Part III: Epistemic Logic

W. van der Hoek

Modal logic

- philosophical logic
- a formal treatment of intensional notions
- various 'flavours':
  - epistemic / doxastic
  - temporal / dynamic (action logic)
  - deontic

Extensionality

- Classical logic is extensional:
  - $\models (\alpha \leftrightarrow \beta) \rightarrow (\psi \leftrightarrow \psi[\alpha / \beta])$

defining knowledge

p	Kp	Kp	Kp	K
0	~~0~~	~~1~~	~~0~~	~~1~~
1	~~1~~	~~0~~	~~0~~	~~1~~

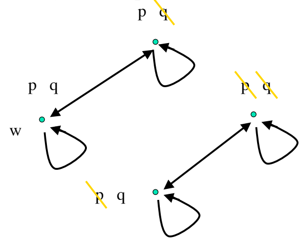
Varieties of modal logics

Alethic logic	$\Box\varphi$	φ must be the case
Dynamic logic	$[\alpha]\varphi$	after α, φ holds
Deontic logic	$O\ \varphi$	φ should be
Temporal logic	$\Box\varphi$	always, φ
Doxastic logic	$B\varphi$	φ is believed
Epistemic logic	$K\varphi$	φ is known
Arithmetic logic	$\Box\varphi$	φ is provable

Semantics of modal logic

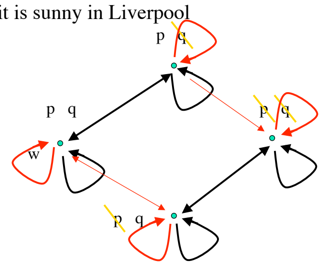
p: it is sunny in Liverpool

q: it is sunny in London



Semantics of modal logic

p: it is sunny in Liverpool q: it is sunny in London



ercise 0. Agent 1 is in Liverpool, agent 2 in London.

Modal logic, semantics

- Kripke models: M = (W, π, R)
  - W: set of possible worlds
  - π: truth assignment function
  - R: accessibility relation
- R(w) = {w′ | R(w,w′)} set of accessil worlds from w

Modal logic, semantics

- M, w |= □φ
- iff M, w′ |= φ
  - for every w′ such that R(w, w′)
- M, w |= ◇φ
- iff M, w′ |= φ

Modal logic, ctd.

- modal logic = 'logic of □ and ◇'
- 'neutral reading': necessity / poss
- basic property (K):
  - (φ→ψ) → (φ→ ψ), or equivalently
  - (((φ→ψ) ∧ φ) → ψ)
- and Necessitaion

epistemic logic

System is called **S5**

as `difficult' as propositional!

R is an equivalence

no nestings needed:
K¬KK¬p ↔ ¬K¬p

no iterations needed:
K¬(K(K¬p v ¬Kq) → K¬Kq)
is unneccesary complex

- K(ϕ → ψ) → (
  - *agents reason*
- Kϕ → ϕ
  - *veridicality*
- Kϕ → KKϕ
  - *positive intro.*
- ¬Kϕ → K¬Kϕ
  - *negative intro*
- |– ϕ ⇒ |– Kϕ
  - *agents know*

Semantics

- Let E = {M = <W,R,V> | R is equiv
- Let U = {M = <W,R,V> | R is unive
- Let Th(M) = {φ | M |= φ}
- Then: Th(E) = Th(U)
  - ⊆ straightforward

Semantics

- E |= φ ⇔ U |= φ ⇔ **S5** |- φ
- easy to verify:
  - KKφ ≡ Kφ
  - K¬Kφ ≡ ¬ Kφ
  - ¬ KKφ ≡ ¬ Kφ
  - ¬ K ¬ Kφ ≡ Kφ

Semantics

- E |= φ ⇔ U |= φ ⇔ **S5** |- φ
- easy to verify:
  - φ is satisfiable iff
  - φ is satisfiable in a model of size with a |states
  - |p| = 1, |φ ∧ ψ| = 1 + |φ| + |ψ|
  - |¬φ| = |Kφ| = |φ| + 1

Small model property

- Suppose <S,V>,s |= φ
- f_s : Sub(φ) → 2^S
  - fs(p) = { }, atoms p in Sub(φ)
  - fs(φ ∧ ψ) = fs(φ) ∪ fs(ψ)
  - fs(¬φ) = fs(φ)
  - fs(Kφ) =
    - {t} if some <S,V>,t |= φ

Small model property

- Let S′ = {s} ∪ $\bigcup_{\psi \in Sub(\varphi)} f_s(\psi)$
- V′ = $V_{|S'}$
- Then: <S′,V′ >,s |= φ
- Proof: for all s′ in S′ : all ψ ∈ Sub(φ)
  - <S,V> |= ψ ⇔ <S′,V'> |= ψ

Epistemic and Doxastic lo

- Kφ → φ
- Kφ → KKφ *knowledge*
- ¬Kφ → K¬Kφ

- ¬B⊥
- Bφ → BBφ *belief*
- ¬Bφ → B¬Bφ

Logical Omniscience

(LO1) Bφ ∧ B(φ → ψ) → Bψ

(Closure under impl

(LO2) |= φ ⇒ |= Bφ

(belief of valid fo

(LO3) |= φ → ψ ⇒ |= Bφ → Bψ

(Closure under valid impl

Logical omniscience (2)

(LO4) $\models \varphi \leftrightarrow \psi \Rightarrow \models B\varphi \leftrightarrow B\psi$
(Belief of equivalent fo

(LO5) $(B\varphi \wedge B\psi) \rightarrow B(\varphi \wedge \psi)$
(Closure under conju

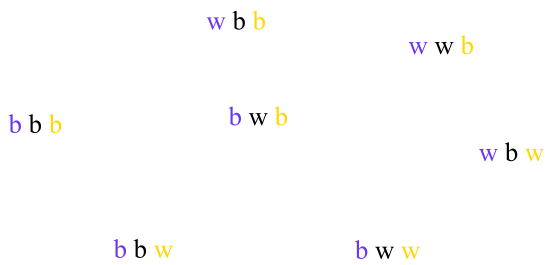
(LO6) $B\varphi \rightarrow B(\varphi \vee \psi)$
(Weakening of

(LO7) $B\varphi \rightarrow \neg B\neg\varphi$

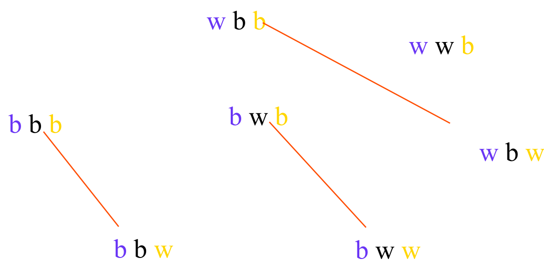
2 white, 3 black hats

	A	B	C
rules out:	w	w	any

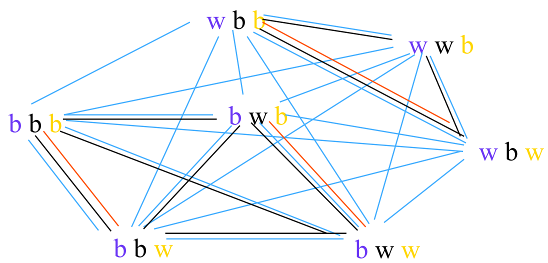
3 x b, 2 x w



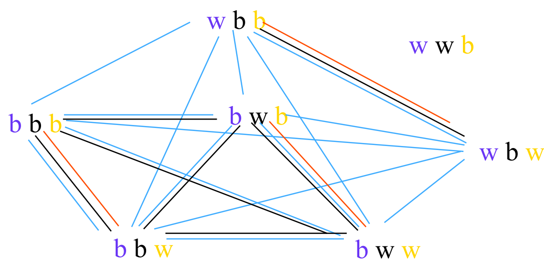
3 x b, 2 x w



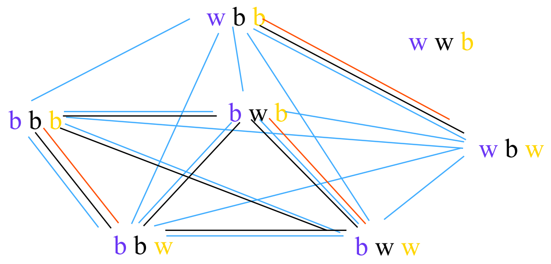
3 x b, 2 x w



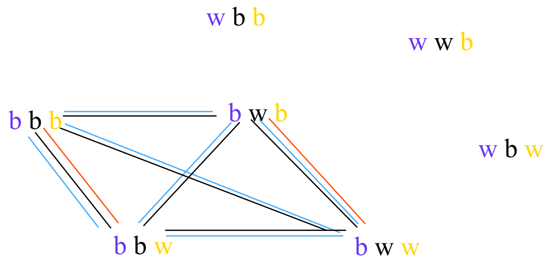
C: "I don't know my colou



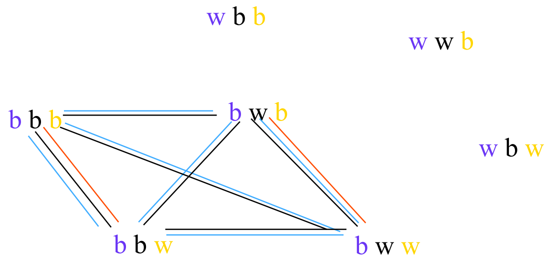
in w b b and w b w, agent B knows his co



B: "I don't know my colou either"



A: "I know mine!"



