINT Tag

Schülerstudierende

Informatik Olympiade
- Workshops
- Selektionsrunde

Informatik Olympiade

Gold für Bern

André
Burgdorf

Jasmin
Lerbermatt

Ema
Kirchenfeld

Pascal
Hofwil

Fabian
Neufeld

Informatik Olympiade: Ablauf

Erste Runde: September

Zweite Runde: 1. Oktober – 30. November

Workshops (Okt. – Nov.)

Trainingslager (Februar)

Finalrunde (März)

Team Selektion (Mai)

Internationale Wettbewerbe (Sommer)

Erste Runde

40-minütiges Online-Quiz mit Multiple-Choice-Fragen

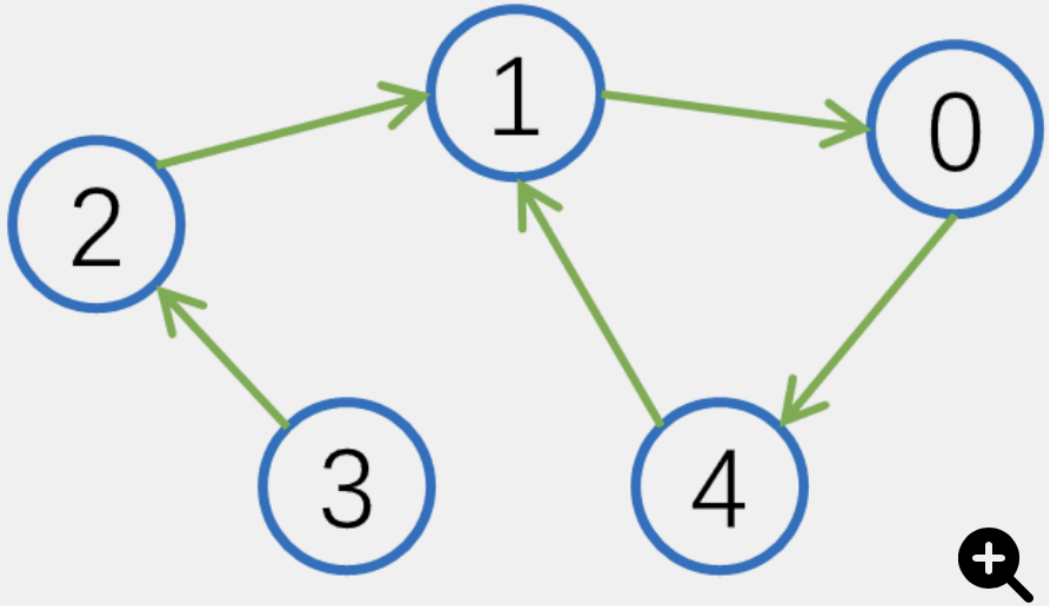
Keine Vorkenntnisse nötig

Eignet sich gut zum Lösen im Unterricht mit einer ganzen Klasse

Erste Runde: Beispiele

Frage 6

Gegeben seien 5 Städte (nummeriert $0, 1, 2, 3, 4$), die durch Einbahnstrassen verbunden sind. Du darfst genau eine neue Einbahnstrasse zwischen zwei Städten hinzufügen, zwischen denen bisher noch keine Strasse existiert (insbesondere darf keine Strasse hinzugefügt werden, wenn bereits eine Strasse in die entgegengesetzte Richtung existiert). Auf wie viele verschiedene Arten kannst du eine solche Strasse hinzufügen, sodass anschliessend jede Stadt von jeder anderen Stadt aus erreichbar ist, wenn man den Richtungen der Einbahnstrassen folgt?



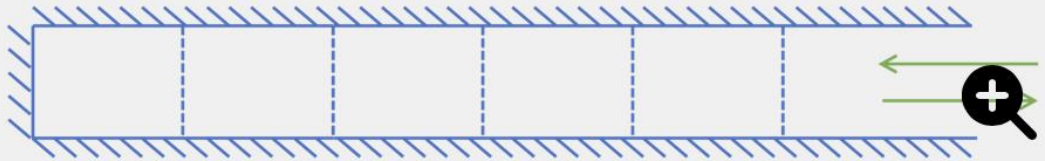
0 | 1 | 2 | 3

4

Erste Runde: Beispiele

Frage 7

Es gibt einen schmalen Parkplatz mit 5 nebeneinanderliegenden Stellplätzen in einer Reihe. Insbesondere kann ein Auto nur ausparken, wenn zwischen ihm und der Ausfahrt kein anderes Auto steht. Die fünf Autos A, B, C, D und E fahren nacheinander auf den Parkplatz (A zuerst, dann B, dann C, dann D, dann E).
Hinweis: Autos dürfen den Parkplatz verlassen, bevor alle fünf eingetroffen sind.
Welche der folgenden Ausparkreihenfolgen ist nicht möglich?

