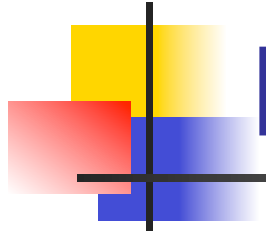


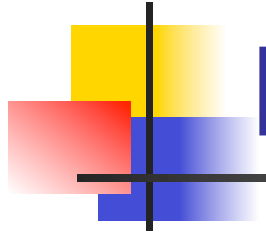
Part III: Epistemic Logic

W. van der Hoek



Modal logic

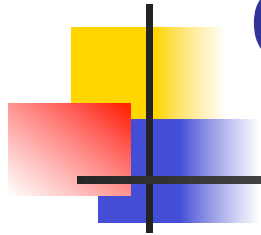
- philosophical logic
- a formal treatment of **intensional** notions
- various 'flavours':
 - epistemic / doxastic
 - temporal / dynamic (action logic)
 - deontic
 - combinations (BDI, KARO)



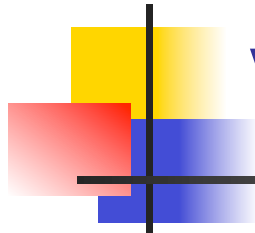
Extensionality

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

defining knowledge

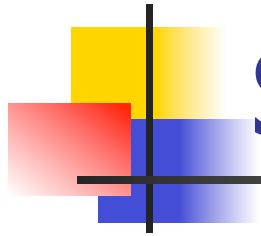


p	Kp	Kp	Kp	Kp
0	~~0~~	~~1~~	~~0~~	~~1~~
1	~~1~~	~~0~~	~~0~~	~~1~~



Varieties of modal logics

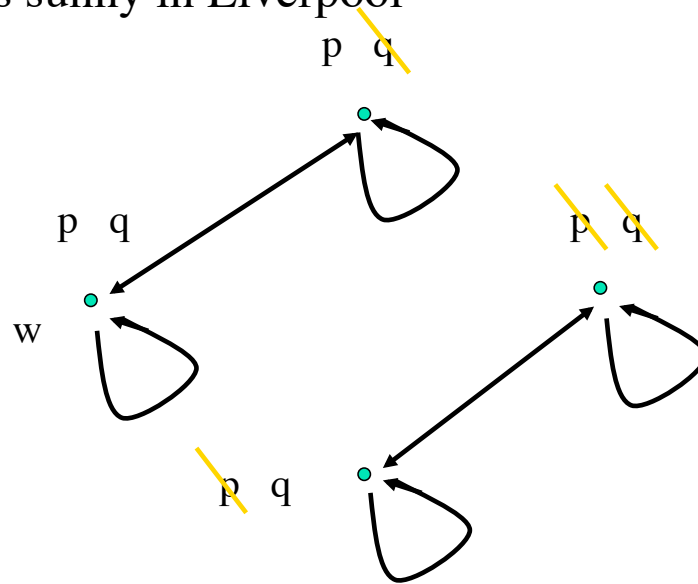
Alethic logic	$\Box\varphi$	φ must be the case
Dynamic logic	$[\alpha]\varphi$	after α , φ holds
Deontic logic	$O\varphi$	φ should be
Temporal logic	$\Box\varphi$	always, φ
Doxastic logic	$B\varphi$	φ is believed
Epistemic logic	$K\varphi$	φ is known
Arithmetic logic	$\Box\varphi$	φ is provable



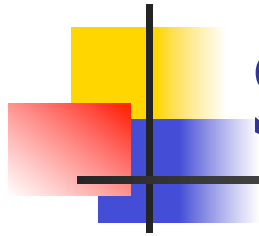
Semantics of modal logic

p : it is sunny in Liverpool

q : it is sunny in London



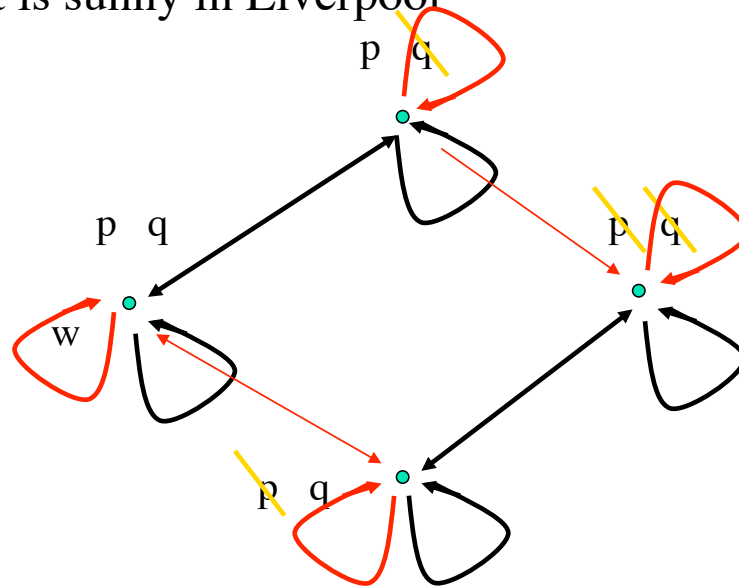
$$M, w \models Kp \wedge \neg Kq \quad \wedge \quad KKp$$



Semantics of modal logic

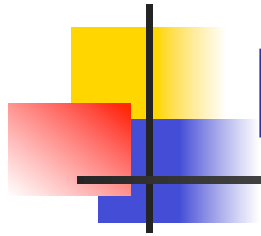
p: it is sunny in Liverpool

q: it is sunny in London



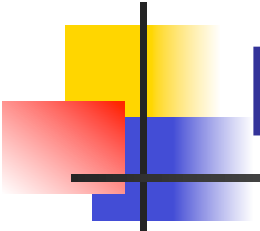
Exercise 0. Agent 1 is in Liverpool, agent 2 in London. Make the accessibility of agent 2 red. Verify whether:

$$M, w \models K_2 K_1 (K_2 q \vee K_2 \neg q)$$



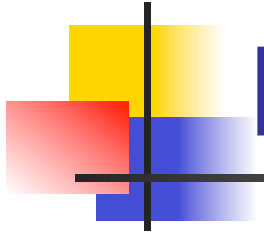
Modal logic, semantics

- Kripke models: $M = (W, \pi, R)$
 - W : set of possible worlds
 - π : truth assignment function
 - R : accessibility relation
- $R(w) = \{w' \mid R(w, w')\}$ set of accessible worlds from w



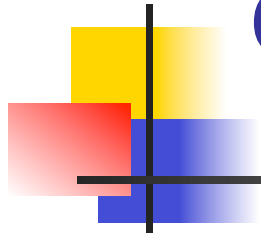
Modal logic, semantics

- $M, w \models \Box \varphi$
- iff $M, w' \models \varphi$
 - for every w' such that $R(w, w')$
- $M, w \models \Diamond \varphi$
- iff $M, w' \models \varphi$
 - for some w' such that $R(w, w')$



Modal logic, ctd.

- modal logic = 'logic of $\Box$ and $\Diamond$ '
- 'neutral reading': **necessity** / **possibility**
- basic property (K):
 - $(\varphi \rightarrow \psi) \rightarrow (\Box \varphi \rightarrow \Box \psi)$, or equivalently:
 - $((\varphi \rightarrow \psi) \wedge \Box \varphi) \rightarrow \Box \psi$
- and Necessitation
 - $\models \varphi \Rightarrow \models \Box \varphi$ which is **not** $\models \varphi \rightarrow \Box \varphi$!!!!!



epistemic logic

System is called **S5**

as 'difficult' as propositional!

R is an equivalence

no nestings needed:

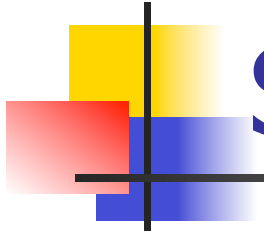
$$K\neg KK\neg p \leftrightarrow \neg K\neg p$$

no iterations needed:

$$K\neg(K(K\neg p \vee \neg Kq) \rightarrow K\neg Kq)$$

is unnecessary complex

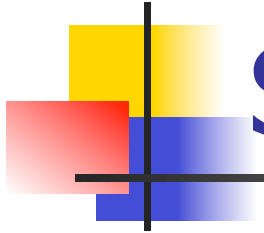
- $K(\phi \rightarrow \psi) \rightarrow (K\phi \rightarrow K\psi)$
 - *agents reason rationally*
- $K\phi \rightarrow \phi$
 - *veridicality*
- $K\phi \rightarrow KK\phi$
 - *positive introspection*
- $\neg K\phi \rightarrow K\neg K\phi$
 - *negative introspection*
- $\vdash \phi \Rightarrow \vdash K\phi$
 - *agents know tautologies*



Semantics

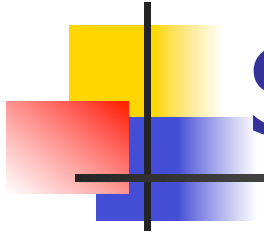
- Let $E = \{M = \langle W, R, V \rangle \mid R \text{ is equivalence}\}$
- Let $U = \{M = \langle W, R, V \rangle \mid R \text{ is universal}\}$
- Let $\text{Th}(M) = \{\varphi \mid M \models \varphi\}$

- Then: $\text{Th}(E) = \text{Th}(U)$
 - $\subseteq$ straightforward
 - $\subseteq$ modal logic cannot distinguish!



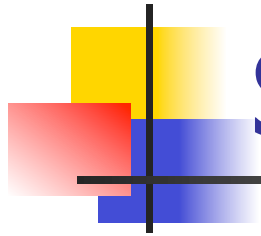
Semantics

- $E \models \varphi \Leftrightarrow U \models \varphi \Leftrightarrow S5 \vdash \varphi$
- easy to verify:
 - $KK\varphi \equiv K\varphi$
 - $K\neg K\varphi \equiv \neg K\varphi$
 - $\neg KK\varphi \equiv \neg K\varphi$
 - $\neg K\neg K\varphi \equiv K\varphi$



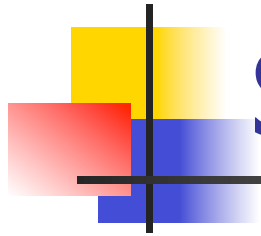
Semantics

- $E \models \varphi \Leftrightarrow U \models \varphi \Leftrightarrow S5 \vdash \varphi$
- easy to verify:
 - φ is satisfiable iff
 - φ is satisfiable in a model of size with at most $|\varphi|$ states
 - $|p| = 1, |\varphi \wedge \psi| = 1 + |\varphi| + |\psi|$
 - $|\neg\varphi| = |K\varphi| = |\varphi| + 1$



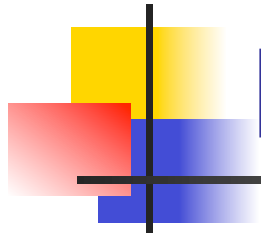
Small model property

- Suppose $\langle S, V \rangle, s \models \varphi$
- $f_s : \text{Sub}(\varphi) \rightarrow 2^S$
 - $f_s(p) = \{ \}$, atoms p in $\text{Sub}(\varphi)$
 - $f_s(\varphi \wedge \psi) = f_s(\varphi) \cup f_s(\psi)$
 - $f_s(\neg \varphi) = f_s(\varphi)$
 - $f_s(K\varphi) =$
 - $\{t\}$, if some $\langle S, V \rangle, t \models \varphi$
 - $\{ \}$ otherwise



Small model property

- Let $S' = \{s\} \cup \bigcup_{\psi \in \text{Sub}(\varphi)} f_s(\psi)$
- $V' = V|_{S'}$
- Then: $\langle S', V' \rangle, s \models \varphi$
- Proof: for all s' in S' : all $\psi \in \text{Sub}(\varphi)$:
 - $\langle S, V \rangle \models \psi \Leftrightarrow \langle S', V' \rangle \models \psi$



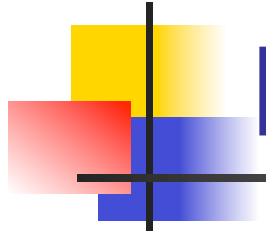
Epistemic and Doxastic logic

- $K\varphi \rightarrow \varphi$
- $K\varphi \rightarrow KK\varphi$
- $\neg K\varphi \rightarrow K\neg K\varphi$

knowledge

- $\neg B\bot$
- $B\varphi \rightarrow BB\varphi$
- $\neg B\varphi \rightarrow B\neg B\varphi$

belief



Logical Omniscience

(LO1) $B\varphi \wedge B(\varphi \rightarrow \psi) \rightarrow B\psi$

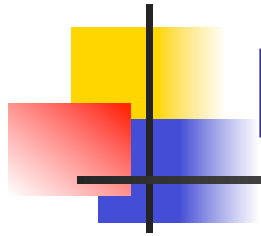
(Closure under implication)

(LO2) $\models \varphi \Rightarrow \models B\varphi$

(belief of valid formulas)

(LO3) $\models \varphi \rightarrow \psi \Rightarrow \models B\varphi \rightarrow B\psi$

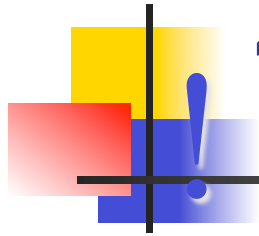
(Closure under valid implication)



Logical omniscience (2)

- (LO4) $\models \varphi \leftrightarrow \psi \Rightarrow \models B\varphi \leftrightarrow B\psi$
(Belief of equivalent formulas)
- (LO5) $(B\varphi \wedge B\psi) \rightarrow B(\varphi \wedge \psi)$
(Closure under conjunction)
- (LO6) $B\varphi \rightarrow B(\varphi \vee \psi)$
(Weakening of belief)
- (LO7) $B\varphi \rightarrow \neg B\neg\varphi$
(Consistency of beliefs)

2 white, 3 black hats



A

rules out:

w

w

?



B

w

any

?



C

any

any

3 x b, 2 x w

w b b

w w b

b b b

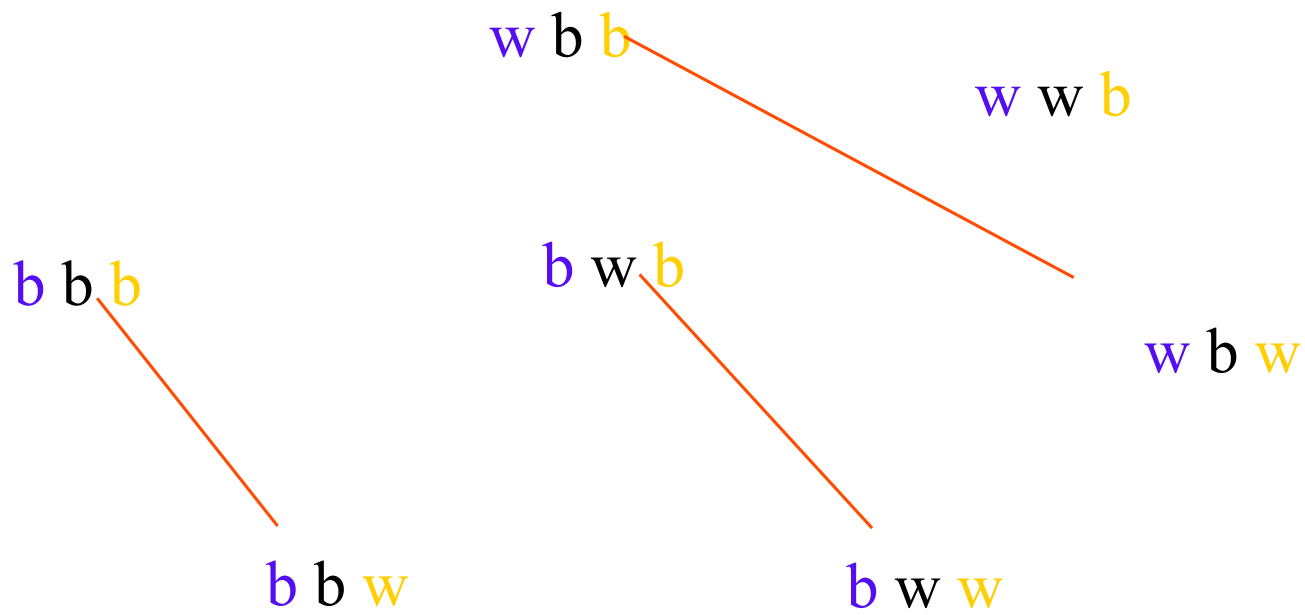
b w b

w b w

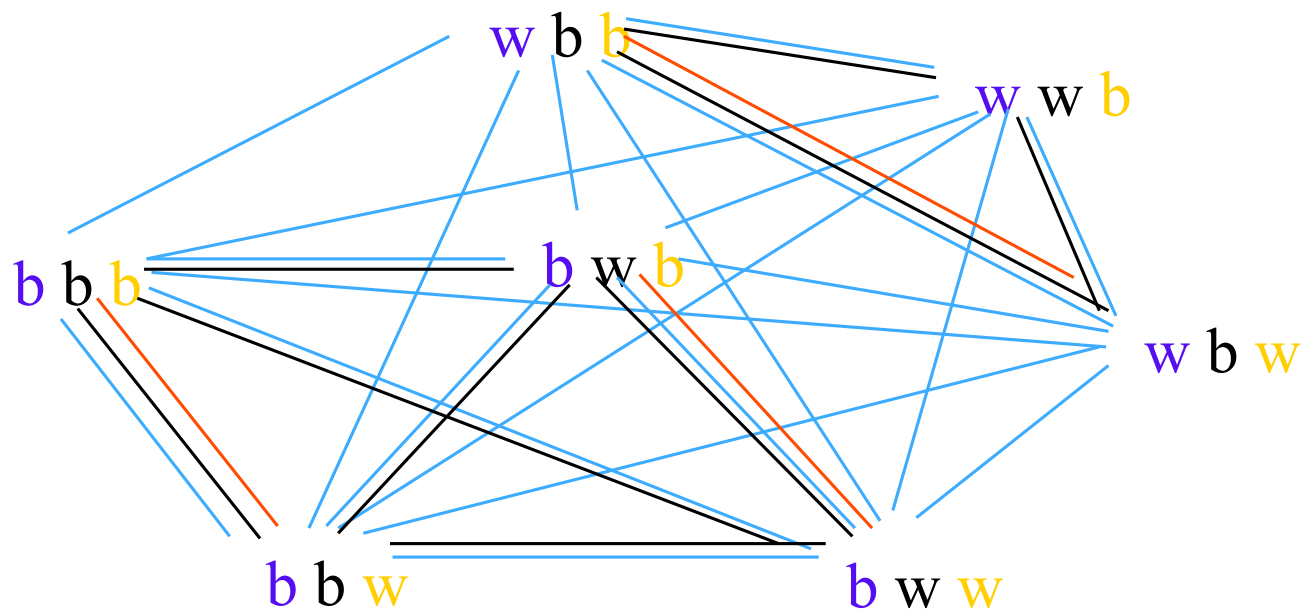
b b w

b w w

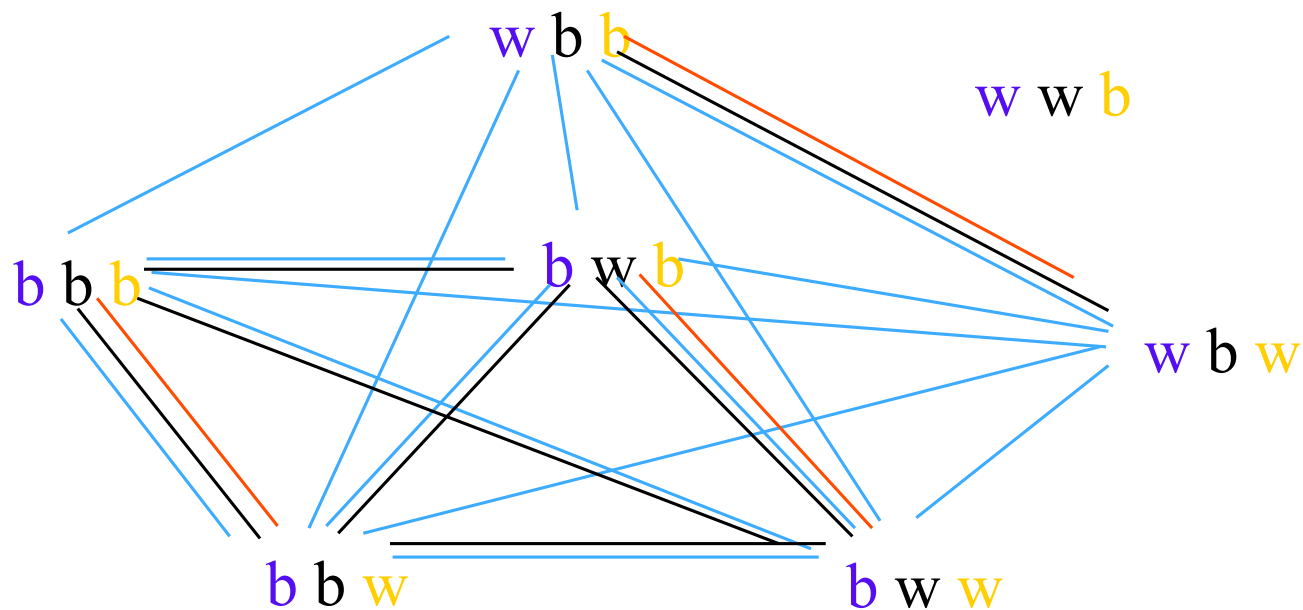
3 x b, 2 x w



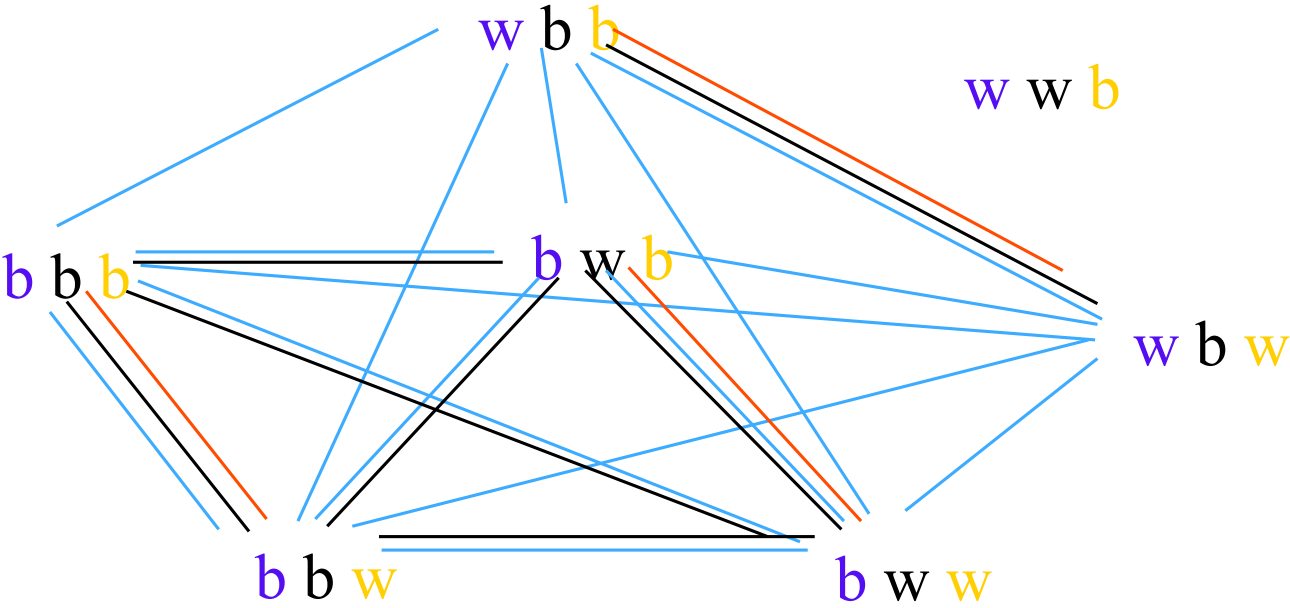
3 x b, 2 x w



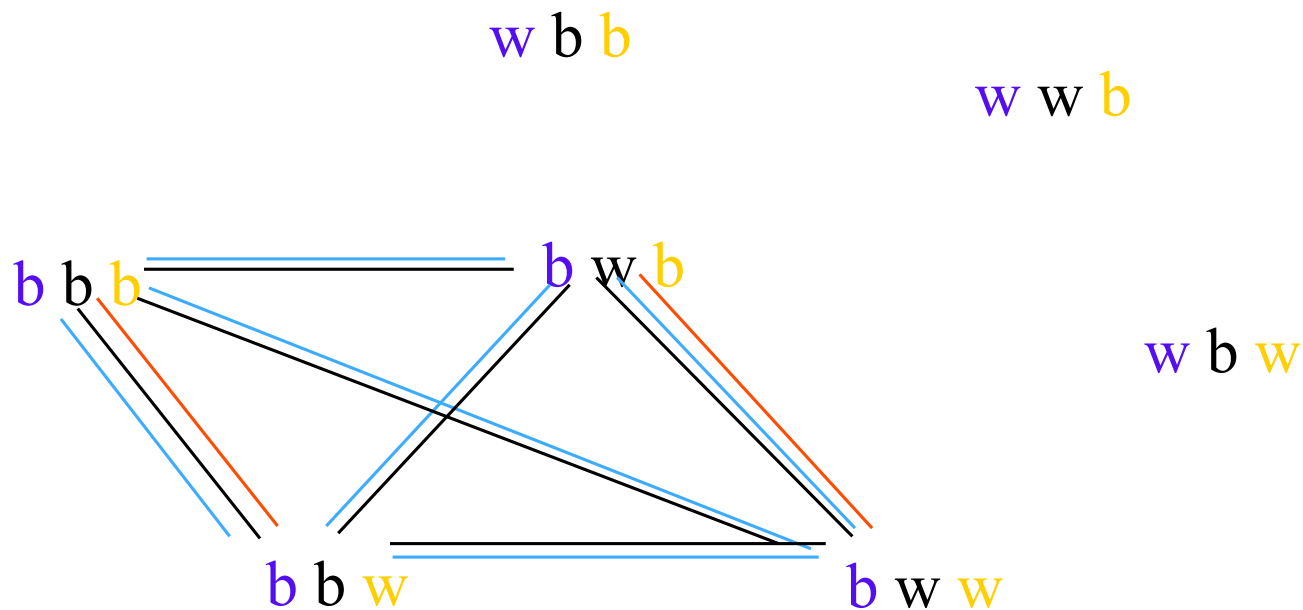
C: "I don't know my colour"



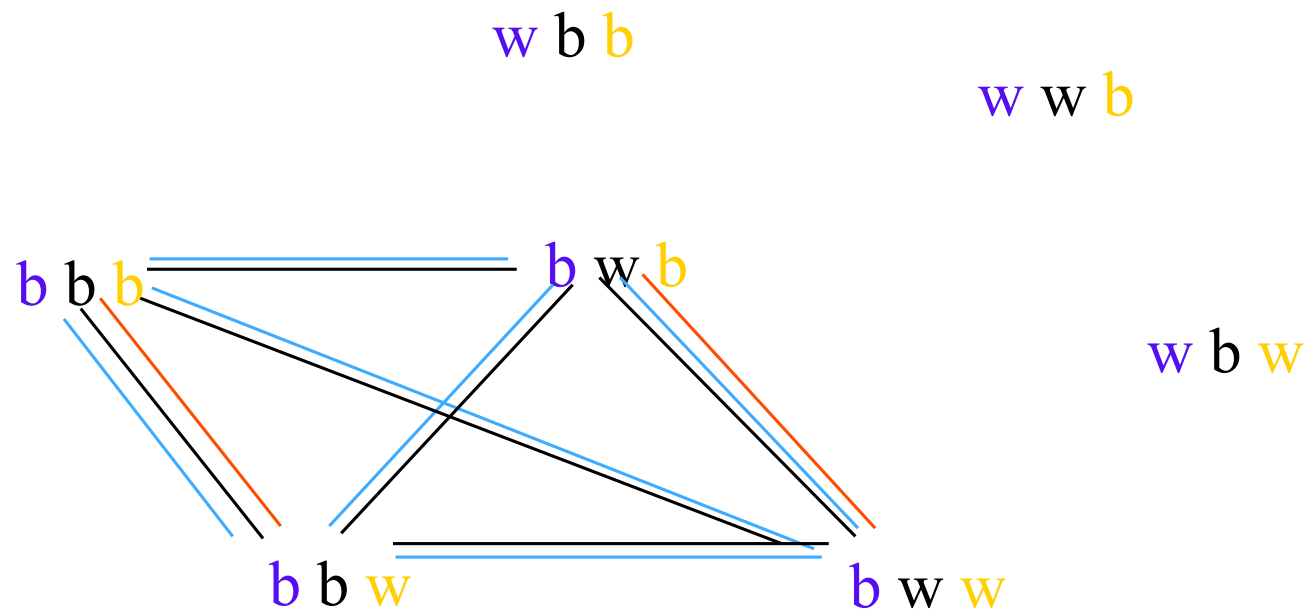
in w b b and w b w, agent B knows his colour

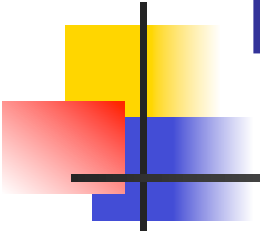


B: "I don't know my colour either"



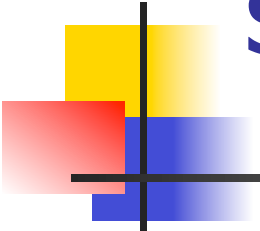
A: "I know mine!"





