Cut-Elimination for Modal Fixed Point Logics

Thomas Studer

based on joint work with
Kai Brünnler, Samuel Bucheli, Gerhard Jäger, Mathis Kretz, Roman Kuznets,
Grigori Mints

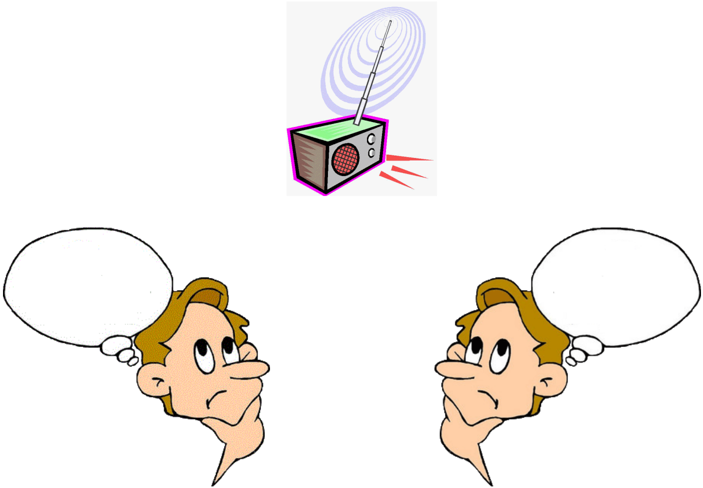
Institute of Computer Science and Applied Mathematics
University of Bern
Switzerland

September 2013

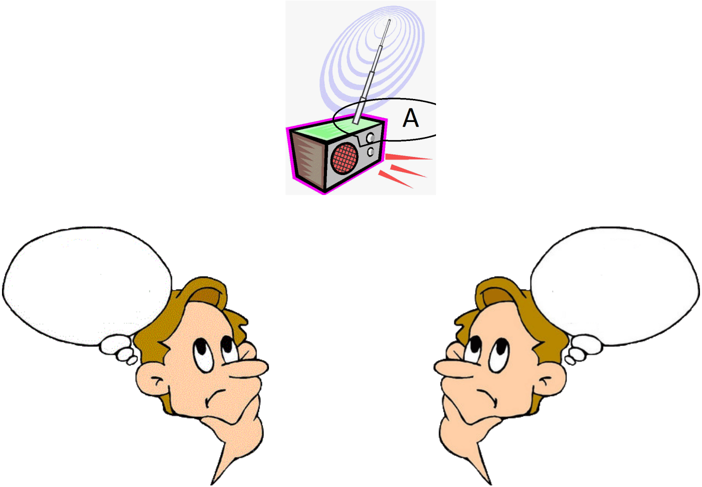
Roadmap

- Hilbert system for common knowledge
- Infinitary system based on an ω-rule
- Syntactic cut-elimination
- Infinite branches
- The situation for the μ-calculus
- Justification logic and common knowledge