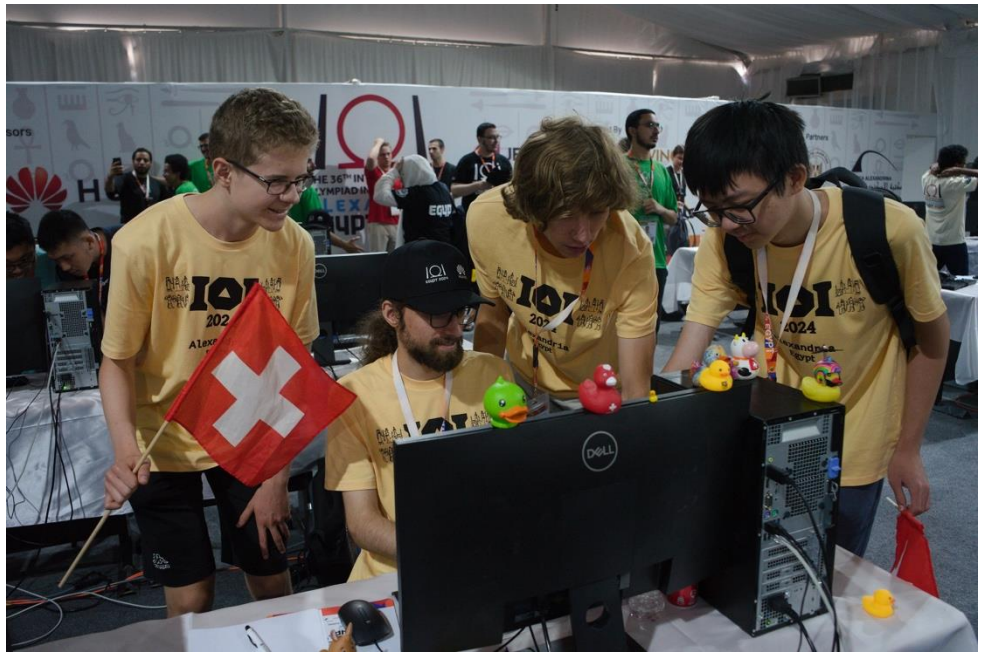


- A, B, C, D, E
- B, A, D, C, E
- C, B, E, D, A
- E, D, C, B, A
- B, C, E, A, D

Internationale Wettbewerbe

EGOI 2026
Cesenatico, Italy

European Girls' Olympiad in Informatics



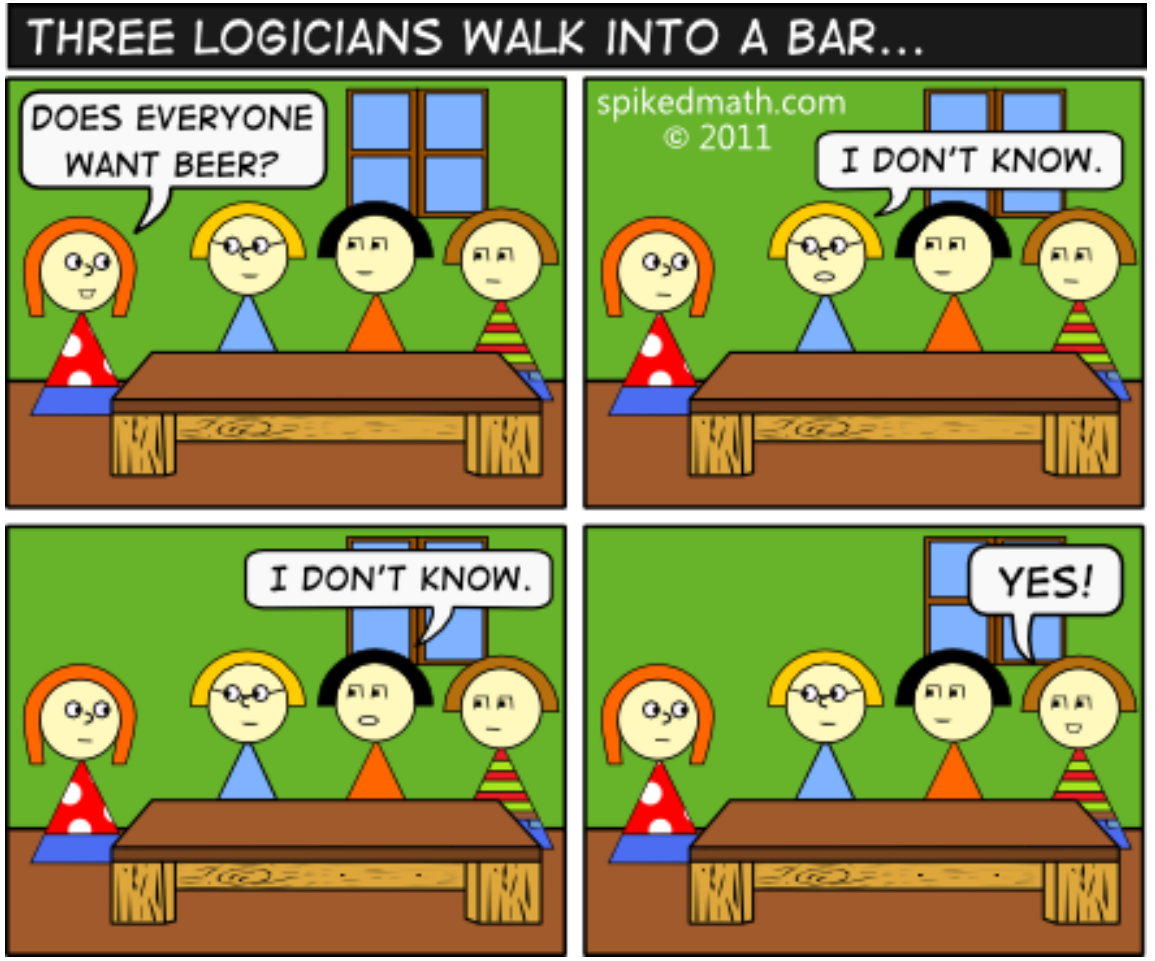
International Olympiad in Informatics

UZBEKISTAN
IOI 2026 TASHKENT

Forschung

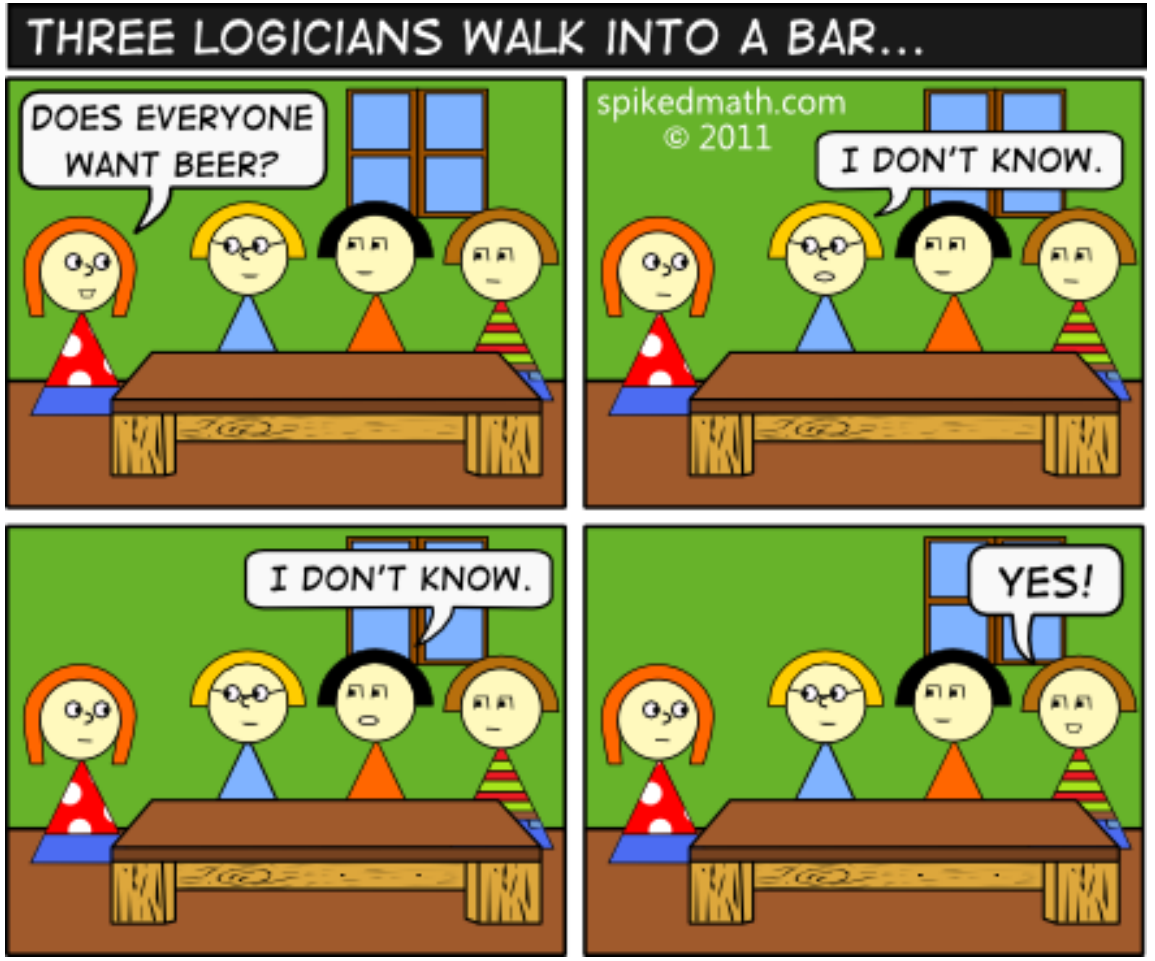
- Wissenslogik
- Beweistheorie

u^b Wissenslogik



beer	alle wollen Bier
K_C beer	C weiss, dass alle Bier wollen
$\neg K_C$ beer	C weiss nicht, dass alle Bier wollen
$K_C K_B$ beer	C weiss, dass B weiss, dass alle Bier wollen

Wissenslogik



K_A beer und K_B beer und K_C beer

Alle wissen, dass alle Bier wollen E beer

Wissenslogik

Alle wissen, dass alle Bier wollen — E beer

Alle wissen,
dass alle wissen, dass alle Bier wollen — E E beer

Alle wissen,
dass alle wissen,
dass alle wissen, dass alle Bier wollen — E E E beer

Wir haben:
E beer und EE beer und EEE beer und …

Es ist **Allgemeinwissen**, dass alle Bier wollen.