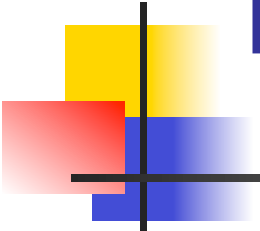
Protocol

- Sender and Receiver
- input for S: $X = \langle x_0, x_1, x_2, \dots \rangle$
- S reads X, sends data to R, who writes T
- deletion errors: reception not guaranteed
- required: protocol that satisfies
 - safety: for some Y, we have $X = T;Y$
 - liveness: every x_i of X appears eventually in T



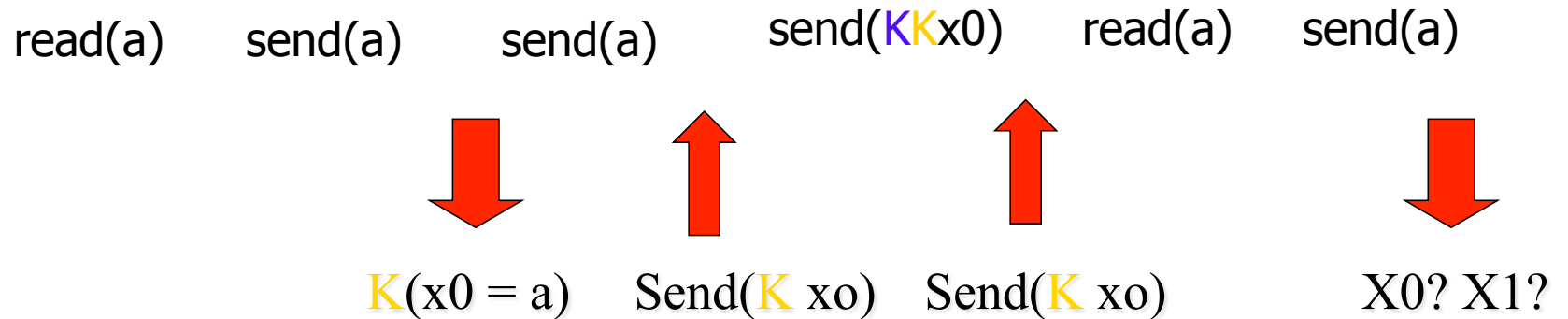
specification

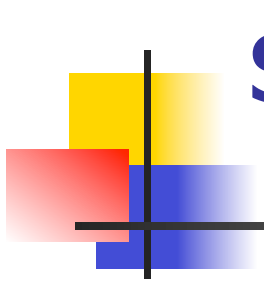
- $i := 0;$
- while true do
- begin read(xi)
 - send(xi) until KK xi;
 - $i := i + 1$
- end
- when K x0 set $i := 0;$
- while true do
- begin write (xi)
 - send(K xi) until $K(x(i+1))$
 - $i := i+1$
- end



not correct

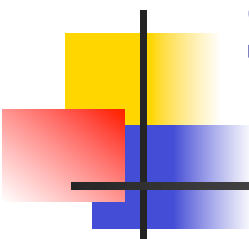
■ $X = \langle a, a, a, c, a, b, \dots \rangle$





specification

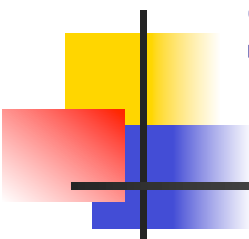
- $i := 0;$
- while true do
- begin read(xi)
 - send(xi) until KK xi;
 - send(KK xi) until KKKK xi
 - $i := i + 1$
- end
- when K x0 set $i := 0;$
- while true do
- begin write (xi)
 - send(Kxi) until KKK xi
 - send(KKK xi) until K xi+1
 - $i := i+1$
- end



specification

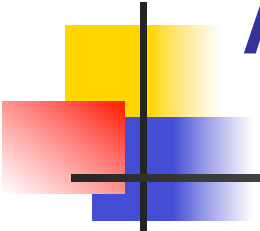
- $i := 0;$
 - while true do
 - begin read(xi)
 - send(xi) until KK xi ;
 - send(KK xi) until KKKK xi
 - $i := i + 1$
 - end
- when K x0 set $i := 0;$
 - while true do
 - begin write (xi)
 - send(Kxi) until KKK xi
 - send(KKK xi) until $\text{K xi}+1$
 - $i := i+1$
 - end

Need three acknowledgements: a_1, a_2, a_3



specification

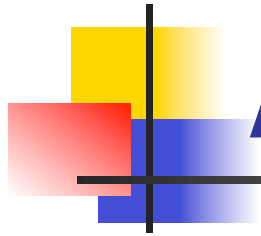
- $i := 0;$
- while true do
- begin read(xi)
 - send(xi) until a_1 recvd;
 - send(a_2) until a_3 recvd;
 - $i := i + 1$
- end
- when x0 recvd set $i := 0;$
- while true do
- begin write (xi)
 - send(a_1) until a_2 recvd;
 - send(a_3) until xi+1 recvd;
 - $i := i+1$
- end



Alternating Bit Protocol

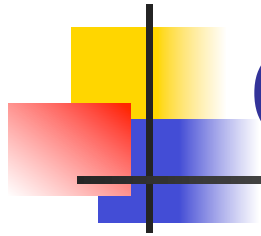
$\text{clr}(m,i) = m0$ if i is even, $m1$ else

- $i := 0;$
- while true do
- begin read(x_i)
 - send $\text{clr}(x_i,i)$ until $\text{clr}(\text{ack},i)$ recvd;
 - $i := i + 1$
- end
- when x_0 recvd set $i := 0;$
- while true do
- begin write (x_i)
 - send $\text{clr}(\text{ack},i)$ until x_{i+1} recvd;
 - $i := i+1$
- end



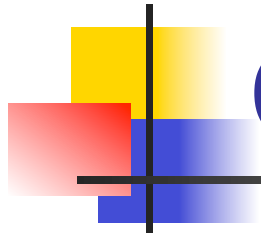
Alternating bit protocol

- knowledge of depth 4 is essential
- provable:
 - S sends $x_{i+1} \rightarrow$
 - $K_S \square (R \text{ receives } x_{i+1} \rightarrow K_R K_S K_R(x_i))$



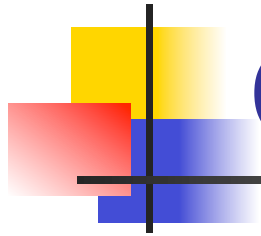
Card Games

- 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:
 - black for 1, green for 2 and red for 3



Card Games (ctd)

- draw the appropriate $S5_{(3)}$ Kripke model
- 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

rbw



rbw



wrb



wbr

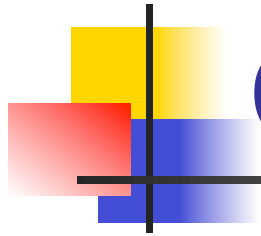


brw



bwr





Card Games: HEXA

rbw



rbw

wrb

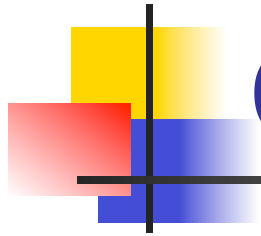


wbr

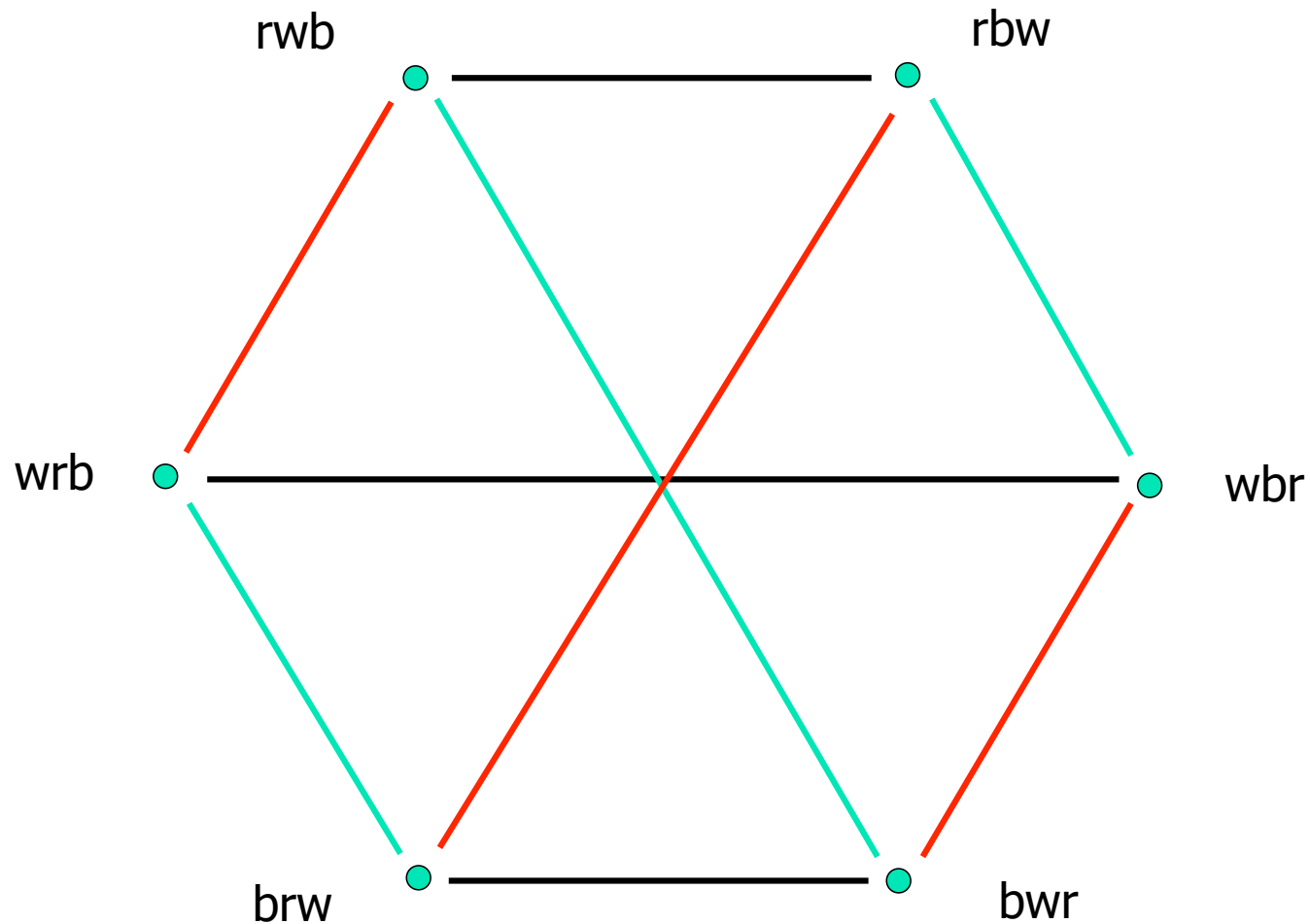
brw

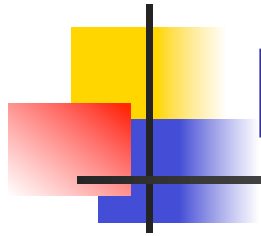


bwr

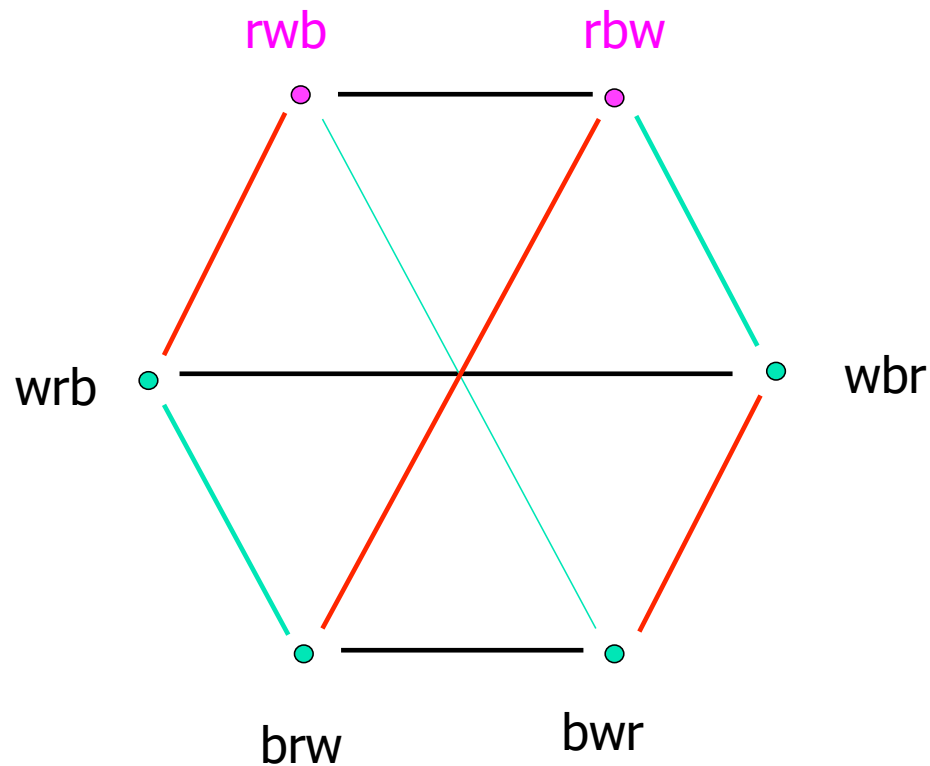


Card Games: HEXA

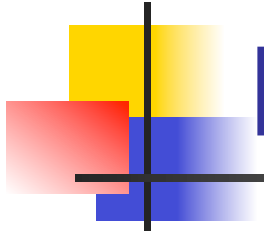




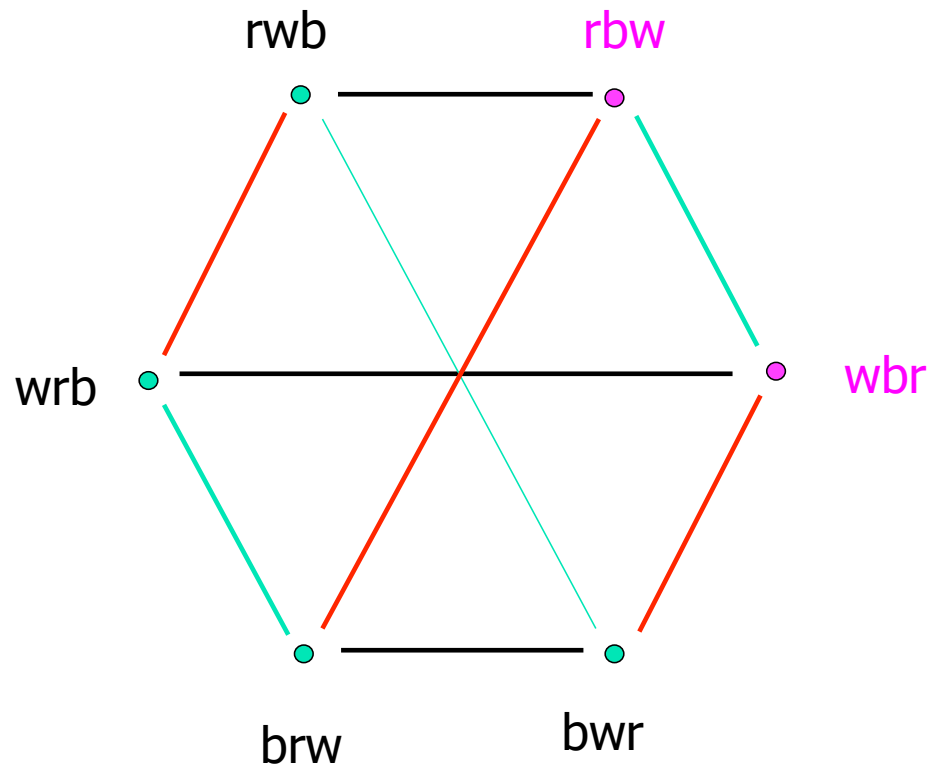
Properties of HEXA



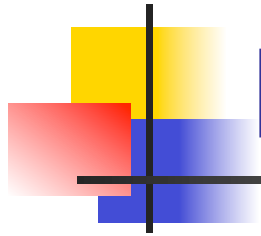
- $M, \text{rwb} \models K_1 r_1$ since
 - $M, \text{rwb} \models r_1$ and
 - $M, \text{rbw} \models r_1$



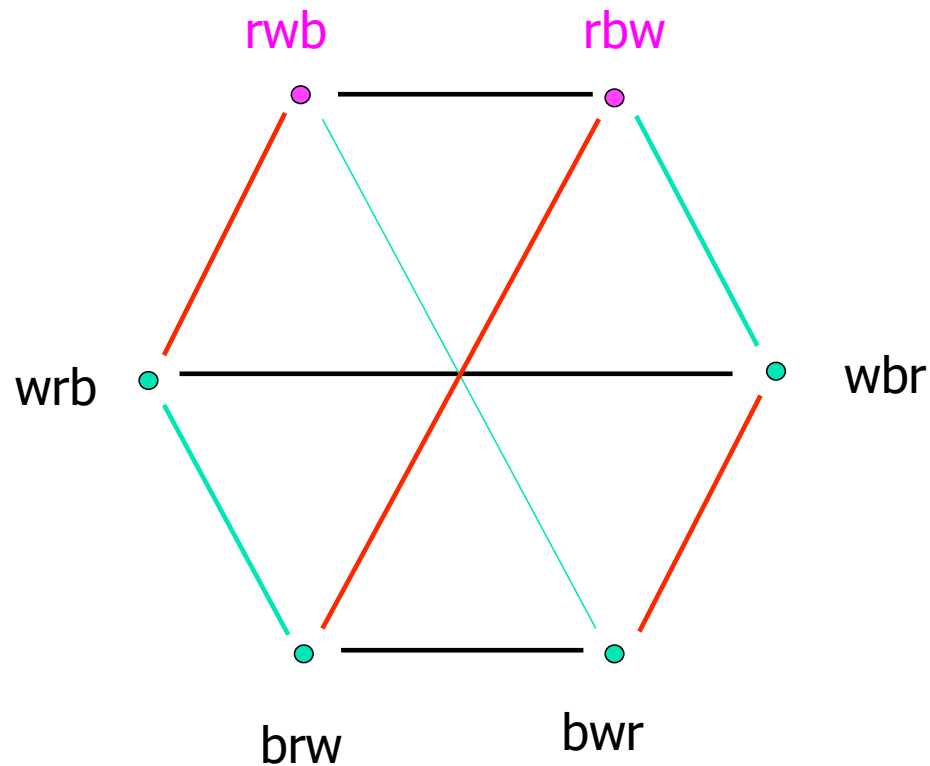
Properties of HEXA



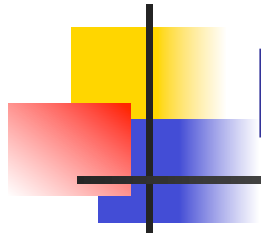
- $K_1(K_2\neg r_2) \wedge K_1(\neg K_2r_1 \wedge \neg K_2r_3)$
- $M, \text{rbw} \models K_1K_2\neg r_2$, since
 - $M, \text{rbw} \models K_2\neg r_2$, since
 - $M, \text{rbw} \models \neg r_2$ and
 - $M, \text{bwr} \models \neg r_2$
 - $M, \text{rbw} \models K_2\neg r_2$, since
 - $M, \text{rbw} \models \neg r_2$ and
 - $M, \text{bwr} \models \neg r_2$



Properties of HEXA

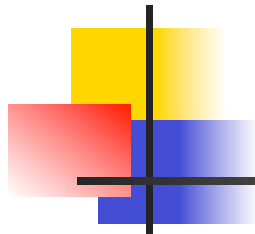


- $K_1(K_2 \neg r_2) \wedge K_1(\neg K_2 r_1 \wedge \neg K_2 r_3)$
- $M, \text{rwb} \models K_1(\neg K_2 r_1 \wedge \neg K_2 r_3)$
- since
 - $M, \text{rwb} \models \neg K_2 r_1 \wedge \neg K_2 r_3$ since
 - $M, \text{bwr} \models \neg r_1$ and
 - $M, \text{rwb} \models \neg r_3$
 - $M, \text{rbw} \models \neg K_2 r_1 \wedge \neg K_2 r_3$ since
 - $M, \text{wbr} \models \neg r_1$ and
 - $M, \text{rbw} \models \neg r_3$



Exercise 3

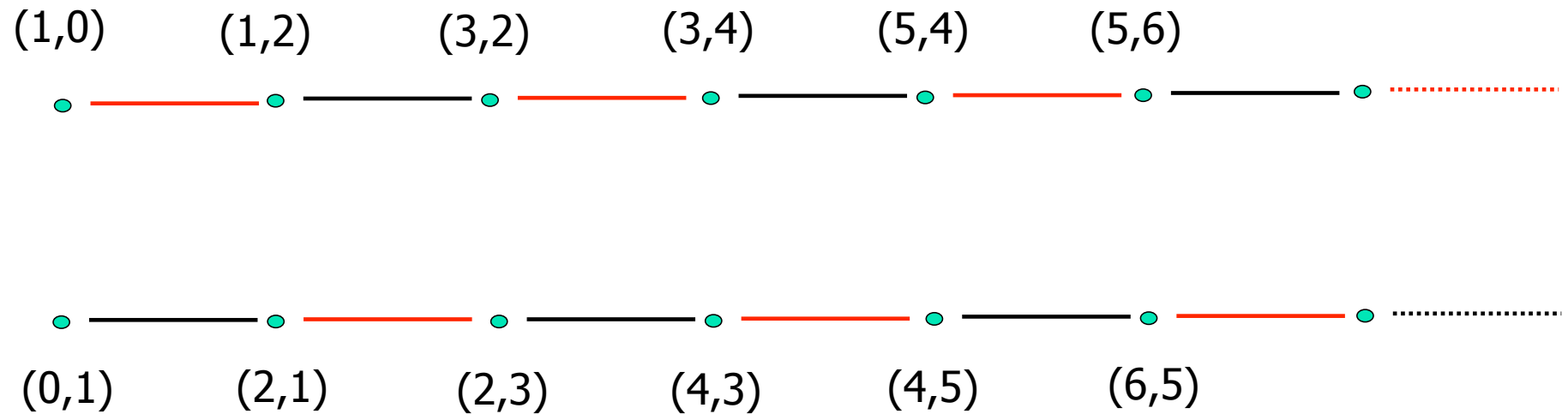
- Ann and Bob each have a number on their head: Ann can only see Bob's, who can only see Ann's. However, it is known by everybody that the numbers are successors of each other, i.e. they are n and $n + 1$ for some n .
- Draw the appropriate model.

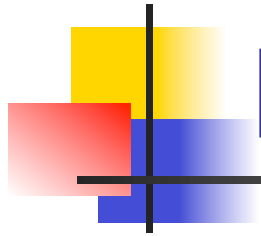


Exercise 3

A: —
B: —

(x,y) : A carries x , B carries y





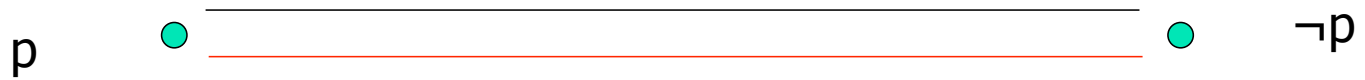
Exercise 4

- Ann and Bob are in a bar, in front of them is an envelop for Ann, with either an invitation to go out in Amsterdam (p) or one to give a lecture ($\neg p$)
 - Draw the corresponding Kripke model when nobody has looked in the envelop yet
 - Suppose A reads the letter in the envelop, and B sees this. Draw the new model.

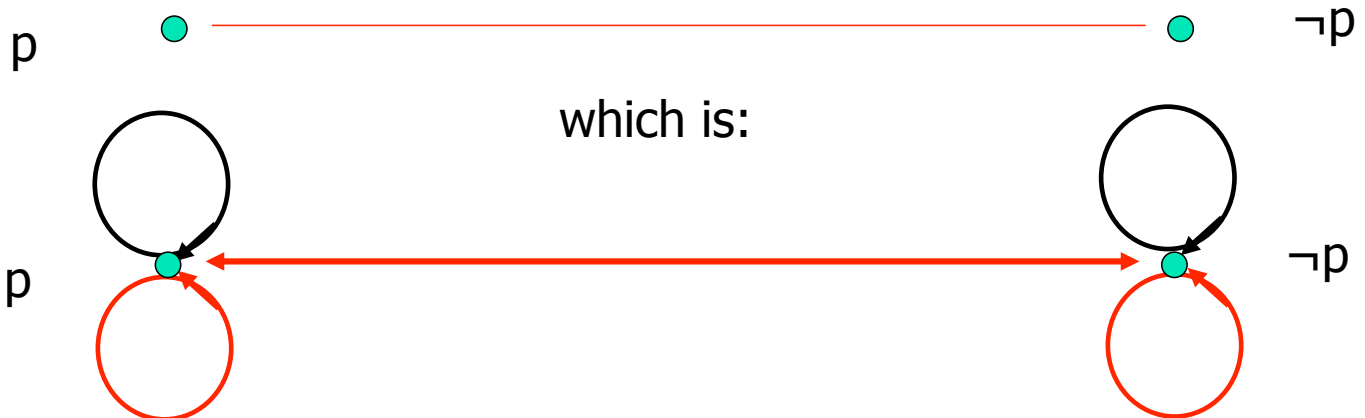
Exercise 4

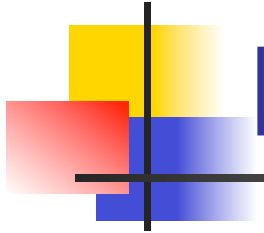
A: _____

B: _____



after A reads, and B sees that:





Exercise 5

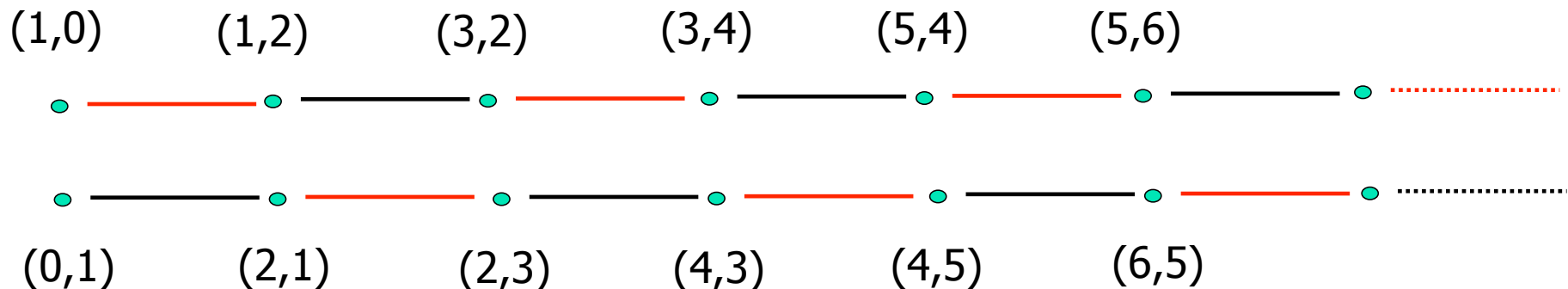
let a_n be: "An has number n", similarly for b_n "Bob has number n"

5a Show: $M, (3,4) \models \neg K_B b_4 \wedge K_A \neg K_B b_4$

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

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

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





Exercise 6

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

6a. Show $M, (3,4) \models \neg M_B M_A K_B b \wedge M_B M_A M_B K_A a$

6b. Suppose Ann says: I don't know my number
Draw the new model M_1 . Show $M_1, (3,4) \models \neg M_B K_A a \wedge M_B M_A K_B b$

6c. Suppose now Bob says: I don't know my number
Draw the new model M_2 . Show $M_2, (3,4) \models \neg K_B b \wedge M_B K_A a$

6d. Suppose now Ann says: I don't know my number
Draw the new model M_3 . Show $M_3, (3,4) \models K_B b$!!

(1,0) (1,2) (3,2) (3,4) (5,4) (5,6)





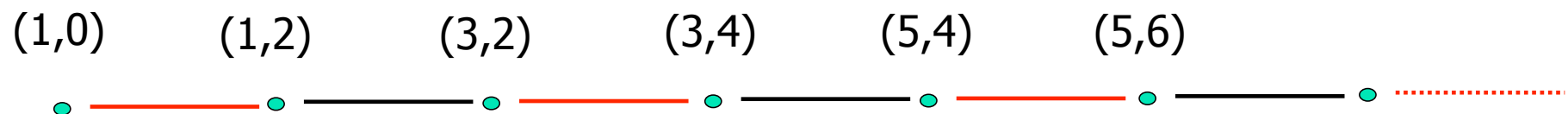
Exercise 6

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

6a. Show $M, (3,4) \models \neg M_B M_A K_B b \wedge M_B M_A M_B K_A a$

First of all, note that $K_B b$ is true nowhere: Bob is uncertain everywhere
 This explains $M, (3,4) \models \neg M_B M_A K_B b$ (in fact $M, x \models \neg M_B M_A K_B b$ for all x)

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





Exercise 6

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

6a. Show $M, (3,4) \models \neg M_B M_A K_B b \wedge M_B M_A M_B K_A a$

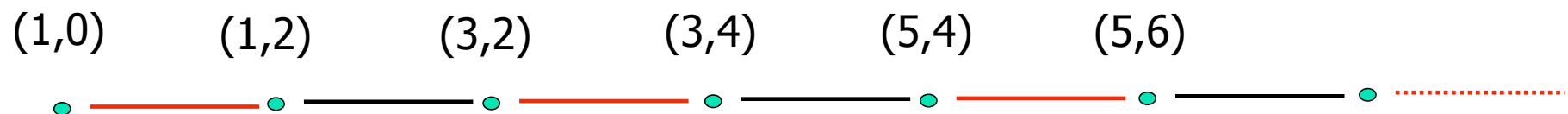
Moreover, $K_A a$ is true only in (1,0). From (3,4) there is a B-A-B path to (1,0).
More precisely:

$M, (1,0) \models K_A a$

$M, (1,2) \models M_B K_A a$

$M, (3,2) \models M_A M_B K_A a$

$M, (3,4) \models M_B M_A M_B K_A a$





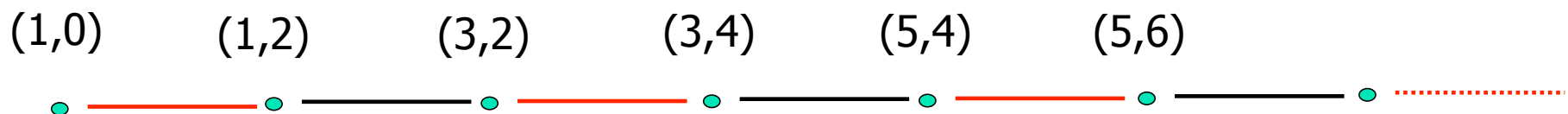
Exercise 6

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

6a. Show $M, (3,4) \models \neg M_B M_A K_B b \wedge M_B M_A M_B K_A a$

First of all, note that $K_B b$ is true nowhere: Bob is uncertain everywhere
This explains $M, (3,4) \models \neg M_B M_A K_B b$ (in fact $M, x \models \neg M_B M_A K_B b$ for all x)

Moreover, $K_A a$ is true only in (1,0). From (3,4) there is a B-A-B path to (1,0).
so, $M, (3,4) \models M_B M_A M_B K_A a$





Exercise 6

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

6b. Suppose Ann says: I don't know my number

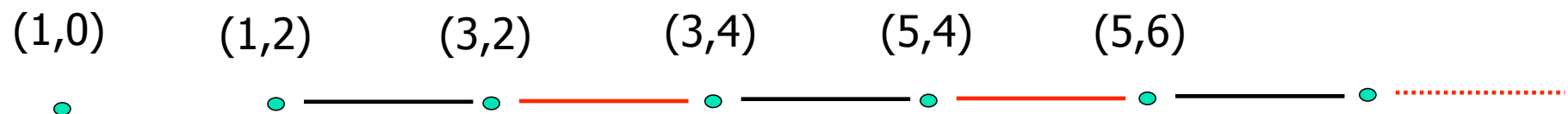
Draw the new model M_1 . Show $M_1, (3,4) \models \neg M_B K_A a \wedge M_B M_A K_B b$

There is no point at which $K_A a$ holds, so $M_1, (3,4) \models \neg M_B K_A a$

$K_B b$ is true at (1,2), and there is a B-A path to (1,2), hence

$M_1, (3,4) \models M_B M_A K_B b$

$M_1, (1,2) \models K_B b$, thus $M_1, (3,2) \models M_A K_B b$ thus $M_1, (3,4) \models M_B M_A K_B b$





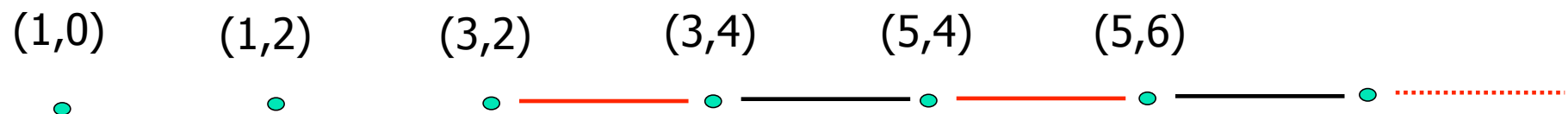
Exercise 6

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

6c. Suppose now Bob says: I don't know my number
 Draw the new model M_2 . Show $M_2, (3,4) \models \neg K_B b \wedge M_B K_A a$

There is no point where $K_B b$ is true, hence $(3,4) \models \neg K_B b$

$K_A a$ is true at (3,2), hence $(3,4) \models M_B K_A a$



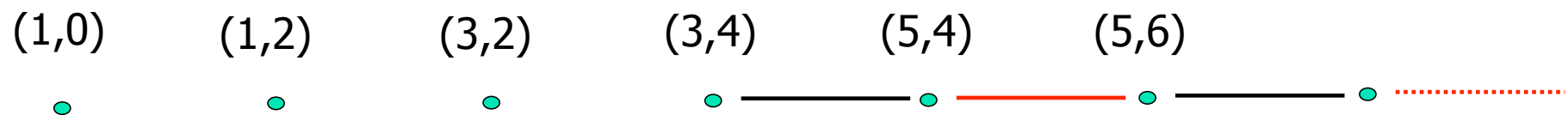


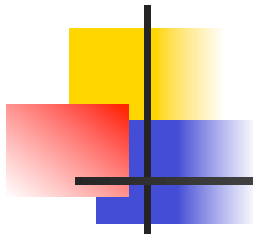
Exercise 6

let a_n be: "An has number n ", similarly for b_n "Bob has number n ". Suppose the real world is $(3,4)$. Call the model M_3 (see below).

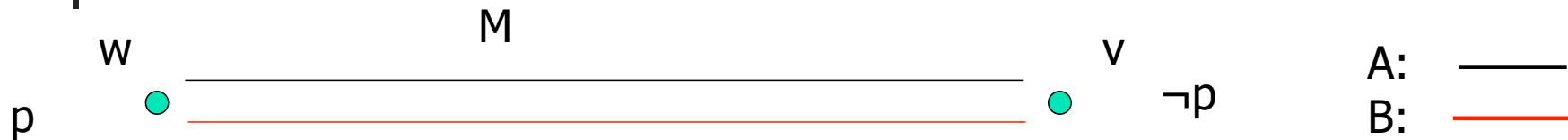
6d. Suppose now Ann says: I don't know my number
Draw the new model M_3 . Show $M_3, (3,4) \models K_B b$!!

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





Exercise 7



For any item, start from M again.

