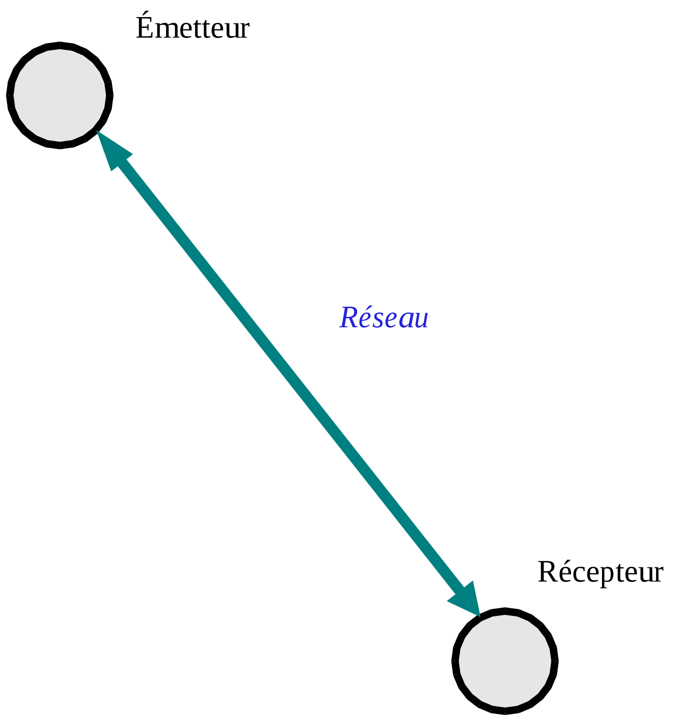
La logique de la connaissance

Un protocole émetteur-récepteur

Les noeuds ◯ transmettent les messages entre l'émetteur et le récepteur :

– ils peuvent dupliquer des messages,
– ils peuvent perdre des messages,
– cependant, ils ne peuvent pas perdre indéfiniment un même message.

C'est le principe d'**Internet** : «faire de son mieux» (en anglais «the best effort»). Le protocole s'appelle **TCP** (pour Transmission Control Protocol).


Émetteur
Réseau
Récepteur

Un protocole émetteur-récepteur *(suite)*

Tant que l'émetteur **ne sait pas** si le récepteur a reçu un message donné m_i, il le ré-émet.

Le récepteur accuse réception d'un message en émettant un message d'accusé réception ack_i tant qu'il **ne sait pas** si l'émetteur a reçu cet accusé réception.

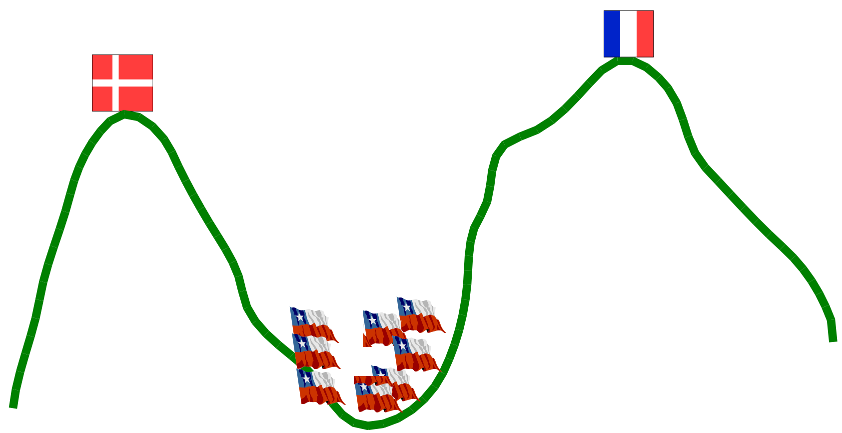
L’attaque coordonnée

- Deux généraux et leurs armées sur deux collines,
- Ils doivent attaquer ensemble et chaque général doit être sûr que l’autre général attaquera en même temps.
- Ils communiquent par des messagers
  - qui mettent une heure pour aller d’un camp à l’autre,
  - qui peuvent se perdre dans le noir ou être capturés.