Formal: C beer

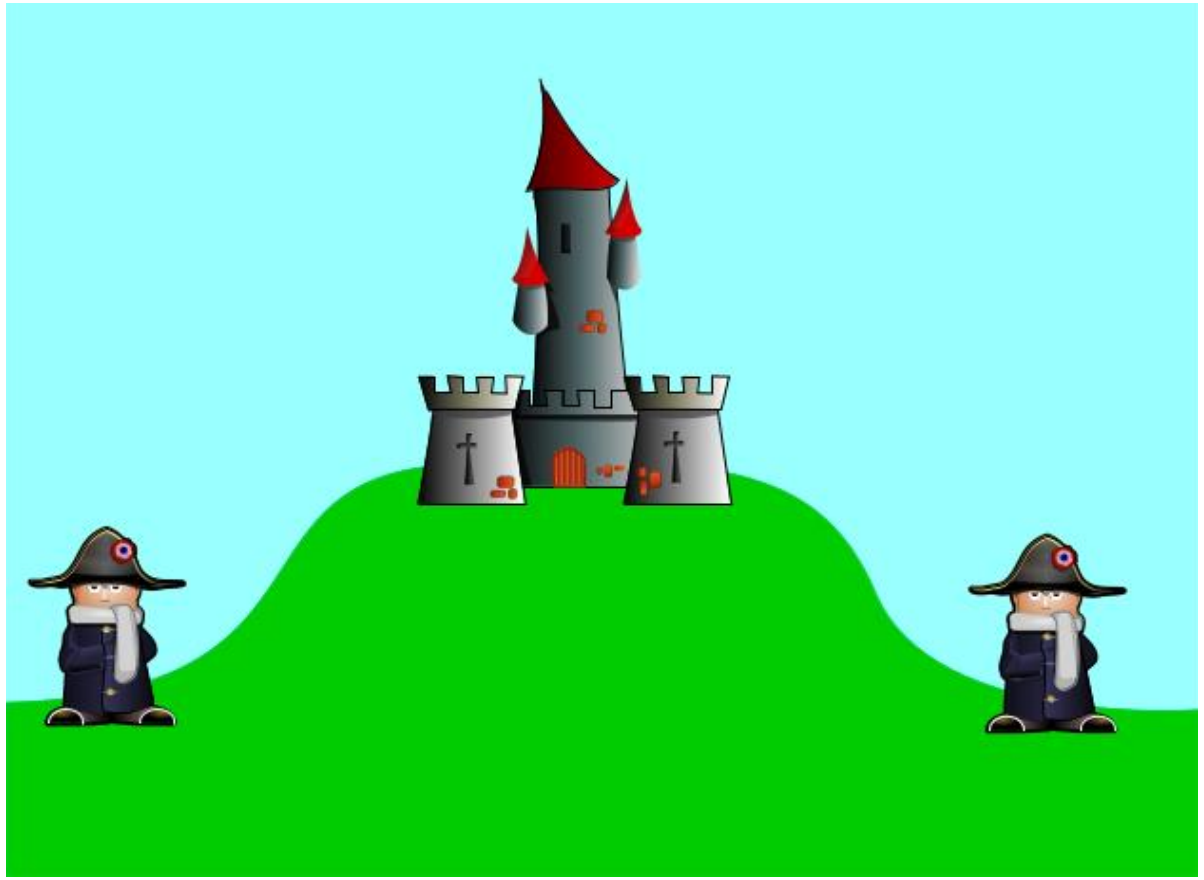
Coordinated Attack

Zwei Divisionen einer Armee, die sich an verschiedenen Orten befinden, stehen kurz davor, ihren Feind anzugreifen.

Um die Schlacht zu gewinnen, müssen beide Divisionen gleichzeitig angreifen.

Die beiden Generäle haben sich zwar darauf geeinigt, dass sie angreifen werden, aber sie haben sich noch nicht auf einen Zeitpunkt für den Angriff geeinigt.

Sie verfügen über Kommunikationsmittel, die jedoch unzuverlässig sein können, d.h. Nachrichten können verloren gehen.



u^b Coordinated Attack

General A

General B

$\neg K_B \text{time}$

u^b Coordinated Attack

General A

General B

$\neg \mathsf{K}_B \mathsf{time}$

$\xrightarrow{\mathsf{time}}$

$\mathsf{K}_B \mathsf{time}$

u^b Coordinated Attack

General A | General B

$\neg K_B time$

$\xrightarrow{time}$

$K_B time$

$\neg K_A K_B time$

A weiss nicht, dass B die Zeit kennt.

A hält es für möglich, dass B die Zeit nicht kennt.

A hält es für möglich, dass B nicht angreift.

A greift nicht an.

u^b Coordinated Attack

General A

General B

$\neg \mathsf{K}_B \mathsf{time}$

time $\longrightarrow$

$\mathsf{K}_B \mathsf{time}$

$\neg \mathsf{K}_A \mathsf{K}_B \mathsf{time}$

ack $\longleftarrow$

$\mathsf{K}_A \mathsf{K}_B \mathsf{time}$

u^b Coordinated Attack

General A		General B