Protocol

- Sender and Receiver
- input for S: X = <x0,x1,x2,....... >
- S reads X, sends data to R, who writ
- deletion errors: reception not guarar
- required: protocol that satisfies
  - safety: for some Y, we have X = T;Y
  - liveness: every xi of X appears eventually i

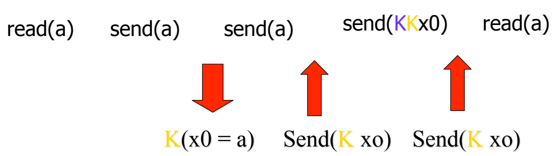
specification

- i := 0;
- while true do
- begin read(xi)
  - send(xi) until KK xi;
  - i := i + 1
- end

- when K x0 set i :=(
- while true do
- begin write (xi)
  - send(Kxi) until K(x
  - i := i+1
- end

not correct

- X = <a, a, a, c, a, b,.......>



specification

:= 0;
vhile true do
begin read(xi)

- send(xi) until KK xi;
- send(KK xi) until KKKK xi
- i := i + 1

end

- when K x0 set i :
- while true do
- begin write (xi)
  - send(Kxi) until K
  - send(KKK xi) un
  - i := i+1
- end

specification

i := 0;
while true do
begin read(xi)

- send(xi) until KK xi;
- send(KK xi) until KKKK xi
- i := i + 1

end

- when K x0 set i :=
- while true do
- begin write (xi)
  - send(Kxi) until KK
  - send(KKK xi) until
  - i := i+1
- end

specification

i := 0;
while true do
begin read(xi)

- send(xi) until a_1 recvd;
- send(a_2) until a_3 recvd;
- i := i + 1

end

- when x0 recvd s
- while true do
- begin write (xi)
  - send(a_1) until a_2
  - send(a_3) until xi
  - i := i+1
- end

Alternating Bit Protocol

clr(m,i) = m0 if i is even, m1 else

i := 0;
while true do
begin read(xi)

- send clr(xi,i) until clr(ack,i) recvd;
- i := i + 1

- when x0 recvd se
- while true do
- begin write (xi)
  - send clr(ack,i) u recvd;
  - i := i+1

Alternating bit protocol

- knowledge of depth 4 is essential
- provable:
  - S sends xi+1 →
  - K_S □ (R receives xi+1 → $K_R K_S K_R$(xi)

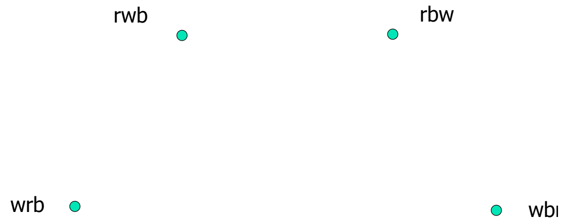
Card Games

- there are three cards: r, w and b
- three players: 1, 2 and 3
- every player sees its own card
- use names for worlds:
  - rwb for 1 has red, 2 white, 3 black, etc.
- use colors for accessibilities:

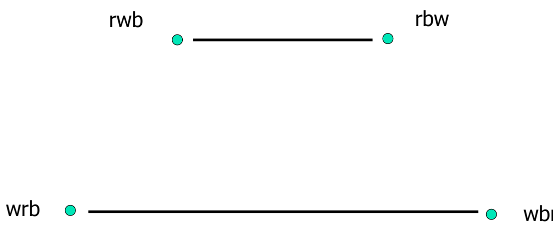
Card Games (ctd)

- draw the appropriate $S5_{(3)}$ Kripke mo
- show that in rwb it holds that:
  - $K_1 r_1$
  - $K_1(K_2 \neg r_2) \wedge K_1(\neg K_2 r_1 \wedge \neg K_2 r_3)$

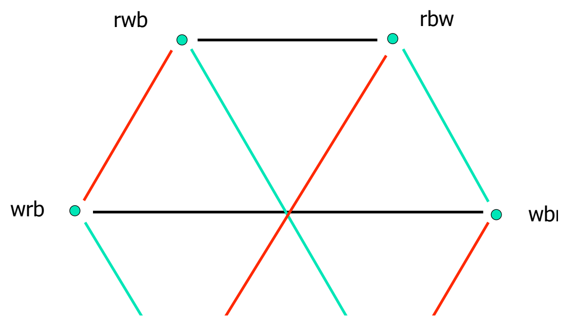
Card Games: HEXA



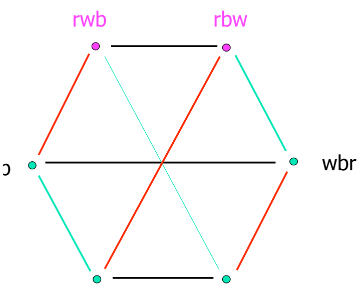
Card Games: HEXA



Card Games: HEXA

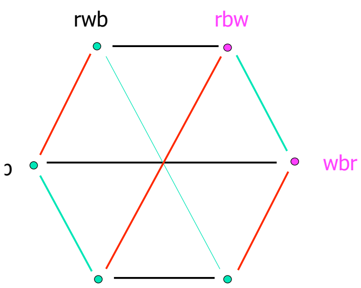


Properties of HEXA



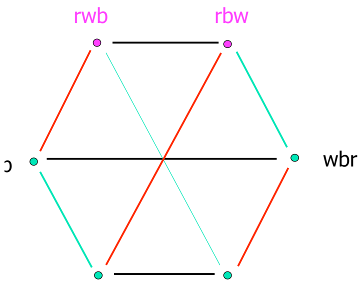
- M, rwb |= K_1r
  - M, rwb |= r_1
  - M, rbw |= r_1

Properties of HEXA



- $K_1(K_2 \neg r_2) \wedge K_1(\neg K_2 r_1$
- M,rwb |= $K_1 K_2 \neg r_2$, si
  - M,rwb |= $K_2 \neg r_2$, since
    - M,rwb |= $\neg r_2$ and
    - M,bwr |= $\neg r_2$
  - M,rbw |= $K_2 \neg r_2$, since
    - M,rwb |= $\neg r_2$ and
    - M,bwr |= $\neg r_2$

Properties of HEXA



- $K_1(K_2\neg r_2) \wedge K_1(\neg K_2 r_1 \wedge$ -
- M,rwb |= $K_1(\neg K_2 r_1 \wedge \neg K$
- since
  - M,rwb |= $\neg K_2 r_1 \wedge \neg K_2 r_3$ s
    - M,bwr |= $\neg r_1$ and
    - M,rwb |= $\neg r_3$
  - M,rbw |= $\neg K_2 r_1 \wedge \neg K_2 r_3$ si
    - M,wbr |= $\neg r_1$ and
    - M,rbw |= $\neg r_3$

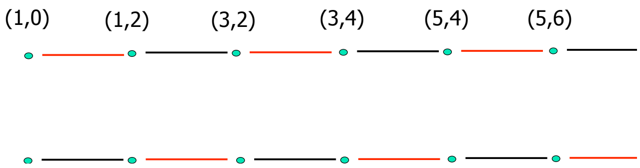
Exercise 3

- Ann and Bob each have a numbe their head: Ann can only see Bob who can only see Ann's. Howeve known by everybody that the nu are successors of each other, i.e. are n and n + 1 for some n.
- Draw the appropriate model.

Exercise 3

A:
B:

(x,y): A carries x, B

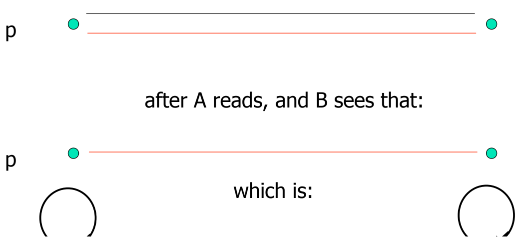


Exercise 4

- Ann and Bob are in a bar, in fron them is an envelop for Ann, with an invitation to go out in Amsterd (p) or one to give a lecture (¬p)
  - Draw the corresponding Kripke mod nobody has looked in the envelop y
  - Suppose A reads the letter in the en

Exercise 4

A:
B:



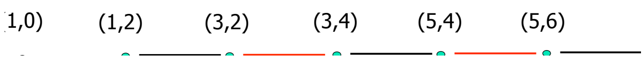
Exercise 5

let a_n be: "An has number n",similarly for b_n "Bob has number n
5a Show: M, (3,4) |= $\neg K_B b_4 \wedge K_A \neg K_B b_4$

let $K_A a$ denote: A knows what her number is, similarly for $K_B b$

5b Show: M,(1,2) |= $M_B K_A a$, or equivalently: M,(3,4) |= $\neg K_B \neg K_A a$

5c Show: M,(3,4) |= $M_B M_A M_B K_A a$, or equivalently: M,(3,4) |= $\neg K_B$k



Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
he real world is (3,4). Call the model M (see below).

5a. Show M, (3,4) |=¬ $M_BM_AK_Bb$ ∧ $M_BM_AM_BK_Aa$

5b. Suppose Ann says: I don't know my number
Draw the new model M_1. Show M_1, (3,4) |= ¬M_BK_Aa ∧ $M_BM_AK_Bb$

5c. Suppose now Bob says: I don't know my number
Draw the new model M_2. Show M_2, (3,4) |= ¬K_Bb ∧ M_BK_Aa

5d. Suppose now Ann says: I don't know my number
Draw the new model M_3. Show M_3, (3,4) |= K_Bb !!

Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
eal world is (3,4). Call the model M (see below).

5a. Show M, (3,4) |=¬ $M_BM_AK_Bb$ ∧ $M_BM_AM_BK_Aa$

First of all, note that K_Bb is true nowhere: Bob is uncertain everywhere
This explains M, (3,4) |=¬ $M_BM_AK_Bb$ (in fact M,x |=¬ $M_BM_AK_Bb$ for all

Moreover, K_Aa is true only in (1,0). From (3,4) there is a B-A-B path t

Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
eal world is (3,4). Call the model M (see below).

5a. Show M, (3,4) |=¬ $M_BM_AK_Bb$ ∧ $M_BM_AM_BK_Aa$

Moreover, K_Aa is true only in (1,0). From (3,4) there is a B-A-B path t
More precisely:

M, (1,0) |= K_Aa
M, (1,2) |= M_BK_Aa
M, (3,2) |= $M_AM_BK_Aa$
M, (3,4) |= $M_BM_AM_BK_Aa$

Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
eal world is (3,4). Call the model M (see below).

5a. Show M, (3,4) |=¬ $M_BM_AK_Bb$ ∧ $M_BM_AM_BK_Aa$

First of all, note that K_Bb is true nowhere: Bob is uncertain everywhere
This explains M, (3,4) |=¬ $M_BM_AK_Bb$ (in fact M,x |=¬ $M_BM_AK_Bb$ for all

Moreover, K_Aa is true only in (1,0). From (3,4) there is a B-A-B path t
so, M, (3,4) |= $M_BM_AM_BK_Aa$

Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
he real world is (3,4). Call the model M (see below).

5b. Suppose Ann says: I don't know my number
Draw the new model M_1. Show M_1, (3,4) |= ¬M_BK_Aa ∧ $M_BM_AK_Bb$

There is no point at which K_Aa holds, so M_1, (3,4) |= ¬M_BK_Aa

K_Bb is true at (1,2), and there is a B-A path to (1,2), hence
M_1, (3,4) |=$M_BM_AK_Bb$

M_1, (1,2) |= K_Bb, thus M_1, (3,2) |= M_AK_Bb thus M_1, (3,4) |= $M_BM_AK_Bb$

Exercise 6

et a_n be: "An has number n",similarly for b_n "Bob has number n. Supp
he real world is (3,4). Call the model M_2 (see below).