L’attaque coordonnée

- Deux généraux et leurs armées sur deux collines,
- Ils doivent attaquer ensemble et chaque général doit être sûr que l’autre général attaquera en même temps.
- Ils communiquent par des messagers
  - qui mettent une heure pour aller d’un camp à l’autre,
  - qui peuvent se perdre dans le noir ou être capturés.

Comment coordonner une attaque ?



La sécurité sur Internet

Transformer des «**je crois que**» en «**je sais que**».

Les messages circulent le réseau public que façon codée, mais ça n'est pas suffisant.

Des intrus sur le réseau, écoutent les messages, les stockent et fabriquent de faux messages.

A a reçu un message de B, A doit pouvoir affirmer «***Je sais que*** *le message que j'ai reçu a bien été émis par* B».

Jouons un peu

Les as et les huit

Il y a huit cartes : quatre as et quatre 8.

Les as et les huit

Il y a huit cartes : quatre as et quatre 8.

Chaque joueur reçoit deux cartes qu'il ne regarde pas,
mais qu'il montre à tout le monde.

Les as et les huit

Il y a huit cartes : quatre as et quatre 8.

Chaque joueur reçoit deux cartes qu'il ne regarde pas,
mais qu'il montre à tout le monde.

Chaque joueur parle à son tour :

- Soit il dit Je ne sais pas,
- Soit il dit
  - J'ai deux as,
  - J'ai deux 8,
  - J'ai un as et un huit.

Les as et les huit

On fait autant de tours qu'il faut.

Il y a toujours un joueur qui peut deviner les cartes qu'il a.

Les as et les huit

On fait autant de tours qu’il faut.

Il y a toujours un joueur qui peut deviner les cartes qu’il a.

Comment cela se peut-il ?

Monsieur *Produit* et Monsieur *Somme*

Étant donnés deux nombres entre 2 et 20.

– Monsieur *Produit* connaît le produit de ces deux nombres,

– et Monsieur *Somme* connaît la somme de ces deux nombres.

Monsieur Produit : - Je ne connais pas les deux nombres.

Monsieur Somme : - Je le sais.

Monsieur Produit : - Alors je connais les deux nombres.

Monsieur Somme : - Alors, moi aussi je connais les deux nombres.

Les modalités

Une modalité est un opérateur qui transforme une sentence en une autre sentence.

On crée un modalité K_A pour chaque agent A.

Une logique avec des modalités s'appelle la logique modale.

Qu'est-ce que la logique de la connaissance ?

- La logique de la connaissance ou logique épistémique est la logique qui formalise
  - "l'agent i sait que p", noté $K_i(p)$,
  - "p est une connaissance commune", noté $C(p)$.

La connaissance commune

$C(p)$ formalise des phrases comme

- “C’est un fait bien connu que p, sauf des fous.”
- “L’agent i sait que l’agent j sait que l’agent i sait que l’agent j sait que, etc.”.

La connaissance commune

$C(p)$ formalise des phrases comme

– “C’est un fait bien connu que p, sauf des fous.”

– “L’agent i sait que l’agent j sait que l’agent i sait que , etc.”.

On a besoin d’une modalité E, dite de “connaissance partagée”, “Tout le monde sait que p”,

$$E_G(p) = \bigwedge_{i \in G} K_i(p).$$

La connaissance commune

$C(p)$ formalise des phrases comme

– “C’est un fait bien connu que p, sauf des fous.”

– “L’agent i sait que l’agent j sait que l’agent i sait que , etc.”.

On a besoin d’une modalité E, dite de “connaissance partagée”, “Tout le monde sait que p”,

$$E_G(p) = \bigwedge_{i \in G} K_i(p).$$

La connaissance commune n’est pas la connaissance partagée.

