

# Deductive Systems for Common Knowledge

Thomas Studer

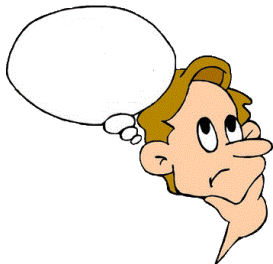
Institute of Computer Science and Applied Mathematics  
University of Bern  
Switzerland

April 2011

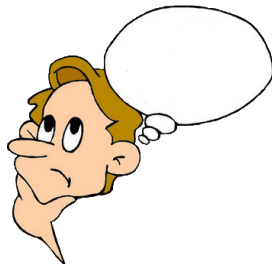
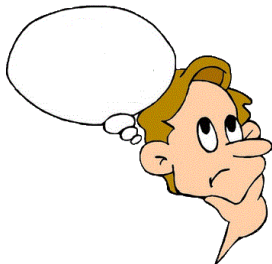
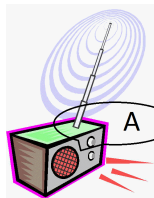
- Hilbert system for common knowledge
- Infinitary system based on an  $\omega$ -rule
- Syntactic cut-elimination
- Infinite branches
- The situation for the  $\mu$ -calculus
- Justification logic and common knowledge



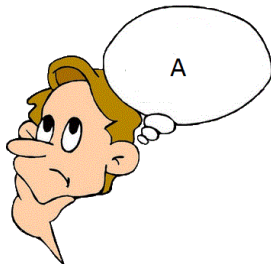
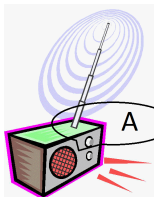
# Common knowledge



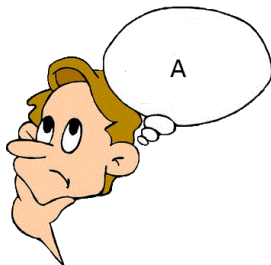
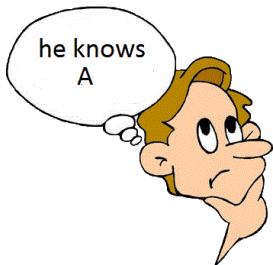
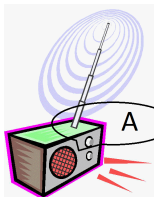
# Common knowledge



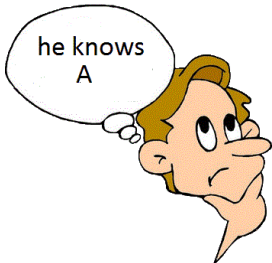
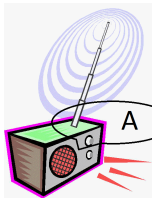
# Common knowledge



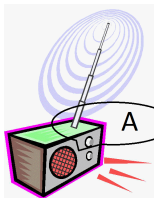
# Common knowledge



# Common knowledge



# Common knowledge





# Common knowledge

Informally, common knowledge of a proposition  $A$  is defined as the infinitary conjunction

everybody knows  $A$  and

everybody knows that everybody knows  $A$  and

everybody knows that everybody knows that everybody knows  $A$  and

...

This is equivalent to:

Common knowledge of  $A$  is the greatest fixed point of

$$\lambda X. \text{everybody knows } A \text{ and everybody knows } X.$$

$$A ::= p \mid \bar{p} \mid (A \vee A) \mid (A \wedge A) \mid \diamond_i A \mid \square_i A \mid \diamond A \mid \square A$$

Abbreviations:

$$\begin{aligned}\square A &= \square_1 A \wedge \dots \wedge \square_h A \\ \diamond A &= \diamond_1 A \vee \dots \vee \diamond_h A \\ \square^n A &= \underbrace{\square \dots \square}_n A \\ &\quad \text{\small } n\text{-times}\end{aligned}$$

Negation and implication are defined as usual

# The Hilbert System $H_R$

(TAUT) all instances of propositional tautologies

$$(MP) \frac{A \quad A \rightarrow B}{B}$$

$$(K) \quad \Box_i A \wedge \Box_i (A \rightarrow B) \rightarrow \Box_i B \quad (NEC) \quad \frac{A}{\Box_i A}$$

$$(CCL) \quad \Box A \rightarrow (\Box A \wedge \Box \Box A)$$

$$(I-R) \quad \frac{B \rightarrow (\Box A \wedge \Box B)}{B \rightarrow \Box A}$$

## Theorem

$H_R$  is a sound and complete deductive system for common knowledge.