5c. Suppose now Bob says: I don't know my number
Draw the new model M_2. Show M_2, (3,4) |= ¬K_Bb ∧ M_BK_Aa

There is no point where K_Bb is true, hence (3,4) |= ¬K_Bb

K_Aa is true at (3,2), hence (3,4) |= M_BK_Aa

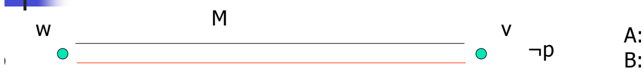
Exercise 6

etia$_n$ be: "An has number n",similarly for b_n "Bob has number n. Supp
he real world is (3,4). Call the model M_3 (see below).

5d. Suppose now Ann says: I don't know my number
Draw the new model M_3. Show M_3, (3,4) |= $K_B b$!!

This is clear: in (3,4), Bob has no doubt!

Exercise 7



or any item, start from M again.

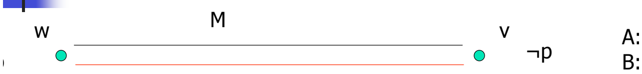
a. Suppose Ann reads the letter aloud: it says p! Draw the model M_1

b. Bob holds it for possible that A read the letter. Draw M_2

c. An outsider tells A and B that one of them has read the letter. Draw

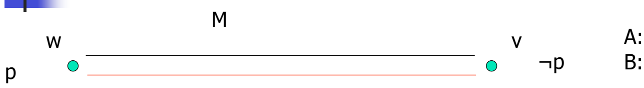
d. An outsider tells A and B that one of them may have read the letter

Exercise 7

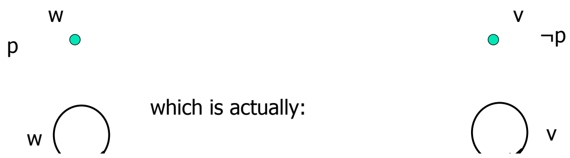


a. Suppose Ann reads the letter aloud: it says p! Draw the model M_1

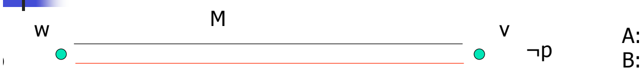
Exercise 7



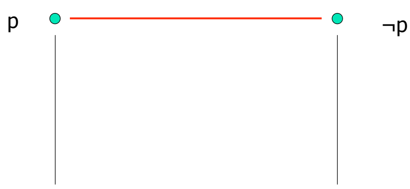
a. Suppose Ann reads the letter aloud: it says p! Draw the model M_1



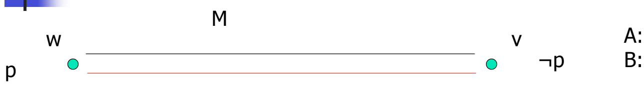
Exercise 7



b. Bob holds it for possible that A read the letter. Draw M_2

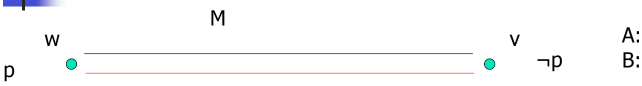


Exercise 7

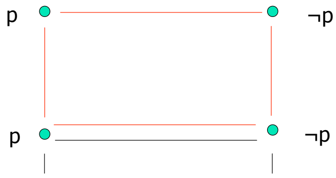


c. An outsider tells A and B that one of them has read the letter. Draw

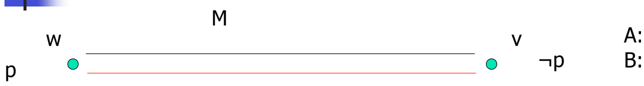
Exercise 7



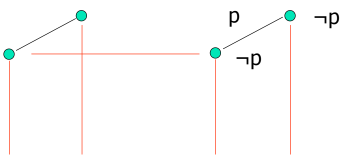
d. An outsider tells A and B that one of them may have read the letter



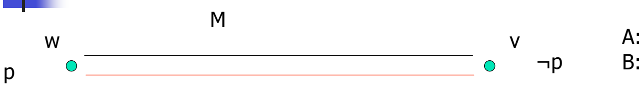
Exercise 7



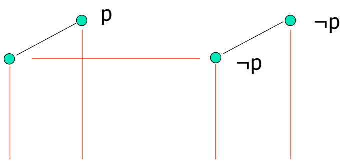
e. An outsider tells A and B that some (0, 1 or 2) of them may have re



Exercise 7



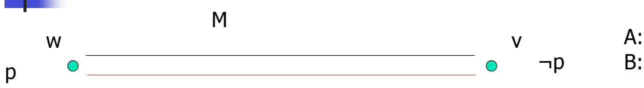
e. An outsider tells A and B that some (0, 1 or 2) of them may have re



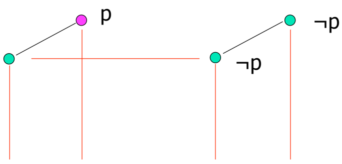
Suppose only B read the

$K_Bp \wedge M_B K_Ap \wedge M_B \neg K_Ap$

Exercise 7



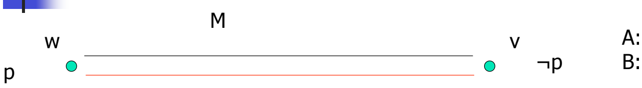
e. An outsider tells A and B that some (0, 1 or 2) of them may have re



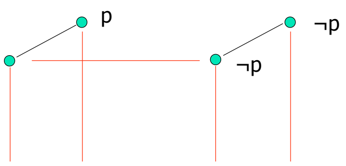
Suppose A and B read th

$K_Bp \wedge K_Ap \wedge M_B \neg K_Ap \wedge$ M

Exercise 7



e. An outsider tells A and B that some (0, 1 or 2) of them may have re



Suppose nobody read the

$\neg K_Bp \wedge \neg K_Ap \wedge M_B K_Ap \wedge$

Different Modal Systems

- Propositional Tautologies — A1
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$ — A2
- $K_i\phi \rightarrow \phi$ — A3
- $K_i\phi \rightarrow K_iK_i\phi$ — A4
- $\neg K\phi \rightarrow K\neg K\phi$ — A5
- $\vdash \phi \Rightarrow \vdash K_i\phi$ — Nec

Different Modal Systems

- K ▪ $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$ A2
- T ▪ $K_i\phi \rightarrow \phi$ A3
- 4 ▪ $K_i\phi \rightarrow K_iK_i\phi$ A4
- 5 ▪ $\neg K_i\phi \rightarrow K_i\neg K_i\phi$ A5

Different Modal Systems

- Propositional tautologies, Nec
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
- $K_i\phi \rightarrow \phi$
- $K_i\phi \rightarrow K_iK_i\phi$
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$

K(m) **T(m)** **S**

Different Modal Systems

- Propositional tautologies, Nec
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
- $\neg K_i\bot$
- $K_i\phi \rightarrow K_iK_i\phi$
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$

K(m) **KD(m)** **KD4(**

Different Semantic Systen

- Kripke Models
- Accessibility Relations R_i
- R_i is reflexive
- R_i is transitive
- R_i is Euclidean

$\mathcal{K}_{(m)}$ $\mathcal{T}_{(m)}$ $\mathcal{S}4$

Different Semantic Systen

- Kripke Models
- Accessibility Relations R_i
- R_i is serial
- R_i is transitive
- R_i is Euclidean

$\mathcal{K}_{(m)}$ $\mathcal{KD}_{(m)}$ $\mathcal{KD}4_{(m)}$

Relating the Systems

$\models \varphi \Rightarrow \mathcal{KD}_{(m)} \models \varphi \Rightarrow \mathcal{T}_{(m)} \models \varphi \Rightarrow \mathcal{S}4_{(m)} \models \varphi \Rightarrow$

⇕ ⇕ ⇕ ⇕

$) \vdash \varphi \Rightarrow \mathbf{KD}_{(m)} \vdash \varphi \Rightarrow \mathbf{T}_{(m)} \vdash \varphi \Rightarrow \mathbf{S4}_{(m)} \vdash \varphi \Rightarrow$

Example Derivation

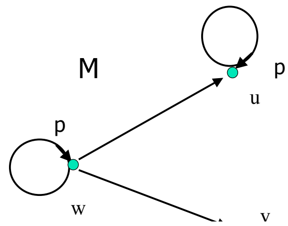
S5$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$

- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
- $K_i\neg K_i\phi \rightarrow \neg K_i\phi$
- $\neg K_i\phi \leftrightarrow K_i\neg K_i\phi$

Counterexamples

S4$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$?

Answer is NO! Because $S4_{(m)} \not\models \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$



M, $\not\models$ $\neg K_i\phi \leftrightarrow K_i\neg$I

Because

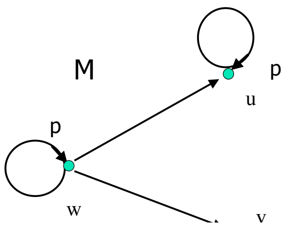
M,w $\models$ $\neg K_i p$

Because M,v $\models$

Counterexamples

S4$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$?

Answer is NO! Because $S4_{(m)} \not\models \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$



M $\not\models$ $\neg K_i\phi \leftrightarrow K_i\neg$I

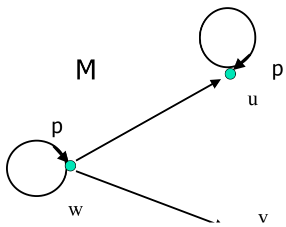
Because

M,w $\models$ $\neg K_i$p, and
M,w $\models$ $\neg K_i\neg K_i$p

Counterexamples

S4$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$?

Answer is NO! Because $S4_{(m)} \not\models \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$



M $\not\models$ $\neg K_i\phi \leftrightarrow K_i\neg$I

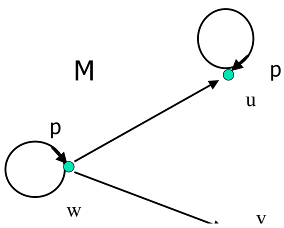
Because

M,w $\models$ $\neg K_i$p, and
M,w $\models$ $\neg K_i\neg K_i$p

Counterexamples

S4$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$?