		$\neg \mathsf{K}_B \mathsf{time}$
	$\xrightarrow{\text{time}}$	
		$\mathsf{K}_B \mathsf{time}$
$\neg \mathsf{K}_A \mathsf{K}_B \mathsf{time}$		
	$\xleftarrow{\text{ack}}$	
$\mathsf{K}_A \mathsf{K}_B \mathsf{time}$		
		$\neg \mathsf{K}_B \mathsf{K}_A \mathsf{K}_B \mathsf{time}$

B weiss nicht, dass A weiss, dass B die Zeit kennt.

B hält es für möglich, dass A nicht weiss, dass B die Zeit kennt.

B hält es für möglich, dass A nicht angreift.

B greift nicht an.

u^b Coordinated Attack

General A		General B
		$\neg \mathsf{K}_B \mathsf{time}$
	$\xrightarrow{\text{time}}$	
		$\mathsf{K}_B \mathsf{time}$
$\neg \mathsf{K}_A \mathsf{K}_B \mathsf{time}$		
	$\xleftarrow{\text{ack}}$	
$\mathsf{K}_A \mathsf{K}_B \mathsf{time}$		
		$\neg \mathsf{K}_B \mathsf{K}_A \mathsf{K}_B \mathsf{time}$
	⋮	

Alle wissen, dass…

Nach der 1. Runde alle wissen die Zeit

Alle wissen, dass…

Nach der 1. Runde alle wissen die Zeit

Aber A weiss nicht, dass dies der Fall ist, weil A das Acknowledgment von B noch nicht erhalten hat.

Alle wissen, dass…

Nach der 1. Runde	alle wissen die Zeit
Nach der 2. Runde	alle wissen, dass alle die Zeit wissen

Alle wissen, dass…

Nach der 1. Runde alle wissen die Zeit

Nach der 2. Runde alle wissen, dass alle die Zeit wissen

Aber B weiss nicht, dass dies der Fall ist, weil B das Acknowledgment von A noch nicht erhalten hat.