Les règles et les axiomes

Les règles

C'est une logique qui se présente à la Hilbert.

$$\frac{\vdash \varphi \qquad \vdash \varphi \Rightarrow \psi}{\vdash \psi}\,(MP)$$

La règle de généralisation de la connaissance

$$\frac{\vdash \varphi}{\vdash K_i\varphi}\vdash (GK)$$

Les axiomes

Il y tous les théorèmes de la logique classique propositionnelle classique.

$$\frac{}{\vdash \varphi}\,(\mathbf{Cl}) \qquad \text{si } \varphi \text{ est un théorème de la logique classique.}$$

Les axiomes

Il y a quatre axiomes

L'axiome de distribution

$$\frac{}{\vdash K_i\varphi \Rightarrow K_i(\varphi \Rightarrow \psi) \Rightarrow K_i\psi}\,(\mathbf{K})$$

L'axiome de la connaissance

$$\frac{}{\vdash K_i\varphi \Rightarrow \varphi}\,(\mathbf{T})$$

Les axiomes

L'axiome d'introspection positive

$$\frac{}{\vdash K_i\varphi \Rightarrow K_iK_i\varphi}\,(\mathbf{4})$$

L'axiome d'introspection négative

$$\frac{}{\vdash \neg K_i\varphi \Rightarrow K_i\neg K_i\varphi}\,(\mathbf{5})$$

Attention

En logique modale on n'a pas la règle de déduction

«*De* $G, \varphi \vdash \psi$ *je déduis* $G \vdash \varphi \Rightarrow \psi$»

Les axiomes de la connaissance commune

Défintion de E_G

$$\frac{}{\vdash E_G(\varphi) \Leftrightarrow \bigwedge_{i \in G} K_i(\varphi)}\,(C1)$$

$C_G\varphi$ satisfait l'inégalité $\psi \Rightarrow E_G(\varphi \wedge \psi)$.

$$\frac{}{\vdash C_G\varphi \Rightarrow E_G(\varphi \wedge C_G\varphi)}\,(C2)$$

Les règles de la connaissance commune

$C_G\varphi$ est le plus petit dans un certain sens, c'est-à-dire si un ψ satisfait $\psi \Rightarrow E_G(\varphi \wedge \psi)$ alors $\psi \Rightarrow C_G\varphi$.

$$\frac{\vdash \psi \Rightarrow E_G(\psi \wedge \varphi)}{\vdash \psi \Rightarrow C_G\varphi}\,(RC1)$$

Les modèles

Les modèles de Kripke

On reprend des modèles de Kripke avec des relations d'équivalence.

Un jeu très simple

2 agents, 3 cartes $\{A, B, C\}$.