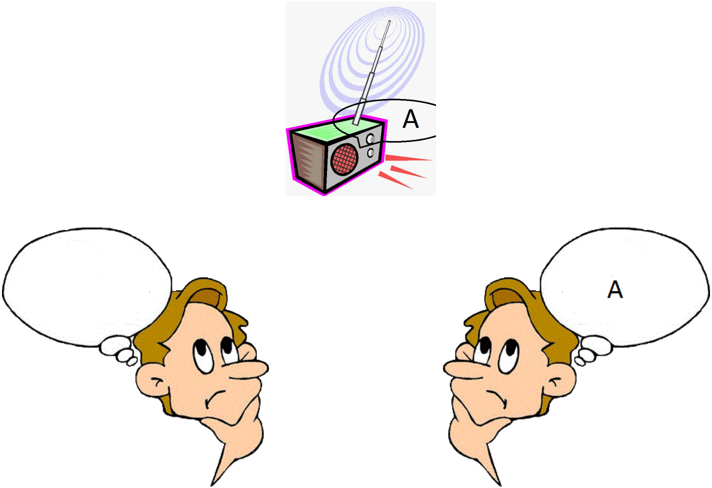
Common knowledge



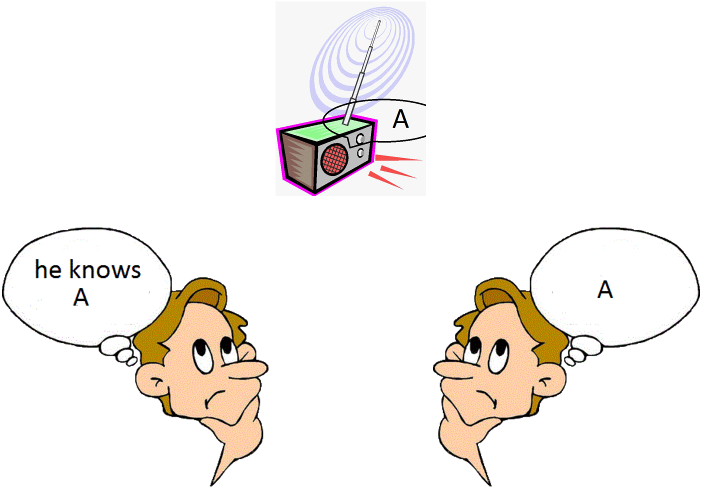
Common knowledge



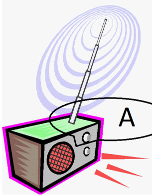
Common knowledge

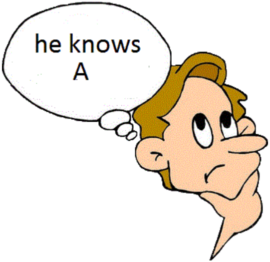


Common knowledge

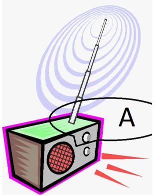


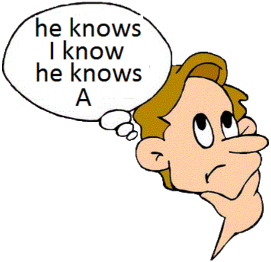
Common knowledge





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

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

The Language

$$A ::= p \mid \bar{p} \mid (A \vee A) \mid (A \wedge A) \mid \Diamond_i A \mid \Box_i A \mid \circledast A \mid \boxast A$$

Abbreviations:

$$\begin{aligned} \Box A &= \Box_1 A \wedge \ldots \wedge \Box_h A \\ \Diamond A &= \Diamond_1 A \vee \ldots \vee \Diamond_h A \\ \Box^n A &= \underbrace{\Box \ldots \Box}_{n-\text{times}} A \end{aligned}$$

Negation and implication are defined as usual

The Hilbert System H_R

(TAUT) all instances of propositional tautologies

$$(\mathsf{MP})\ \frac{A \quad A \to B}{B}$$

$$(\mathsf{K})\quad \Box_i A \wedge \Box_i (A \to B) \to \Box_i B \qquad (\mathsf{NEC})\ \frac{A}{\Box_i A}$$

$$(\mathsf{CCL})\quad \circledast A \to (\Box A \wedge \Box \circledast A)$$

$$(\mathsf{I\text{-}R})\ \frac{B \to (\Box A \wedge \Box B)}{B \to \circledast A}$$

Theorem

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

The ω-rule: System $\mathsf{G_C}$

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

$$\Box_i\ \frac{\Gamma, \circledast\Delta, A}{\Diamond_i\Gamma, \circledast\Delta, \Box_i A, \Sigma}$$

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

Theorem

$\mathsf{G_C}$ is a sound and complete deductive system for common knowledge.

The problem of cut-elimination

$$
\dfrac{
  \square_i \; \dfrac{\dfrac{\pi_1}{A, \Gamma, \circledast \bar{B}}}{\square_i A, \Diamond_i \Gamma, \Sigma, \circledast \bar{B}}
  \qquad
  \boxed{*} \; \dfrac{\cdots \quad \dfrac{\pi_{2k}}{\square^k B, \Delta} \quad \cdots}{\boxed{*} B, \Delta} \; 1 \leq k < \omega
}{\square_i A, \Diamond_i \Gamma, \Sigma, \Delta} \; \text{cut}
$$

Typical cut-elimination procedure yields:

$$
\square_i \; \dfrac{
  \dfrac{
    \dfrac{\pi_1}{A, \Gamma, \circledast \bar{B}}
    \qquad
    \boxed{*} \; \dfrac{\cdots \quad \dfrac{\pi_{2k}}{\square^k B, \Delta} \quad \cdots}{\boxed{*} B, \Delta} \; 1 \leq k < \omega
  }{A, \Gamma, \Delta} \; \text{cut}
}{\square_i A, \Diamond_i \Gamma, \Sigma, \Diamond_i \Delta}
$$

System $\mathsf{D_C}$

Nested sequents:

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

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

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

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

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

Properties of $\mathsf{D_C}$

Lemma (Structural rules and invertibility)

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

Theorem (Cut-elimination for the deep system)

If $\mathsf{D_C} \vdash^{\alpha}_{\omega \cdot n} \Gamma$*, then* $\mathsf{D_C} \vdash^{\varphi_1^n(\alpha)}_{0} \Gamma$*.*