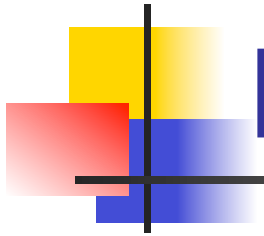
7a. Suppose Ann reads the letter aloud: it says p ! Draw the model M_1

7b. Bob holds it for possible that A read the letter. Draw M_2

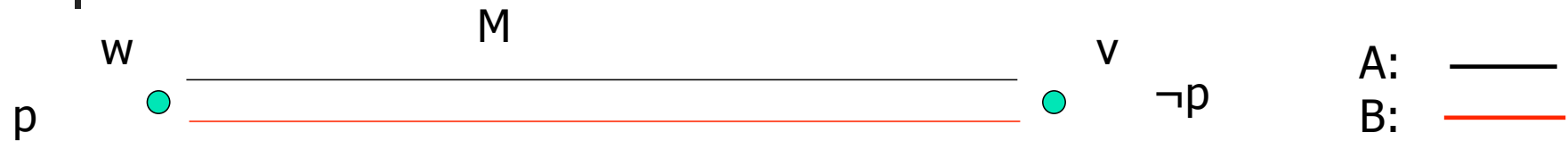
7c. An outsider tells A and B that one of them has read the letter. Draw M_3

7d. An outsider tells A and B that one of them may have read the letter. Draw M_4

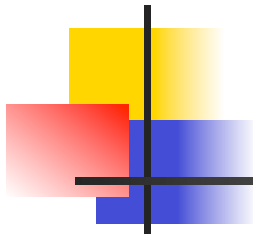
7e. An outsider tells A and B that some (0, 1 or 2) of them may have read the letter.
Draw M_5



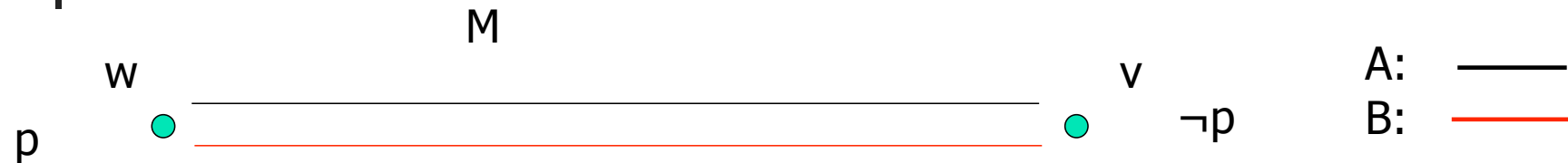
Exercise 7



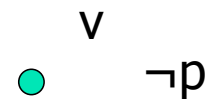
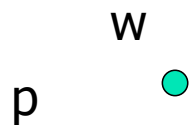
7a. Suppose Ann reads the letter aloud: it says p ! Draw the model M_1



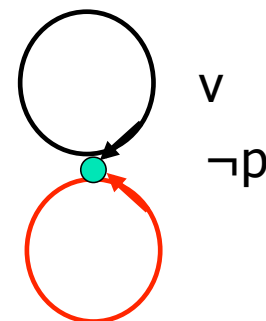
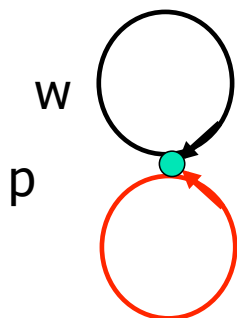
Exercise 7



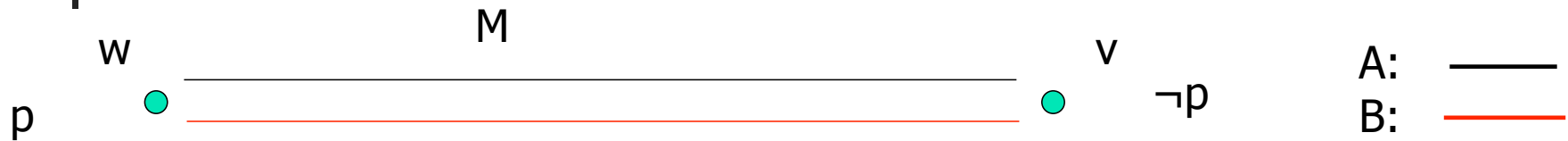
7a. Suppose Ann reads the letter aloud: it says p! Draw the model M_1



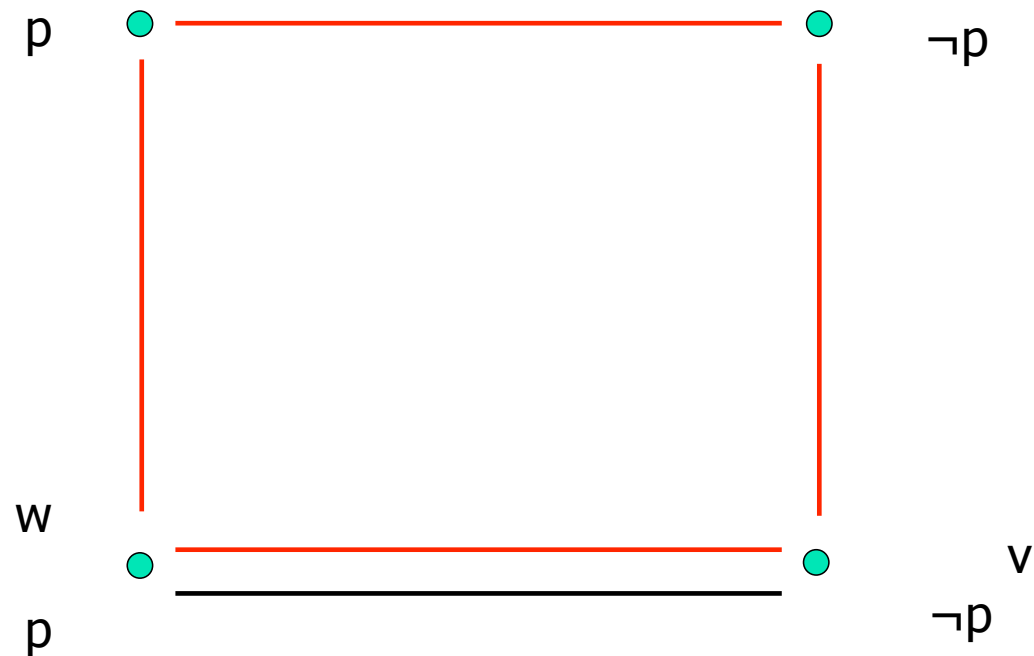
which is actually:



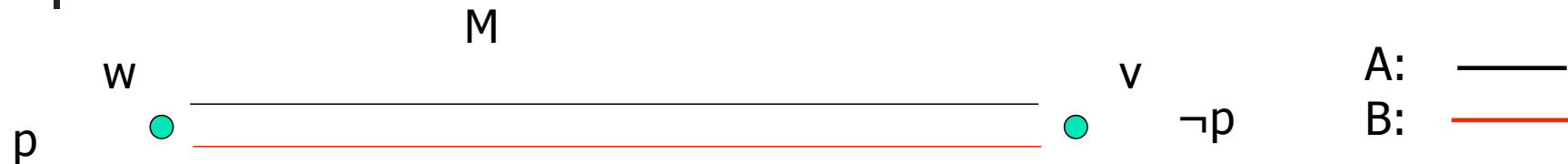
Exercise 7



7b. Bob holds it for possible that A read the letter. Draw M_2

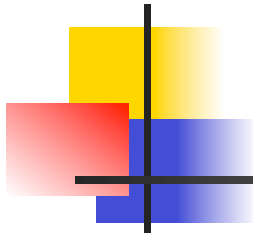


Exercise 7

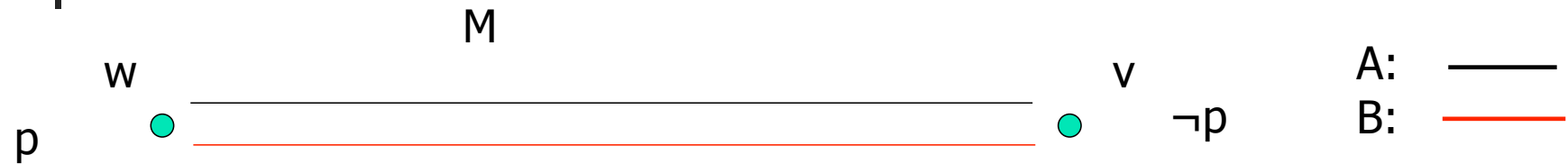


7c. An outsider tells A and B that one of them has read the letter. Draw M_3

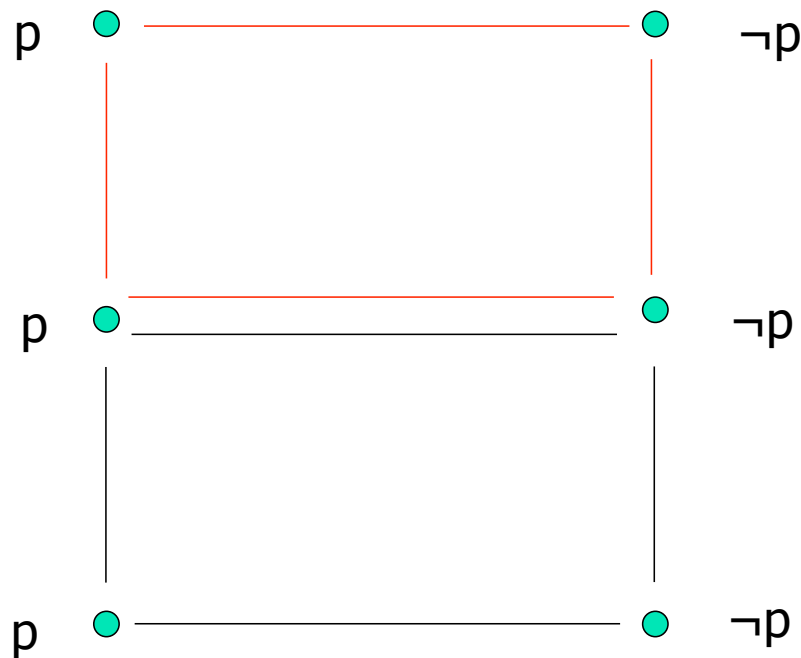


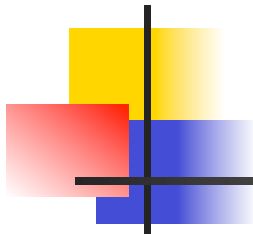


Exercise 7

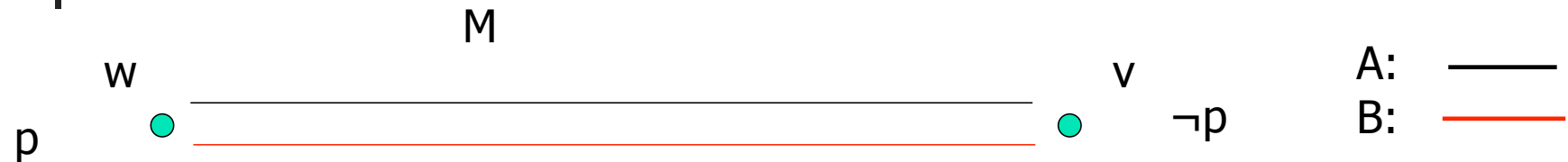


7d. An outsider tells A and B that one of them may have read the letter. Draw M_4

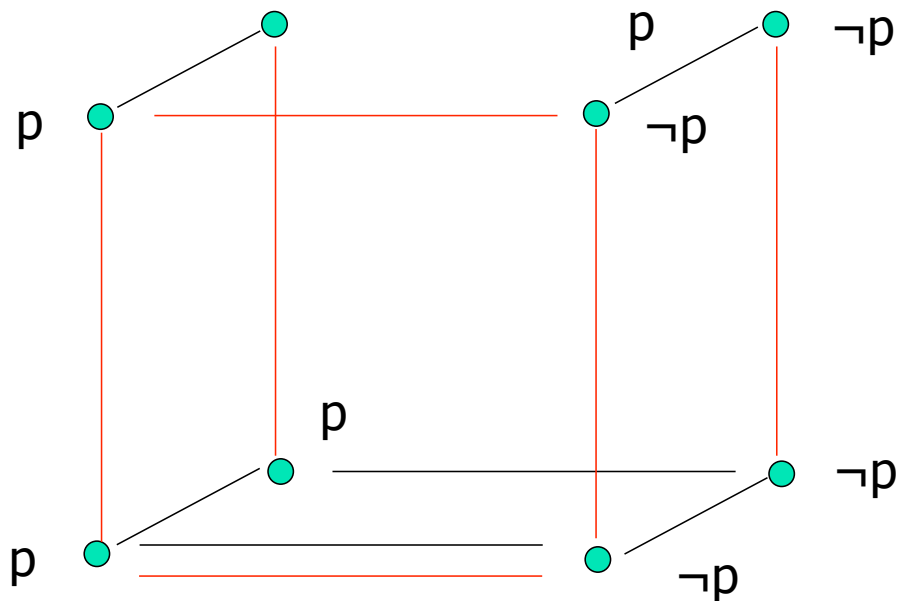




Exercise 7



7e. An outsider tells A and B that some (0, 1 or 2) of them may have read the letter.





A:

B:



$$K_B p \wedge M_B K_A p \wedge M_B \neg K_A p$$



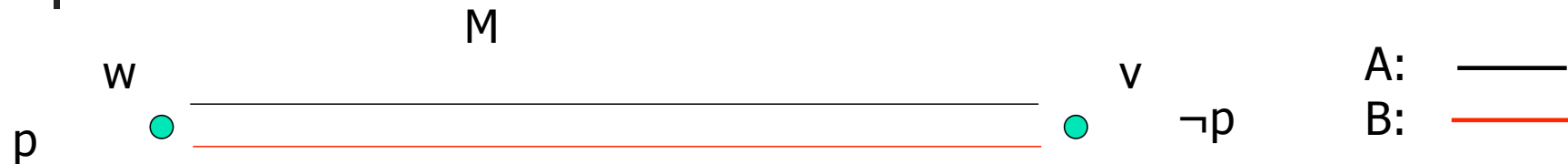
A:

B:

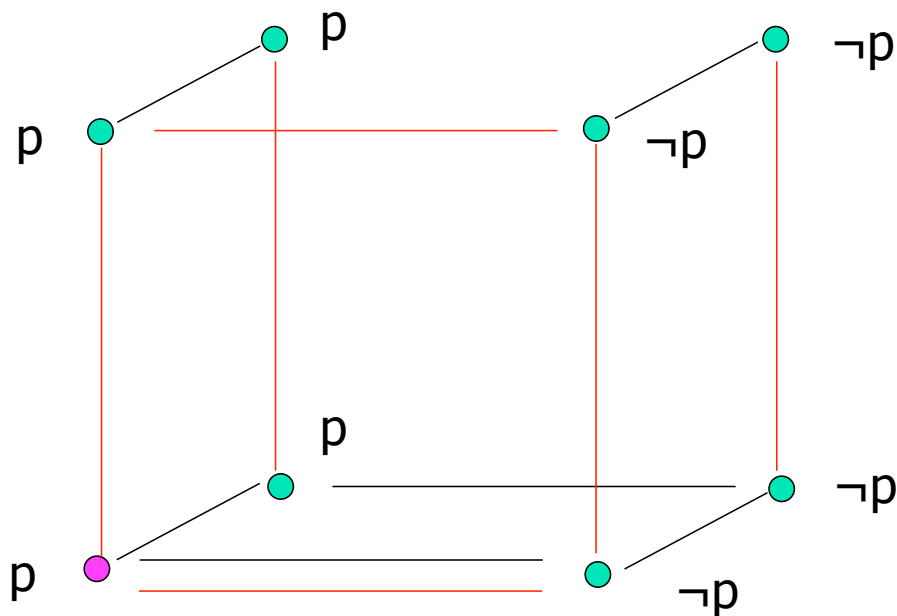


64

Exercise 7

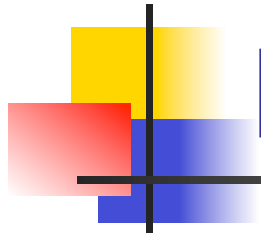


7e. An outsider tells A and B that some (0, 1 or 2) of them may have read the letter.



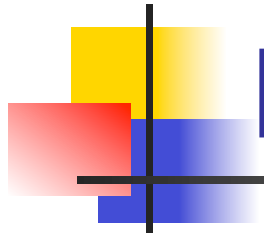
Suppose nobody read the letter: p

$$\neg K_B p \wedge \neg K_A p \wedge M_B K_A p \wedge M_A K_B p$$



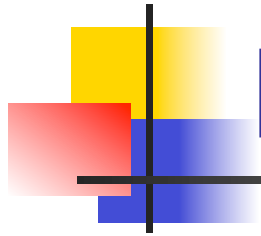
Different Modal Systems

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

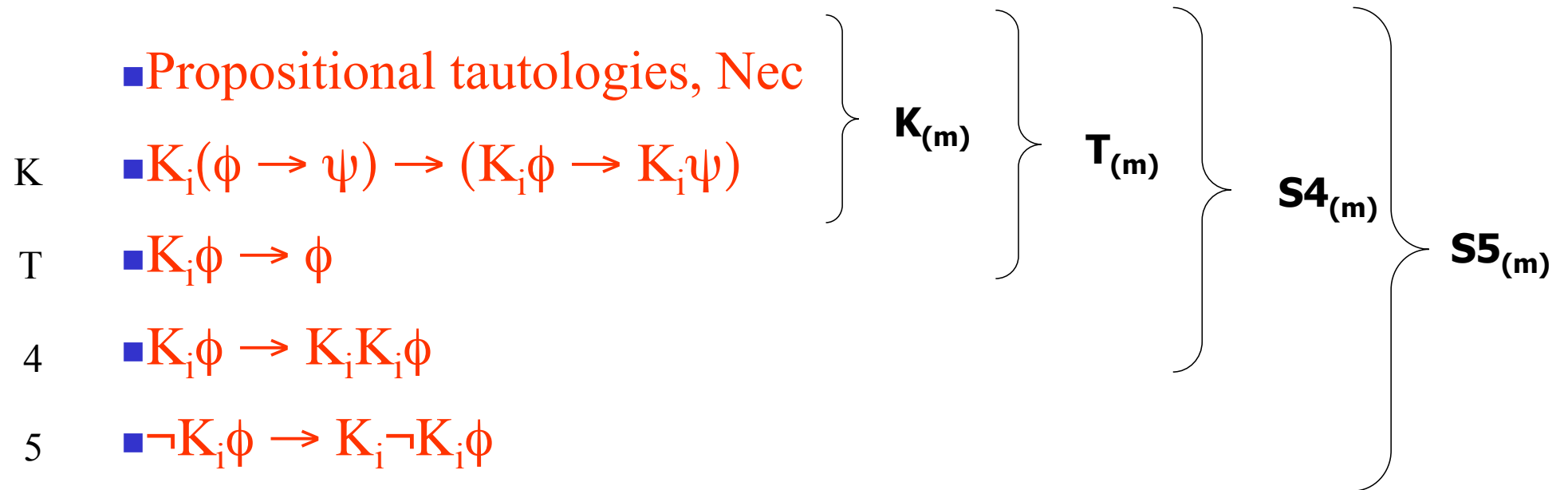


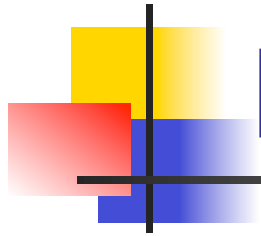
Different Modal Systems

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

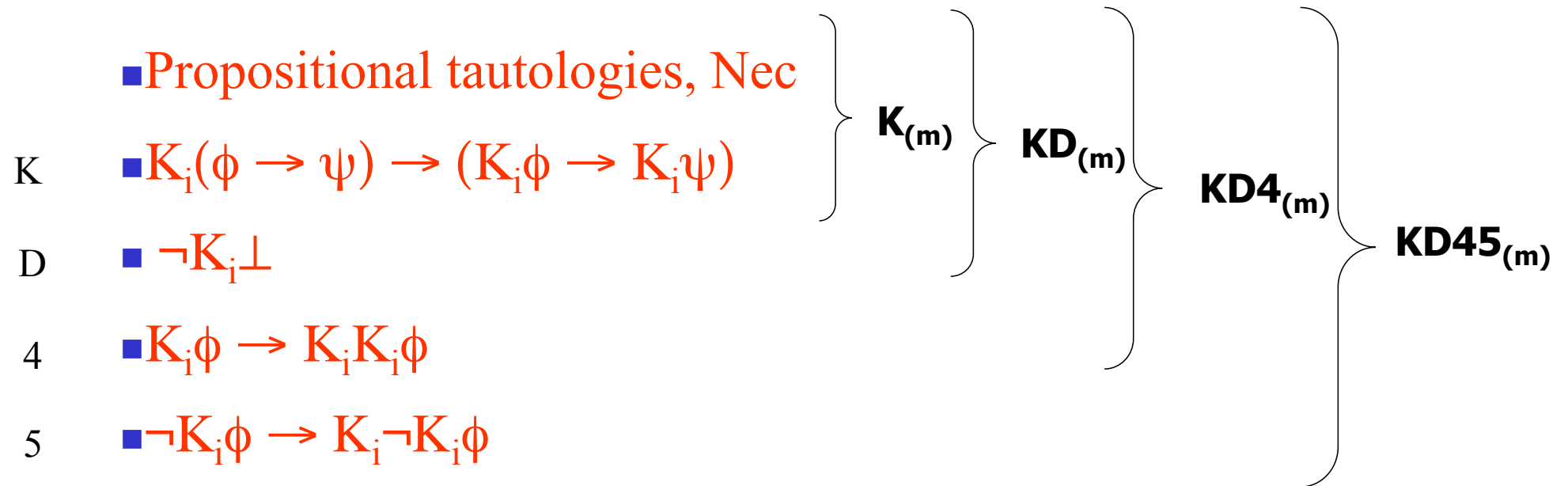


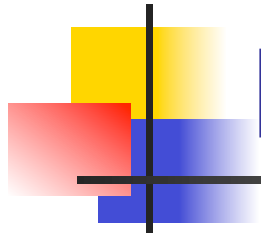
Different Modal Systems





Different Modal Systems





Different Semantic Systems

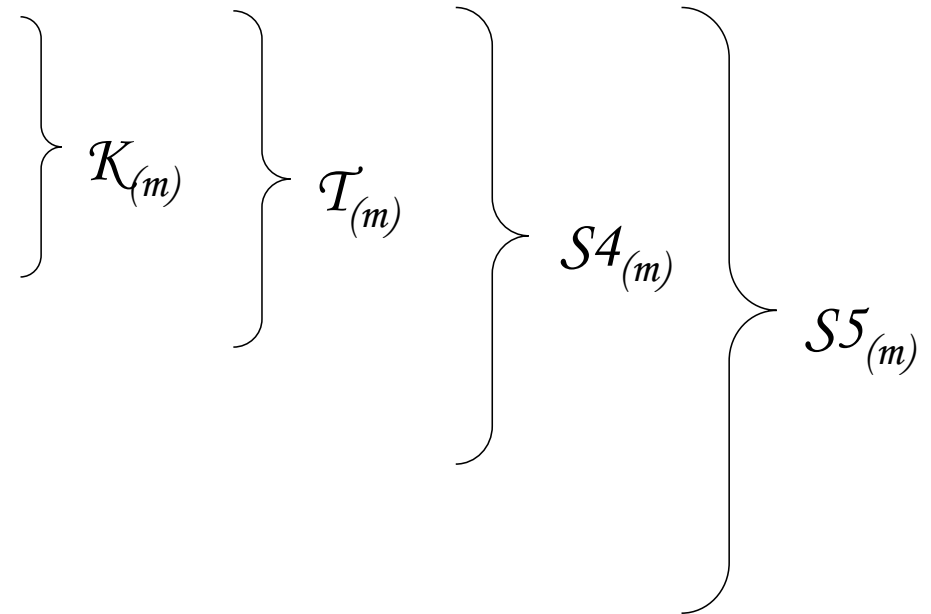
- Kripke Models

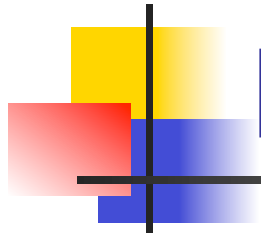
K ■ Accessibility Relations R_i

T ■ R_i is reflexive

4 ■ R_i is transitive

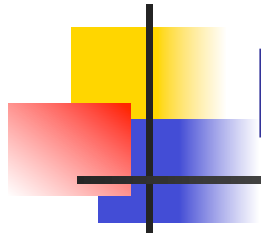
5 ■ R_i is Euclidean





Relating the Systems

$$\begin{array}{ccccccccc} \mathcal{K}_{(m)} \models \varphi & \Rightarrow & \mathcal{KD}_{(m)} \models \varphi & \Rightarrow & \mathcal{T}_{(m)} \models \varphi & \Rightarrow & S4_{(m)} \models \varphi & \Rightarrow & S5_{(m)} \models \varphi \\ \Updownarrow & & \Updownarrow & & \Updownarrow & & \Updownarrow & & \Updownarrow \\ \mathbf{K}_{(m)} \vdash \varphi & \Rightarrow & \mathbf{KD}_{(m)} \vdash \varphi & \Rightarrow & \mathbf{T}_{(m)} \vdash \varphi & \Rightarrow & \mathbf{S4}_{(m)} \vdash \varphi & \Rightarrow & \mathbf{S5}_{(m)} \vdash \varphi \end{array}$$



Example Derivation

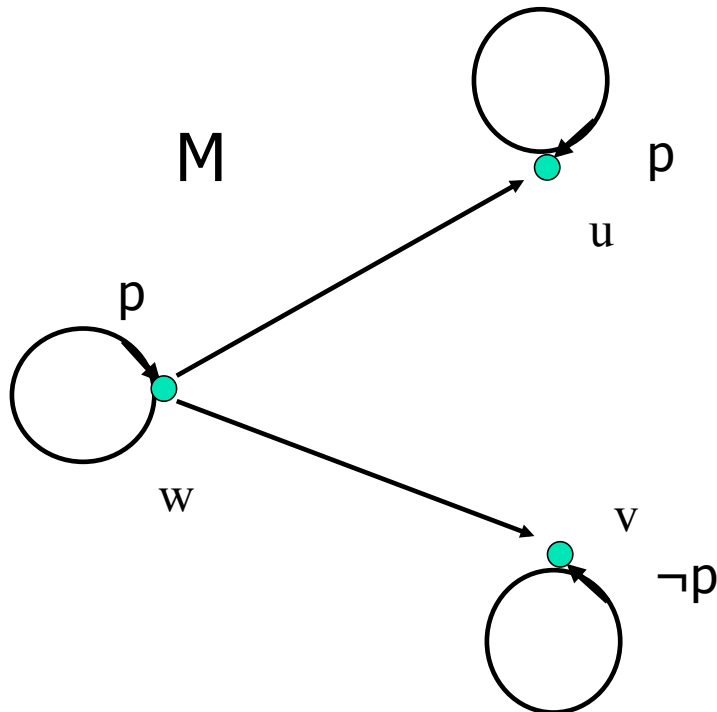
$$S5_{(m)} \vdash \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$$

- $\neg K_i \phi \rightarrow K_i \neg K_i \phi$ A5
- $K_i \neg K_i \phi \rightarrow \neg K_i \phi$ A3
- $\neg K_i \phi \leftrightarrow K_i \neg K_i \phi$ 1,2,A1

Counterexamples

$$S4_{(m)} \vdash \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi \quad ?$$

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



$$M, \not\models \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi$$

Because

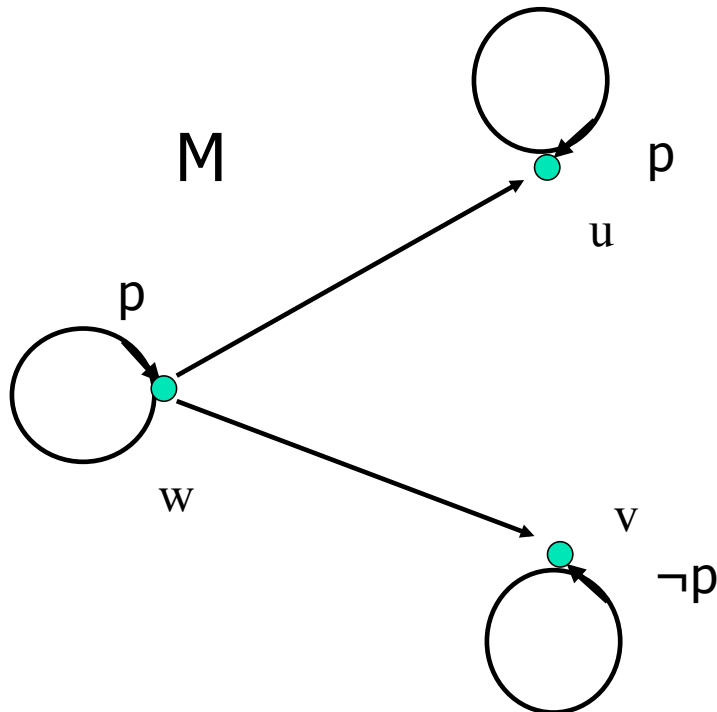
$$M, w \models \neg K_i p$$

$$\text{Because } M, v \models \neg p$$

Counterexamples

$$S4_{(m)} \vdash \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi \quad ?$$

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



$$M \not\models \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi$$

Because

$$M, w \models \neg K_i p, \text{ and}$$

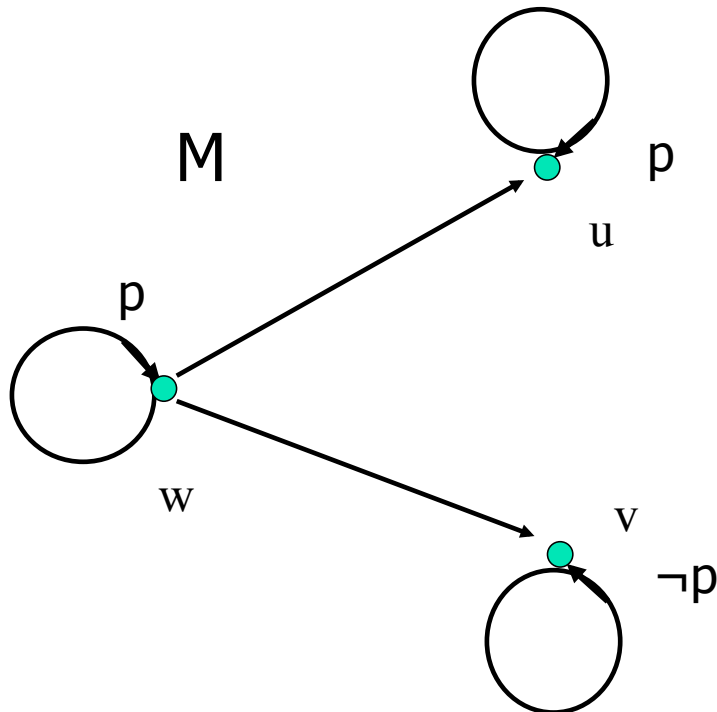
$$M, w \models \neg K_i \neg K_i p$$

because this is $M, w \models M_i K_i p$
and $M, u \models K_i p$

Counterexamples

$$S4_{(m)} \vdash \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi \quad ?$$

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



$$M \not\models \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi$$

Because

$$M, w \models \neg K_i p, \text{ and}$$

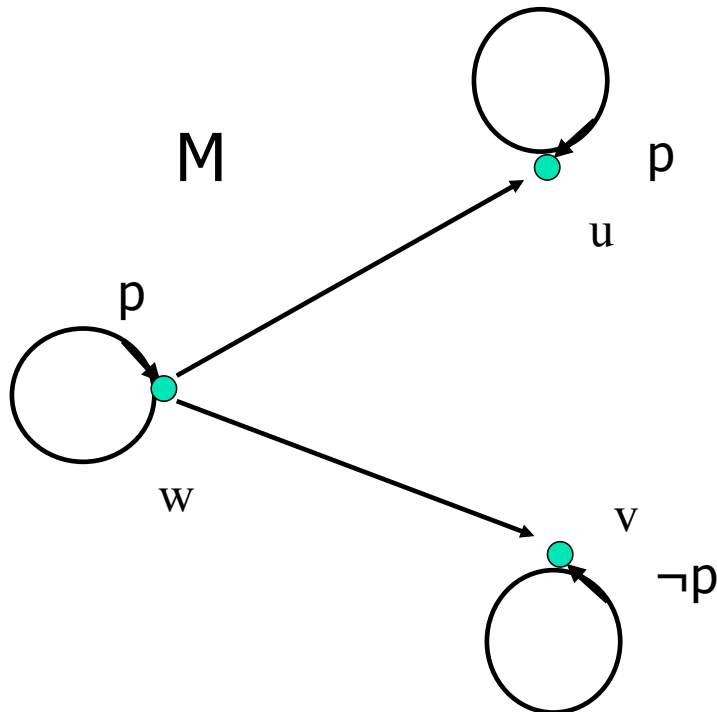
$$M, w \models \neg K_i \neg K_i p$$

$$\text{So } M, w \models \neg (\neg K_i p \Leftrightarrow K_i \neg K_i p)$$

Counterexamples

$$S4_{(m)} \vdash \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi \quad ?$$

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

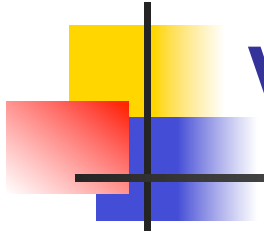


$$M \not\models \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi$$

and

$$M \in S4_{(m)}$$

$$\text{hence } S4_{(m)} \not\models \neg K_i \phi \Leftrightarrow K_i \neg K_i \phi$$



Validities

We already derived: $S5_{(m)} \vdash \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

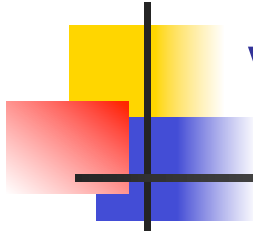
We could also have proved: $S5_{(m)} \models \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

First of all, $\neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

is equivalent to $\neg \neg K_i \phi \leftrightarrow \neg K_i \neg K_i \phi$

is equivalent to $K_i \phi \leftrightarrow \neg K_i \neg K_i \phi$

is equivalent to $K_i \phi \leftrightarrow M_i K_i \phi$



Validities

We already derived: $S5_{(m)} \vdash \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

We could also have proved: $S5_{(m)} \models \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

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

Let $M \in S5_{(m)}$ and w a world in M . To prove: $M, w \models K_i \phi \leftrightarrow M_i K_i \phi$

Suppose $M, w \models K_i \phi$

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

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

Validities

We already derived: $S5_{(m)} \vdash \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

We could also have proved: $S5_{(m)} \models \neg K_i \phi \leftrightarrow K_i \neg K_i \phi$

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

Let $M \in S5_{(m)}$ and w a world in M . To prove: $M, w \models K_i \phi \leftrightarrow M_i K_i \phi$

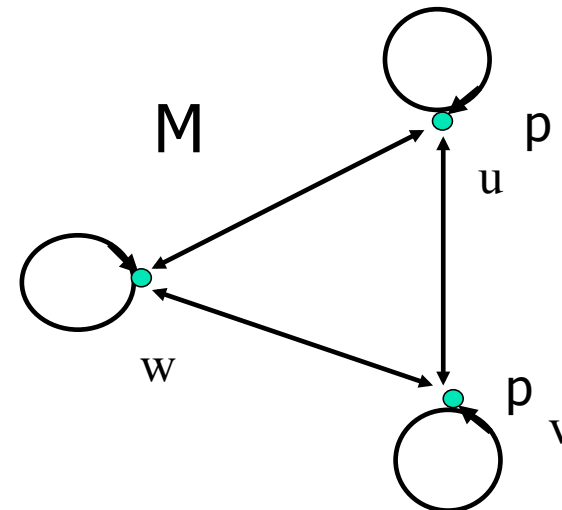
Suppose $M, w \models M_i K_i \phi$

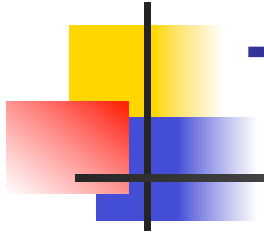
There is u , $R_i w u$ and $M, u \models K_i \phi$

Take v , $R_i w v$. To prove: $M, v \models \phi$

Since R_i is Euclidean, we have $R_i u v$. So $M, v \models \phi$

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



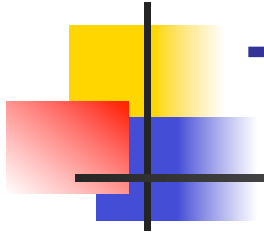


Tactics

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 $\mathbf{X}_{(m)} \not\vdash \psi$
use soundness and show $\mathcal{X}_{(m)} \not\models \varphi$



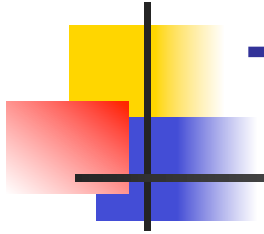
Tactics

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 $\mathbf{M} \in \mathcal{X}_{(m)}$
so that $\mathbf{M}, w \models \psi$

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
for some $\mathbf{M} \in \mathcal{X}_{(m)}$ we have $\mathbf{M}, w \models \psi$

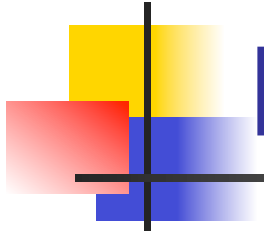


Tactics

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

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

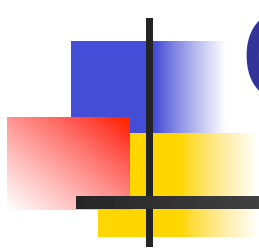
A formula ψ is $\mathbf{X}_{(m)}$ -derivable if
 $\mathbf{X}_{(m)} \vdash \psi$ if



Exercise 8

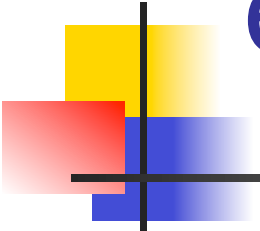
Are the following formulas valid with respect to $\mathbf{K}_{(m)}$? $\mathbf{T}_{(m)}$? $\mathbf{S4}_{(m)}$? $\mathbf{S5}_{(m)}$?