Alle wissen, dass…

Nach der 1. Runde alle wissen die Zeit

Nach der 2. Runde alle wissen, dass alle die Zeit wissen

Aber B weiss nicht, dass dies der Fall ist, weil B das Acknowledgment von A noch nicht erhalten hat.

.

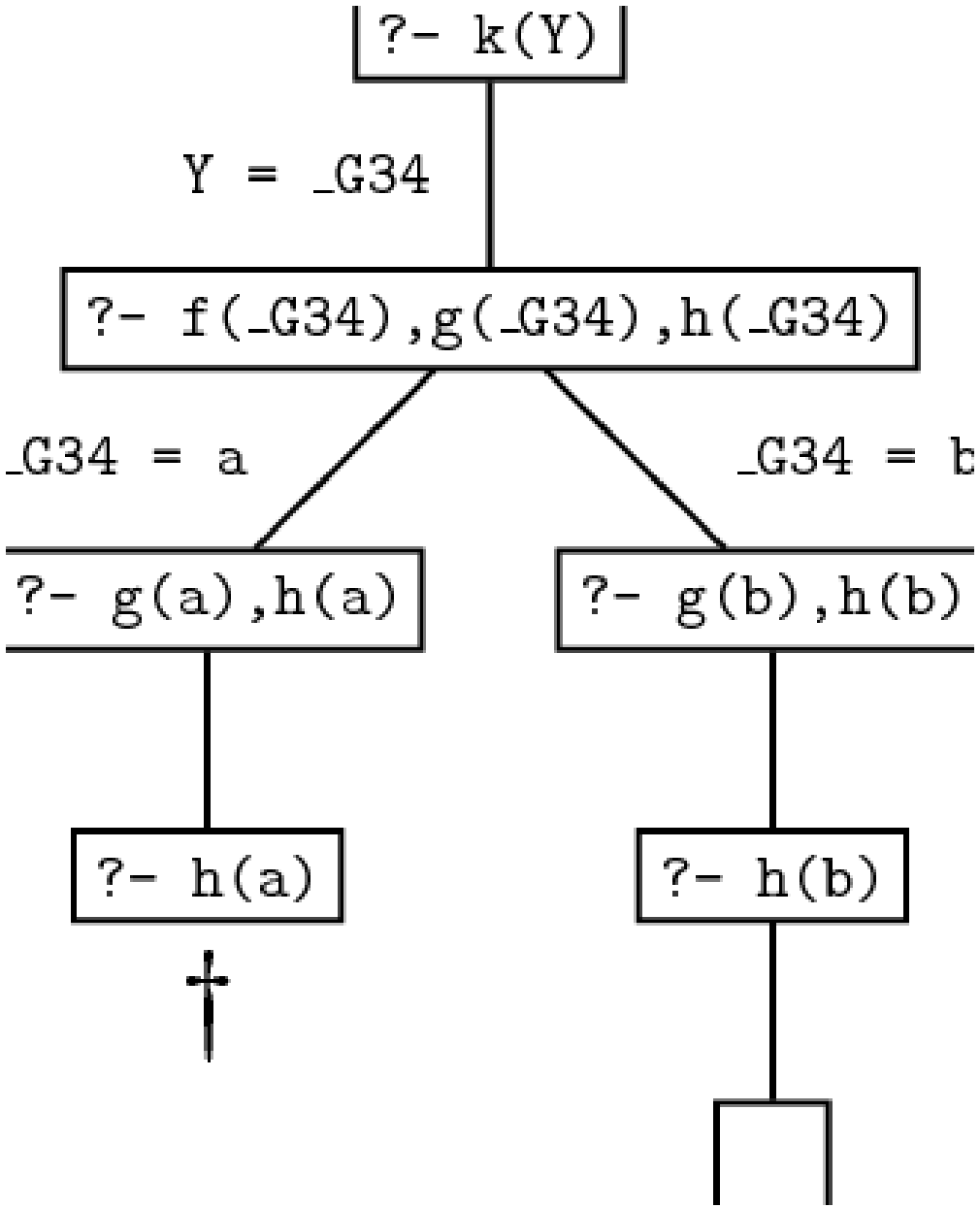
.

.

Es wird nie der Fall sein, dass die Zeit Allgemeinwissen ist.

Die Generäle werden nie angreifen.

Beweistheorie



Beweissuche und automatische Verifikation

Logische Formeln können Eigenschaften von Software / Hardware / Protokollen ausdrücken.

Eigenschaften zu verifizieren bedeutet, logische Formeln zu beweisen.

Für die automatisierte Verifizierung benötigen wir Algorithmen zur Beweissuche.