Answer is NO! Because $S4_{(m)} \not\models \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$



M $\not\models$ $\neg K_i\phi \leftrightarrow K_i\neg$I

and

M $\in S4_{(m)}$

Validities

We already derived: **S5**$_{(m)}$ $\vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$
We could also have proved: $S5_{(m)} \models \neg K_i\phi \leftrightarrow K_i\neg K_i$

t of all, $\neg K_i\phi \leftrightarrow K_i\neg K_i\phi$
quivalent to $\neg\neg K_i\phi \leftrightarrow \neg K_i\neg K_i\phi$
quivalent to $K_i\phi \leftrightarrow \neg K_i\neg K_i\phi$
quivalent to $K_i\phi \leftrightarrow M_iK_i\phi$

Validities

We already derived: $\mathbf{S5_{(m)}} \vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$
We could also have proved: $\mathcal{S5}_{(m)} \models \neg K_i\phi \leftrightarrow K_i\neg K_i$

First of all, $\neg K_i\phi \leftrightarrow K_i\neg K_i\phi$ is equivalent to $K_i\phi \leftrightarrow M_i$

.et M $\in \mathcal{S5}_{(m)}$ and w a world in M. To prove: M,w $\models K_i\phi$

Suppose M,w $\models K_i\phi$

Since R_i is reflexive, we have $R_i$ww and hence M,w $\models M_iK_i\phi$

This proves M,w $\models K_i\phi \rightarrow M_iK_i\phi$

Validities

We already derived: $\mathbf{S5_{(m)}} \vdash \neg K_i\phi \leftrightarrow K_i\neg K_i\phi$
We could also have proved: $\mathcal{S5}_{(m)} \models \neg K_i\phi \leftrightarrow K_i\neg K_i$

First of all, $\neg K_i\phi \leftrightarrow K_i\neg K_i\phi$ is equivalent to $K_i\phi \leftrightarrow M_i$

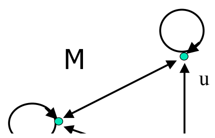
.et M $\in \mathcal{S5}_{(m)}$ and w a world in M. To prove: M,w $\models K_i\phi$

uppose M,w $\models M_iK_i\phi$

here is u, $R_i$wu and M,u $\models K_i\phi$

ake v, $R_i$wv. To prove: M,v $\models \phi$

ince R_i is Euclidean, we have $R_i$uv. So M,v $\models \phi$



Tactics

Let $\mathbf{X_{(m)}}$ be any logic, for which $\mathbf{X_{(m)}} \vdash \varphi \Leftrightarrow \mathcal{X}_{(m)} \models \varphi$

To prove $\mathbf{X_{(m)}} \vdash \psi$
either use the axioms and rules of $\mathbf{X_{(m)}}$
or use completeness and show $\mathcal{X}_{(m)} \models \varphi$

To prove $\mathbf{X_{(m)}} \not\vdash \psi$

Tactics

Let $\mathbf{X_{(m)}}$ be any logic, for which $\mathbf{X_{(m)}} \vdash \varphi \Leftrightarrow \mathcal{X}_{(m)} \models \varphi$

A formula ψ is $\mathcal{X}_{(m)}$-satisfiable if there is a M $\in \mathcal{X}_{(m)}$ so that M,w $\models \psi$

A formula ψ is $\mathbf{X_{(m)}}$–consistent if
$\mathbf{X_{(m)}} \not\vdash \neg\psi$ if
$\mathcal{X}_{(m)} \not\models \neg\psi$ if

Tactics

Let $\mathbf{X_{(m)}}$ be any logic, for which $\mathbf{X_{(m)}} \vdash \varphi \Leftrightarrow \mathcal{X}_{(m)} \models \varphi$

A formula ψ is $\mathcal{X}_{(m)}$-valid if
for all M $\in \mathcal{X}_{(m)}$: M,w $\models \psi$

A formula ψ is $\mathbf{X_{(m)}}$–derivable if
$\mathbf{X_{(m)}} \vdash \psi$ if

Exercise 8

Are the following formulas valid with respect to $\mathbf{K_{(m)}}$? $\mathbf{T_{(m)}}$? $\mathbf{S4_{(m)}}$? $\mathbf{S5_{(m)}}$?

(a) $\phi \rightarrow K_i\phi$
(b) $\phi \rightarrow K_i\neg K_i\neg\phi$
(c) $K_i\phi \rightarrow \neg K_i\neg\phi$
(d) $\neg K_i\phi \rightarrow K_i\neg\phi$

Group Notionss

W. van der Hoek

epistemic logic

- $K(\phi \rightarrow \psi) \rightarrow (K$
  - *agents reason r*
- $K\phi \rightarrow \phi$
  - *veridicality*
- $K\phi \rightarrow KK\phi$
  - *positive introsp*
- $\neg K\phi \rightarrow K\neg K\phi$
  - *negative introsp*
- $\vdash \phi \Rightarrow \vdash K\phi$
  - *agents know tau*

Everybody knows

- $E\varphi$: Everybody knows φ
- definition: $E\varphi \equiv K_1\varphi \wedge K_2\varphi \wedge \ldots K_n\varphi$
- veridical? introspective?

Distributed knowledge

- $D\varphi$: it is distributed knowledge that
- idea: $(K_1\varphi \wedge K_2(\varphi \rightarrow \psi)) \rightarrow D\psi$
- veridical? introspective?
- `wise man' to whom everybody tells
- also called "implicit knowledge" ($I\varphi$)

Group notions

- $E\phi \equiv K_1\phi \wedge K_2\phi \wedge \ldots \wedge K_n\phi$
  - *everybody knows* φ
- $K_i\phi \rightarrow D\phi$
  - *if one knows it, it is distributed*
- $D(\phi \rightarrow \psi) \rightarrow (D\phi \rightarrow D\psi)$
- $D\phi \rightarrow \phi$
- $D\phi \rightarrow DD\phi$
- $\neg D\phi \rightarrow D\neg D\phi$

- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi$
  - *agents reason rat*
- $K_i\phi \rightarrow \phi$
  - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
  - *positive introspec*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
  - *negative introspec*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
  - *agents know tauto*

Distributed knowledge

- Consider the following derivation rule:

$$\text{D} \quad \frac{(\varphi_1 \wedge \varphi_2 \wedge \ldots\ldots \wedge \varphi_n) \rightarrow \psi)}{(K_1\varphi_1 \wedge K_2\varphi_2 \ldots\ldots \wedge K_n\varphi_n) \rightarrow D\psi}$$

dding RD as a rule or $K_i\phi \rightarrow D\phi$ as an axiom is equ

Group notions: semantics

- $E\phi \equiv K_1\phi \wedge K_2\phi \wedge \ldots K_n\phi$
  - *everybody knows φ*
- $K_i\phi \rightarrow D\phi$
  - *if one knows it, it is distributed*
- $R_E = R_1 \cup R_2 \cup$ ..
  - *taking the union*
- $R_D \subseteq R_1 \cap R_2 \cap$ ..
  - *not an equivalenc*

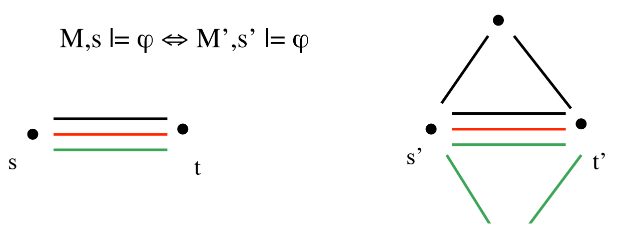
Group notions: semantics

R_1, R_2, R_D

$V(t) = V'(t) = V'(t1) = V'(t2)$

$M,s \models \varphi \Leftrightarrow M',s' \models \varphi$

- $R_D \subseteq R_1 \cap R_2 \cap$ ..
  - *not an equivalenc*



Multi-agent knowledge

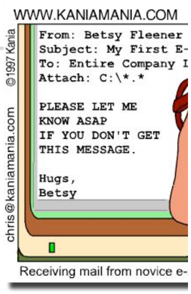
K_A a: A knows a

B sends m to A

K_B m ?

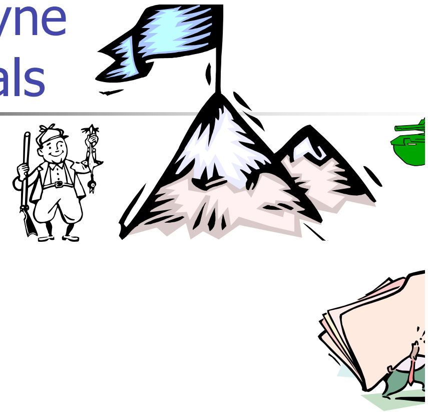
K_AK_B m?

$K_BK_AK_B$ m?



Bizantyne Generals

A



K_Am

Common Knowledge

- $C(\phi \rightarrow \psi) \rightarrow (C\,\phi \rightarrow C\,\psi)$
  - *agents reason rationally*
- $C\phi \rightarrow \phi$
  - *veridicality*
- $C\phi \rightarrow EC\,\phi$
  - *and vice versa*
- $\vdash \phi \Rightarrow \vdash C\phi$
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi$
  - *agents reason rati*
- $K_i\phi \rightarrow \phi$
  - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
  - *positive introspec*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
  - *negative introspe*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
  - *agents know tautc*

Common Knowledge

- $C(\phi \rightarrow \psi) \rightarrow (C\,\phi \rightarrow C\,\psi)$
  - *agents reason rationally*
- $C\phi \rightarrow \phi$
  - *veridicality*
- $C\phi \rightarrow EC\,\phi$
  - *and vice versa*
- $C(\phi \rightarrow E\psi) \rightarrow (\phi \rightarrow C\psi)$
  - *"induction"*
- $\vdash \phi \Rightarrow \vdash C\phi$
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi$
  - *agents reason rati*
- $K_i\phi \rightarrow \phi$
  - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
  - *positive introspec*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
  - *negative introspe*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
  - *agents know tautc*

Common Knowledge

- $C(\phi \to \psi) \to (C\phi \to C\psi)$
  - *agents reason rationally*
- $C\phi \to \phi$
  - *veridicality*
- $C\phi \to EC\phi$
  - *and vice versa*
- $C(\phi \to E\psi) \to (\phi \to C\psi)$
  - *"induction"*
- $\vdash \phi \Rightarrow \vdash C\phi$

- Semantically, i
  boils down to
- $R_C = R_E^*$
- that is, the refl
  transitive closu

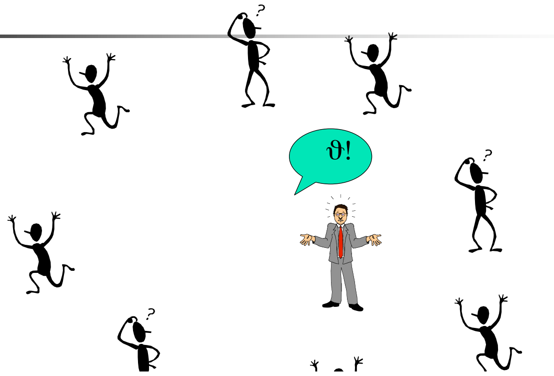
Common Knowledge

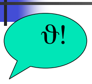
- Eφ: Everybody knows φ
- $E\varphi \not\to EE\varphi$
- Cφ: it is Common Knowledge that φ
- idea: Cφ = Eφ & EEφ & EEEφ & EEE
  & …..
- so: ¬Cφ if somebody
  - considers it possible that
    - somebody considers it possible that

Alco at a conference

- A is at a conference. He decides to leave the roo
  and have a drink at the bar.
  - There is an announcement φ: no talks tomorrow mor
    - E φ? C φ?
  - Then, A leaves the bar for a walk outside.
  - B says: "A is not here!" President: "intercom in bar!"
    - E φ? EE φ? C φ?
  - A is told all the above
    - E φ? EE φ? EEE φ? C φ?