# The $\omega$ -rule: System $G_C$

$$\Gamma, p, \bar{p} \quad \wedge \frac{\Gamma, A \quad \Gamma, B}{\Gamma, A \wedge B} \quad \vee \frac{\Gamma, A, B}{\Gamma, A \vee B}$$

$$\square_i \frac{\Gamma, \diamond \Delta, A}{\diamond_i \Gamma, \diamond \Delta, \square_i A, \Sigma}$$

$$[*] \frac{\Gamma, \square^k A \quad \text{for all } k \geq 1}{\Gamma, [*] A}$$

$$[\diamond] \frac{\Gamma, \diamond A, \diamond A}{\Gamma, [\diamond] A}$$

## Theorem

$G_C$  is a sound and complete deductive system for common knowledge.

# The problem of cut-elimination

$$\text{cut} \frac{\frac{\frac{\pi_1}{A, \Gamma, \diamond \bar{B}}{\square_i A, \diamond_i \Gamma, \Sigma, \diamond \bar{B}}}{\square_i A, \diamond_i \Gamma, \Sigma, \Delta} \quad \frac{\frac{\frac{\pi_{2k}}{\square^k B, \Delta}}{\square^k B, \Delta}}{\square^k B, \Delta}}{\square_i A, \diamond_i \Gamma, \Sigma, \Delta}}{\square_i A, \diamond_i \Gamma, \Sigma, \Delta} \quad 1 \leq k < \omega$$

Typical cut-elimination procedure yields:

$$\text{cut} \frac{\frac{\frac{\pi_1}{A, \Gamma, \diamond \bar{B}}}{A, \Gamma, \Delta} \quad \frac{\frac{\frac{\pi_{2k}}{\square^k B, \Delta}}{\square^k B, \Delta}}{\square^k B, \Delta}}{\square_i A, \diamond_i \Gamma, \Sigma, \diamond_i \Delta}}{\square_i A, \diamond_i \Gamma, \Sigma, \diamond_i \Delta} \quad 1 \leq k < \omega$$

Nested sequents:

- make  $\Box_i$  a structural rule
- allow deep application of rules

Ex:  $A, B, [C, [D]_i]_j$  corresponds to  $A \vee B \vee \Box_j(C \vee \Box_i D)$

$$\Gamma\{p, \bar{p}\} \quad \wedge \frac{\Gamma\{A\} \quad \Gamma\{B\}}{\Gamma\{A \wedge B\}} \quad \vee \frac{\Gamma\{A, B\}}{\Gamma\{A \vee B\}}$$

$$\Box_i \frac{\Gamma\{[A]_i\}}{\Gamma\{\Box_i A\}} \quad \Diamond_i \frac{\Gamma\{\Diamond_i A, [\Delta, A]_i\}}{\Gamma\{\Diamond_i A, [\Delta]_i\}}$$

$$\Box^* \frac{\Gamma\{\Box^k A\} \quad \text{for all } k \geq 1}{\Gamma\{\Box^* A\}} \quad \Diamond^* \frac{\Gamma\{\Diamond^* A, \Diamond^k A\}}{\Gamma\{\Diamond^* A\}}$$

# Properties of $D_C$

## Lemma (Structural rules and invertibility)

- (i) *The rules necessitation, weakening and contraction are admissible for system  $D_C$ .*
- (ii) *All rules in  $D_C$  are invertible for  $D_C$ .*

## Theorem (Cut-elimination for the deep system)

*If  $D_C \frac{\alpha}{\omega \cdot n} \Gamma$  then  $D_C \frac{\varphi_1^n(\alpha)}{0} \Gamma$ .*

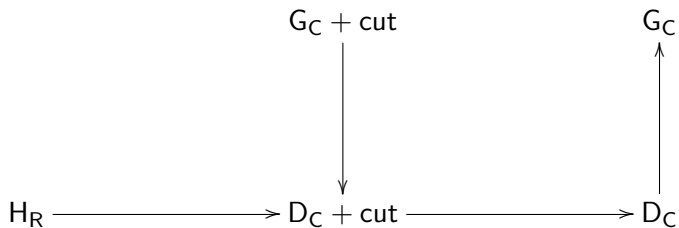
## Theorem (Cut-elimination for the shallow system)