Ein Beweissystem

Axiome:

$$P \to (Q \to P)$$

$$\big(P \to (Q_1 \to Q_2)\big) \to \big((P \to Q_1) \to (P \to Q_2)\big)$$

$$\big((P \to \bot) \to \bot\big) \to P$$

Modus Ponens:

$$\frac{A \quad A \to B}{B}$$

Ein Beweissystem

Axiome:

$$P \to (Q \to P)$$

$$\big(P \to (Q_1 \to Q_2)\big) \to \big((P \to Q_1) \to (P \to Q_2)\big)$$

$$\big((P \to \bot) \to \bot\big) \to P$$

Modus Ponens:

$$\frac{A \quad A \to B}{B}$$

Beweissuche ist schwierig

Um eine Formel B zu beweisen, benötigt man eine andere Formel A, die nicht aus B bestimmt werden kann.

Beispiel

Axiome: $P \to (Q \to P)$

$\big(P \to (Q_1 \to Q_2)\big) \to \big((P \to Q_1) \to (P \to Q_2)\big)$

$\big((P \to \bot) \to \bot\big) \to P$

Modus Ponens: $\dfrac{A \quad A \to B}{B}$

A $\to$ A

Beispiel

Axiome:

$$P \to (Q \to P)$$

$$\big(P \to (Q_1 \to Q_2)\big) \to \big((P \to Q_1) \to (P \to Q_2)\big)$$

$$\big((P \to \bot) \to \bot\big) \to P$$

Modus Ponens:

$$\frac{A \quad A \to B}{B}$$

$$\frac{A \to (B \to A) \qquad (A \to (B \to A)) \to (A \to A)}{A \to A}$$

Beispiel

Axiome:

$$P \to (Q \to P)$$

$$\big(P \to (Q_1 \to Q_2)\big) \to \big((P \to Q_1) \to (P \to Q_2)\big)$$

$$\big((P \to \bot) \to \bot\big) \to P$$

Modus Ponens:

$$\frac{A \quad A \to B}{B}$$

$$\frac{\dfrac{A \to ((B \to A) \to A) \qquad (A \to ((B \to A) \to A)) \to ((A \to (B \to A)) \to (A \to A))}{(A \to (B \to A)) \to (A \to A)} \qquad A \to (B \to A)}{A \to A}$$

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

Bezeichnet eine Menge von Formeln: $\Gamma \cup \{ p, \neg p \}$

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

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

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

$$\frac{p \wedge q,\ \neg p \vee \neg q}{(p \wedge q) \vee (\neg p \vee \neg q)}$$

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

$$\frac{\dfrac{p,\ \neg p \vee \neg q \qquad q,\ \neg p \vee \neg q}{p \wedge q,\ \neg p \vee \neg q}}{(p \wedge q) \vee (\neg p \vee \neg q)}$$

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

$$\dfrac{\dfrac{\dfrac{p,\ \neg p,\ \neg q}{p,\ \neg p \vee \neg q} \qquad q,\ \neg p \vee \neg q}{p \wedge q,\ \neg p \vee \neg q}}{(p \wedge q) \vee (\neg p \vee \neg q)}$$

Beweissuche

$$\Gamma,\ p,\ \neg p$$

$$\frac{\Gamma,\ A \qquad \Gamma,\ B}{\Gamma,\ A \wedge B}$$

$$\frac{\Gamma,\ A,\ B}{\Gamma,\ A \vee B}$$

$$\dfrac{\dfrac{\dfrac{p,\ \neg p,\ \neg q}{p,\ \neg p \vee \neg q} \qquad \dfrac{q,\ \neg p,\ \neg q}{q,\ \neg p \vee \neg q}}{p \wedge q,\ \neg p \vee \neg q}}{(p \wedge q) \vee (\neg p \vee \neg q)}$$

Beweissuche mit Allgemeinwissen

$$
\dfrac{
\dfrac{\text{(ax')}}{\neg A,\ \tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \mathsf{E}A}\ (\mathsf{E})
\qquad
\dfrac{
\dfrac{
\dfrac{
\dfrac{
\dfrac{\text{(ax')}}{\neg A,\ A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \mathsf{C}A}
\quad
\dfrac{\vdots}{\neg A,\ \tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{C}A}}\ (\mathsf{C})
}{\neg A,\ A \wedge \tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{C}A}}\ (\wedge)
}{\tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{EC}A}}\ (\mathsf{E})
}{\tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A) \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{EC}A}}\ (\vee)
}{\tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{EC}A}}\ (\tilde{\mathsf{C}})
}{
\dfrac{\tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{E}A \wedge \mathsf{EC}A}}{\tilde{\mathsf{E}}\neg A,\ \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A),\ \underline{\mathsf{C}A}}\ (\mathsf{C})
}\ (\wedge)
$$