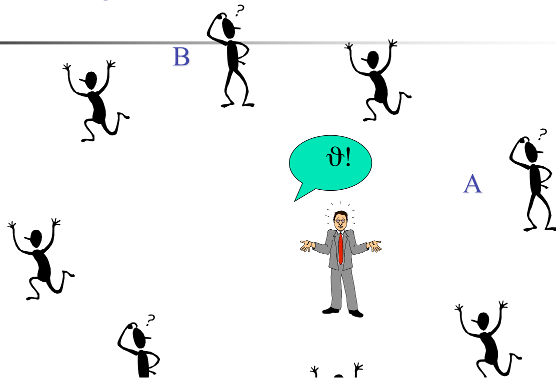
c children, m are muddy



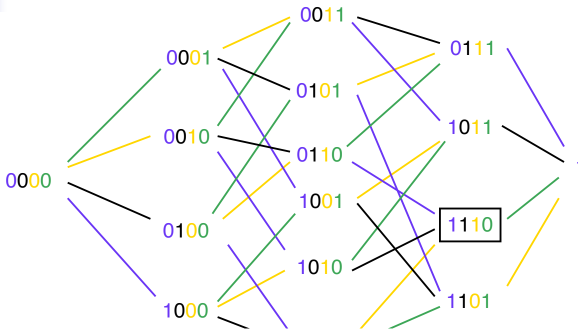


At least one of you is muddy.
If you know that you are, step forwar

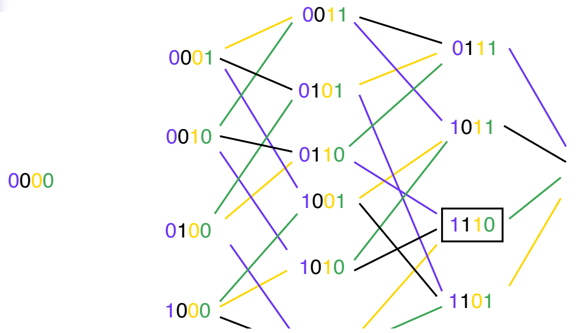
c = 8, m = 3



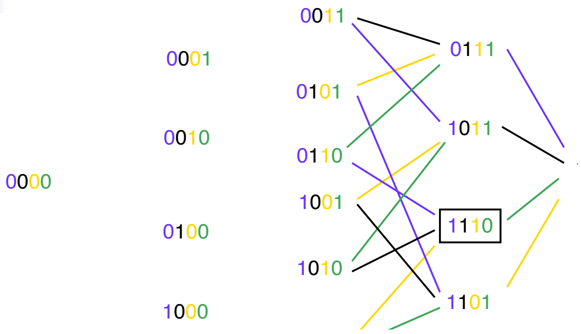
c = 4, m = 3 (Kripke mod



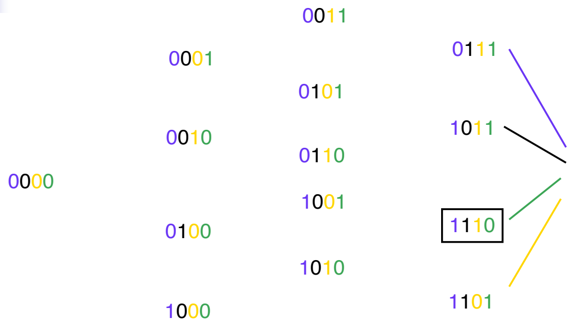
c = 4, m = 3 (Kripke mod



c = 4, m = 3 (Kripke mod



c = 4, m = 3 (Kripke mod



Group Knowledge

$K_1\varphi \wedge K_2(\varphi \rightarrow \psi) \rightarrow D\varphi$

$C\varphi \Rightarrow E\varphi \Rightarrow K_i\varphi \Rightarrow D\varphi \Rightarrow \varphi$

"any fool knows"

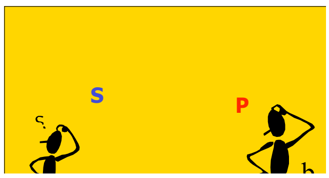
"a wise man knows"

Common Knowledge cannot be obtained through communica

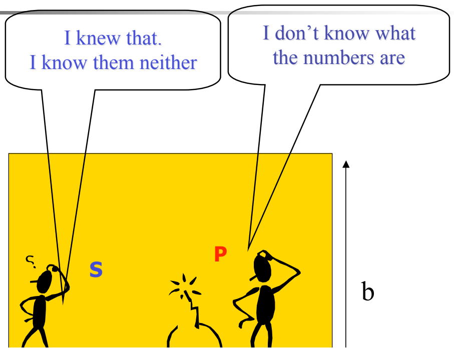
$C\varphi \leftrightarrow EC\varphi$

Ignorance

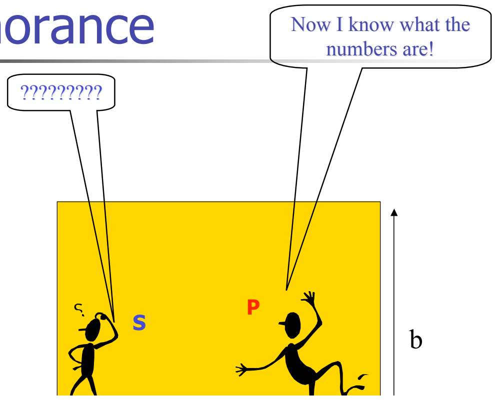
- P and S are in a room, l x b
- $2 \leq b \leq l \leq 99$
- P knows l x b
- S knows l + b



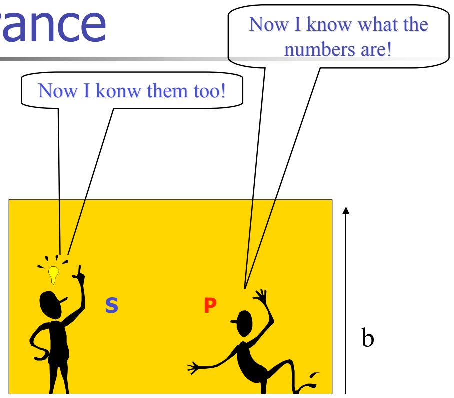
Ignorance



Ignorance



Ignorance



Advanced Byzantine Gene

- S and R are involved in a protoco
- It is common knowledge that:
- messages derive either immediat with ε time delay

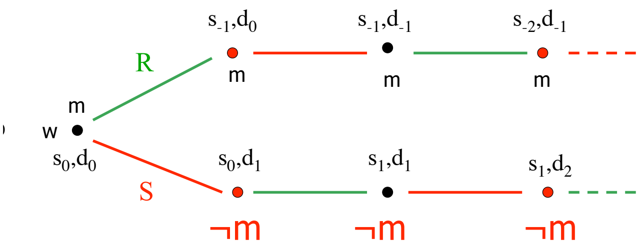
Advanced Byzantine Gene

- S and R are involved in a protocol
- It is common knowledge that:
  - messages derive either immediately or v time delay
- S sends m at t_0.
- When do we have Cm ???????

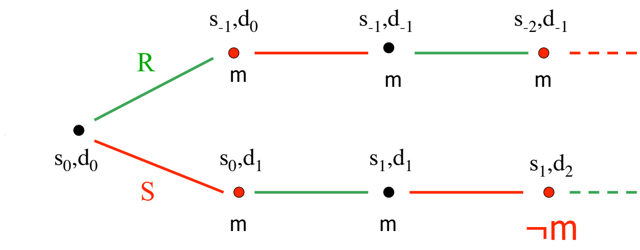
Advanced Byzantine Gene

- let s: "sent", d: "delivered" e: "delay"
- suppose there is no delay
- time: t_0, $t_1 = t_0 + \varepsilon$, ..., $t_n = t_0 + n\varepsilon$
- Sender is red, Receiver is green
- reflexive arrows are implicit
- • means delay, • means no delay
- m means: message has arrived

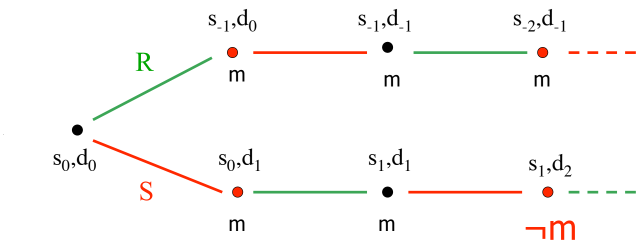
Advanced Byzantine Gene



Advanced Byzantine Gene



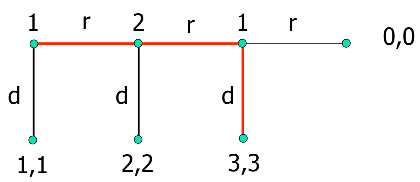
Advanced Byzantine Gene



Advance Byzantine Gener

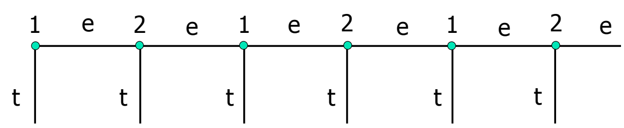
- S and R are involved in a protocol
- It is common knowledge that:
  - messages derive either immediately or
    time delay
- S sends m at t_0.
- When do we have Cm ???????

Backward Induction



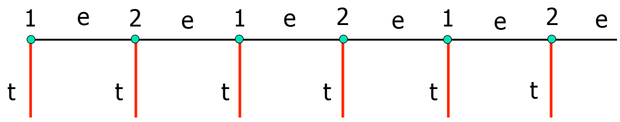
Centipede

- 1 and 2 divide n marbles; they choo
  turn, if somebody picks two, the ga
  over



Centipede

- Intuitively correct?



Gossiping

- six friends each have a gossip. They call each oth
- at each call, they share their information
- at least how many calls are needed to bring all of to date with respect to all the gossips?

7? 8? 9?