L'agent 1 reçoit une carte

L'agent 2 reçoit un carte

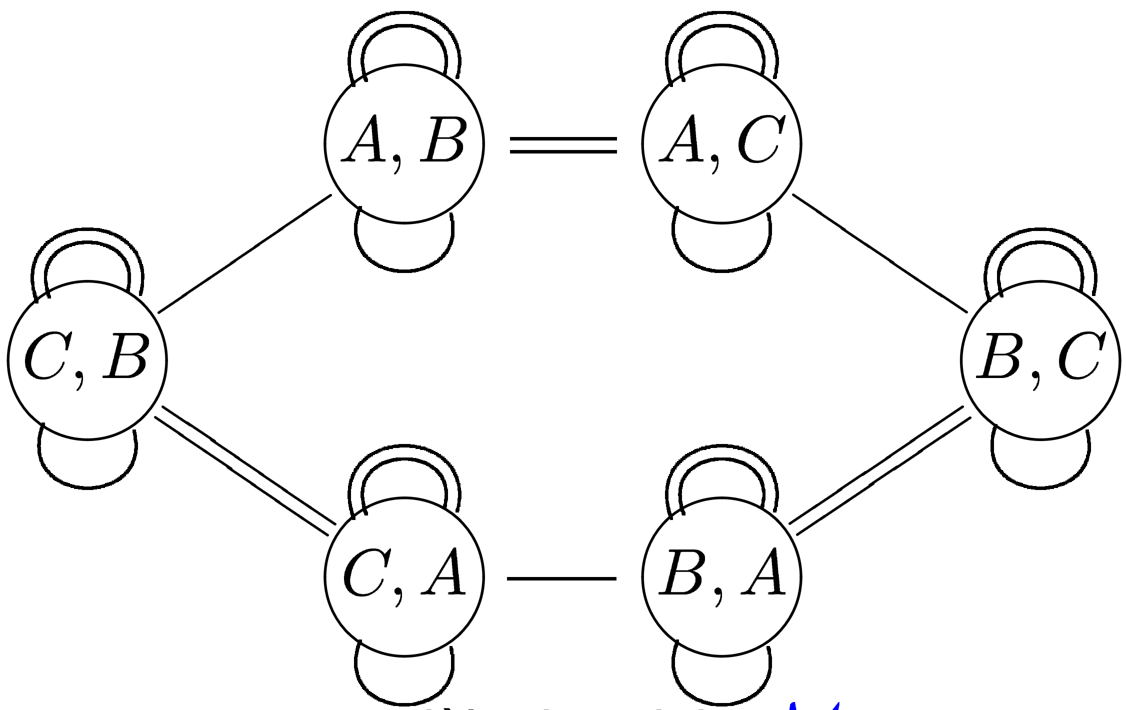
La troisième carte est retournée face contre la table/

Il y a six mondes possibles :

$$(A, B), (A, C), (B, A)(B, C), (C, A), (C, B).$$

Un jeu très simple

Dans le monde (A, B) l'agent 1 (sa relation d'accessibilité est noté par $=\!=$) envisage deux mondes possibles à savoir (A, B) et (A, C).



Le modèle de Kripke $\mathcal{M}$.

Un jeu très simple

Les propositions primitives sont

- $1A$ le joueur (l'agent) 1 détient la carte A,
- $2A$ le joueur (l'agent) 2 détient la carte A,
- $1B$ le joueur (l'agent) 1 détient la carte B,
- $2B$ le joueur (l'agent) 2 détient la carte B,
- $1C$ le joueur (l'agent) 1 détient la carte C,
- $2C$ le joueur (l'agent) 2 détient la carte C.

Des assertions de forçage

$(A, B) \Vdash 1A \wedge 2B$,

$(A, B) \Vdash K_1(2B \vee 2C$,

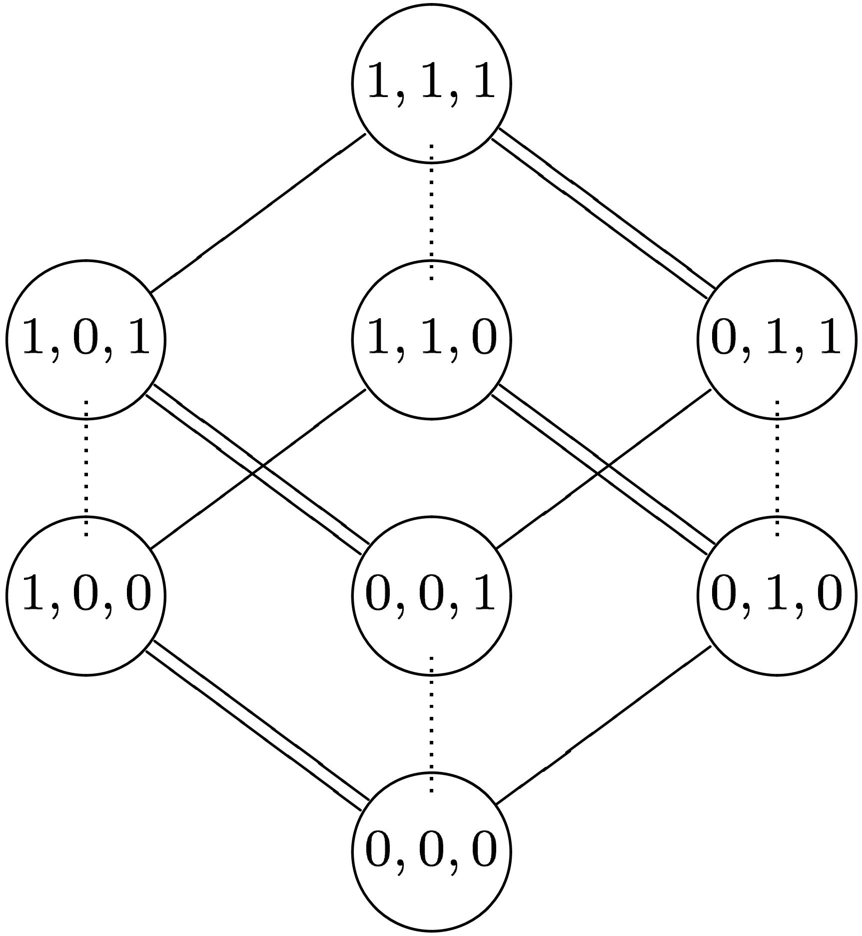
$(A, B) \Vdash K_1 \neg K_2(1A)$.