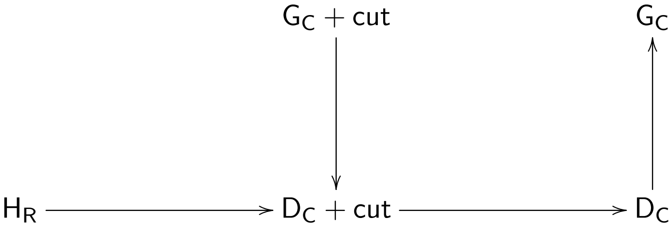
Theorem (Cut-elimination for the shallow system)

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

Theorem (Upper bounds)

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

Cut-elimination on one slide



Infinite branches

The infinitary system S:

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

$$\Box_i\,\frac{\Gamma, A}{\Diamond_i \Gamma, \Box_i A, \Sigma}$$

$$\boxast\,\frac{\Gamma, \Box A \wedge \Box \boxast A}{\Gamma, \boxast A} \qquad \circledast\,\frac{\Gamma, \Diamond A \vee \Diamond \circledast A}{\Gamma, \circledast A}$$

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

An S-proof for the induction axiom

$$
\dfrac{\vdots}{\neg A, \Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\boxast A}}\ (\boxast)
$$

$$
\dfrac{\dfrac{(\text{ax'})}{\neg A, A, \diamondast(A \wedge \Diamond\neg A), \boxast A} \qquad \neg A, \Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\boxast A}}{\neg A, A \wedge \Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\boxast A}}\ (\wedge)
$$

$$
\dfrac{\neg A, A \wedge \Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\boxast A}}{\Diamond\neg A, \Diamond(A \wedge \Diamond\neg A), \Diamond\diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}\ (\Box)
$$

$$
\dfrac{\Diamond\neg A, \Diamond(A \wedge \Diamond\neg A), \Diamond\diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}{\Diamond\neg A, \Diamond(A \wedge \Diamond\neg A) \vee \Diamond\diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}\ (\vee)
$$

$$
\dfrac{\Diamond\neg A, \Diamond(A \wedge \Diamond\neg A) \vee \Diamond\diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}{\Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}\ (\diamondast)
$$

$$
\dfrac{\dfrac{\dfrac{(\text{ax'})}{\neg A, A}}{\Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \Box A}\ (\Box) \qquad \Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\Box\boxast A}}{\Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\Box A \wedge \Box\boxast A}}\ (\wedge)
$$

$$
\dfrac{\Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\Box A \wedge \Box\boxast A}}{\Diamond\neg A, \diamondast(A \wedge \Diamond\neg A), \underline{\boxast A}}\ (\boxast)
$$

Completeness for S

Let $\mathcal{T}$ be a proof search tree for Γ. Define an infinite game on it where player I tries to show that Γ 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 $\circledast$-thread.

Theorem

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

Completeness for S

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 $\mathsf{S}_{\mathsf{Dis}}$-disproof for A.
That disproof induces a counter model for A.

The situation for μ

H_μ is a Hilbert system for the modal μ-calculus

Theorem

H_μ *is a sound and complete deductive system for the* μ*-calculus.*

Proof: very involved

The situation for μ

H_μ is a Hilbert system for the modal μ-calculus

Theorem

H_μ *is a sound and complete deductive system for the* μ*-calculus.*

Proof: very involved

G_μ is a Gentzen system (with an ω-rule) for the modal μ-calculus

Theorem

G_μ *is a sound and complete deductive system for the* μ*-calculus.*

Proof of soundness: uses finite model property
Proof of completeness: canonical model construction

The situation for μ (2)

D_μ is a nested sequent system (with an ω-rule) for the modal μ-calculus

Theorem

1. D_μ *is a sound and complete deductive system for the* $\nu\Box$*-fragment (aka continuous fragement).*
2. D_μ *enjoys syntactic cut-elimination.*
3. D_μ *is* not *complete for the modal* μ*-calculus.*

Proofs:

1. Syntactic embedding of the $\nu\Box$-fragment of G_μ
2. Standard
3. Counter example: accessible part may be larger than ω, i.e. the valid formula $\Box(\mu X.\Box X) \to \mu X.\Box X$ is not derivable.

The situation for μ (3)

S_μ is a system with infinite proof branches for the modal μ-calculus

Theorem

S_μ is a sound and complete deductive system for the μ-calculus.

Proof: using determinacy

Finitary Systems

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 $\mathsf{G_C}^{<\omega}$)

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

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

Finitary Systems

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 $\mathsf{G_C}^{<\omega}$)

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

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

Other possibilities

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

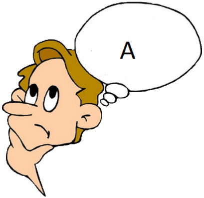
Why is it so difficult?