Common Knowledge

A7 $C\phi \rightarrow \phi$
- *veridicality*

A8 $C\phi \rightarrow EC\,\phi$
- *building iterations*

A9 $C(\phi \rightarrow \psi) \rightarrow (C\,\phi \rightarrow C\,\psi)$
- *agents reason rationally*

A10 $C(\phi \rightarrow E\psi) \rightarrow (\phi \rightarrow C\,\psi)$
- *"induction"*

R3 $\vdash \phi \Rightarrow \vdash C\phi$

- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow$
  - *agents reason rationa*
- $K_i\phi \rightarrow \phi$
  - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
  - *positive introspection*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
  - *negative introspectio*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
  - *agents know tautolog*

Different Modal Systems

1 Propositional tautologies, Nec
$K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
7 $C\phi \rightarrow \phi$
8 $C\phi \rightarrow EC\,\phi$
9 $C(\phi \rightarrow \psi) \rightarrow (C\,\phi \rightarrow C\,\psi)$
10 $C(\phi \rightarrow E\psi) \rightarrow (\phi \rightarrow C\,\psi)$
3 $\vdash \phi \Rightarrow \vdash C\phi$
} $\mathbf{KEC_{(m)}}$

$K_i\phi \rightarrow \phi$
} $\mathbf{TEC_{(m)}}$

$K_i\phi \rightarrow K_iK_i\phi$
} $\mathbf{S4EC_{(m)}}$

Lemma (X-distribution)

Let X be a necessity operator. Then:
$\mathbf{K_{(m)}} \vdash \phi \rightarrow \psi \Rightarrow \mathbf{K_{(m)}} \vdash X\phi \rightarrow X\psi$

Proof. Let X be a necessity operator.

suppose $\mathbf{K_{(m)}} \vdash \phi \rightarrow \psi$

then, by necessitation, $\mathbf{K_{(m)}} \vdash X(\phi \rightarrow \psi)$

we also have $\mathbf{K_{(m)}} \vdash X(\phi \rightarrow \psi) \rightarrow (X\phi \rightarrow X\psi)$

Iterations of Modal Opera

For any operator X, define $X^n\phi$ by induction on n:

$X^0\phi = \phi$
$X^{n+1}\phi = XX^n\,\phi$

Example:
$K_2^3\phi = K_2K_2K_2\phi$, $E^5\phi = EEEEE\phi$
and even $(K_2E)^4\phi = K_2E\,K_2E\,K_2E\,K_2E\,\phi$

First Property

Claim: for every n, **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^n\phi$

1 $C\phi \rightarrow \phi$ A7

hence,
$C\phi \rightarrow E^0\phi$ since $E^0\phi = \phi$, by definition of E^0

First Property

Claim: for every n, **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^n\phi$
suppose we already proven: **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^k\phi$

1	$C\phi \rightarrow E^k\phi$	ass
2	$C\phi \rightarrow EC\phi$	A8
3	$EC\phi \rightarrow EE^k\phi$	2, E-distr.
4	$C\phi \rightarrow EE^k\phi$	2,3,A1

hence,
$C\phi \rightarrow E^{(k+1)}\phi$ since $EE^k\phi = E^{(k+1)}\phi$, by definition of

First Property: winding up

KEC$_{(m)}$ $\vdash C\phi \rightarrow E^0\phi$

KEC$_{(m)}$ $\vdash C\phi \rightarrow E^1\phi$

if **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^k\phi$ then **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^{(k+1)}\phi$

KEC$_{(m)}$ $\vdash C\phi \rightarrow E^1\phi$ so **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^2\phi$

KEC$_{(m)}$ $\vdash C\phi \rightarrow E^2\phi$ so **KEC$_{(m)}$** $\vdash C\phi \rightarrow E^3\phi$

KEC$_{(m)}$ $\vdash C\phi \rightarrow$ .... so **KEC$_{(m)}$** $\vdash C\phi \rightarrow$ ....

Common Knowledge

$M,w \models E\phi \Leftrightarrow$
$\forall v(R_E wv \Rightarrow M,v \models \phi$
with $R_E = R_1 \cup R_2 \cup$ ..

Definition of closure:

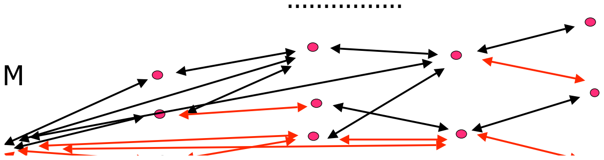
- $\forall x R_E^* xx$
- $R_E xy \Rightarrow R_E^* xy$
- $R_E^* xy \;\&\; R_E yz \Rightarrow R_E^* xz$

$M,w \models C\phi \Leftrightarrow$
$\forall v(R_E^* wv \Rightarrow M,v \models$
with R_E^* is reflexive tr
closure of R_E

Common Knowledge

ition of closure:
$\forall x R_E^* xx$
$R_E xy \Rightarrow R_E^* xy$
$R_E^* xy \;\&\; R_E yz \Rightarrow R_E^* xz$

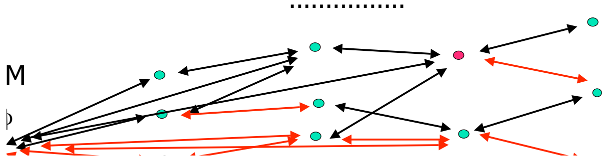
$M,w \models C\phi \Leftrightarrow$
$M,w \models \phi \;\&$
$\forall v(R_E wv \Rightarrow M,v \models \phi) \;\&$
$\forall v \forall u (R_E wv \;\&\; R_E vu \Rightarrow M,u \models$
$\forall v \forall u \forall t (R_E wv \;\&\; R_E vu \;\&\; R_E ut =$
....



Common Knowledge

ition of closure:
$\forall x R_E^* xx$
$R_E xy \Rightarrow R_E^* xy$
$R_E^* xy \;\&\; R_E yz \Rightarrow R_E^* xz$

$M,w \models \neg C\phi \Leftrightarrow$
$M,w \models \neg\phi$ or
$\exists v(R_E wv \;\&\; M,v \models \neg\phi)$ or
$\exists v \exists u (R_E wv \;\&\; R_E vu \;\&\; M,u \models \phi)$
$\exists v \exists u \exists t (R_E wv \;\&\; R_E vu \;\&\; R_E ut \;\&$
....



Soundness and Complete

Given the truth definition M,w|= Cϕ ⇔

∀v(R_E* wv ⇒ M,v |= ϕ)

KEC$_{(m)}$ |– ϕ ⇔ $\mathcal{K}_{(m)}$ |= ϕ

TEC$_{(m)}$ |– ϕ ⇔ $\mathcal{T}_{(m)}$ |= ϕ

S4EC$_{(m)}$ |– ϕ ⇔ $S4_{(m)}$ |= ϕ

S5EC$_{(m)}$ |– ϕ ⇔ $S5_{(m)}$ |= ϕ

Interpreted Systems

W. van der Hoek

Interpreted Systems

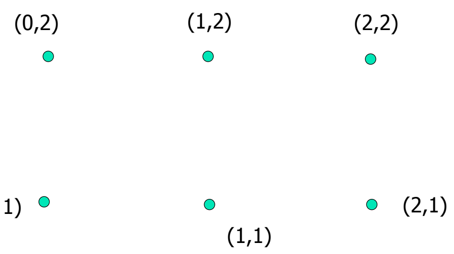
- We have m processors
- each i can be in a number of states ∈
- Now build M =<S,π,R_1, R_2, ..., R
  - S = L_1 x L_2 x .... x L_m
    - = { **s** = <s1, s2, ... sm> | si ∈ L_i
  - π: S → P → {t,f}
  - R = {(s,t) | s = t

ELATION!!

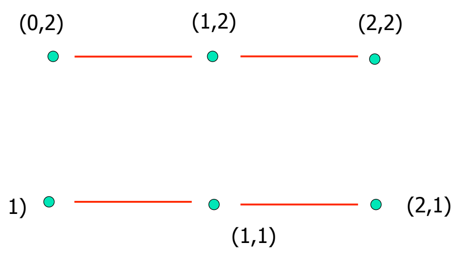
Interpreted Systems: Exa

- Two processors: A and B
- $L_A = L_B = \{0,1,2\}$
- S = L_A x L_B = { (0,0), (0,1), (0,2
- (1,0), (1,1), (1,2
- (1,0), (1,1), (1,2
- R_A **s t** ⇔ R_A (x_1,y_1) (x_2,y_2) ⇔ $x_1 = x_2$

Interpreted Systems: Exa



Interpreted Systems: Exa

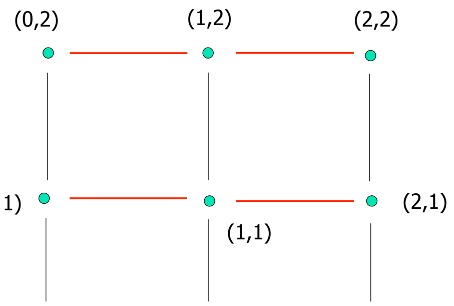


R_B **s t** ⇔

R_B (x_1,y_1) (x

$y_1 = y_2$

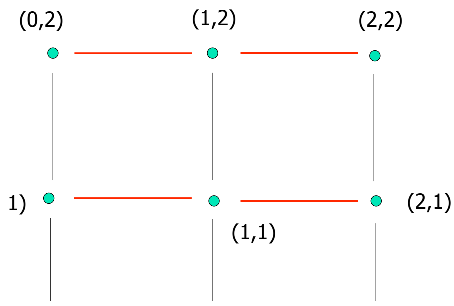
Interpreted Systems: Exa



R_B **s t** ⇔
R_B (x_1,y_1) (
$y_1 = y_2$

R_A **s t** ⇔
R_A (x_1,y_1) (

Interpreted Systems: Exa

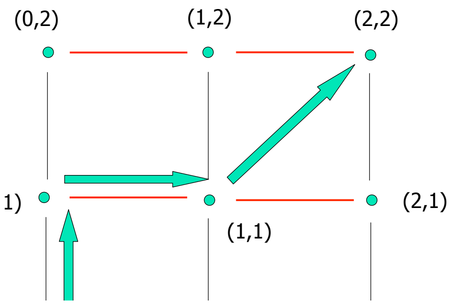


Atoms:
x=0; x=1; x=2 a
y=0; y=1; y=2

M,(0,0) |= K_A

M,(0,0) |= K_A

Interpreted Systems: Run

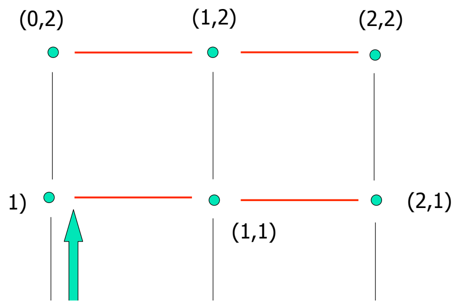


Starting in (0,0), B ch
its value from 0 to 1
A does not notice this
the same in (0,0) and