L'assertion $K_1(2A \vee 2B \vee 2C)$ donc $\mathcal{M} \models K_1(2A \vee 2B \vee 2C)$.

Les enfants sales

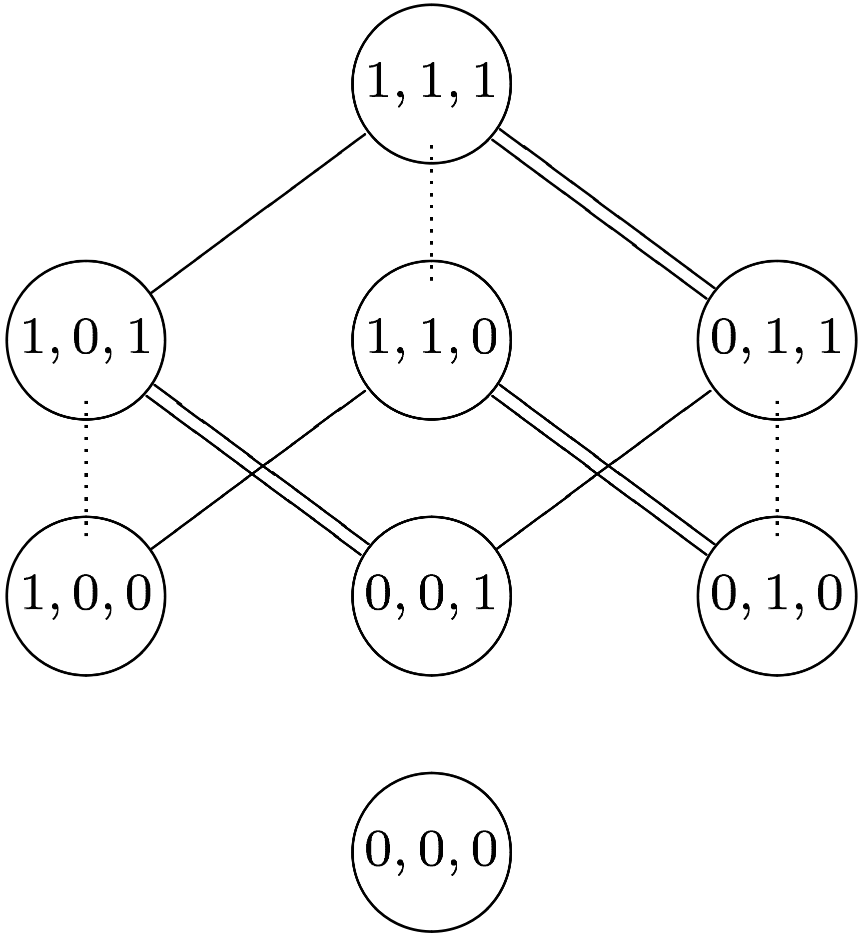
- Il y a n enfants dont certains ont la saleté sur le front.
- Le père déclare «L'un d'entre vous a de la saleté sur le front».
- Puis le père pose plusieurs fois (combien ?) la question «Avez-vous de la saleté sur le front ?».
- Comme les n enfants ont tous de la saleté sur le front.
- Après n questions du père, ils répondent tous ensemble «oui».