*If  $G_C \frac{\alpha}{\omega \cdot n} \Gamma$  then  $G_C \frac{\omega \cdot (\varphi_1^n(\omega \cdot \alpha) + 1)}{0} \Gamma$*

## Theorem (Upper bounds)

*If  $A$  is a valid formula then  $D_C \frac{<\varphi_2^0}{0} A$  and  $G_C \frac{<\varphi_2^0}{0} A$ .*

# Cut-elimination on one slide





The infinitary system S:

$$\begin{array}{c}
 \Gamma, p, \bar{p} \quad \wedge \frac{\Gamma, A \quad \Gamma, B}{\Gamma, A \wedge B} \quad \vee \frac{\Gamma, A, B}{\Gamma, A \vee B} \\
 \\
 \square_i \frac{\Gamma, A}{\diamond_i \Gamma, \square_i A, \Sigma} \\
 \\
 \boxtimes \frac{\Gamma, \square A \wedge \square \boxtimes A}{\Gamma, \boxtimes A} \quad \boxast \frac{\Gamma, \diamond A \vee \diamond \boxast A}{\Gamma, \boxast A}
 \end{array}$$

Global condition: every infinite branch contains a  $\boxtimes$ -thread, i.e. there is a  $\boxtimes A$  unfolded infinitely often.

# An S-proof for the induction axiom

$$\begin{array}{c}
 \text{(ax')} \\
 \hline
 \neg A, A, \diamond(A \wedge \diamond\neg A), \boxtimes A \quad \frac{\vdots}{\neg A, \diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes A}} \text{(\boxtimes)} \\
 \hline
 \frac{\neg A, A \wedge \diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes A}}{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \diamond\boxtimes(A \wedge \diamond\neg A), \underline{\boxtimes\boxtimes A}} \text{(\boxdot)} \\
 \frac{\text{(ax')} \quad \neg A, A}{\diamond\neg A, \diamond(A \wedge \diamond\neg A) \vee \diamond\boxtimes(A \wedge \diamond\neg A), \underline{\boxtimes\boxtimes A}} \text{(\vee)} \\
 \frac{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes\boxtimes A}}{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes\boxtimes A}} \text{(\boxtimes)} \\
 \hline
 \frac{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes\boxtimes A}}{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes A}} \text{(\wedge)} \\
 \hline
 \frac{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes A}}{\diamond\neg A, \diamond(A \wedge \diamond\neg A), \underline{\boxtimes A}} \text{(\boxtimes)}
 \end{array}$$

# Completeness for S

Let  $\mathcal{T}$  be a proof search tree for  $\Gamma$ . Define an infinite game on it where player I tries to show that  $\Gamma$  is provable.

- 1 at any  $(\Box')$  node, player I chooses one of the children,
- 2 at any  $(\wedge)$  node, player II chooses one of the children,

Such a game results in a path in  $\mathcal{T}$ . Finite path: player I wins if the path ends in an axiom. Infinite path: player I wins if the path contains a  $\Box$ -thread.

## Theorem

- 1 *There is a winning strategy for player I if and only if there is an S-proof for  $\Gamma$  contained in  $\mathcal{T}$ .*
- 2 *There is a winning strategy for player II if and only if there is an  $S_{\text{Dis}}$ -disproof for  $\Gamma$  contained in  $\mathcal{T}$ .*
- 3 *The game is determined, i.e. one of the players has a winning strategy.*

## Theorem

*S is a complete deductive system for common knowledge.*

Proof. Let  $A$  be a formula that is not provable in S.

The proof search tree for  $A$  does not contain a proof for  $A$ .

There is no winning strategy for player I.

There must be a winning strategy for player II.

The proof search tree for  $A$  contains a  $S_{\text{Dis}}$ -disproof for  $A$ .

That disproof induces a counter model for  $A$ .

# The situation for $\mu$

$H_\mu$  is a Hilbert system for the modal  $\mu$ -calculus

## Theorem

*$H_\mu$  is a sound and complete deductive system for the  $\mu$ -calculus.*

Proof: very involved

$G_\mu$  is a Gentzen system (with an  $\omega$ -rule) for the modal  $\mu$ -calculus

## Theorem

*$G_\mu$  is a sound and complete deductive system for the  $\mu$ -calculus.*

Proof of soundness: uses finite model property

Proof of completeness: canonical model construction

# The situation for $\mu$ (2)

$D_\mu$  is a nested sequent system (with an  $\omega$ -rule) for the modal  $\mu$ -calculus

## Theorem

- 1  $D_\mu$  is a sound and complete deductive system for the  $\nu\Box$ -fragment.
- 2  $D_\mu$  enjoys syntactic cut-elimination.
- 3  $D_\mu$  is not complete for the modal  $\mu$ -calculus.