Then, A adds 1 to its
B knowing this

Finally, both A and B
computation step: bot
value

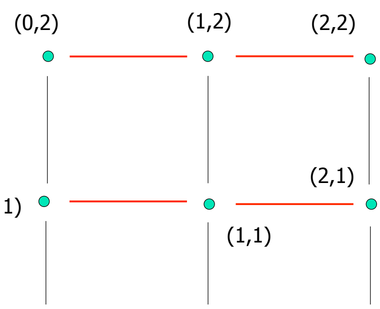
Distr. Systems: Exercise 9



Starting in (0,0), B ch
its value from 0 to 1
A does not notice this
the same in (0,0) and

Formulate what it me
does not notice, and t
the claim

Exercise 10



Atoms:
x=0; x=1; x=2 and
y=0; y=1; y=2

R_A and R_B are reflex
and transitive

11a. show:
M,(0,0) |= E(x=0 v

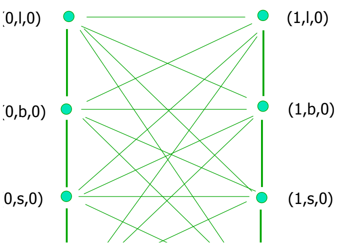
11b. show, for every
M,(0,0) |= EEϕ ⇔

Intr. Systems: Example 2

- Three processors: A, F and T
- L_A = {n, s, b, l}, L_F = {0,1}, L_T =
- use atoms a=s, f=0, t=7, etc, in <f,a,t
- Make a drawing of this system, and s
- M,(1,n,2) |= $M_F K_T$(t=0)

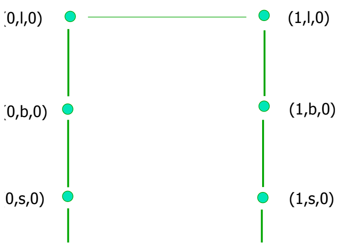
IS: Example 2

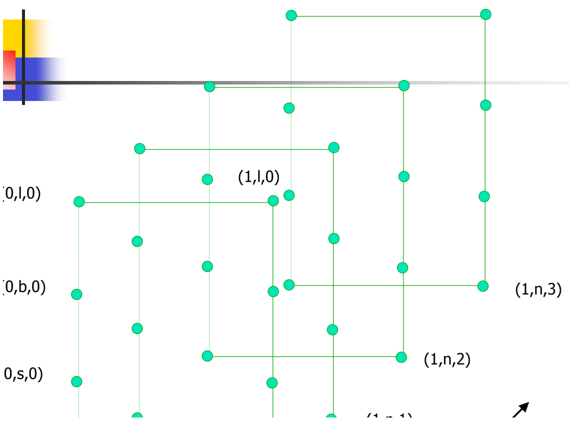
fix t = 0

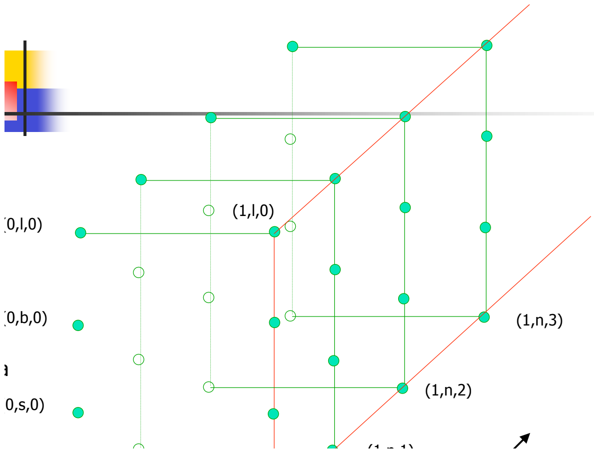


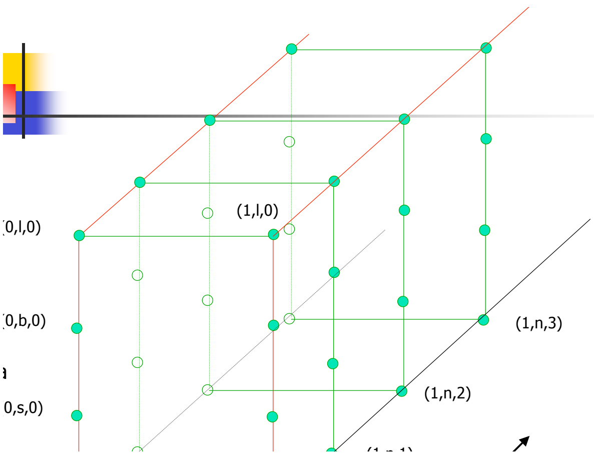
wich we draw as:

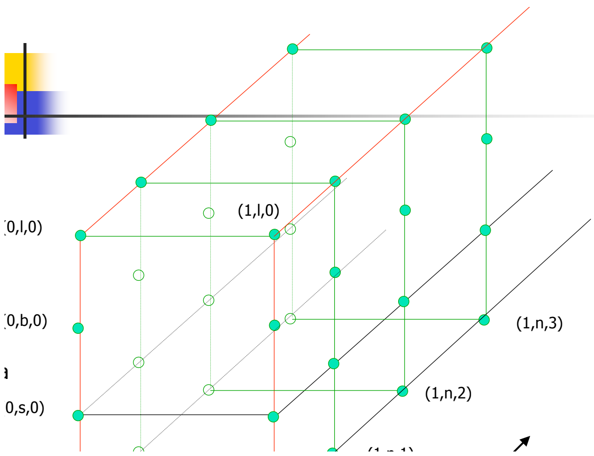
IS: Example 2

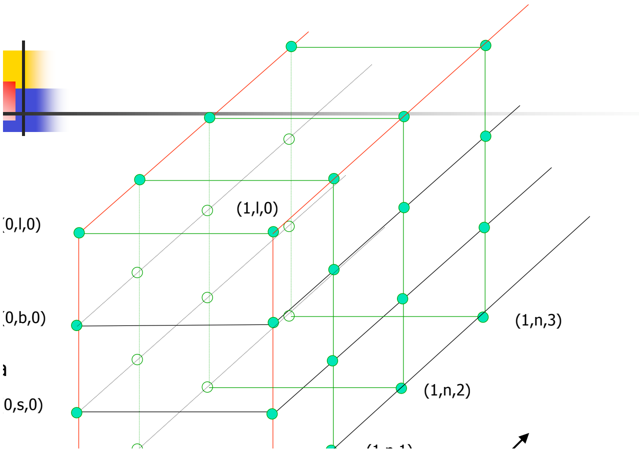


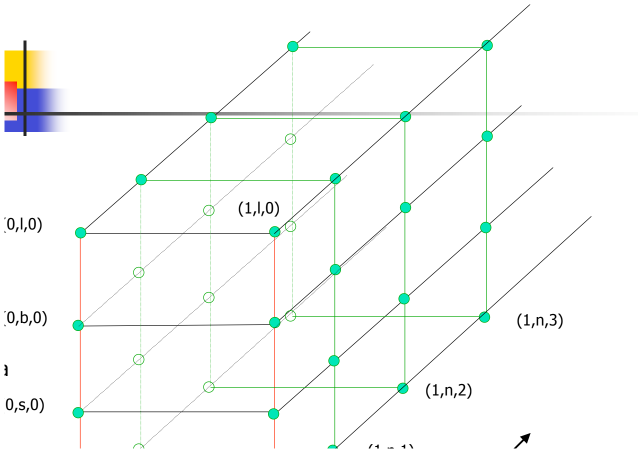


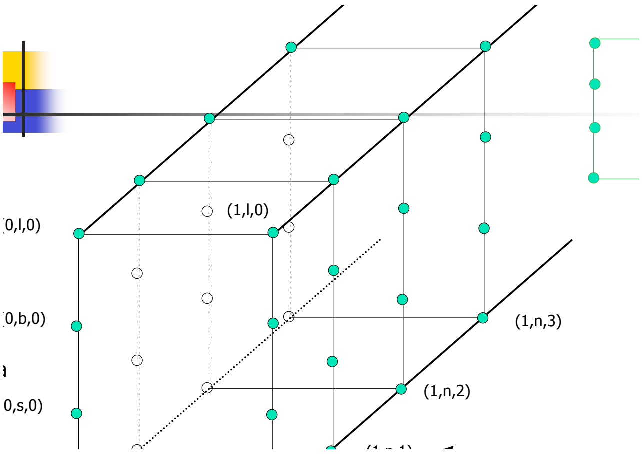


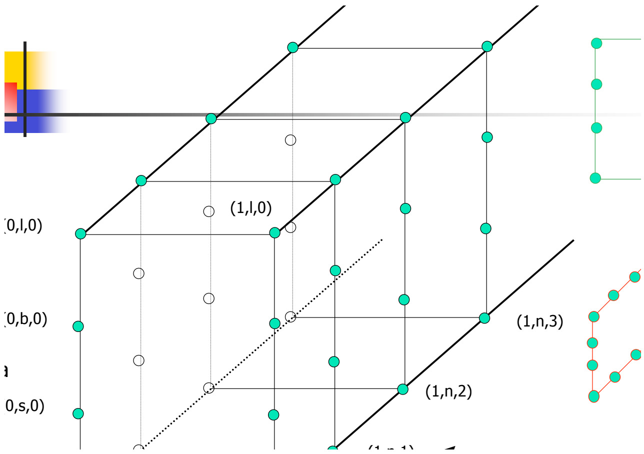


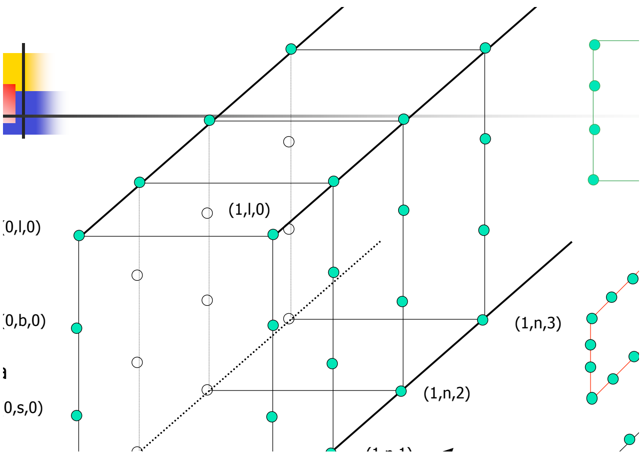


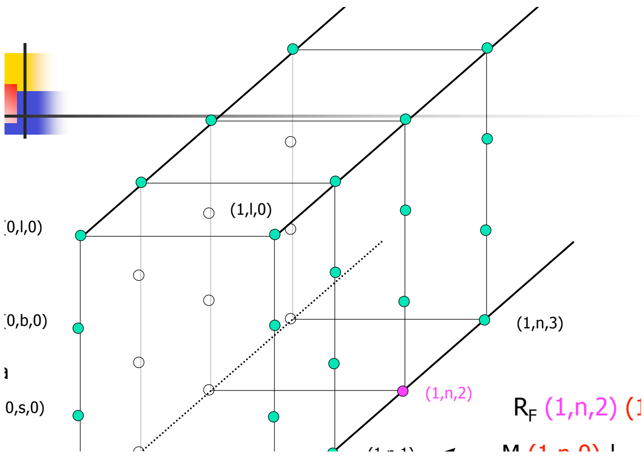

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)