Le modèle de Kripke pour les enfants sales

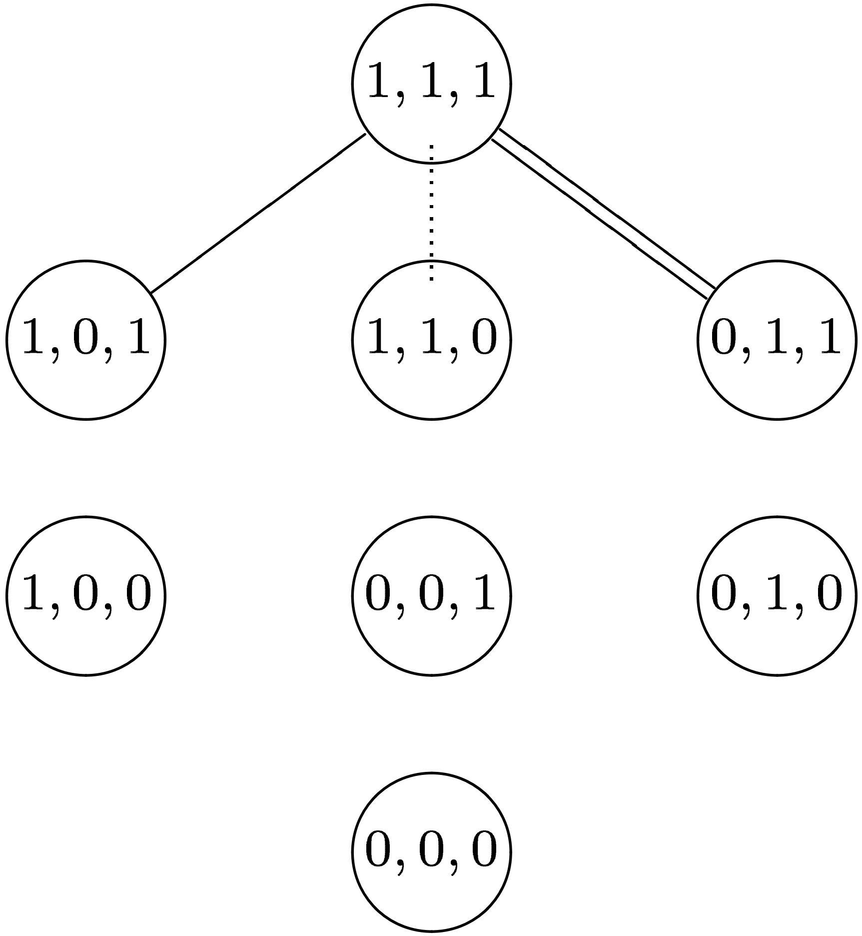


On abandonne les boucles de réflexivité.