Proofs:

- 1 Syntactic embedding of the  $\nu\Box$ -fragment of  $G_\mu$
- 2 Standard
- 3 Counter example: accessible part larger than  $\omega$

# The situation for $\mu$ (3)

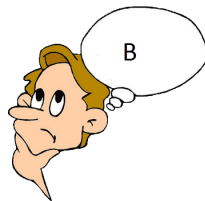
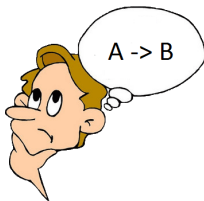
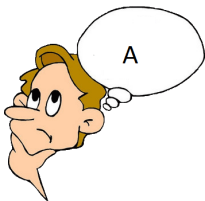
$S_\mu$  is a system with infinite proof branches for the modal  $\mu$ -calculus

## Theorem

*$S_\mu$  is a sound and complete deductive system for the  $\mu$ -calculus.*

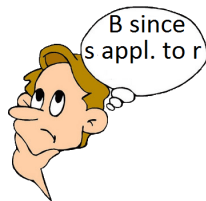
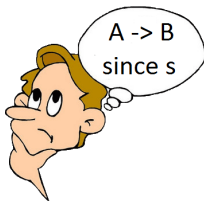
Proof: using determinacy

# Modal Logic (without justifications)



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





$$r:A \wedge s:(A \rightarrow B) \rightarrow s \cdot r:B$$

## Lemma

*If*

$$F_1, \dots, F_m \vdash A,$$

*then there exists a justification term  $t(x_1, \dots, x_m)$  for fresh variables  $x_1, \dots, x_m$  such that*

$$x_1 : F_1, \dots, x_m : F_m \vdash t(x_1, \dots, x_m) : A \quad .$$

Proof idea: for every rule there is a corresponding operation on terms that reflects that rule, i.e. to internalize

$$\text{(MP)} \frac{A \quad A \rightarrow B}{B}$$

we have

$$r : A \wedge s : (A \rightarrow B) \rightarrow s \cdot r : B \quad .$$

How can we internalize the induction rule rule

$$(I-R) \frac{B \rightarrow (\Box A \wedge \Box B)}{B \rightarrow \Box A} \quad ?$$

We don't know. Better use the induction axiom

$$\Box A \wedge \Box(A \rightarrow \Box A) \rightarrow \Box A \quad .$$

This gives

$$r^E : A \wedge s^C : (A \rightarrow t^E : A) \rightarrow \text{ind}(r, s)^C : A \quad .$$

## Definition (Forgetful projection)

If  $A$  is a formula of justification logic, then the modal formula  $A^\circ$  is the result of replacing every term in  $A$  with the corresponding modal operator.

## Theorem

*If  $A$  is a theorem of justified common knowledge, then  $A^\circ$  is a theorem of modal common knowledge.*

# The problem of realization

A realization is a mapping from modal formulae to justified formulae that replaces modal operators with justification terms.

Is there a realization  $r$  such that  $A^r$  is a theorem of justified common knowledge for any theorem  $A$  of modal common knowledge?

Usually, realization is proved using a nice cut-free sequent calculus for modal logic. However,  $G_C$  does not work since we cannot merge infinitely many premises.

Thus, we need a finitary nice cut-free system.

## Lemma (Small model property)

*There is a function  $f$  such that if a formula  $A$  is satisfiable, then there exists a model of size at most  $f(A)$ .*

## Definition (The system $G_C^{<\omega}$ )

The system  $G_C^{<\omega}$  is defined by replacing the  $\omega$ -rule in the system  $G_C$  by the rule

$$\frac{\Gamma, \Box^k A \quad \text{for all } 1 \leq k \leq f(\bigvee \Gamma \vee \Box A)}{\Gamma, \Box A, \Sigma}$$

## Other possibilities

- Use induction rule instead of  $\omega$ -rule (AlberucciJäger05)
- Reformulate focus games as sequent calculi (BrünnlerLange08)
- Tableau systems (AbateGoréWidman07, GorankoShkatov08)

# Why is it so difficult?

## Theorem

*The logic of common knowledge lacks Craig interpolation.*

New ideas are needed to design a nice finitary cut-free system.

Thank you!