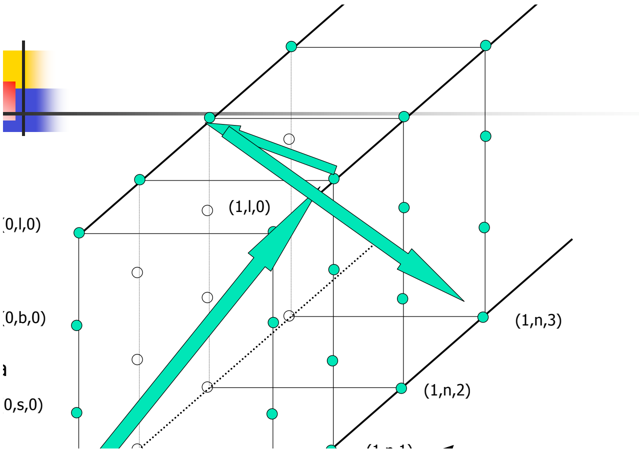

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)

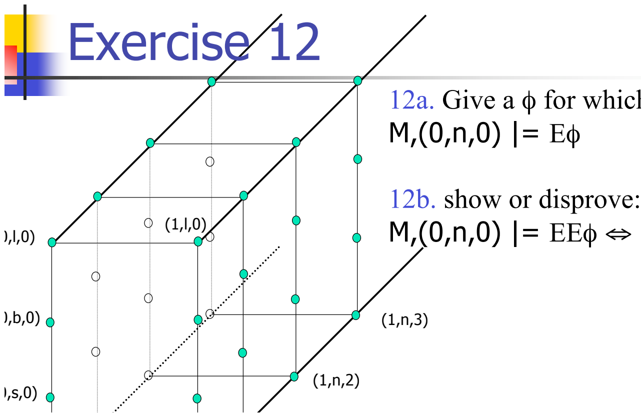

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)

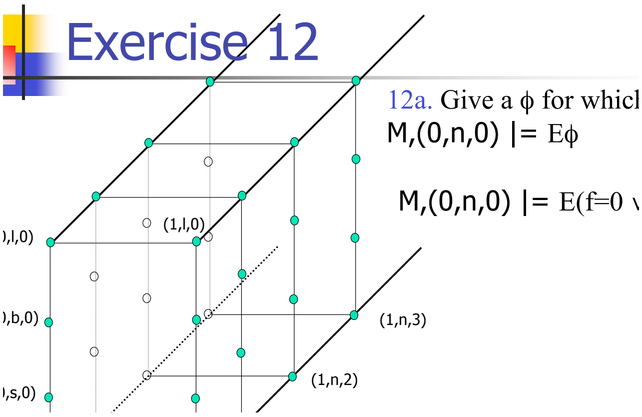

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)

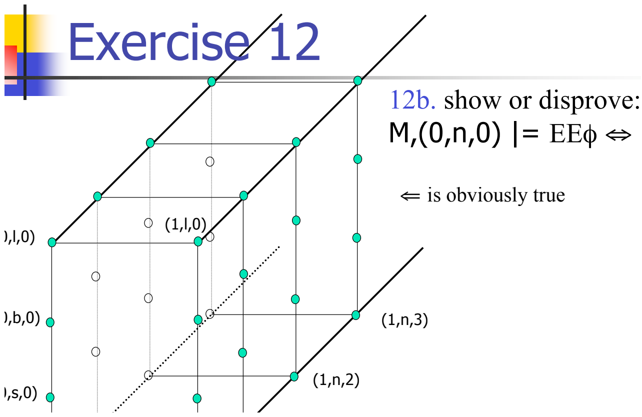

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)

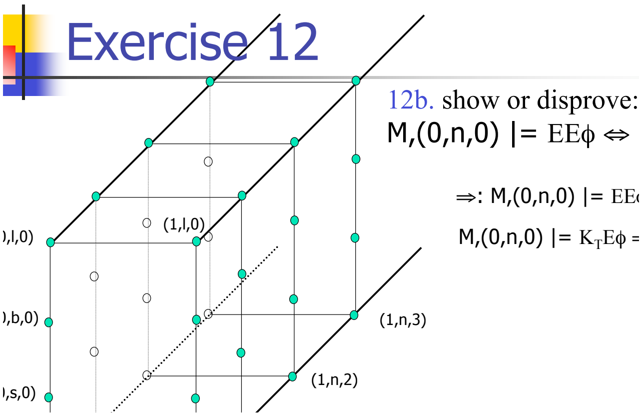

(1,l,0)
0,l,0)
0,b,0)
0,s,0)
(1,n,3)
(1,n,2)
R_F (1,n,2)

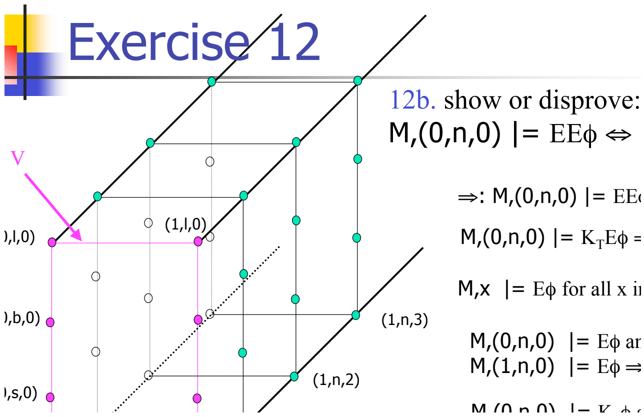

(0,l,0)
(0,b,0)
0,s,0)
(1,l,0)
(1,n,3)
(1,n,2)


Exercise 12
12a. Give a ϕ for whicl
M,(0,n,0) |= Eϕ
12b. show or disprove:
M,(0,n,0) |= EEϕ ⇔
),l,0)
),b,0)
),s,0)
(1,l,0)
(1,n,3)
(1,n,2)

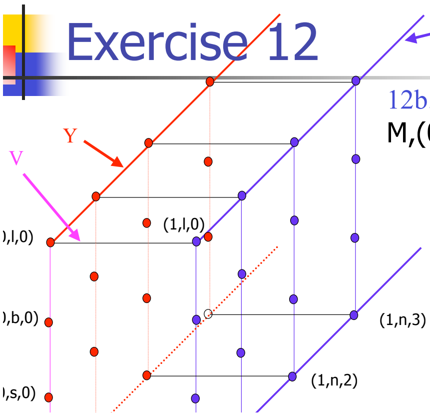

Exercise 12
12a. Give a ϕ for whicl
M,(0,n,0) |= Eϕ
M,(0,n,0) |= E(f=0 ∨
),l,0)
),b,0)
),s,0)
(1,l,0)
(1,n,3)
(1,n,2)


Exercise 12
12b. show or disprove:
M,(0,n,0) |= EEϕ ⇔
⇐ is obviously true
),l,0)
),b,0)
),s,0)
(1,l,0)
(1,n,3)
(1,n,2)


Exercise 12
12b. show or disprove:
M,(0,n,0) |= EEϕ ⇔
⇒: M,(0,n,0) |= EE
M,(0,n,0) |= K_T Eϕ =
),l,0)
),b,0)
),s,0)
(1,l,0)
(1,n,3)
(1,n,2)


Exercise 12
12b. show or disprove:
M,(0,n,0) |= EEϕ ⇔
⇒: M,(0,n,0) |= EE
M,(0,n,0) |= K_T Eϕ =
M,x |= Eϕ for all x i
M,(0,n,0) |= Eϕ ar
M,(1,n,0) |= Eϕ ⇒
V
),l,0)
),b,0)
),s,0)
(1,l,0)
(1,n,3)
(1,n,2)

Exercise 12



12b. show or disprove:
M,(0,n,0) |= EEϕ ⇔

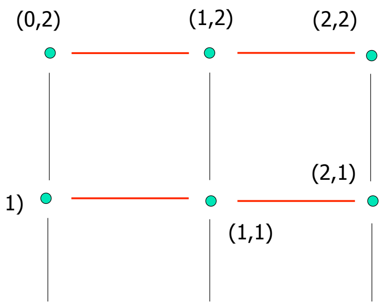
⇒: M,(0,n,0) |= EE

M,(0,n,0) |= K_TEϕ =

M,x |= Eϕ for all x i

M,(0,n,0) |= Eϕ ar
M,(1,n,0) |= Eϕ ⇒

Exercise 13



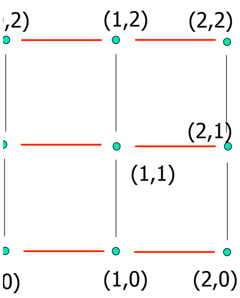
Atoms:
x=0; x=1; x=2 and
y=0; y=1; y=2

R_A and R_B are reflex
and transitive

13a. show:
M,(0,0) |= E(x=0 ∨

13b. show:

Exercise 13: Solution



13b. show:
M,(0,0) |= I(x=0 ∧ y=0)

M,(0,0) |= Iϕ ⇔

∀(x,y) (R_I (0,0)(x,y) ⇒ M,(x,y) |= ϕ ⇔

∀(x,y) (R_A (0,0)(x,y) and R_B (0,0)(x,y) =
M,(x,y) |= ϕ ⇔

∀(x,y) (x=0 and y = 0 ⇒ M,(x,y) |= ϕ)

Exercise 13: solution

3c. show in interpreted systems: M,w |= Dϕ ↔ ϕ

rst of all: the → direction is easy:

M,w |= Dϕ then

,v |= ϕ for all v such that (R_1 ∩ R_2 .... ∩ .... R_n)wv

interpreted systems, $R_i$ww, so (R_1 ∩ R_2 .... ∩ .... R_n)w

M,w |= ϕ

Exercise 13: solution

3c. show in interpreted systems: M,w |= Dϕ ↔ ϕ

ow suppose : M,w |= ϕ . To prove: M,w |= Dϕ

call that w = <w_1, w_2,......., w_n>

ke an arbitrary v for which (R_1 ∩ R_2 .... ∩ .... R_n)wv

$_1$wv, so v_1 = w_1 and R_2wv, so v_2 = w_2 .... and $R_n$wv, sc

ence v = <v_1, v_2,......., v_n> = <w_1, w_2,......., w_n> = w