- (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) $\neg K_i \phi \rightarrow K_i \neg \phi$



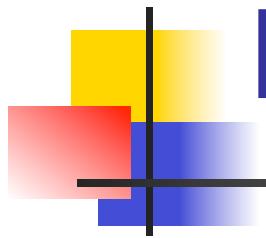
Group Notionss

W. van der Hoek



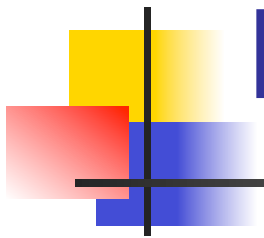
epistemic logic

- $K(\phi \rightarrow \psi) \rightarrow (K\phi \rightarrow K\psi)$
 - *agents reason rationally*
- $K\phi \rightarrow \phi$
 - *veridicality*
- $K\phi \rightarrow KK\phi$
 - *positive introspection*
- $\neg K\phi \rightarrow K\neg K\phi$
 - *negative introspection*
- $\vdash \phi \Rightarrow \vdash K\phi$
 - *agents know tautologies*



Everybody knows

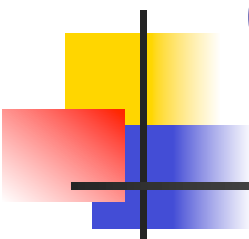
- $E\varphi$: Everybody knows φ
- definition: $E\varphi \equiv K_1\varphi \wedge K_2\varphi \wedge \dots K_n\varphi$
- veridical? introspective?



Distributed knowledge

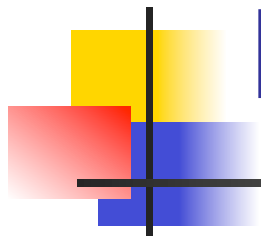
- $D\varphi$: it is distributed knowledge that φ
- idea: $(K_1\varphi \wedge K_2(\varphi \rightarrow \psi)) \rightarrow D\psi$
- veridical? introspective?
- ‘wise man’ to whom everybody tells
- also called “implicit knowledge” ($I\varphi$)

not: $D\psi \equiv K_1\phi \vee K_2\phi \vee \dots \vee K_n\phi$



Group notions

- $E\phi \equiv K_1\phi \wedge K_2\phi \wedge \dots \wedge K_n\phi$
 - *everybody knows ϕ*
- $K_i\phi \rightarrow D\phi$
 - *if one knows it, it is distributed*
- $D(\phi \rightarrow \psi) \rightarrow (D\phi \rightarrow D\psi)$
- $D\phi \rightarrow \phi$
- $D\phi \rightarrow DD\phi$
- $\neg D\phi \rightarrow D\neg D\phi$
- $\vdash \phi \Rightarrow \vdash D\phi$
 - *the wise man is at least as wise as the individuals!*
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
 - *agents reason rationally*
- $K_i\phi \rightarrow \phi$
 - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
 - *positive introspection*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
 - *negative introspection*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
 - *agents know tautologies*

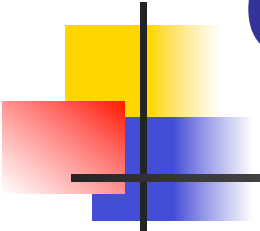


Distributed knowledge

- Consider the following derivation rule:

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

Adding RD as a rule or $K_i\phi \rightarrow D\phi$ as an axiom is equivalent!



Group notions: semantics

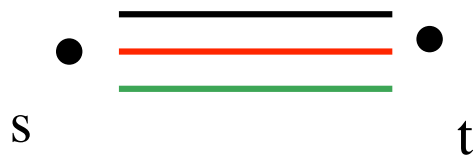
- $E\phi \equiv K_1\phi \wedge K_2\phi \wedge \dots K_n\phi$
 - *everybody knows ϕ*
- $K_i\phi \rightarrow D\phi$
 - *if one knows it, it is distributed*
- $R_E = R_1 \cup R_2 \cup \dots \cup R_n$
 - *taking the union*
- $R_D \subseteq R_1 \cap R_2 \cap \dots \cap R_n$
 - *not an equivalence!*

Group notions: semantics

R_1, R_2, R_D

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

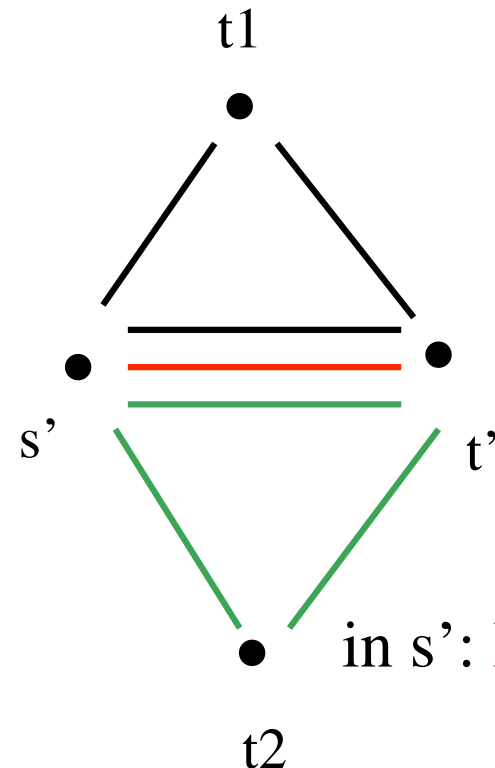
$M, s \models \varphi \Leftrightarrow M', s' \models \varphi$



in s : $R_D = R_1 \cap R_2$

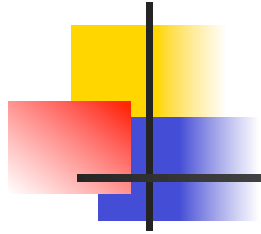
■ $R_D \subseteq R_1 \cap R_2 \cap \dots \cap R_n$

■ *not an equivalence!*



in s' : $R_D \neq R_1 \cap R_2$

Multi-agent knowledge



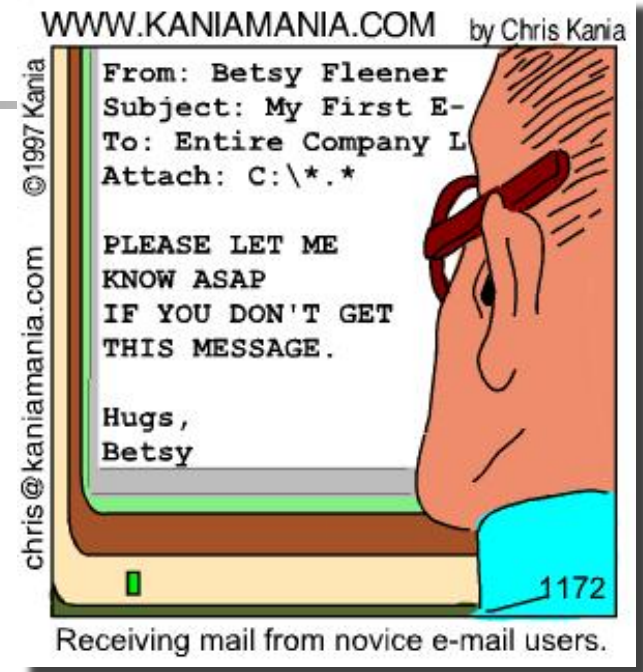
$K_A a$: A knows a

B sends m to A

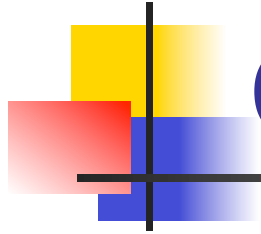
$K_B m$?

$K_A K_B m$?

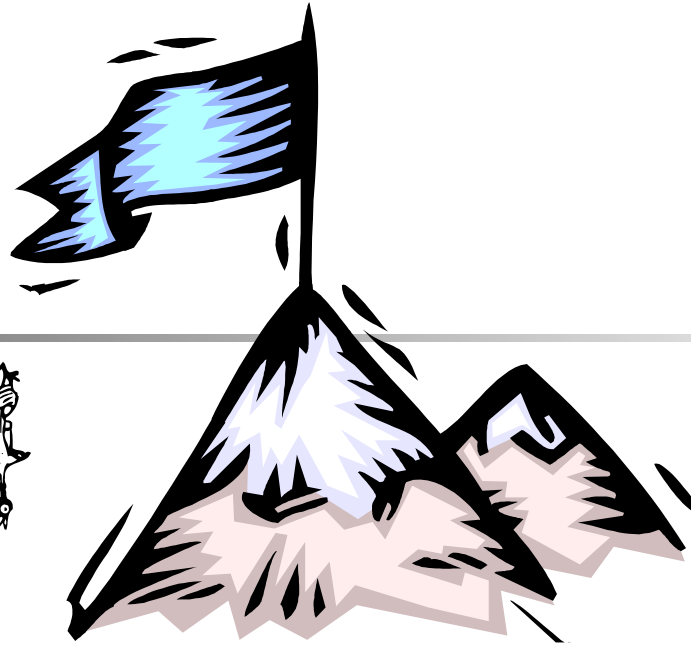
$K_B K_A K_B m$?



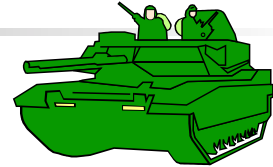
Bizantyne Generals



A



B



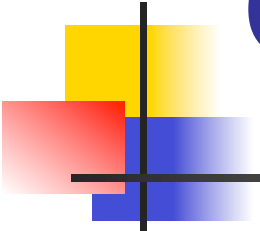
$K_A m$

$K_B m$

$K_A K_B m$

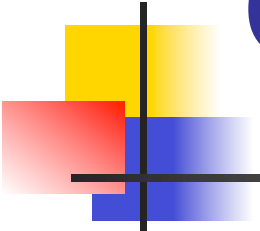
$K_B K_A K_B m$

$\neg K_A K_B K_A K_B m$



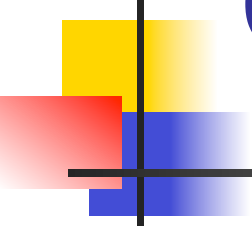
Common Knowledge

- $C(\phi \rightarrow \psi) \rightarrow (C \phi \rightarrow C \psi)$
 - *agents reason rationally*
- $C\phi \rightarrow \phi$
 - *veridicality*
- $C\phi \rightarrow EC \phi$
 - *and vice versa*
- $\vdash \phi \Rightarrow \vdash C\phi$
 - *tautologies are commonly known*
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
 - *agents reason rationally*
- $K_i\phi \rightarrow \phi$
 - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
 - *positive introspection*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
 - *negative introspection*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
 - *agents know tautologies*



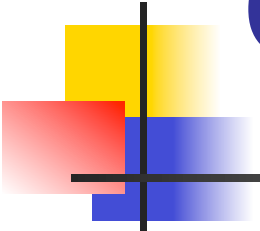
Common Knowledge

- $C(\phi \rightarrow \psi) \rightarrow (C\phi \rightarrow C\psi)$
 - *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”*
- $\vdash \phi \Rightarrow \vdash C\phi$
 - *tautologies are commonly known*
- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$
 - *agents reason rationally*
- $K_i\phi \rightarrow \phi$
 - *veridicality*
- $K_i\phi \rightarrow K_iK_i\phi$
 - *positive introspection*
- $\neg K_i\phi \rightarrow K_i\neg K_i\phi$
 - *negative introspection*
- $\vdash \phi \Rightarrow \vdash K_i\phi$
 - *agents know tautologies*



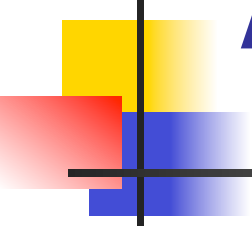
Common Knowledge

- $C(\phi \rightarrow \psi) \rightarrow (C\phi \rightarrow C\psi)$
 - *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”*
- $\vdash \phi \Rightarrow \vdash C\phi$
 - *tautologies are commonly known*
- Semantically, induction boils down to
- $R_C = R_E^*$
- that is, the reflexive transitive closure of R_E



Common Knowledge

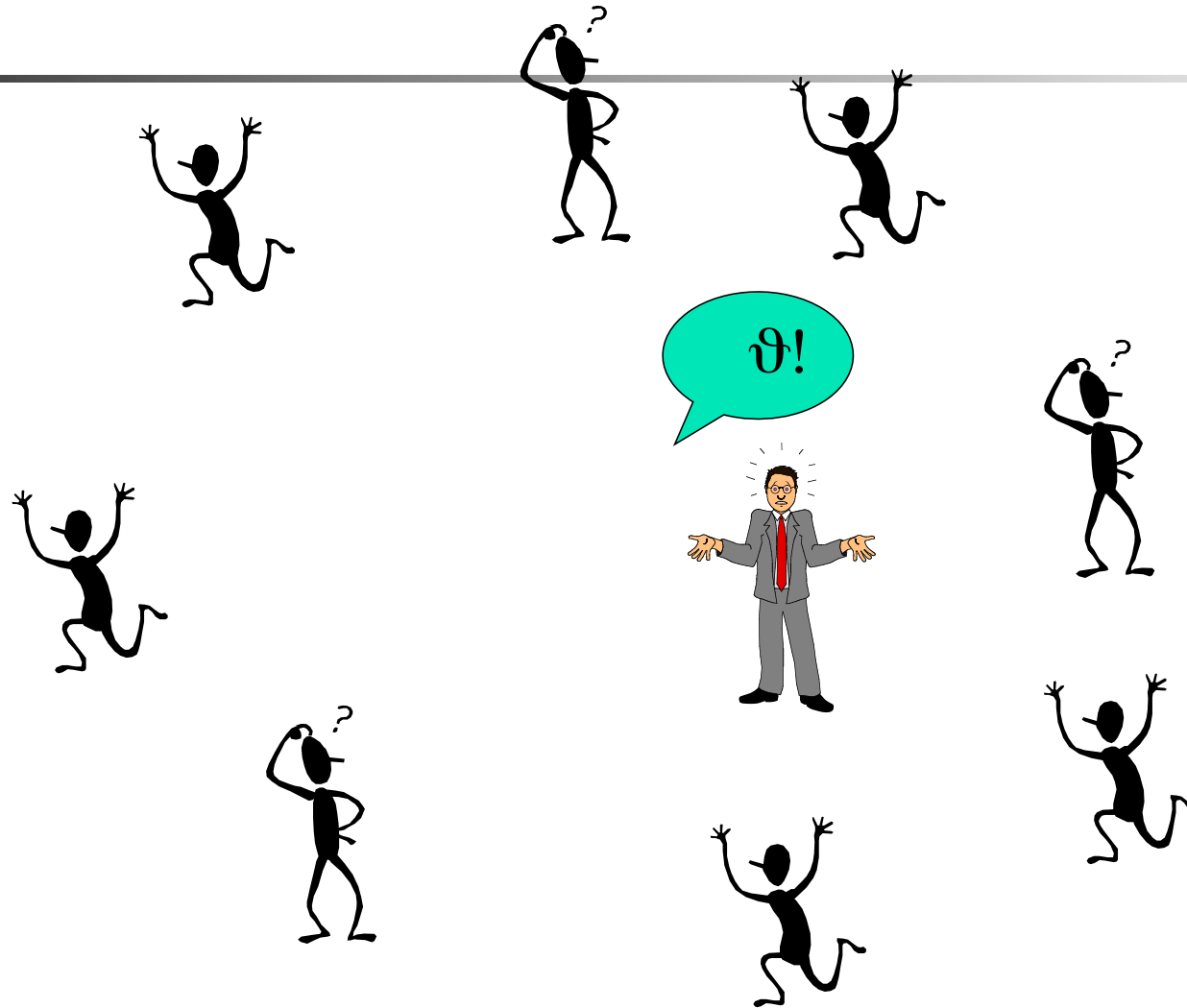
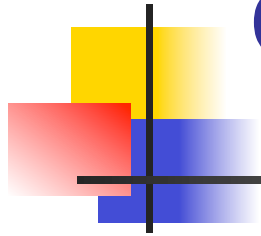
- $E\varphi$: Everybody knows φ
- $E\varphi \not\rightarrow EE\varphi$
- $C\varphi$: it is Common Knowledge that φ
- idea: $C\varphi = E\varphi \ \& \ EE\varphi \ \& \ EEE\varphi \ \& \ EEEE\varphi \ \& \ \dots$
- so: $\neg C\varphi$ if somebody
 - considers it possible that
 - somebody considers it possible that
 - somebody considers it possible that
 - φ does not hold

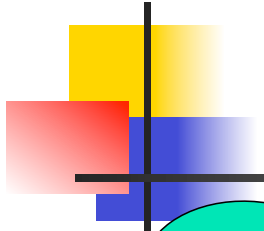


Alco at a conference

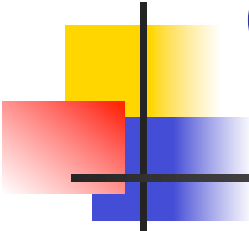
- A is at a conference. He decides to leave the room and have a drink at the bar.
 - There is an announcement φ : no talks tomorrow morning
 - $E \varphi? C \varphi?$
 - Then, A leaves the bar for a walk outside.
 - B says: “A is not here!” President: “intercom in bar!”
 - $E \varphi? EE \varphi? C \varphi?$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

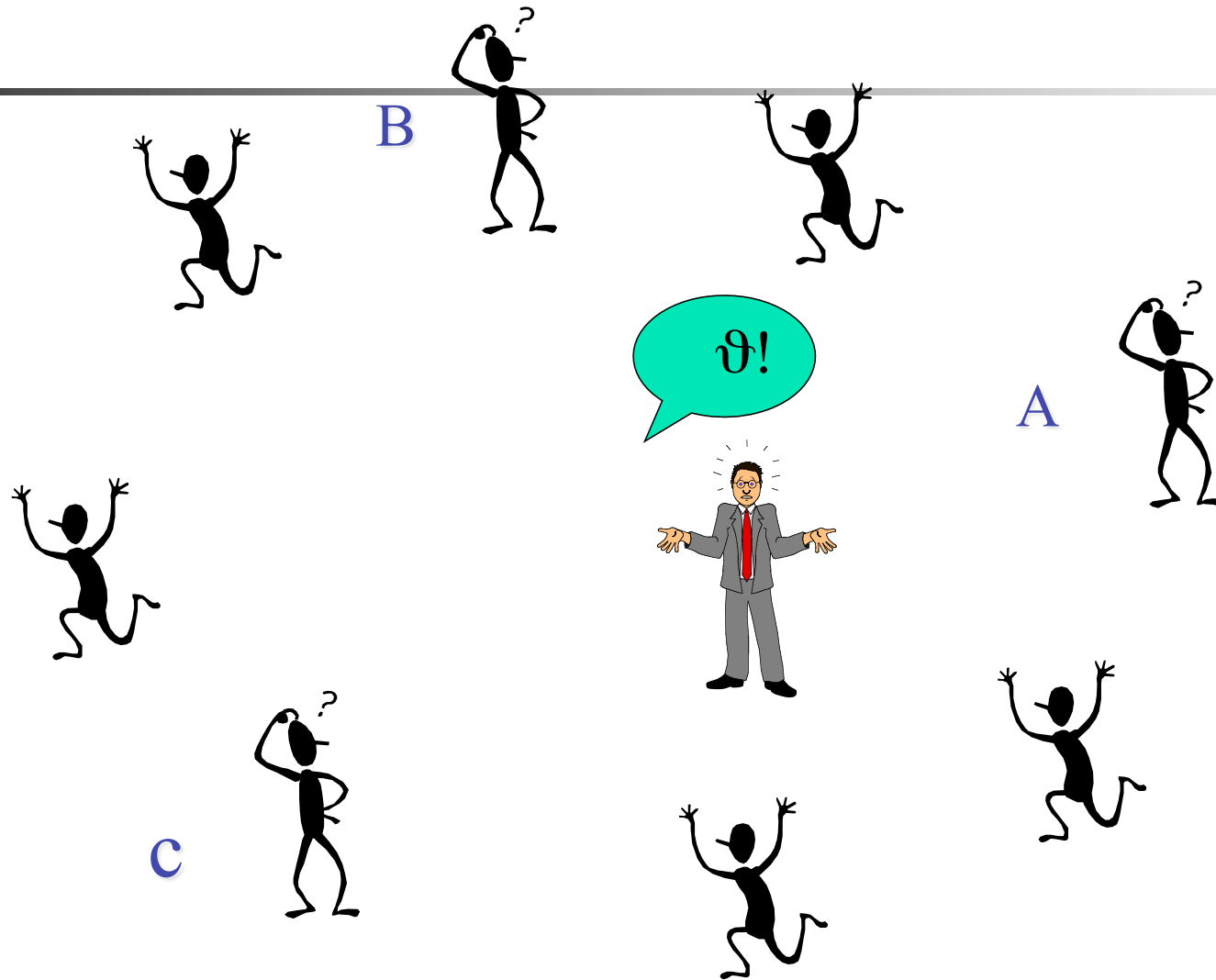
c children, m are muddy

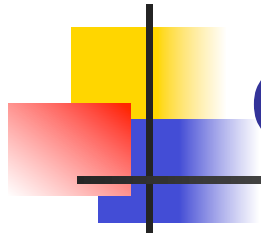




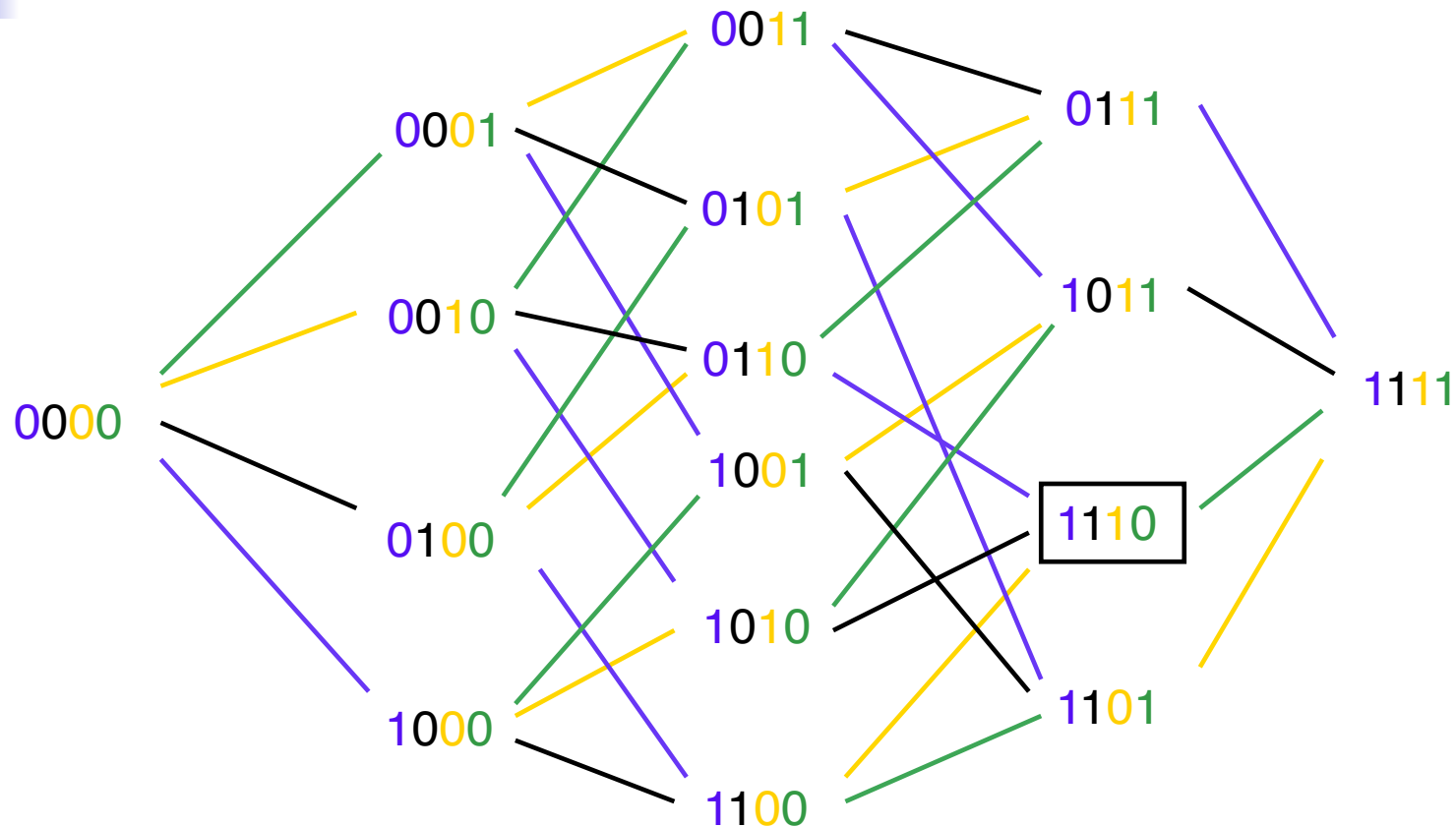
At least one of you is muddy.
If you know that you are, step forward!

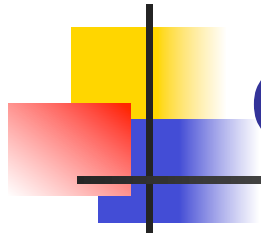

$$c = 8, m = 3$$



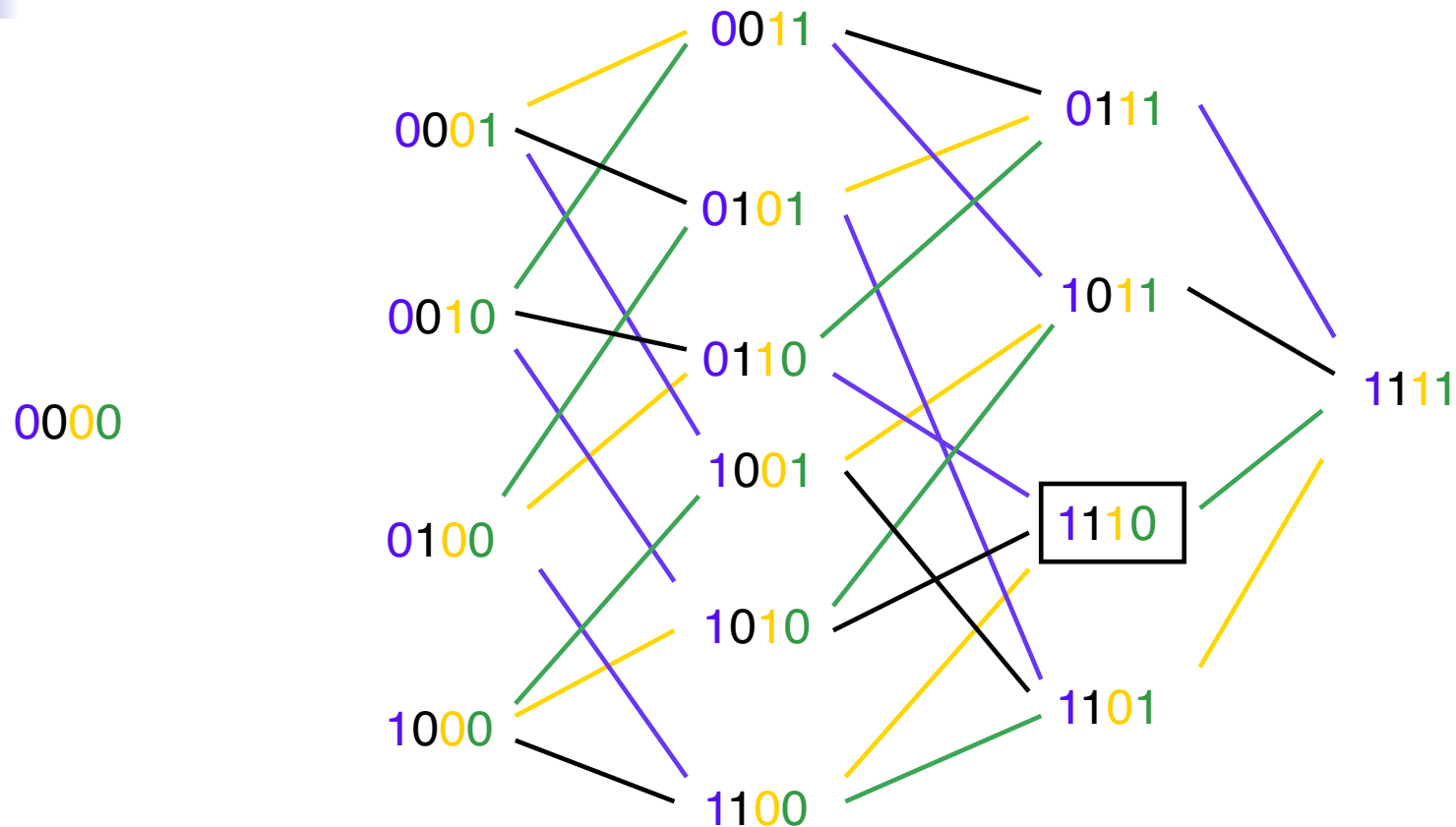


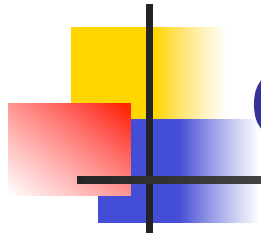
$c = 4, m = 3$ (Kripke models)



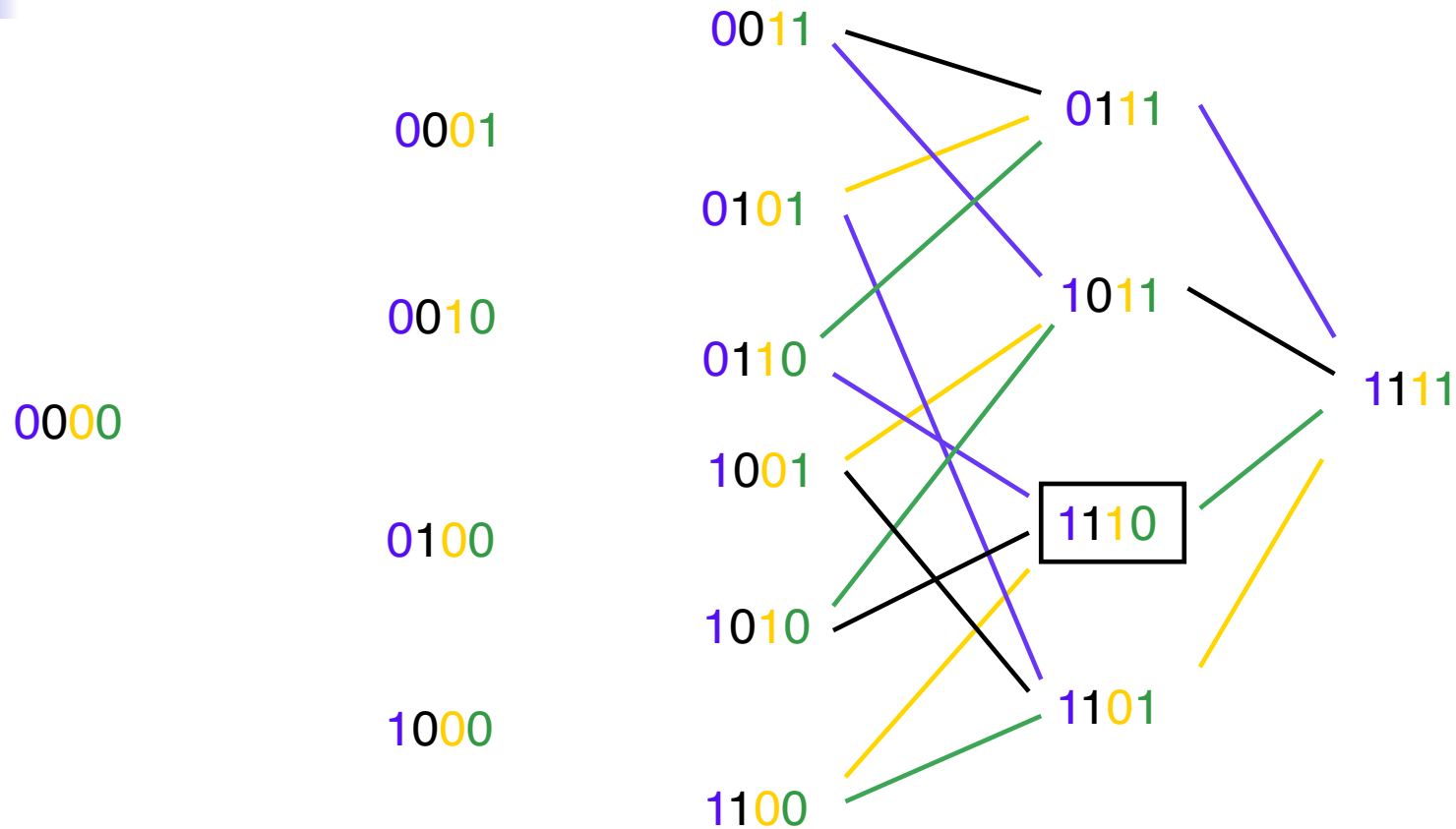


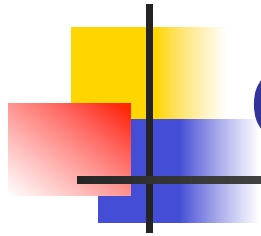
$c = 4, m = 3$ (Kripke models)