Beweissuche mit Allgemeinwisse

Beweis hat die Struktur eines unendlichen Baums

$$\frac{\vdots}{\neg A, \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A}\ (\mathsf{C})$$

$$\frac{\overset{(\text{ax'})}{\neg A, A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A} \qquad \neg A, \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A}{\neg A, A \wedge \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A}\ (\wedge)$$

$$\frac{\neg A, A \wedge \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A), \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}\ (\mathsf{E})$$

$$\frac{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A), \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A) \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}\ (\vee)$$

$$\frac{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{E}}(A \wedge \tilde{\mathsf{E}}\neg A) \vee \tilde{\mathsf{E}}\tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}\ (\tilde{\mathsf{C}})$$

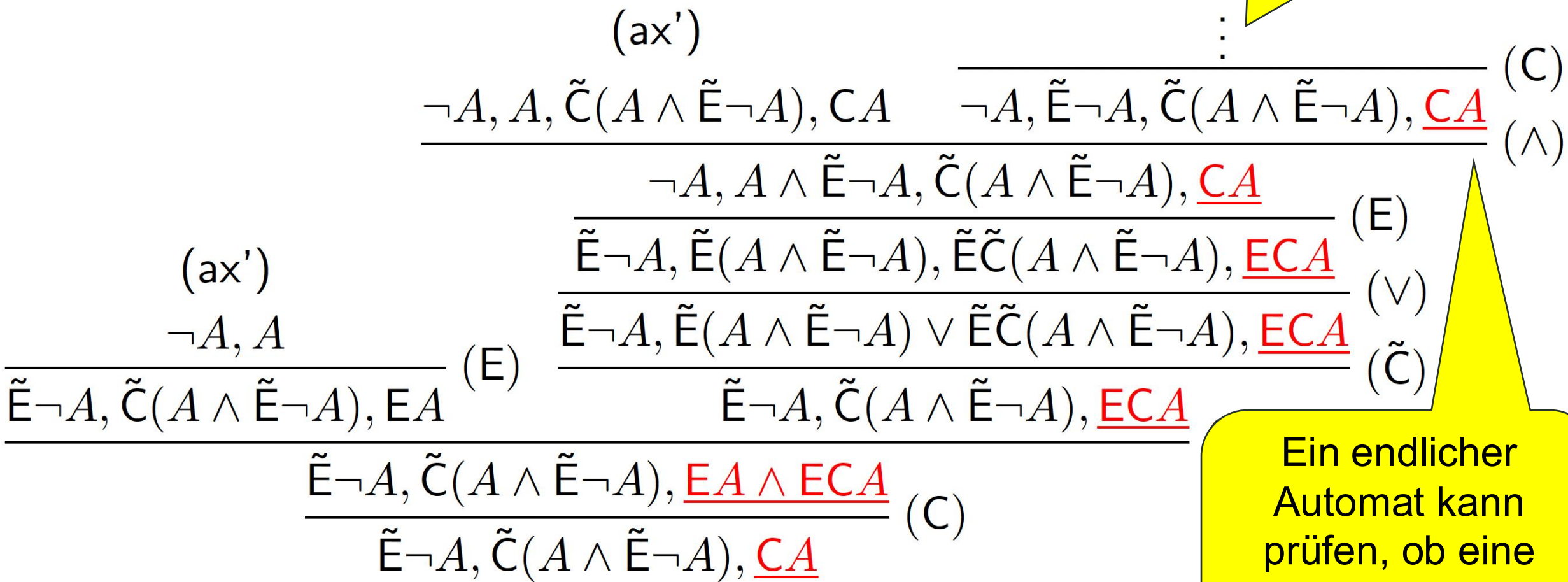
$$\frac{\overset{(\text{ax'})}{\neg A, A}}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{E}A}\ (\mathsf{E})$$

$$\frac{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{E}A \qquad \tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{EC}A}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{E}A \wedge \mathsf{EC}A}\ (\wedge)$$

$$\frac{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{E}A \wedge \mathsf{EC}A}{\tilde{\mathsf{E}}\neg A, \tilde{\mathsf{C}}(A \wedge \tilde{\mathsf{E}}\neg A), \mathsf{C}A}\ (\mathsf{C})$$

u^b Beweissuche mit Allgemeinwisse

Beweis hat die Struktur eines unendlichen Baums



Ein endlicher Automat kann prüfen, ob eine Wiederholung vorkommt

Vielen Dank für die Aufmerksamkeit