Theorem

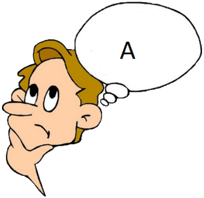
The logic of common knowledge lacks Craig interpolation.

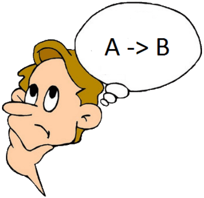
New ideas are needed to design a nice finitary cut-free system.

Modal Logic (without justifications)

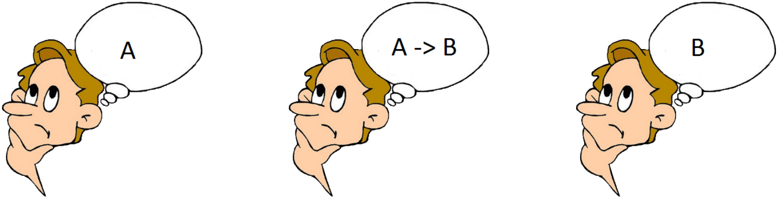


Modal Logic (without justifications)

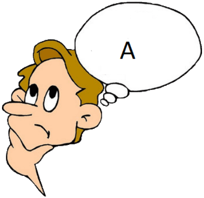


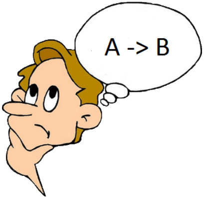


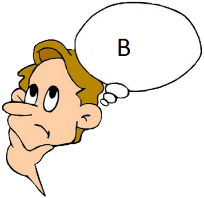
Modal Logic (without justifications)



Modal Logic (without justifications)

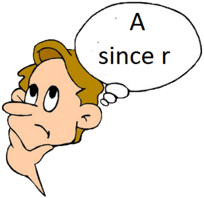




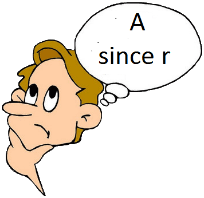


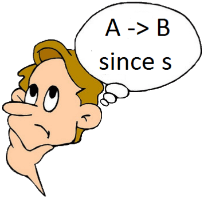
$$\Box A \quad \wedge \quad \Box(A \rightarrow B) \quad \rightarrow \quad \Box B$$

Justification Logic

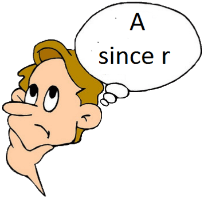


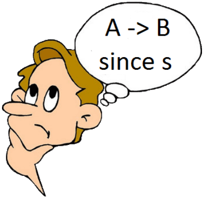
Justification Logic

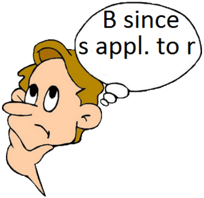




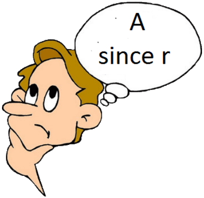
Justification Logic

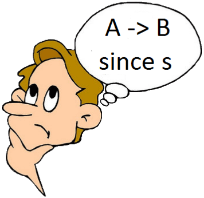


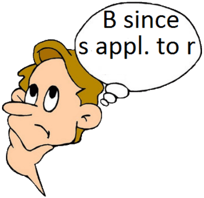




Justification Logic







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

Internalization

Lemma

If

$$F_1, \ldots, F_m \vdash A,$$

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

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

Internalization

Lemma

If

$$F_1, \ldots, F_m \vdash A,$$

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

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

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

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

we have

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

Internalizing common knowledge

How can we internalize the induction rule rule

$$\text{(I-R)}\ \frac{B \to (\Box A \land \Box B)}{B \to \boxast A} \quad ?$$

Internalizing common knowledge

How can we internalize the induction rule rule

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

We don't know.

Internalizing common knowledge

How can we internalize the induction rule rule

$$\text{(I-R)}\ \frac{B \to (\Box A \land \Box B)}{B \to \boxast A} \quad ?$$

We don't know. Better use the induction axiom

$$\Box A \land \boxast(A \to \Box A) \to \boxast A \quad .$$

This gives

$$r^E : A \land s^C : (A \to t^E : A) \to \mathsf{ind}(r, s)^C : A \quad .$$

Forgetful projection

Definition (Forgetful projection)

If A is a formula of justification logic, then the modal formula A° 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° 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 realiation r such that A^r is a theorem of justified common knowledge for any theorem A 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 realiation 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 infintely many premises.

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

Thank you!