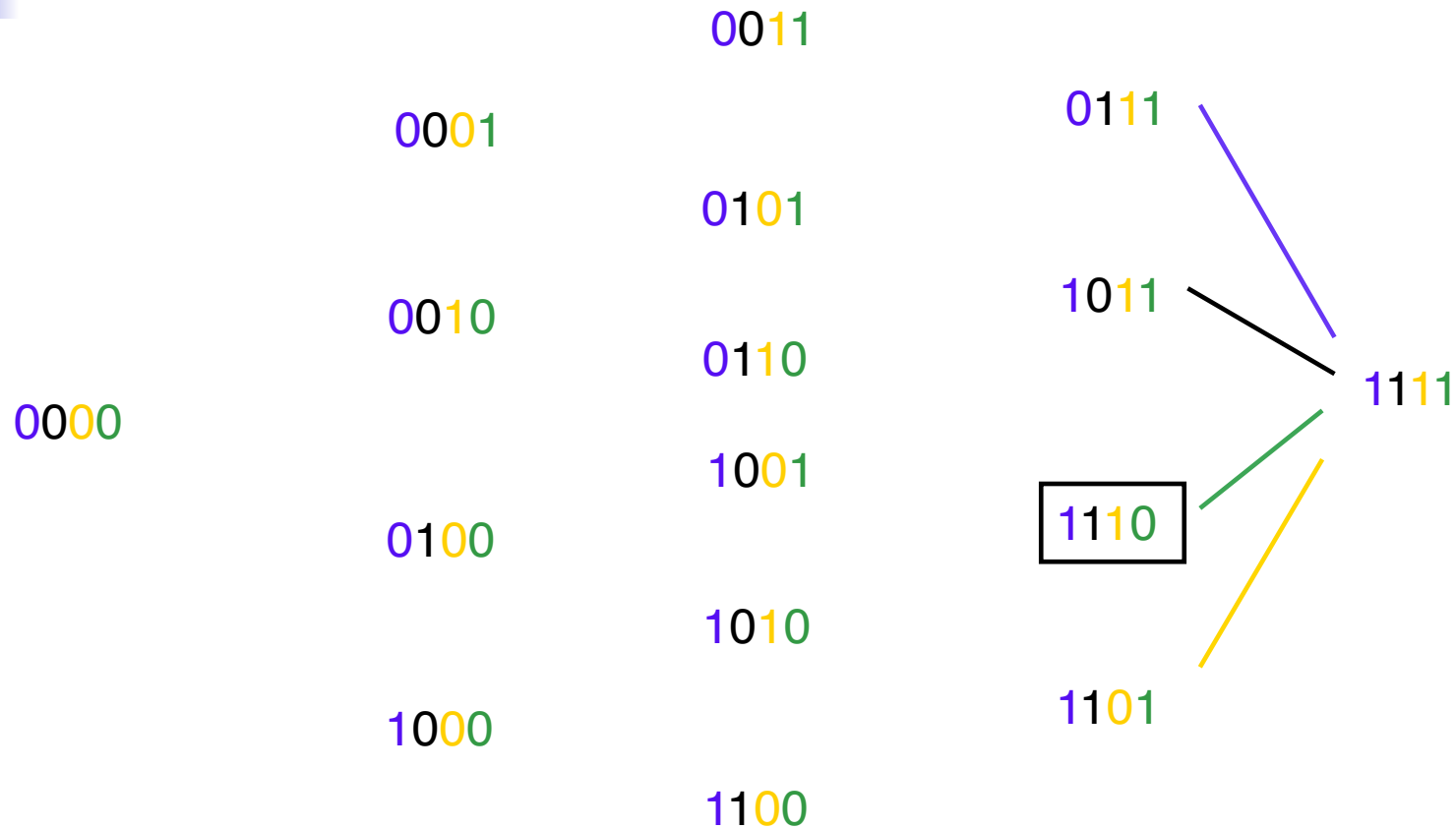


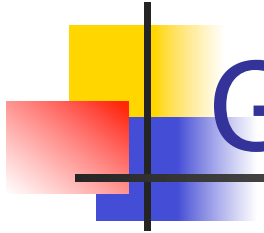
$c = 4, m = 3$ (Kripke models)





$c = 4, m = 3$ (Kripke models)





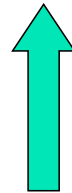
Group Knowledge

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

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



"any fool knows"



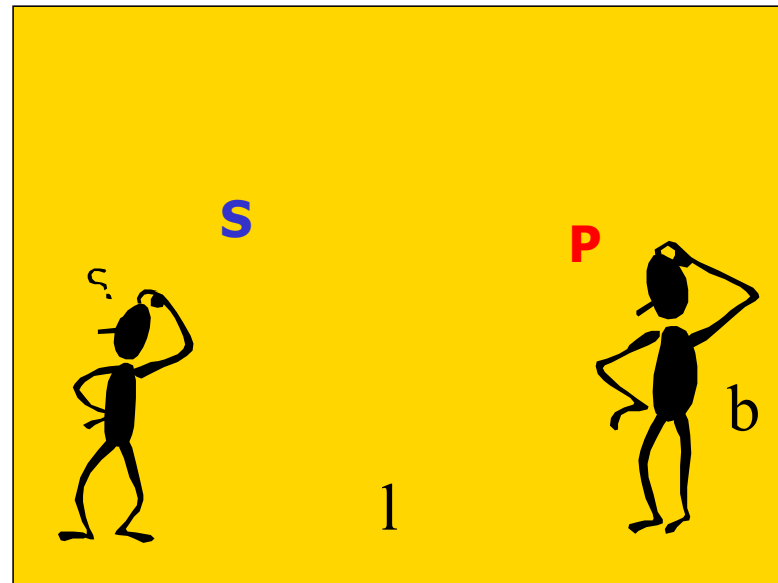
"a wise man knows"

Common Knowledge cannot be obtained through communication

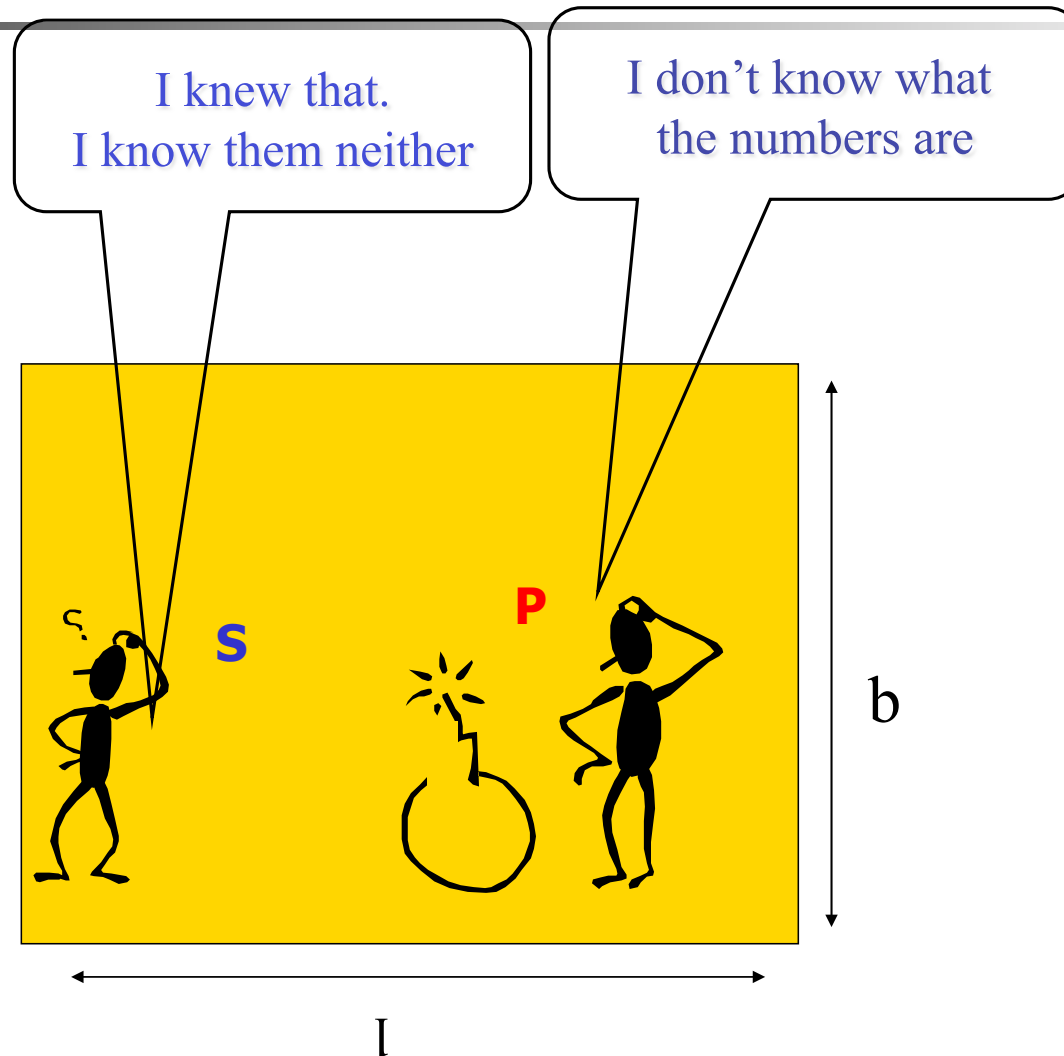
$$C\varphi \leftrightarrow EC\varphi$$

Ignorance

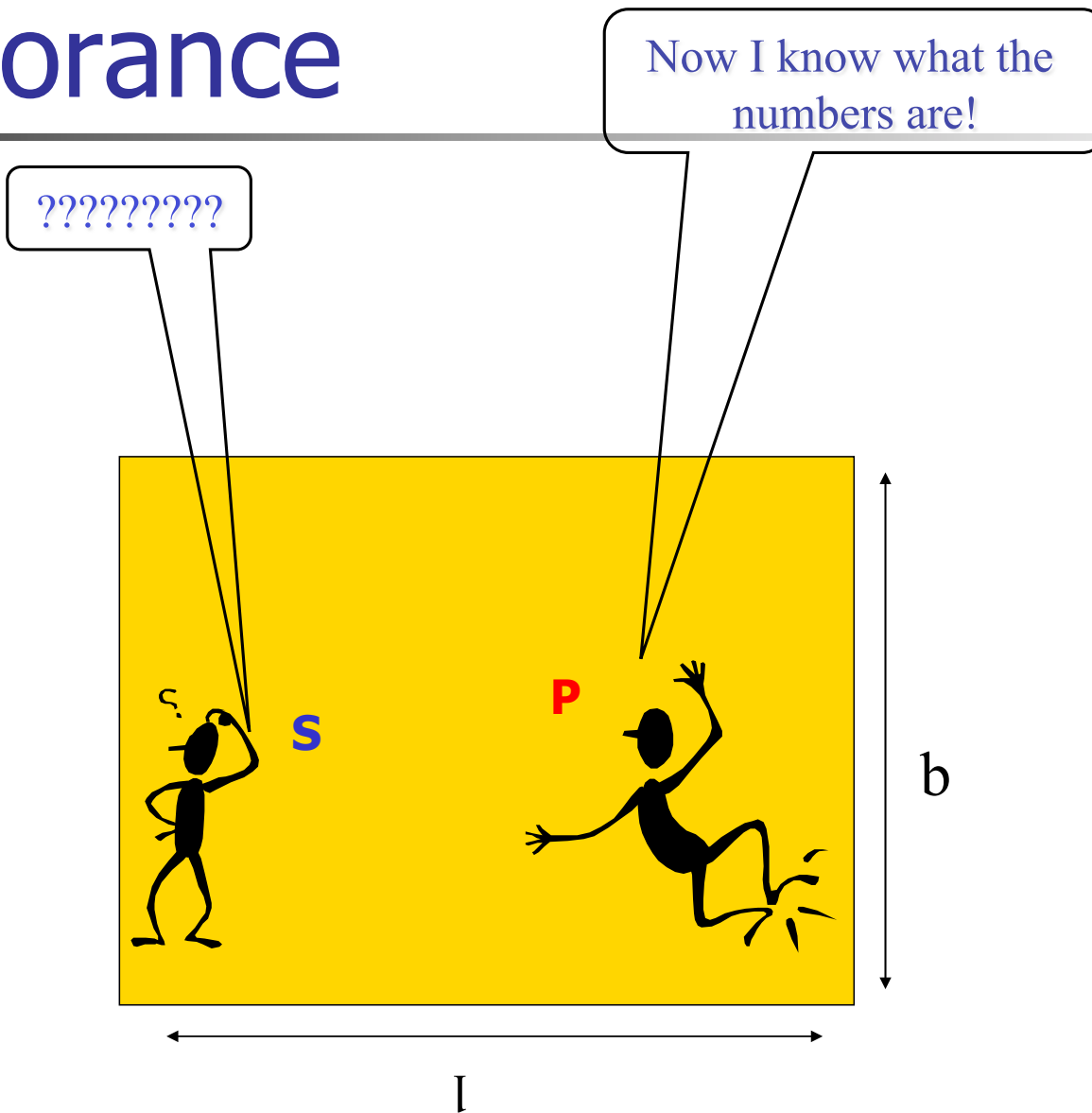
- **P** and **S** are in a room, $1 \times b$
- $2 \leq b \leq 1 \leq 99$
- **P** knows $1 \times b$
- **S** knows $1 + b$



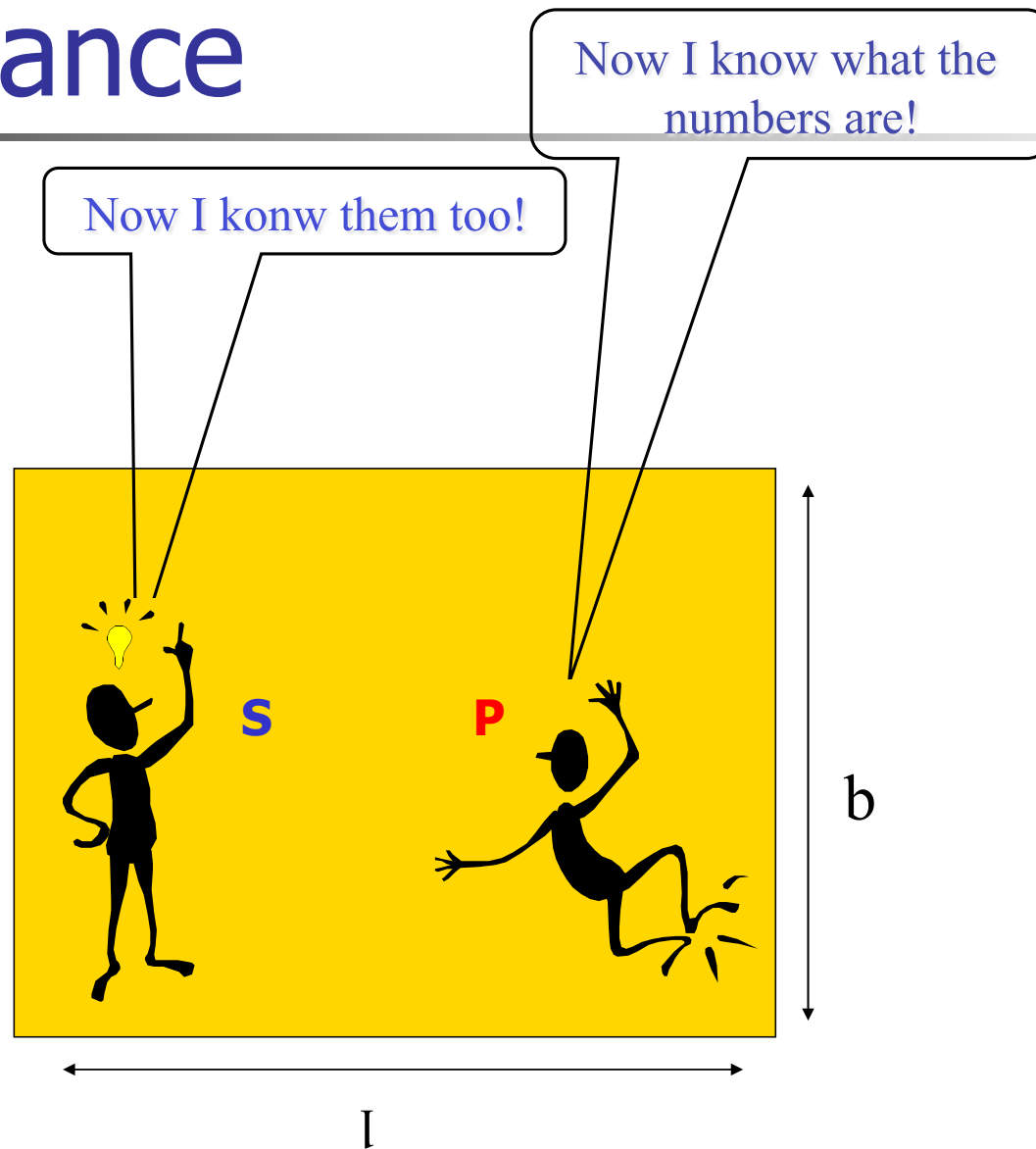
Ignorance

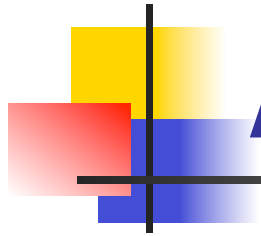


Ignorance



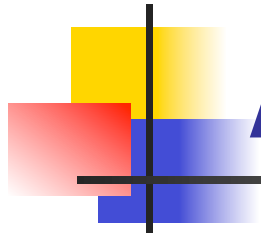
Ignorance





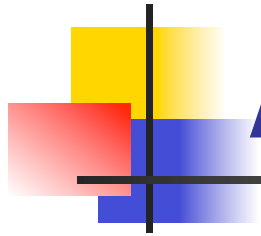
Advanced Byzantine Generals

- S and R are involved in a protocol.
- It is common knowledge that:
 - messages derive either immediately or with ε time delay



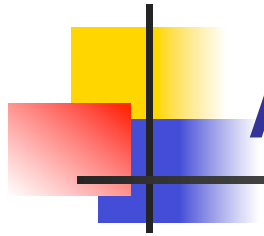
Advanced Byzantine Generals

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

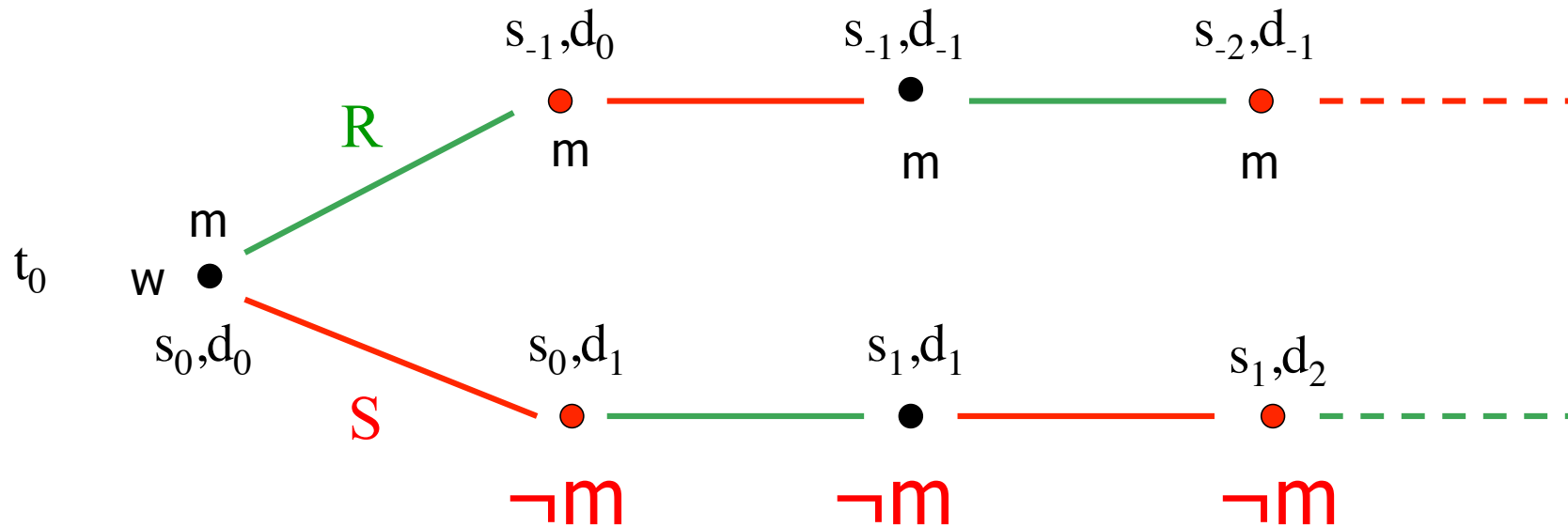


Advanced Byzantine Generals

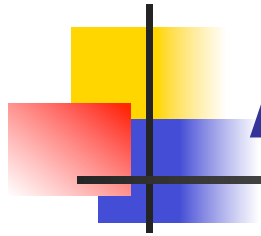
- let s: “sent”, d: “delivered” e: “delay”
- suppose there is no delay
- time: $t_0, t_1 = t_0 + \varepsilon, \dots, t_n = t_0 + n\varepsilon$
- Sender is red, Receiver is green
- reflexive arrows are implicit
- $\bullet$ means delay, $\bullet$ means no delay
- m means: message has arrived



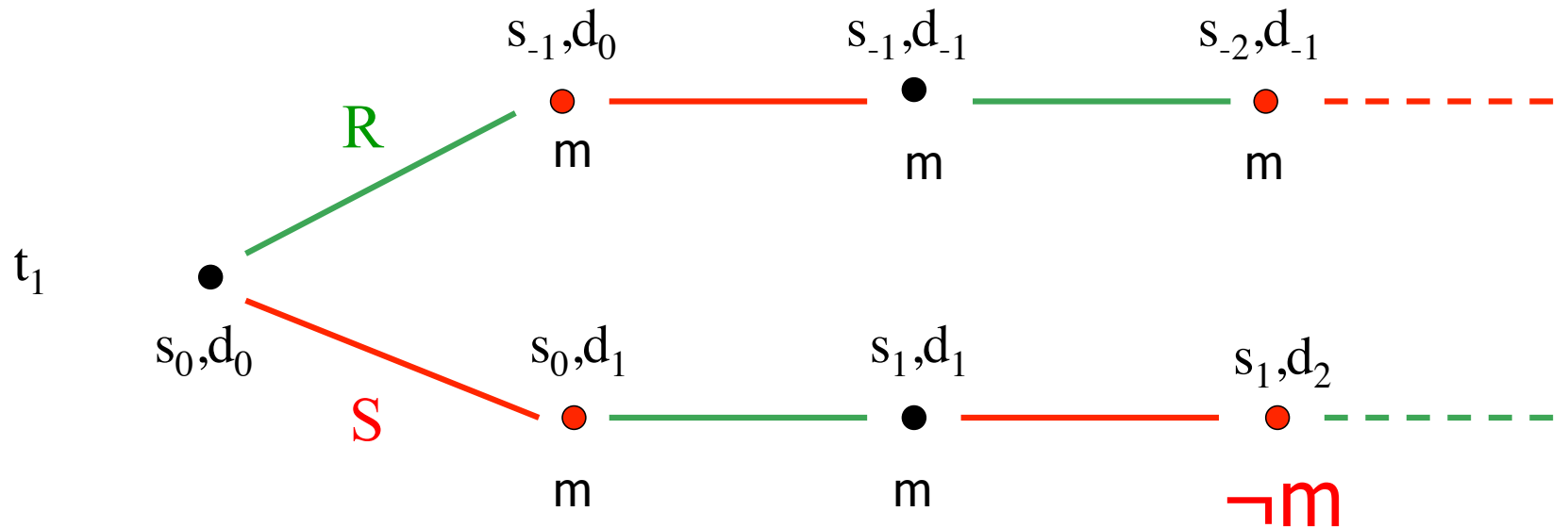
Advanced Byzantine Generals



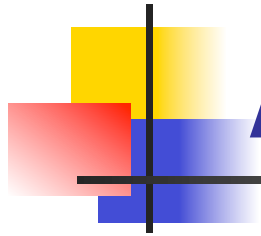
$$M, w \models K_R m \wedge \neg K_S m$$



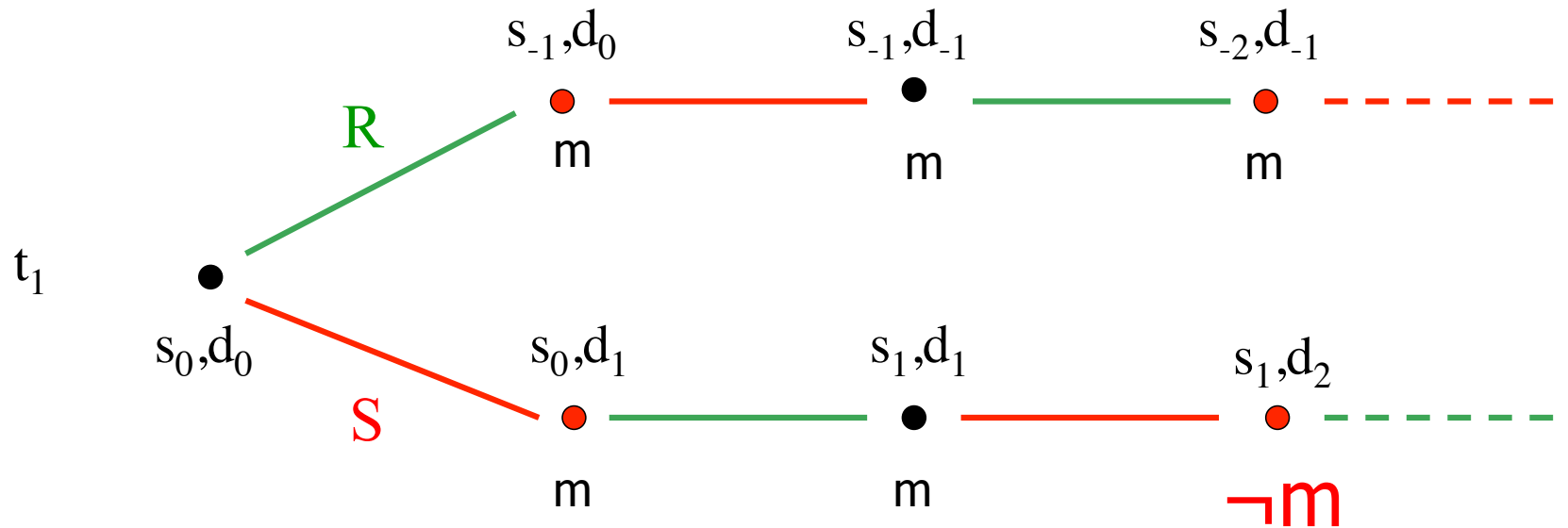
Advanced Byzantine Generals



$$M, w \models Em \wedge EEm \wedge \neg K_S K_R K_S m$$

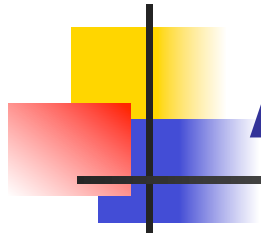


Advanced Byzantine Generals



after t seconds, world with s_t, d_{t+1} is the ‘first’ where $\neg m$ holds

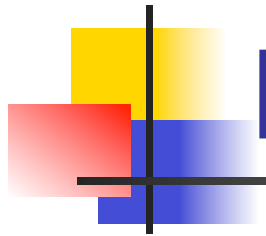
$$M, w \models E^{t+1}m \wedge \neg K_S (K_R K_S)^t m$$



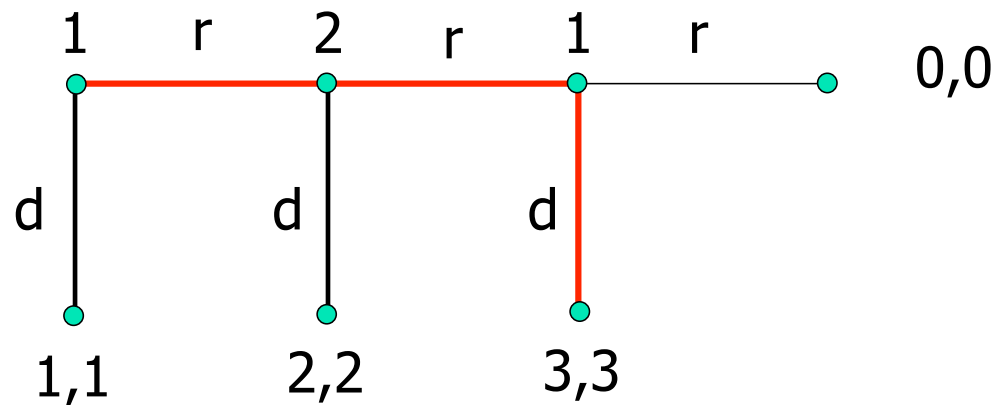
Advance Byzantine Generals

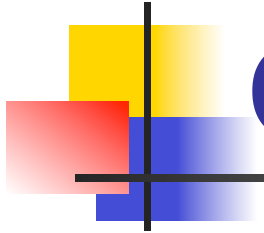
- S and R are involved in a protocol
- It is common knowledge that:
 - messages derive either immediately or with ϵ time delay
- S sends m at t_0 .
- When do we have C_m ???????

NEVER!!!!!!!!!!



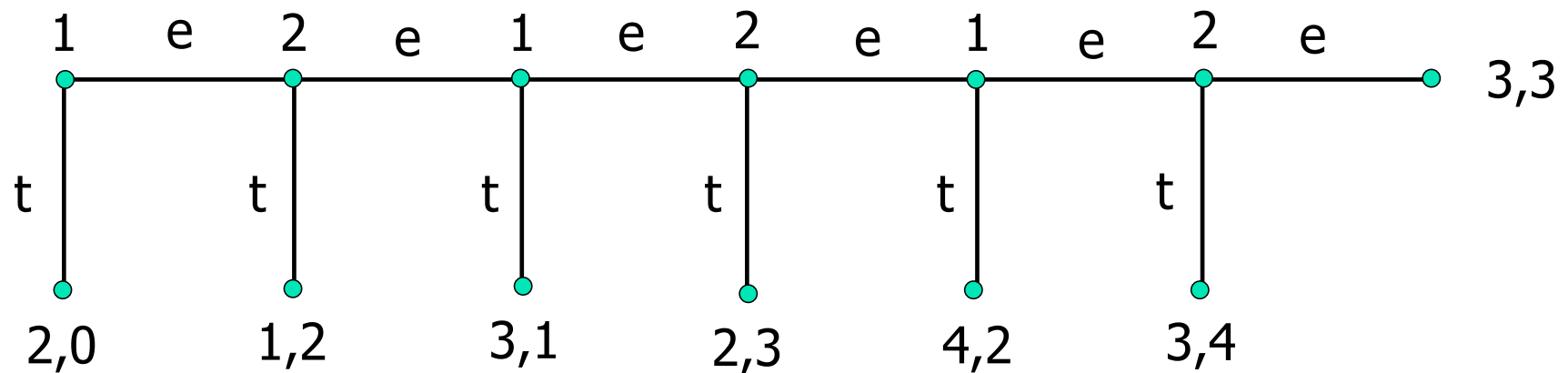
Backward Induction

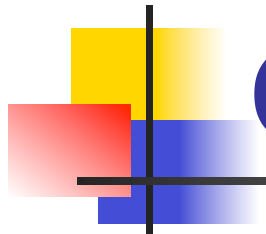




Centipede

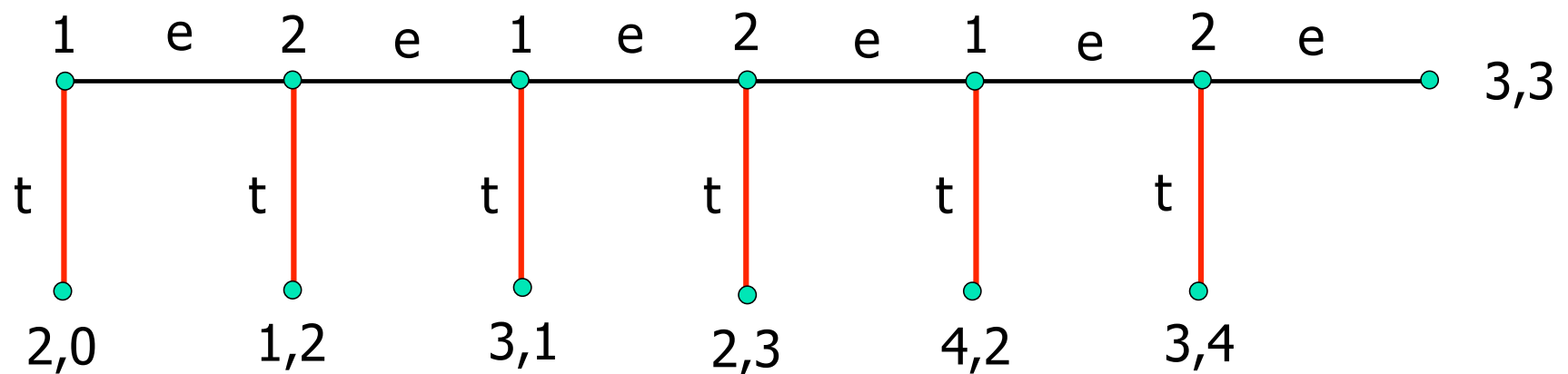
- 1 and 2 divide n marbles; they choose in turn, if somebody picks two, the game is over

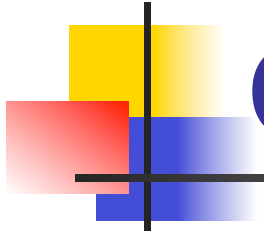




Centipede

- Intuitively correct?