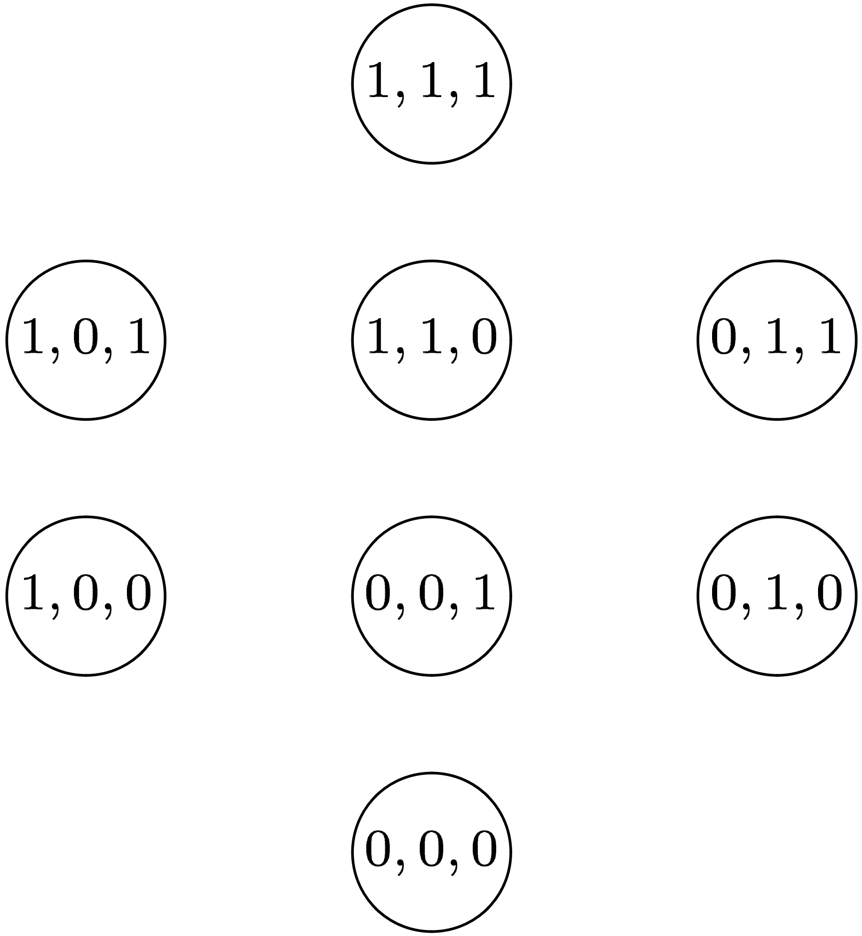
Après que le père ait parlé



Après que le père ait posé sa première question



Après que le père ait posé sa deuxième question



Correction

Théorème : Si $\vdash \varphi$ alors $\models \varphi$.

Pourquoi pas la règle de déduction ?

Si on avait la règle de déduction

«De $G, \varphi \vdash \psi$ *je déduis* $G \vdash \varphi \Rightarrow \psi$*»*

alors du jugement $\varphi \vdash K_i\varphi$ on aurait $\varphi \vDash K_i\varphi$,

c'est-à-dire *«Si dans tous les mondes de l'univers en question, φ est vrai, alors chaque agent i sait φ»*

on pourrait déduire $\vDash \varphi \Rightarrow K_i\varphi$

c'est-à-dire *«Si φ est vrai alors chaque agent i sait φ»*.

Une preuve

On peut prouver $\vdash \varphi \Rightarrow K_i \neg K_i \neg \varphi$.

Une preuve

On peut prouver $\vdash \varphi \Rightarrow K_i\neg K_i\neg\varphi$.

$$
\dfrac{\dfrac{}{\vdash \neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(\mathbf{5}) \qquad \dfrac{\dfrac{}{\vdash \psi}\,(Cl) \qquad \dfrac{}{\vdash K_i\neg\varphi \Rightarrow \neg\varphi}\,(\mathbf{T})}{\vdash (\neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi) \Rightarrow \varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(MP)}{\vdash \varphi \Rightarrow K_i\neg K_i\neg\varphi}\,(MP)
$$

où $\psi \equiv (K_i\neg\varphi \Rightarrow \neg\varphi) \Rightarrow (\neg K_i\varphi \Rightarrow K_i\neg K_i\neg\varphi) \Rightarrow \varphi \Rightarrow K_i\neg K_i\neg\varphi$

qui est un théorème classique.

Car c'est un instance de $(B \Rightarrow \neg A) \Rightarrow (\neg B \Rightarrow C) \Rightarrow (A \Rightarrow C)$.