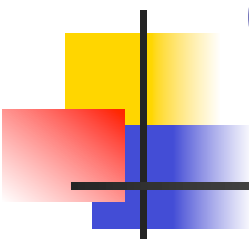
Gossiping

- six friends each have a gossip. They call each other
- at each call, they share their information
- at least how many calls are needed to bring all of them up 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 $\vdash \phi \Rightarrow \vdash C\phi$

- *tautologies are commonly known*

- $K_i(\phi \rightarrow \psi) \rightarrow (K_i\phi \rightarrow K_i\psi)$

- *agents reason rationally*

- $K_i\phi \rightarrow \phi$

- *veridicality*

- $K_i\phi \rightarrow K_iK_i\phi$

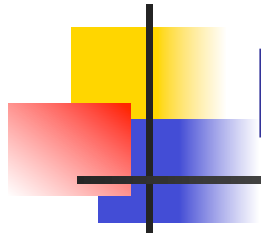
- *positive introspection*

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

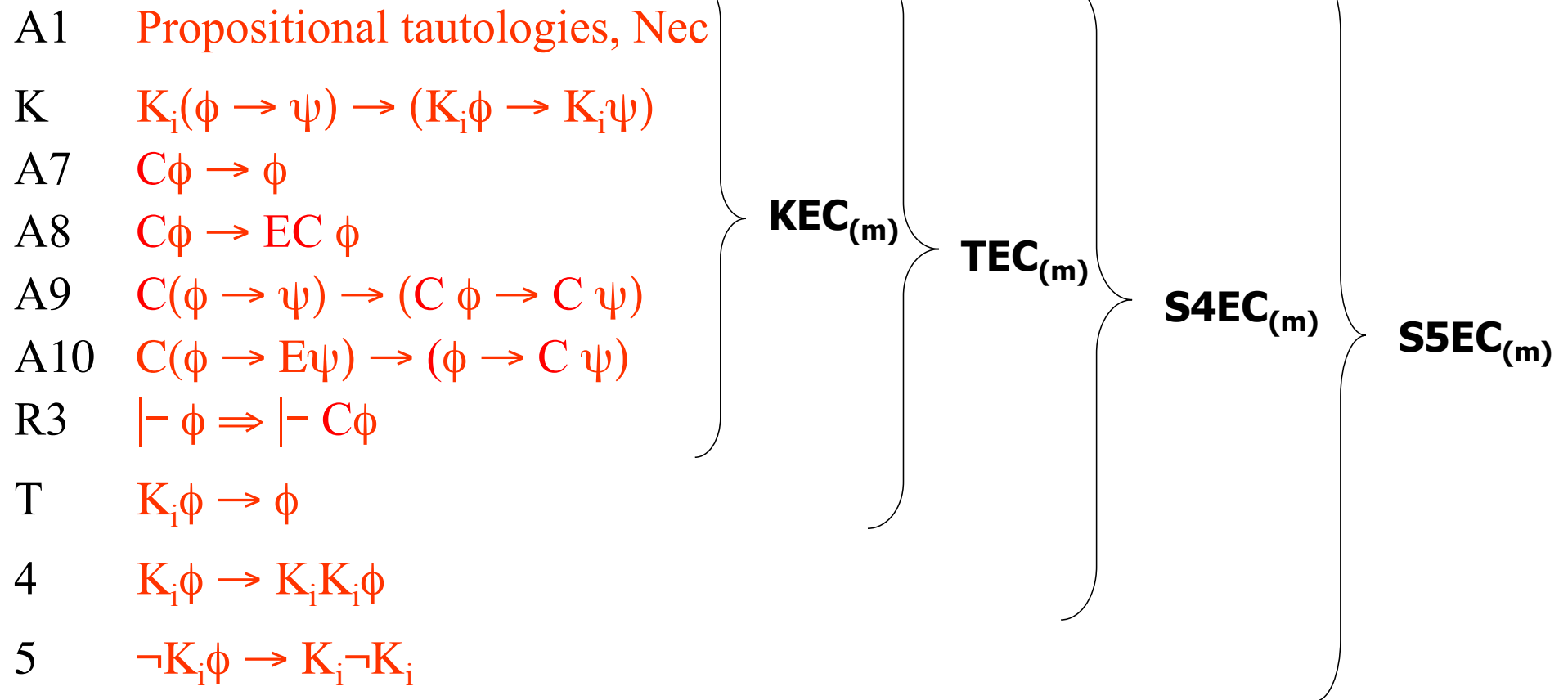
- *negative introspection*

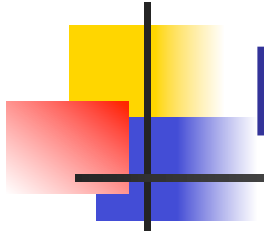
- $\vdash \phi \Rightarrow \vdash K_i\phi$

- *agents know tautologies*



Different Modal Systems





Lemma (X-distribution)

Let X be a necessity operator. Then:

$$\mathbf{K}_{(\mathbf{m})} \vdash \phi \rightarrow \psi \Rightarrow \mathbf{K}_{(\mathbf{m})} \vdash X\phi \rightarrow X\psi$$

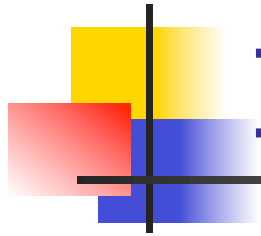
Proof. Let X be a necessity operator.

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

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

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

Modus Ponens then gives $\mathbf{K}_{(\mathbf{m})} \vdash (X\phi \rightarrow X\psi)$



Iterations of Modal Operators

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

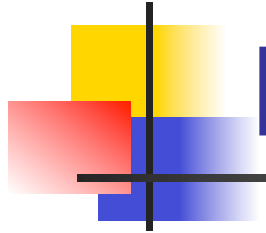
$$X^0\phi = \phi$$

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

Example:

$$K_2^3\phi = K_2K_2K_2\phi, E^5\phi = EEEEE\phi$$

$$\text{and even } (K_2E)^4\phi = K_2E K_2E K_2E K_2E \phi$$



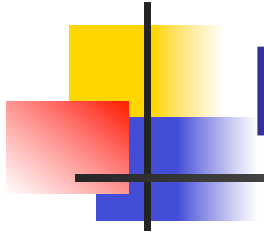
First Property

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

$$1 \quad C\phi \rightarrow \phi \qquad A7$$

hence,

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



First Property

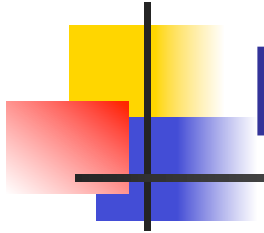
Claim: for every n , $\mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^n\phi$

suppose we already proven: $\mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^k\phi$

- | | | |
|---|-------------------------------|-------------|
| 1 | $C\phi \rightarrow E^k\phi$ | ass |
| 3 | $C\phi \rightarrow EC\phi$ | A8 |
| 4 | $EC\phi \rightarrow EE^k\phi$ | 2, E-distr. |
| 5 | $C\phi \rightarrow EE^k\phi$ | 2,3,A1 |

hence,

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



First Property: winding up

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

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

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

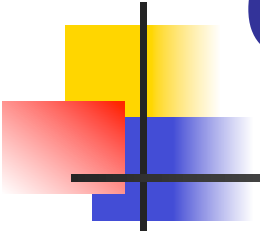
$$\mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^1\phi \quad \text{so } \mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^2\phi$$

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

$$\mathbf{KEC}_{(m)} \vdash C\phi \rightarrow \dots \quad \text{so } \mathbf{KEC}_{(m)} \vdash C\phi \rightarrow \dots$$

$$\mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^{n-1}\phi \quad \text{so } \mathbf{KEC}_{(m)} \vdash C\phi \rightarrow E^n\phi$$

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



Common Knowledge

$$M, w \models E\phi \Leftrightarrow$$

$$\forall v (R_E wv \Rightarrow M, v \models \phi)$$

$$\text{with } R_E = R_1 \cup R_2 \cup \dots \cup R_n$$

■ Definition of closure:

- $\forall x R_E^* xx$

- $R_E xy \Rightarrow R_E^* xy$

- $R_E^* xy \ \& \ R_E yz \Rightarrow R_E^* xz$

$$M, w \models C\phi \Leftrightarrow$$

$$\forall v (R_E^* wv \Rightarrow M, v \models \phi)$$

with R_E^* is reflexive transitive closure of R_E

Common Knowledge

Definition of closure:

- $\forall x R_E^* x x$
- $R_E x y \Rightarrow R_E^* x y$
- $R_E^* x y \ \& \ R_E y z \Rightarrow R_E^* x z$

$$M, w \models C\phi \Leftrightarrow$$

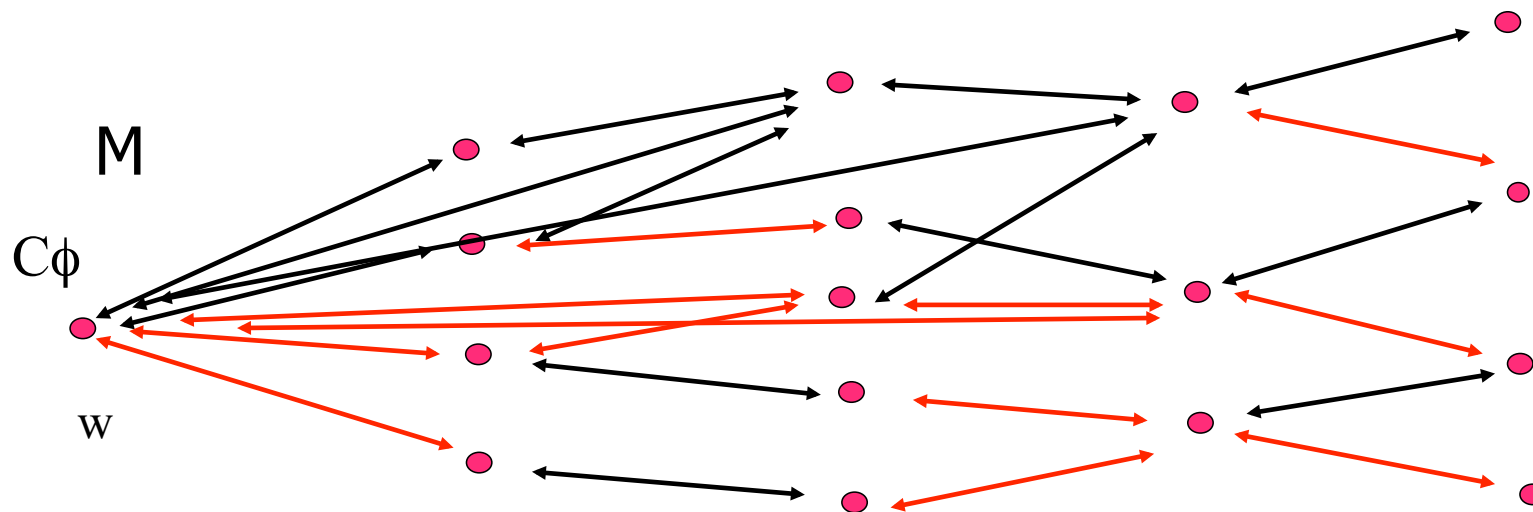
$$M, w \models \phi \ \&$$

$$\forall v (R_E w v \Rightarrow M, v \models \phi) \ \&$$

$$\forall v \forall u (R_E w v \ \& \ R_E v u \Rightarrow M, u \models \phi) \ \&$$

$$\forall v \forall u \forall t (R_E w v \ \& \ R_E v u \ \& \ R_E u t \Rightarrow M, t \models \phi) \ \&$$

.....



Common Knowledge

Definition of closure:

- $\forall x R_E^* x x$
- $R_E x y \Rightarrow R_E^* x y$
- $R_E^* x y \ \& \ R_E y z \Rightarrow R_E^* x z$

$$M, w \models \neg C\phi \Leftrightarrow$$

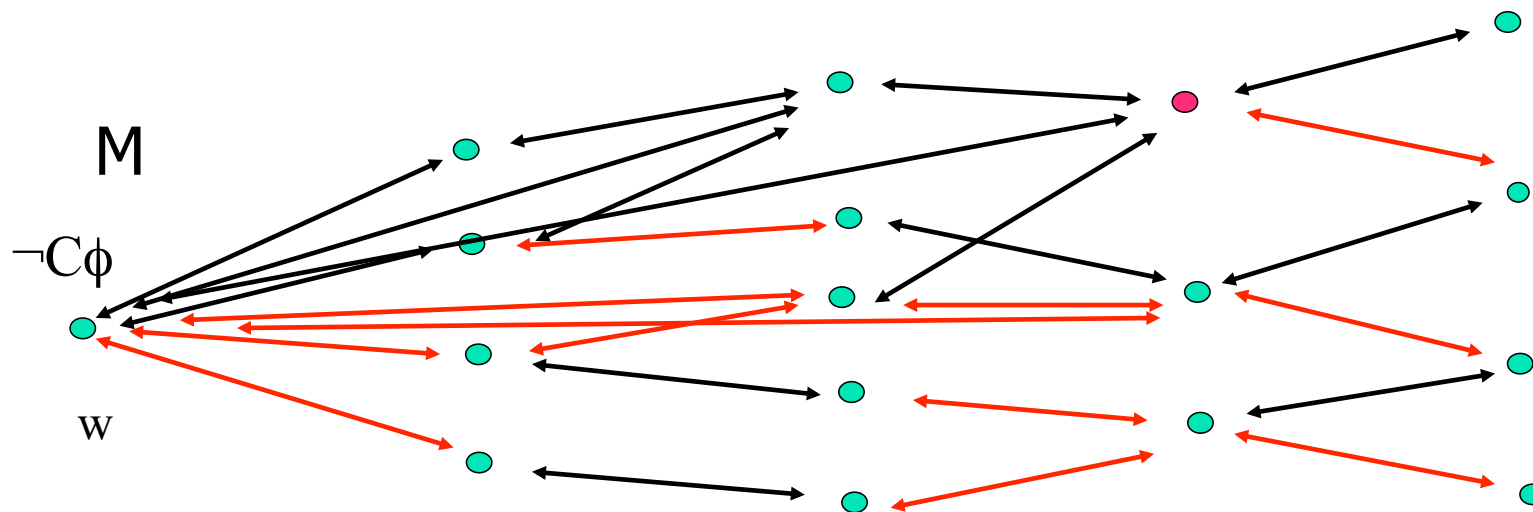
$$M, w \models \neg\phi \text{ or}$$

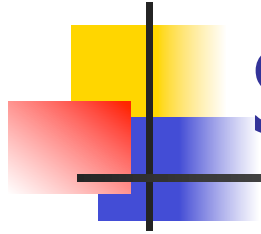
$$\exists v (R_E w v \ \& \ M, v \models \neg\phi) \text{ or}$$

$$\exists v \exists u (R_E w v \ \& \ R_E v u \ \& \ M, u \models \phi) \text{ or}$$

$$\exists v \exists u \exists t (R_E w v \ \& \ R_E v u \ \& \ R_E u t \ \& \ M, t \models \phi) \text{ or}$$

.....





Soundness and Completeness

Given the truth definition $M, w \models C\phi \Leftrightarrow$

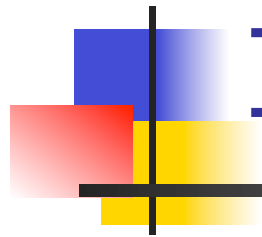
$$\forall v (R_E * wv \Rightarrow M, v \models \phi)$$

$$\mathbf{KEC}_{(m)} \vdash \phi \Leftrightarrow \mathcal{K}_{(m)} \models \phi$$

$$\mathbf{TEC}_{(m)} \vdash \phi \Leftrightarrow \mathcal{T}_{(m)} \models \phi$$

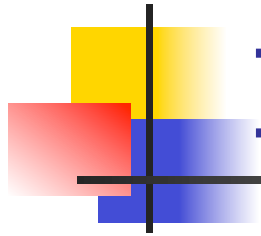
$$\mathbf{S4EC}_{(m)} \vdash \phi \Leftrightarrow \mathcal{S4}_{(m)} \models \phi$$

$$\mathbf{S5EC}_{(m)} \vdash \phi \Leftrightarrow \mathcal{S5}_{(m)} \models \phi$$



Interpreted Systems

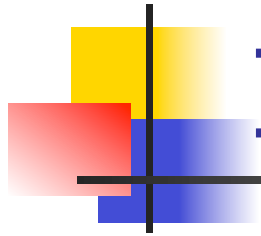
W. van der Hoek



Interpreted Systems

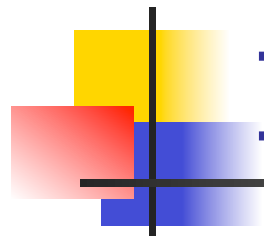
- We have m processors
- each i can be in a number of states $\in L_i$
- Now build $M = \langle S, \pi, R_1, R_2, \dots, R_m \rangle$
 - $S = L_1 \times L_2 \times \dots \times L_m$
 - $= \{ \mathbf{s} = \langle s_1, s_2, \dots, s_m \rangle \mid s_i \in L_i \}$
 - $\pi: S \rightarrow P \rightarrow \{t, f\}$
 - $R_i = \{(\mathbf{s}, \mathbf{t}) \mid s_i = t_i\}$

EQUIVALENCE RELATION!!!!!!!!!!!!!!

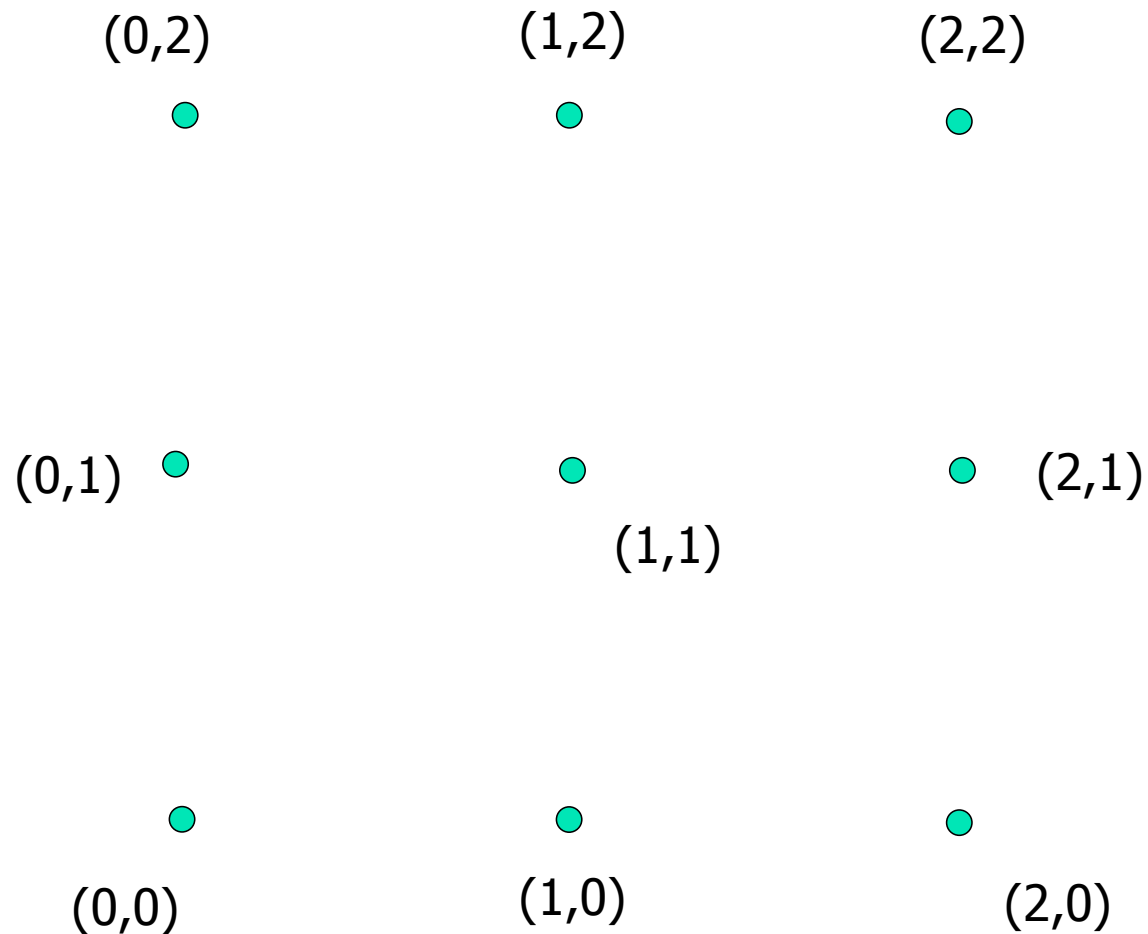


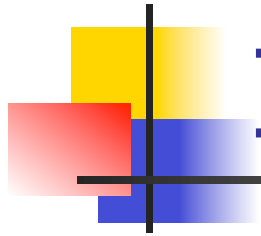
Interpreted Systems: Example

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



Interpreted Systems: Example





Interpreted Systems: Example

(0,2) (1,2) (2,2)



$R_B \mathbf{s} \mathbf{t} \Leftrightarrow$

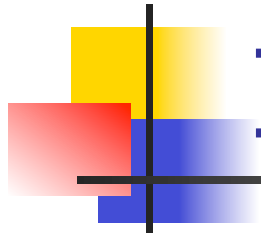
$R_B (x_1, y_1) (x_2, y_2) \Leftrightarrow$
 $y_1 = y_2$

(0,1) (1,1) (2,1)

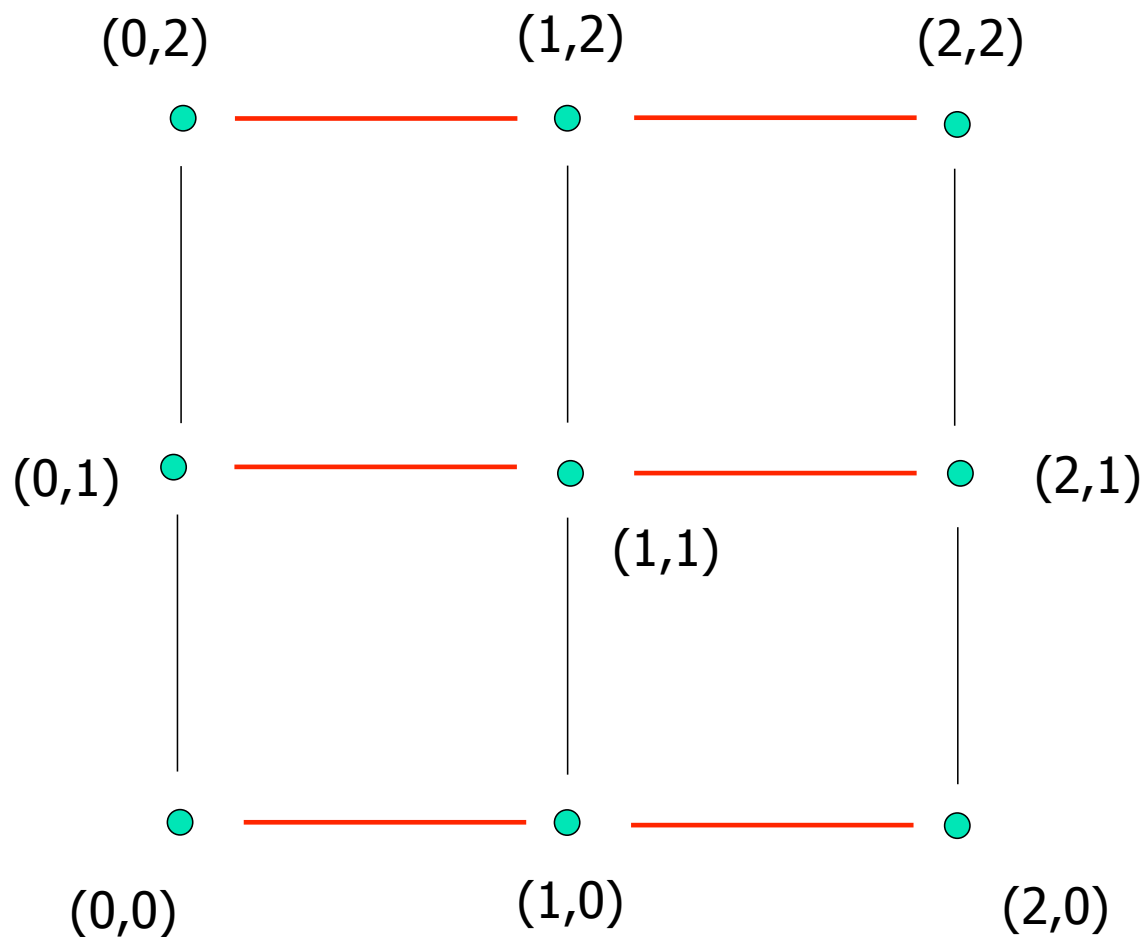


(0,0) (1,0) (2,0)





Interpreted Systems: Example

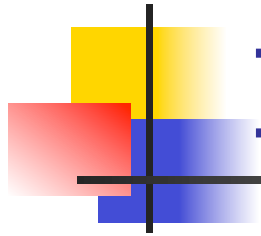


$$R_B \mathbf{s} \mathbf{t} \Leftrightarrow$$

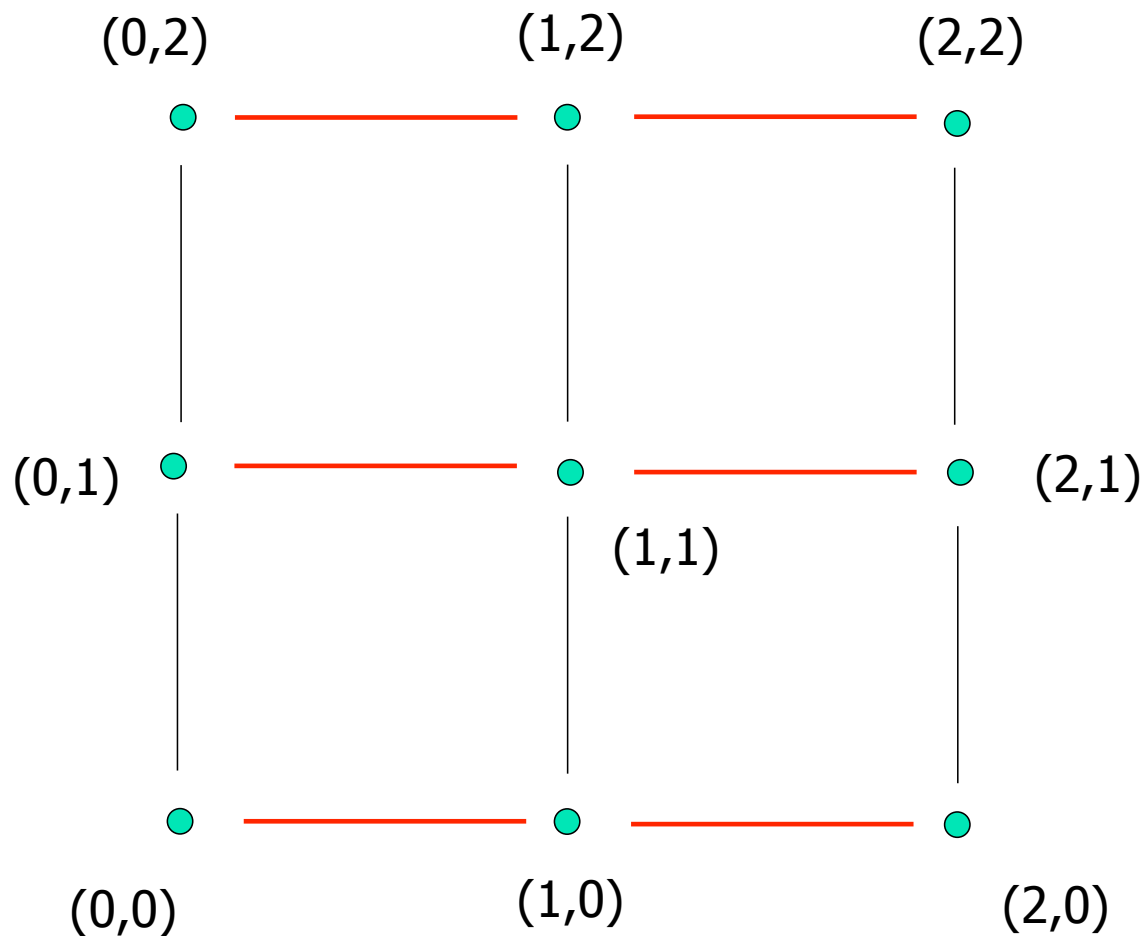
$$R_B (x_1, y_1) (x_2, y_2) \Leftrightarrow y_1 = y_2$$

$$R_A \mathbf{s} \mathbf{t} \Leftrightarrow$$

$$R_A (x_1, y_1) (x_2, y_2) \Leftrightarrow x_1 = x_2$$



Interpreted Systems: Example

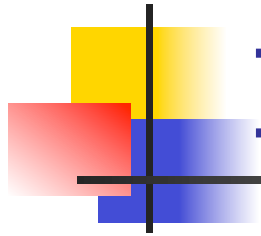


Atoms:

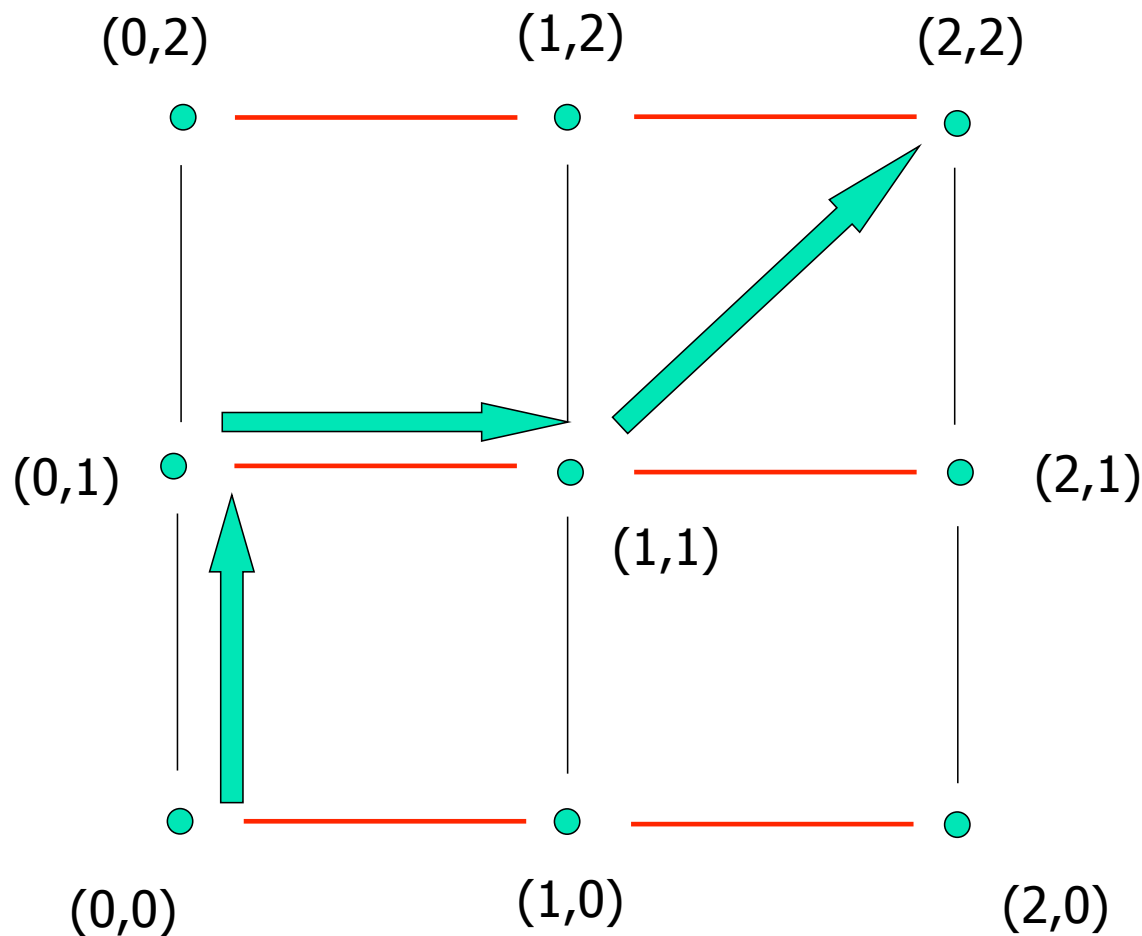
$x=0$; $x=1$; $x=2$ and
 $y=0$; $y=1$; $y=2$

$M, (0,0) \models K_A x=0$

$M, (0,0) \models K_A \neg K_B (x=0)$



Interpreted Systems: Runs

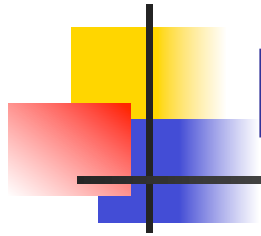


Starting in (0,0), B changes its value from 0 to 1

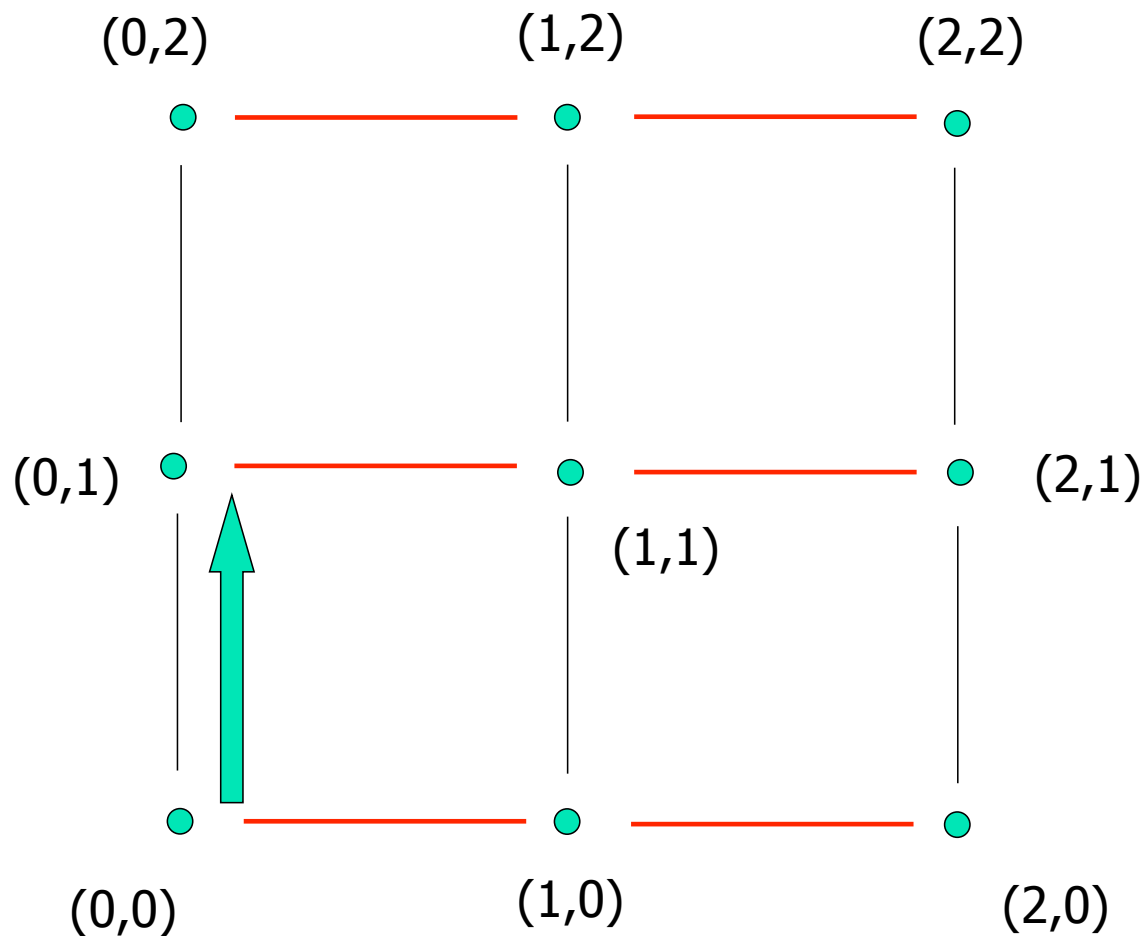
A does not notice this: he knows the same in (0,0) and (0,1)

Then, A adds 1 to its value, without B knowing this

Finally, both A and B do a computation step: both add 1 to their value



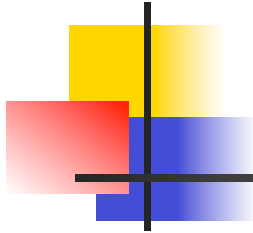
Distr. Systems: Exercise 9



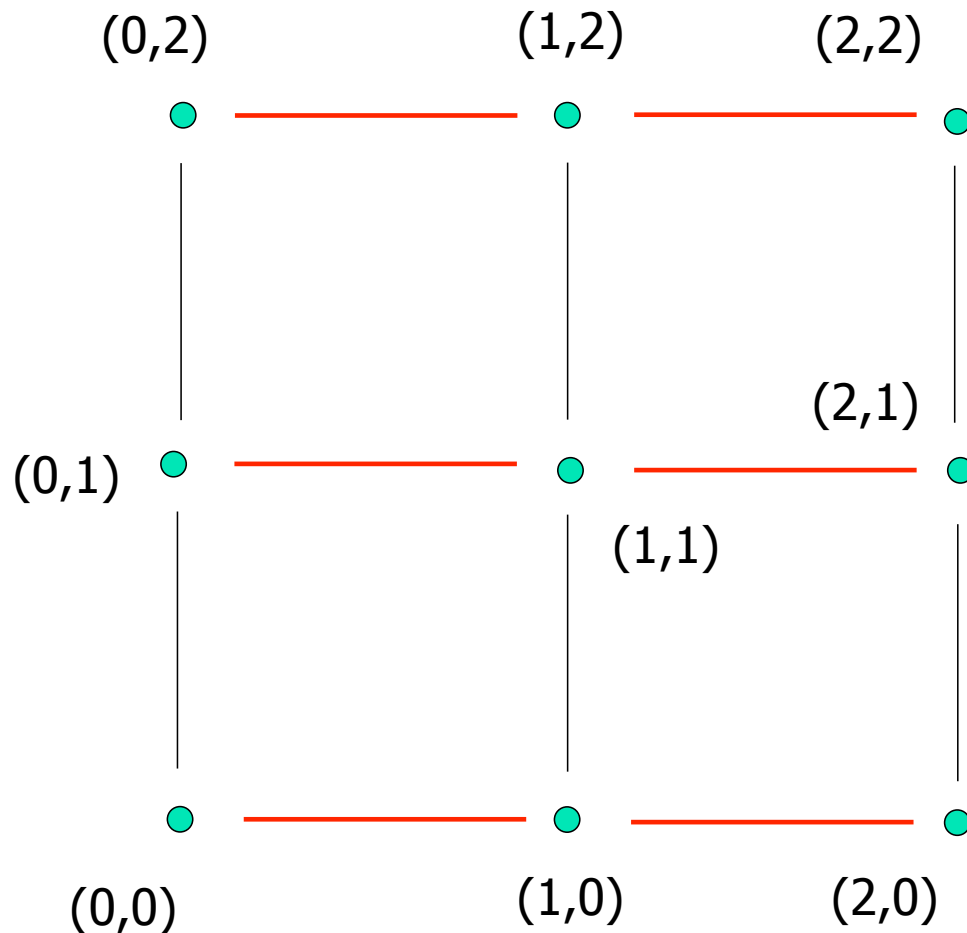
Starting in $(0,0)$, B changes its value from 0 to 1

A does not notice this: he knows the same in $(0,0)$ and $(0,1)$

Formulate what it means that A does not notice, and then prove the claim



Exercise 10



Atoms:

$x=0$; $x=1$; $x=2$ and
 $y=0$; $y=1$; $y=2$

R_A and R_B are reflexive
 and transitive

11a. show:

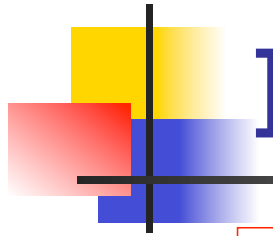
$$M, (0,0) \models E(x=0 \vee y=0)$$

11b. show, for every ϕ

$$M, (0,0) \models EE\phi \Leftrightarrow M \models \phi$$

11c. is there a ϕ such that

$$M, (0,0) \models EE\phi \text{ but } \not\models \phi_{143}$$



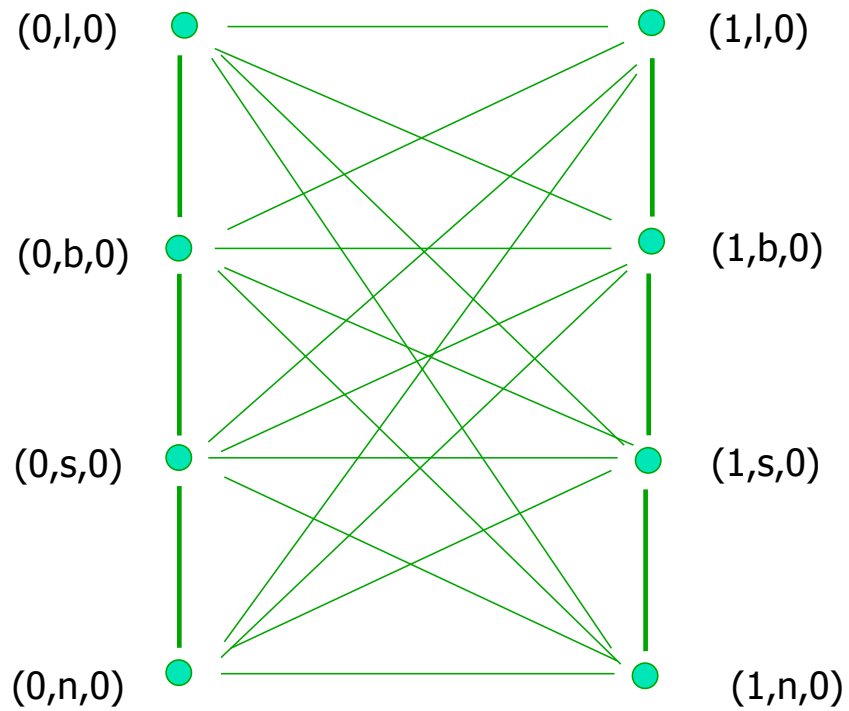
Intr. Systems: Example 2

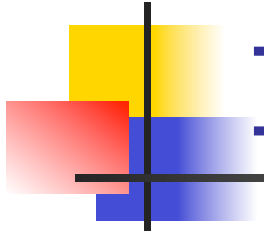
- Three processors: A, F and T
- $L_A = \{n, s, b, l\}$, $L_F = \{0, 1\}$, $L_T = \text{IN}$
- use atoms $a=s$, $f=0$, $t=7$, etc, in $\langle f, a, t \rangle$
- Make a drawing of this system, and show:
- $M_{\langle 1, n, 2 \rangle} \models M_F K_T(t=0)$

IS: Example 2

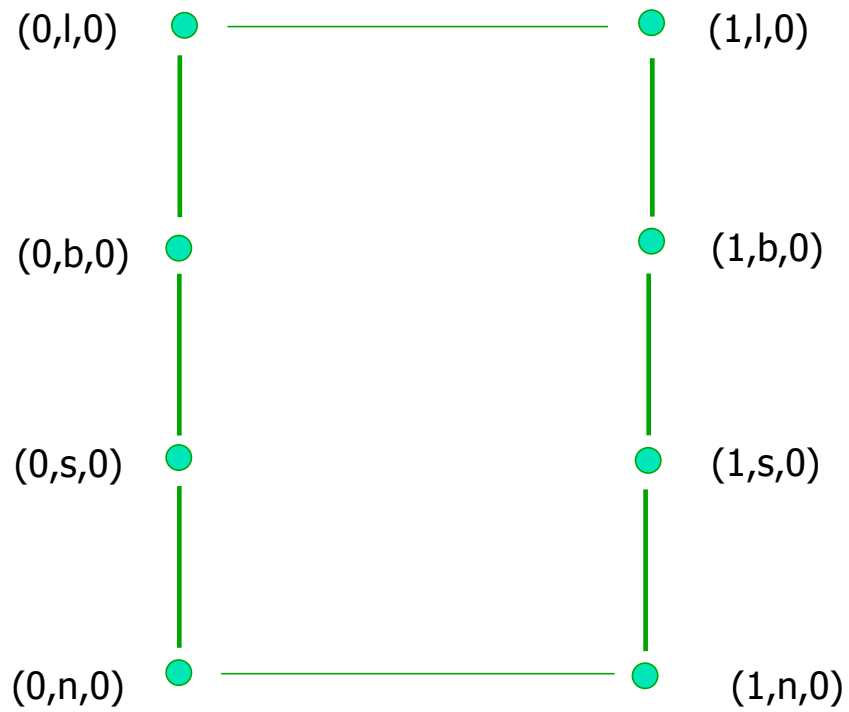
fix $t = 0$

wich we draw as:

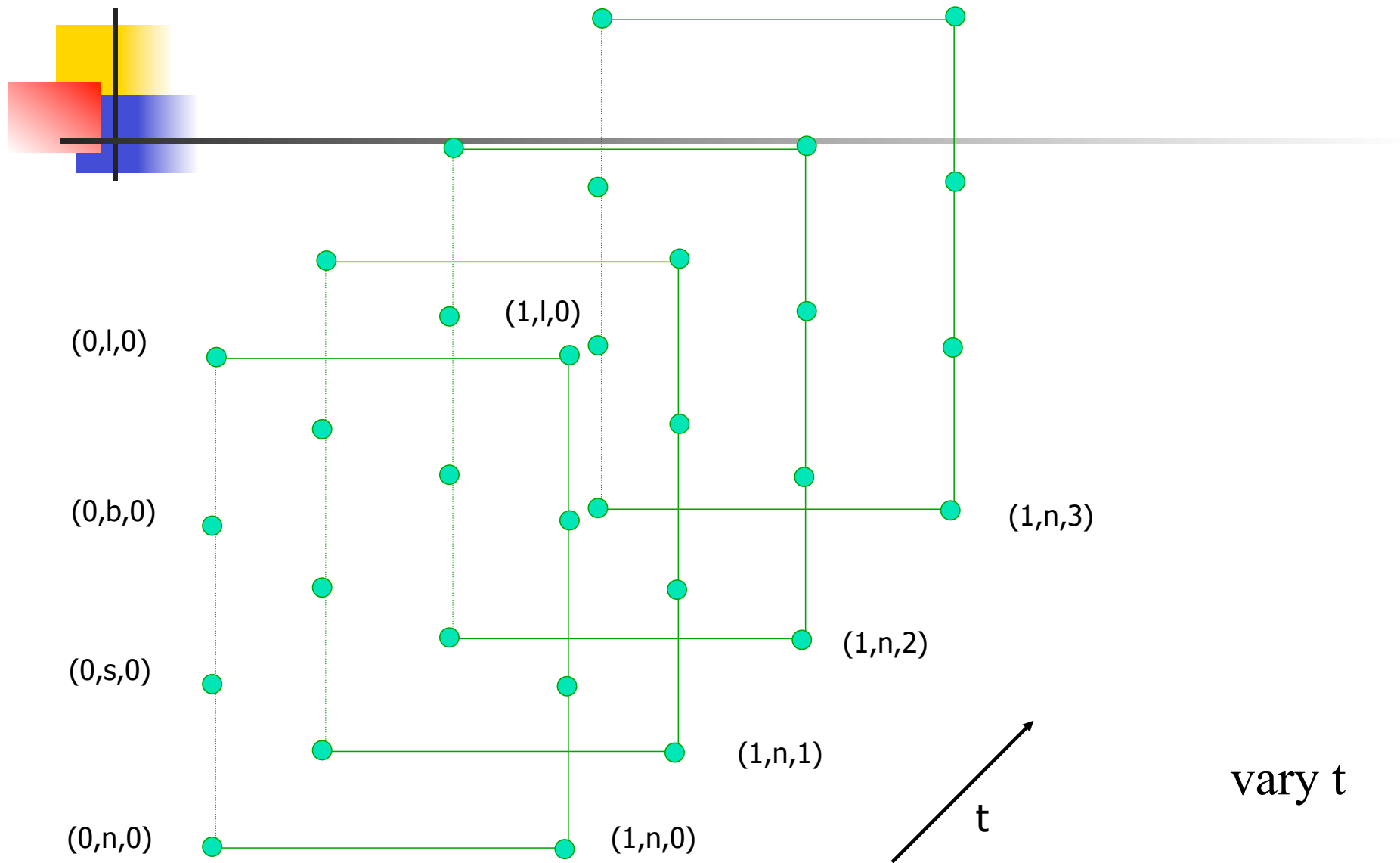


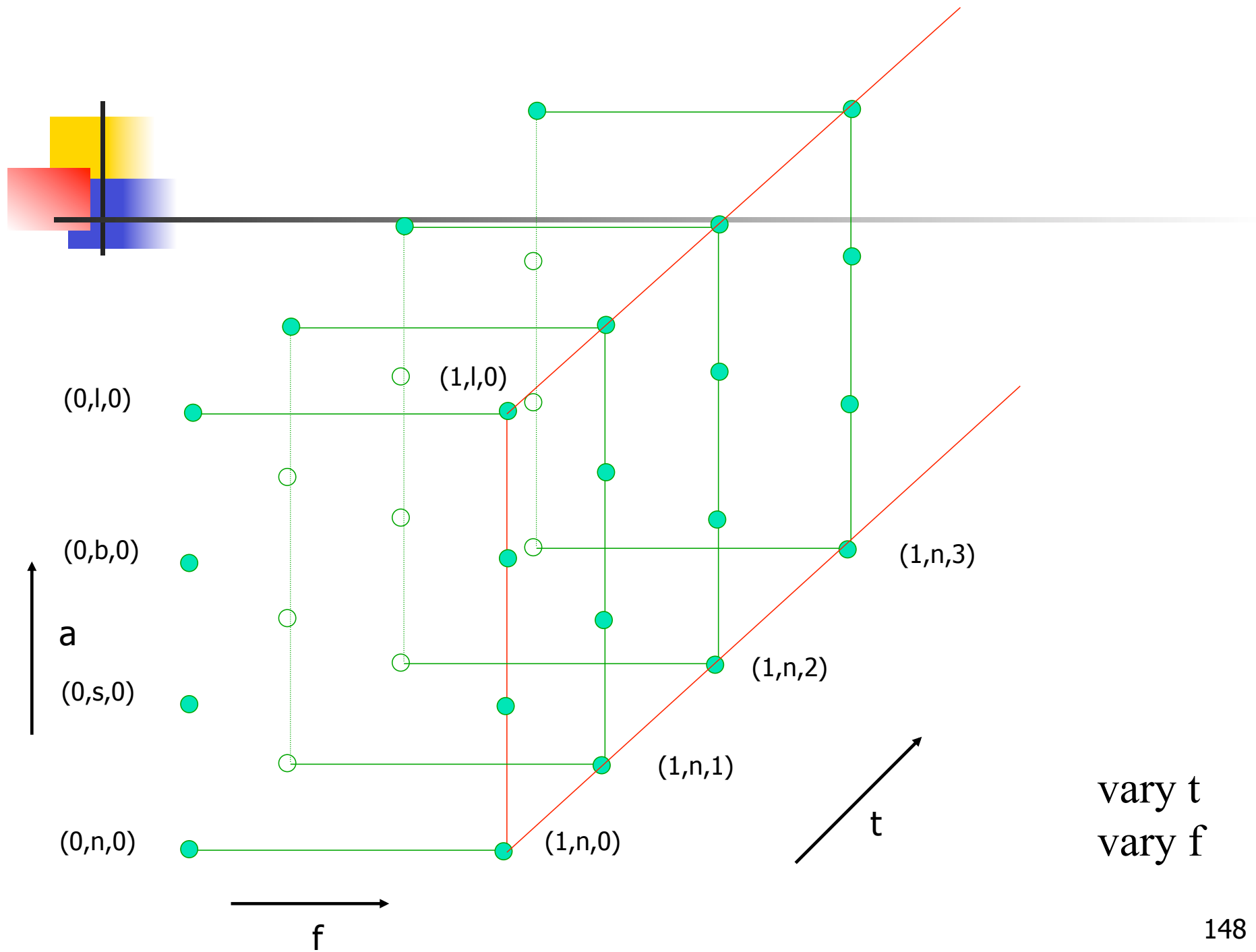


IS: Example 2

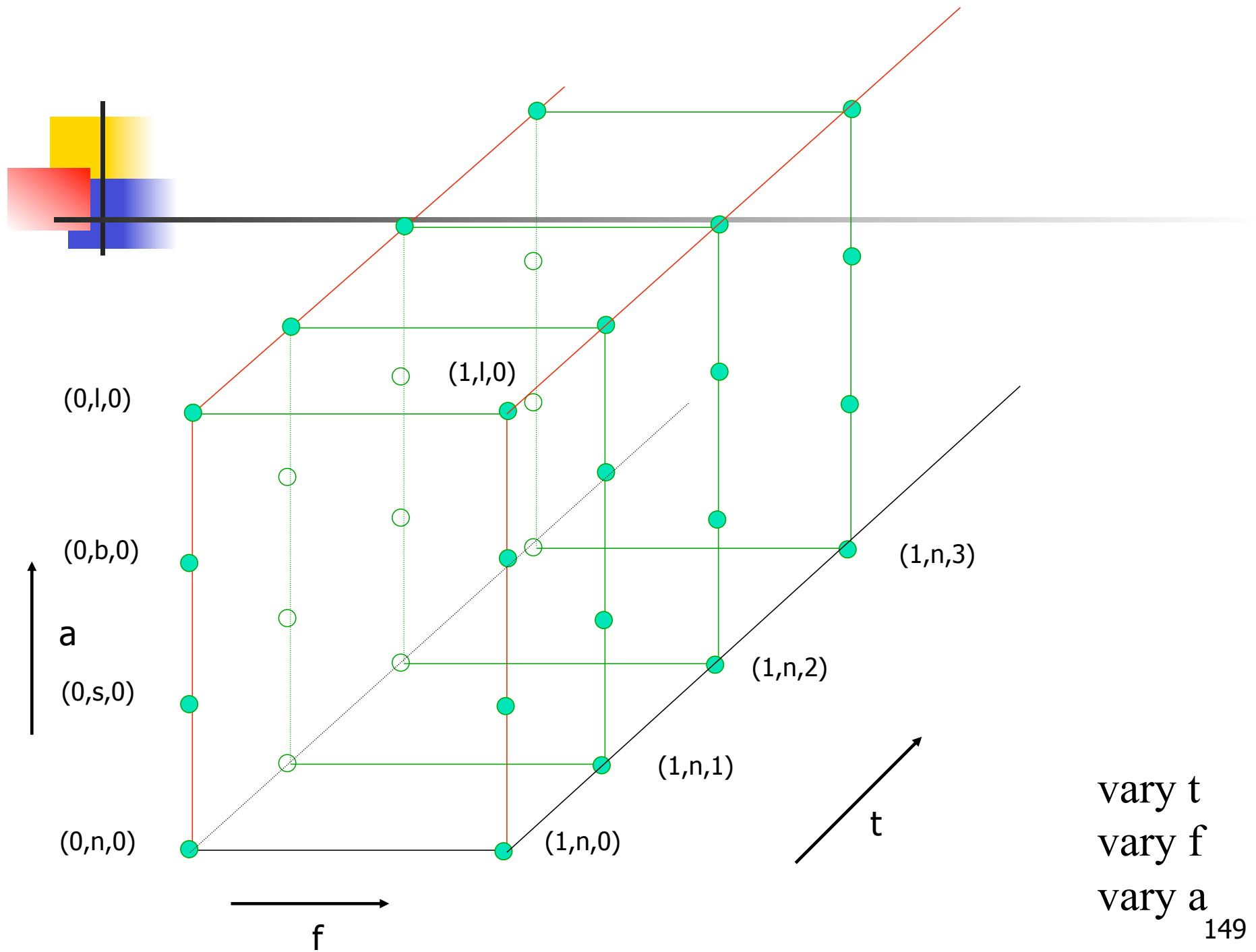


fix $t = 0$

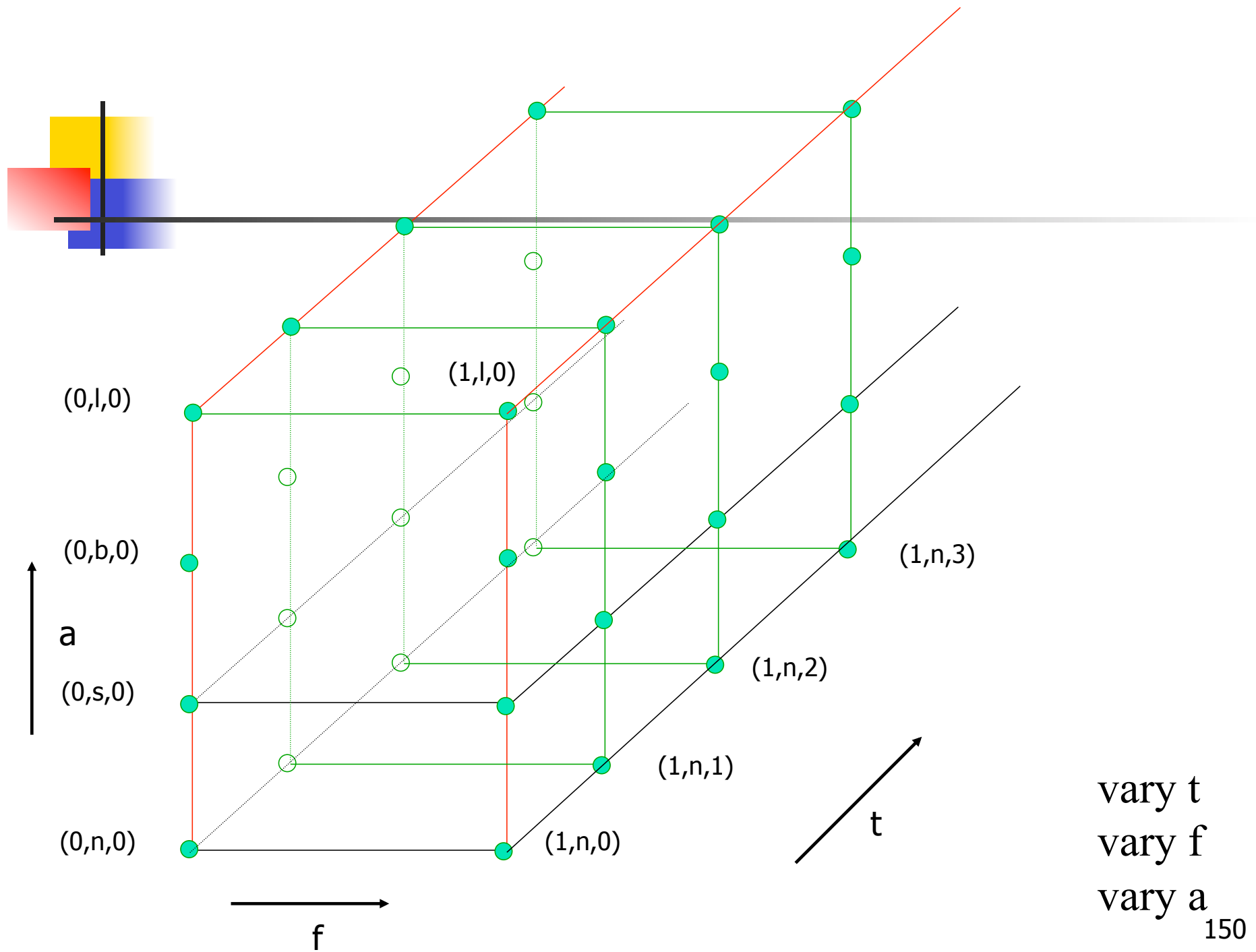




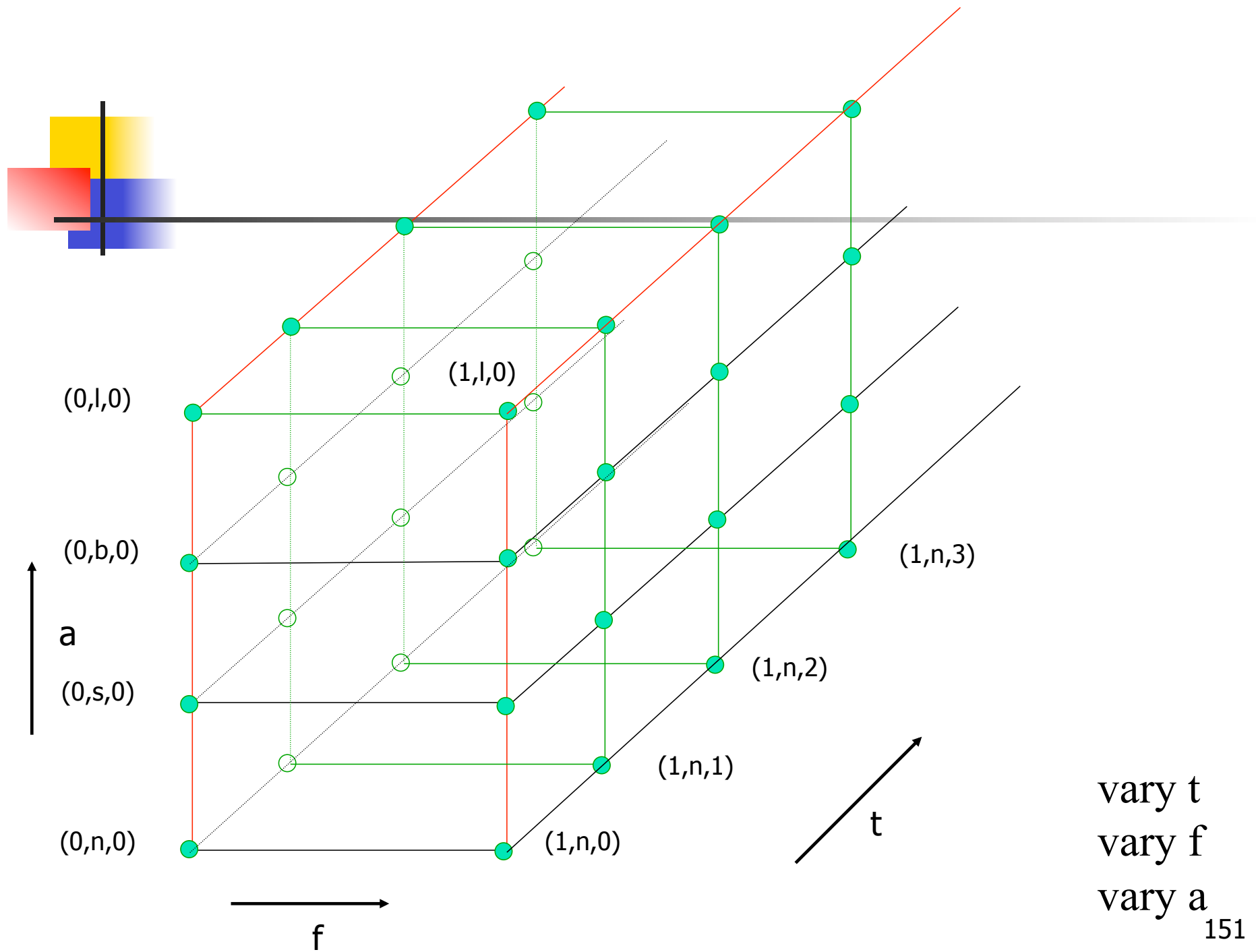
vary t
vary f

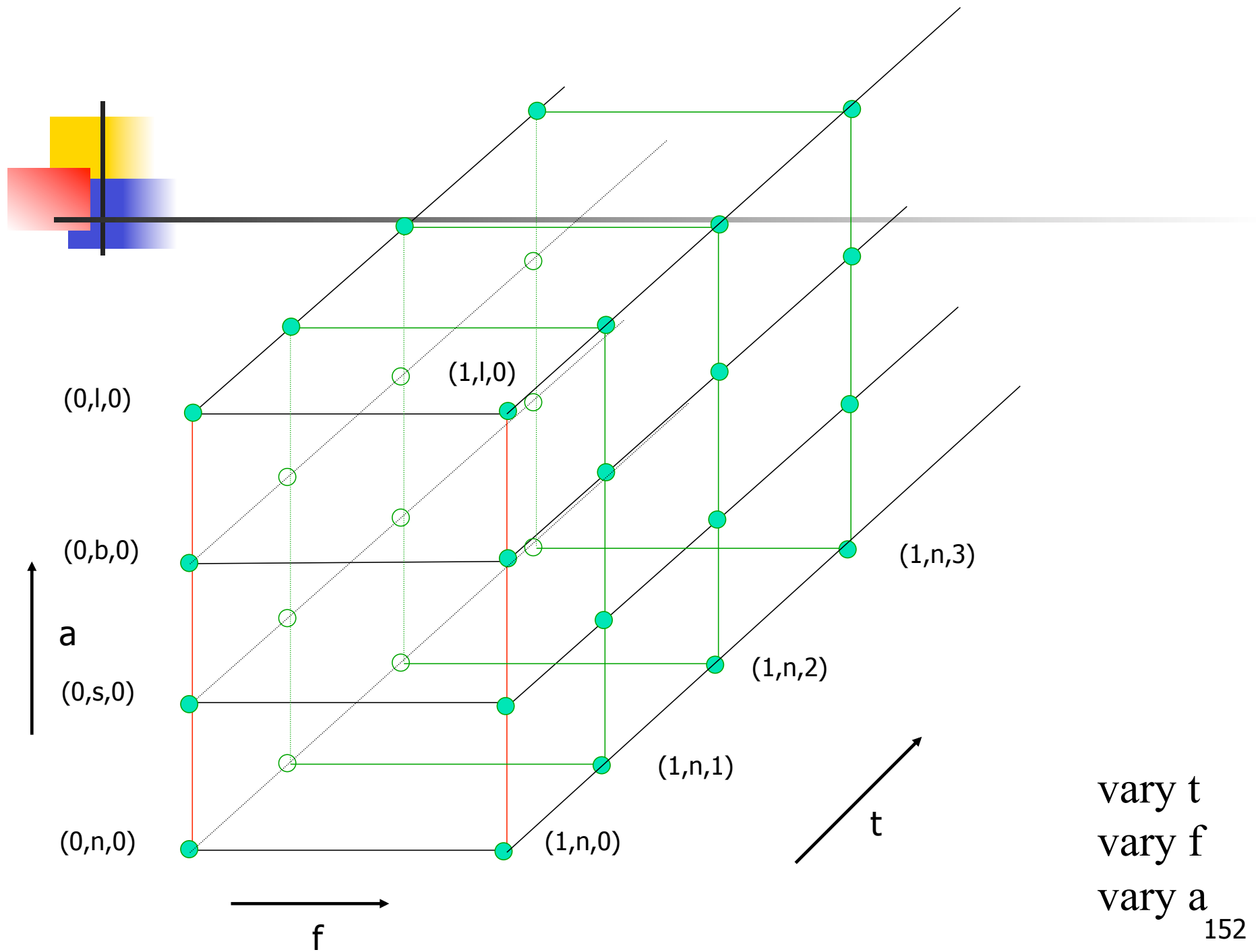


vary t
 vary f
 vary a
 149

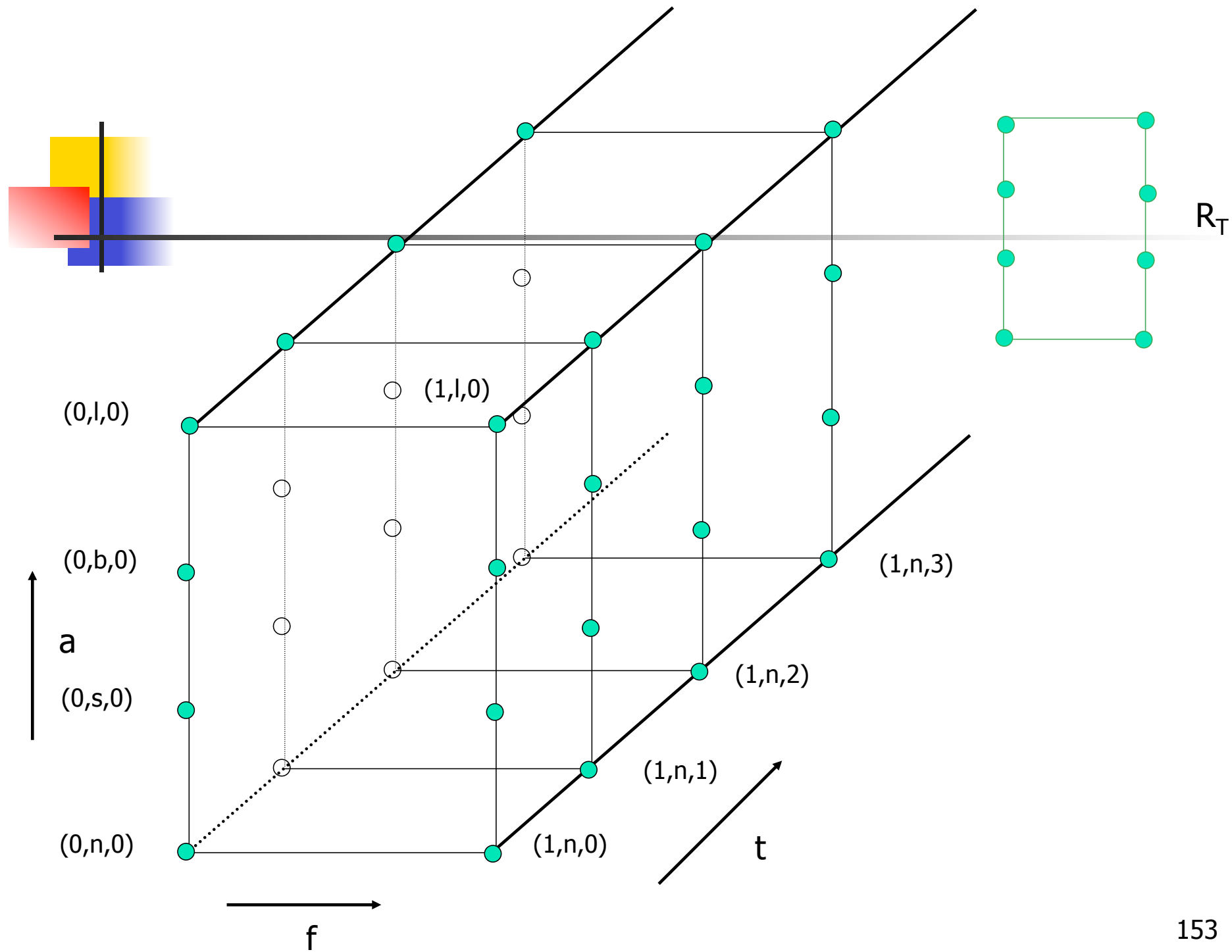


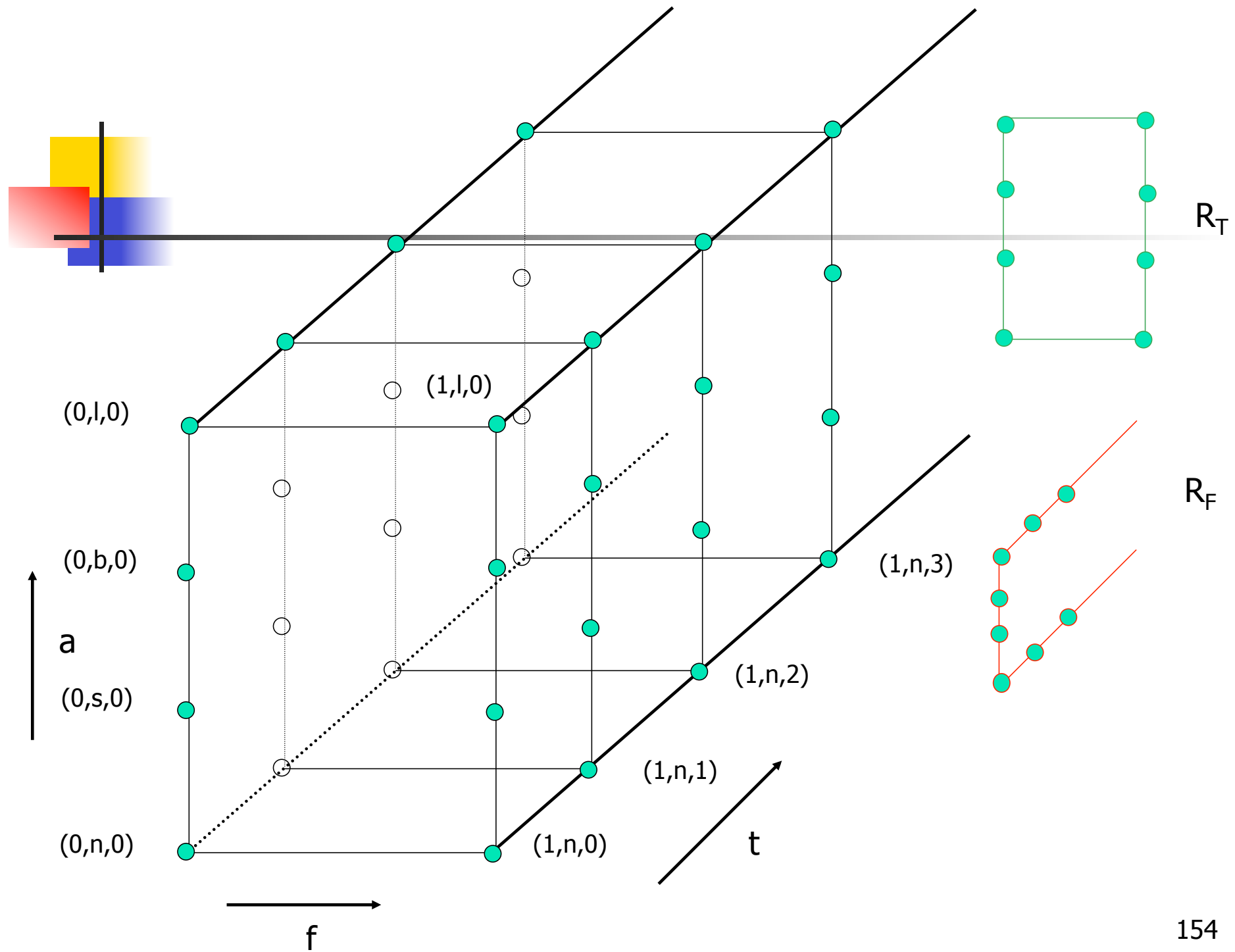
vary t
 vary f
 vary a
 150

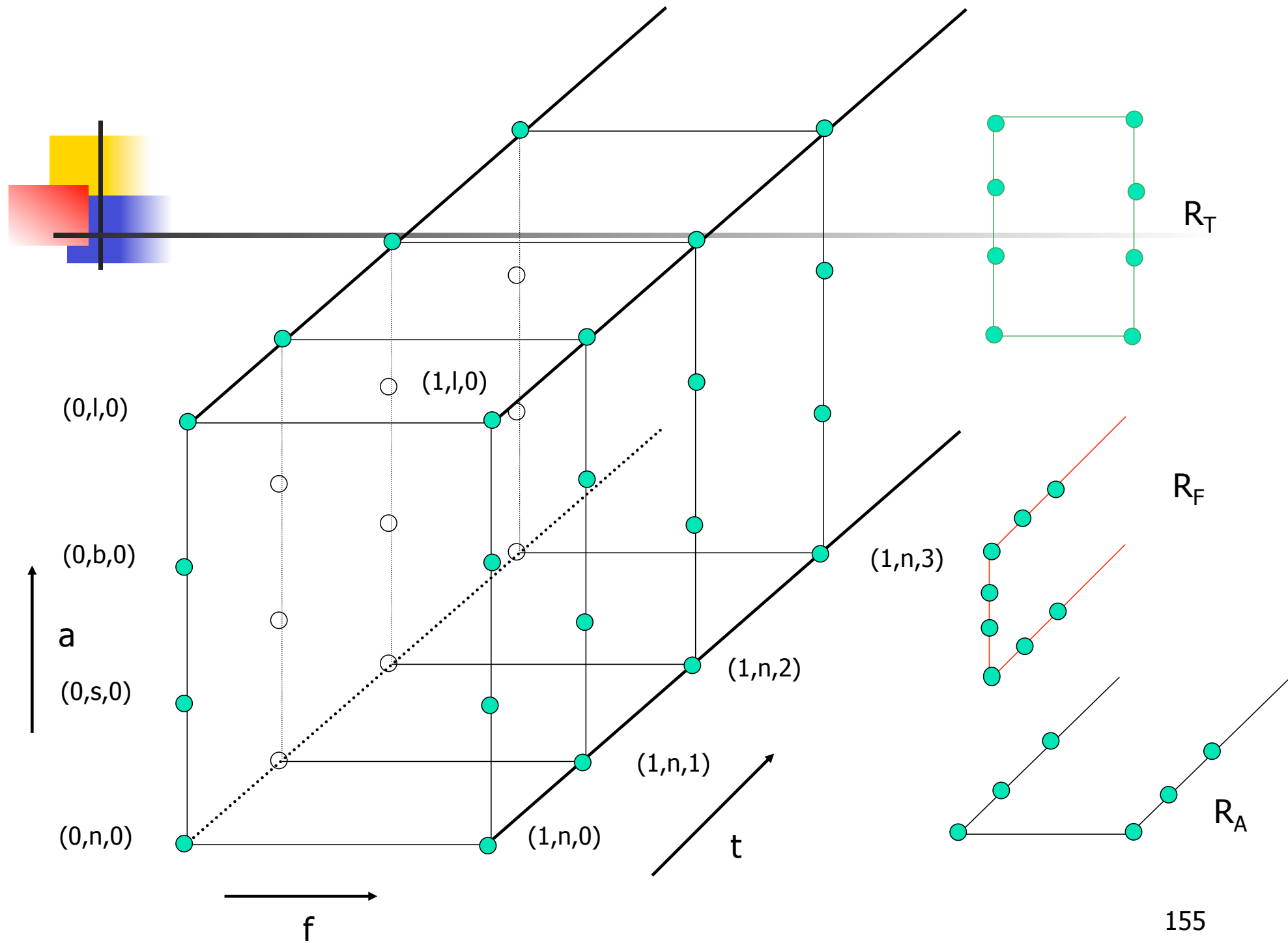


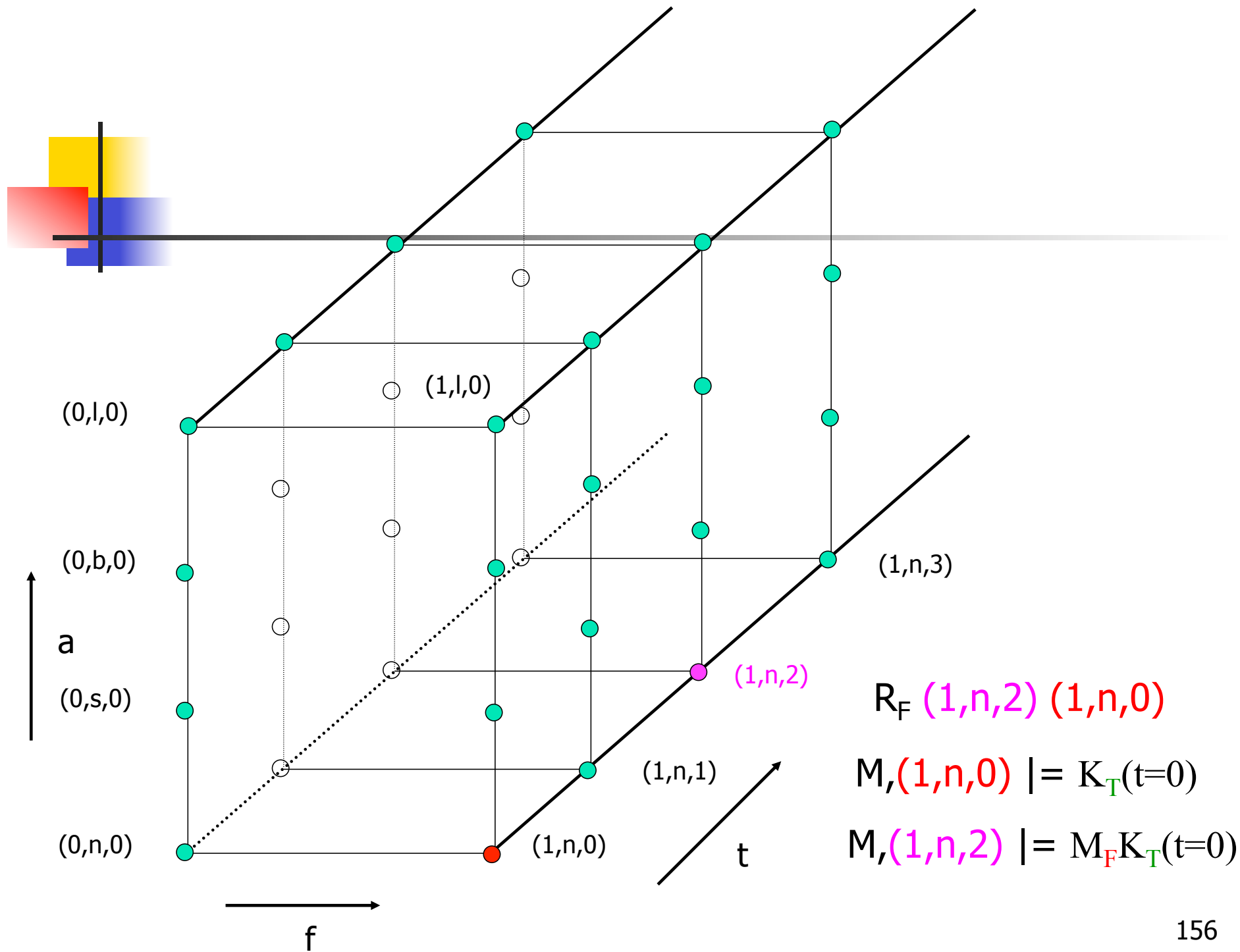


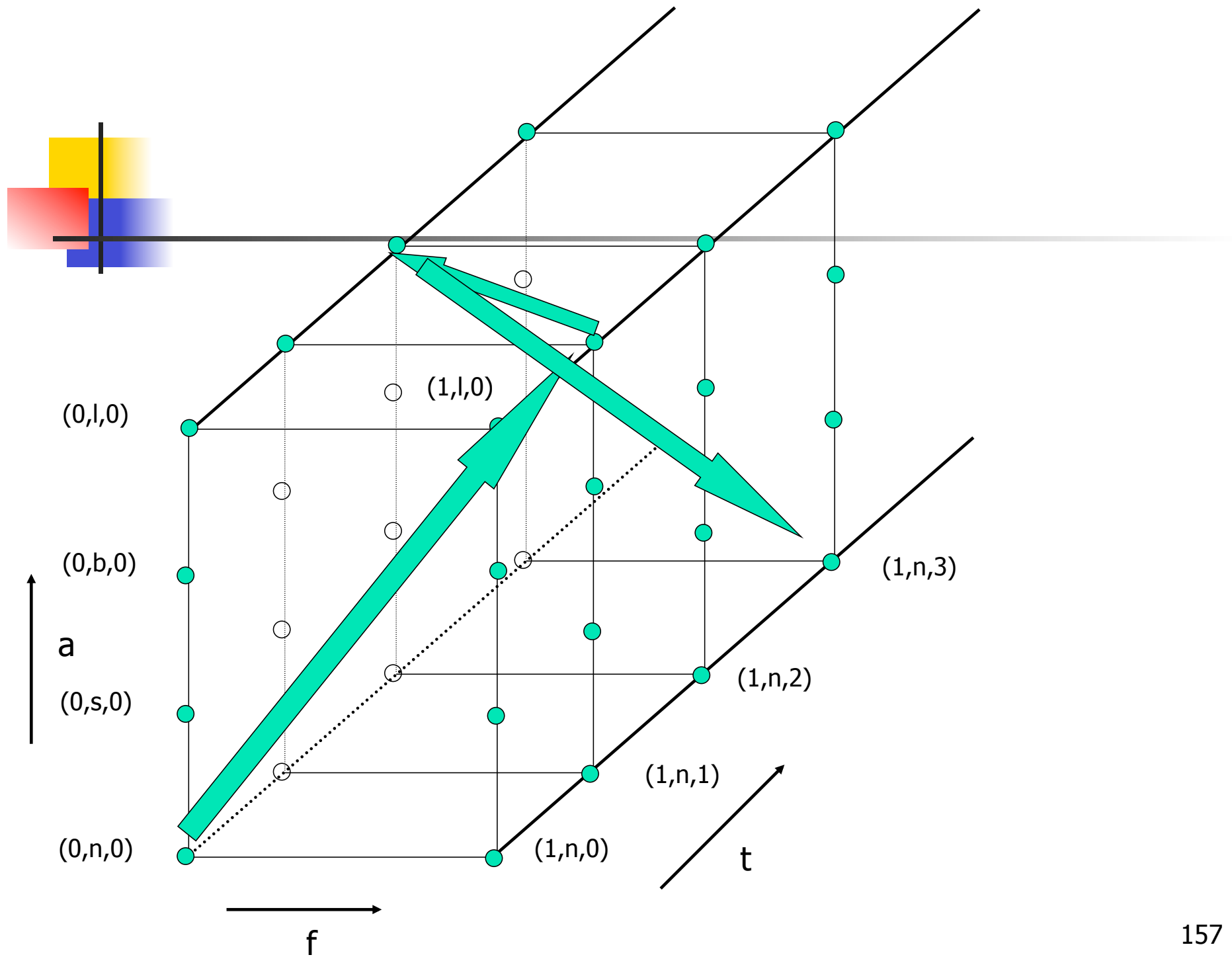
vary t
 vary f
 vary a

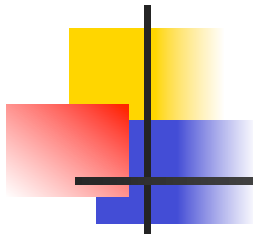




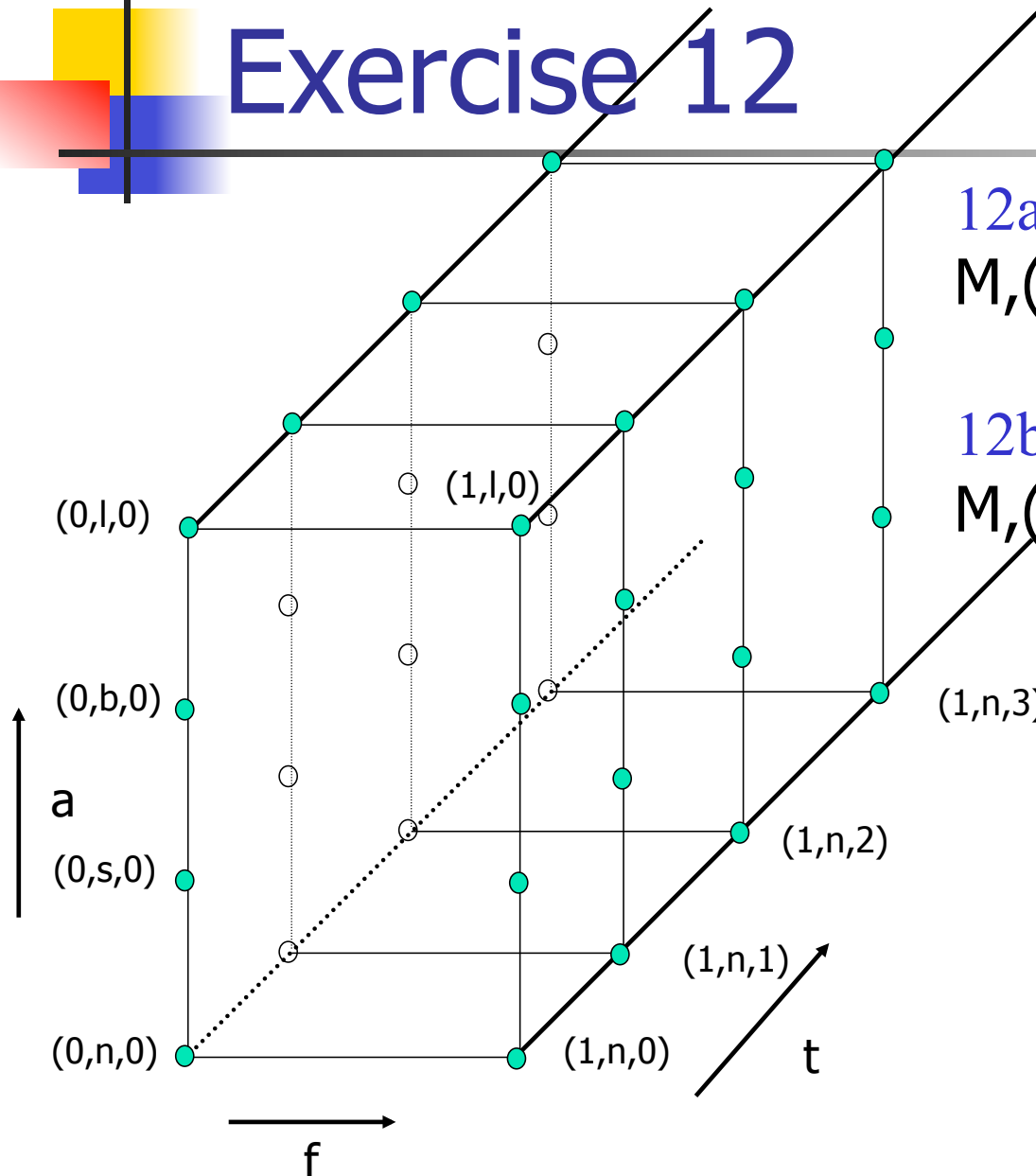








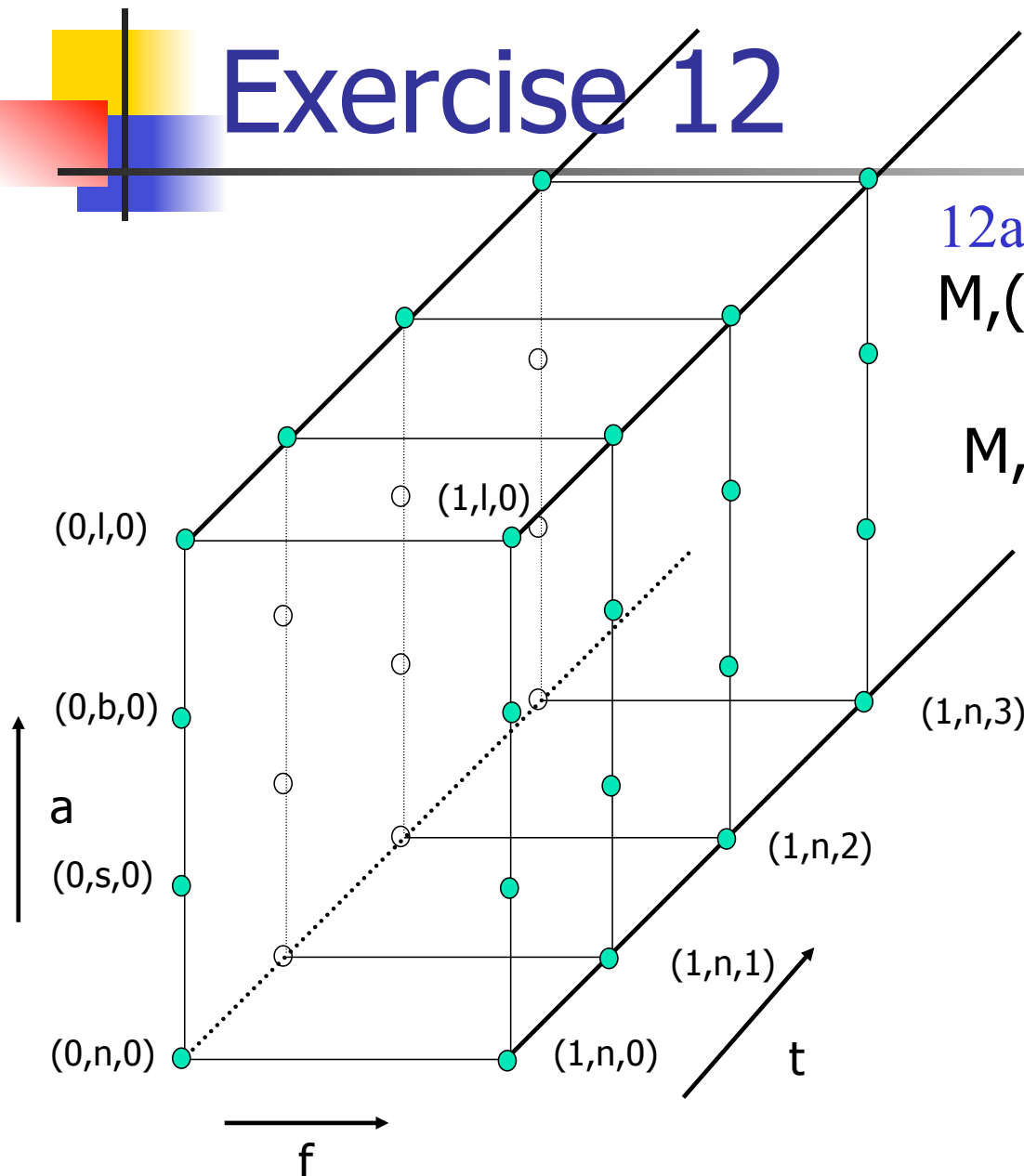
Exercise 12



12a. Give a ϕ for which:
 $M, (0,n,0) \models E\phi$

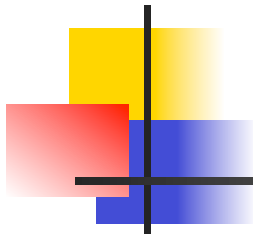
12b. show or disprove: for every ϕ
 $M, (0,n,0) \models EE\phi \Leftrightarrow M \models \phi$

Exercise 12



12a. Give a ϕ for which:
 $M,(0,n,0) \models E\phi$

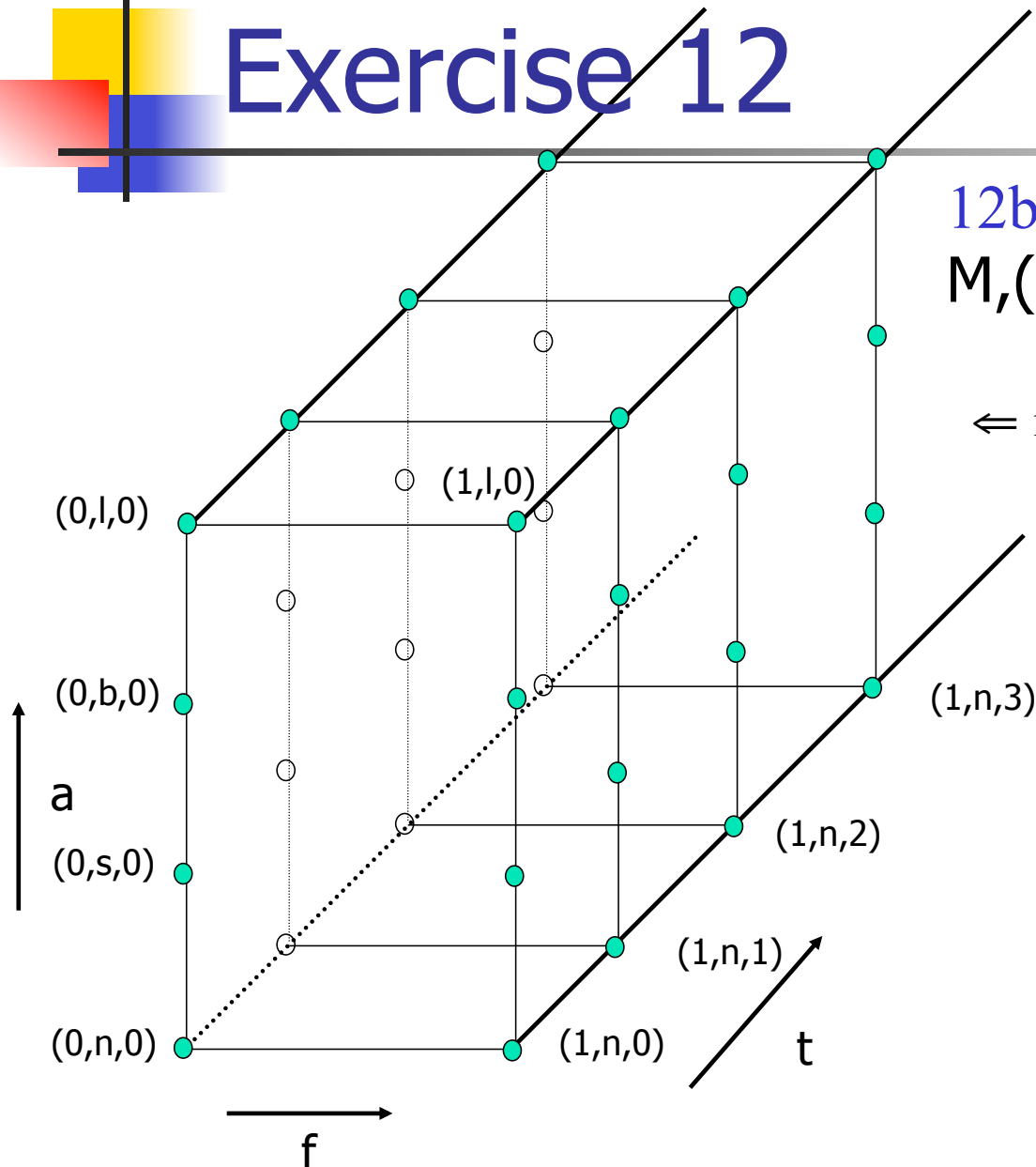
$M,(0,n,0) \models E(f=0 \vee a=n \vee t=0)$



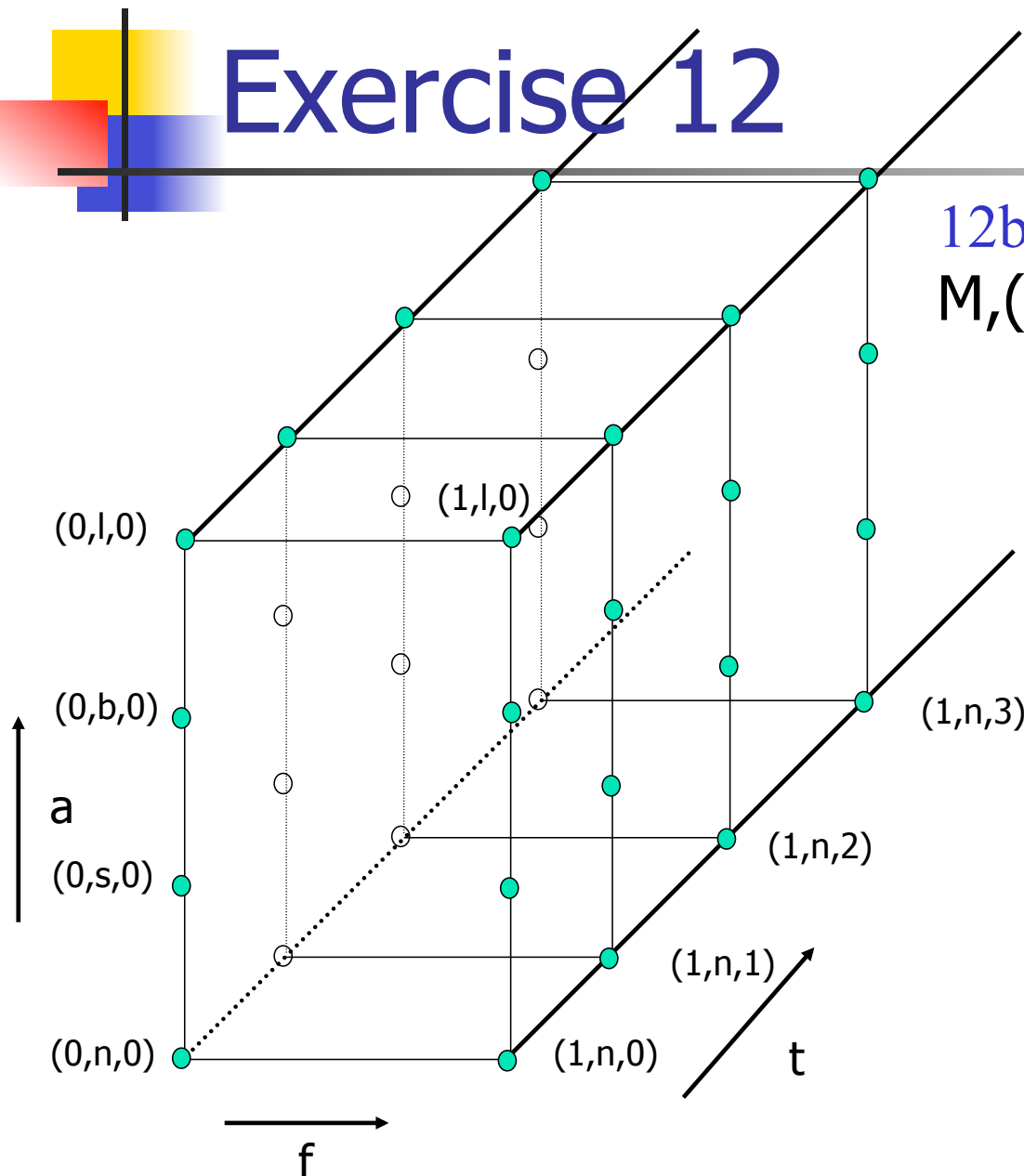
Exercise 12

12b. show or disprove: for every ϕ
 $M, (0, n, 0) \models \text{EE}\phi \Leftrightarrow M \models \phi$

$\Leftarrow$ is obviously true



Exercise 12

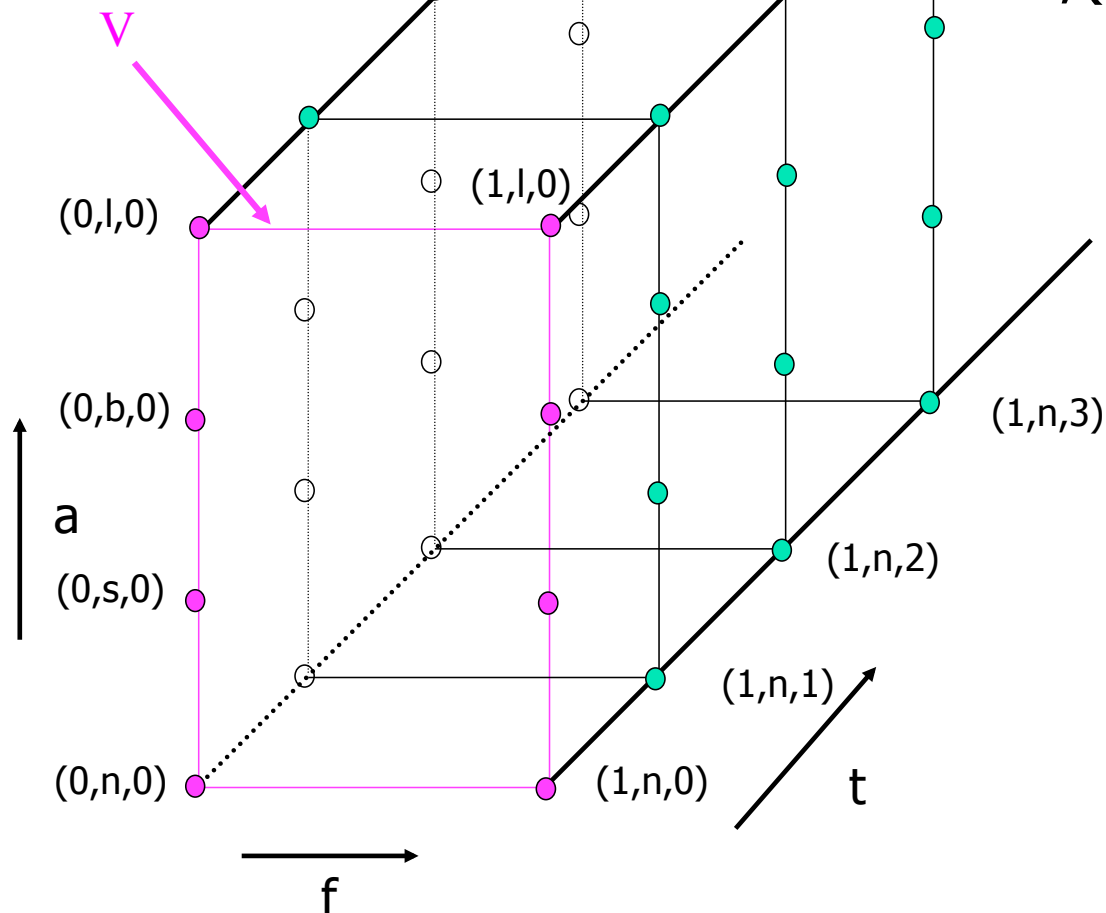


12b. show or disprove: for every ϕ
 $M, (0, n, 0) \models EE\phi \Leftrightarrow M \models \phi$

$\Rightarrow$: $M, (0, n, 0) \models EE\phi \Rightarrow$

$M, (0, n, 0) \models K_T E\phi \Rightarrow$

Exercise 12



12b. show or disprove: for every ϕ
 $M, (0, n, 0) \models EE\phi \Leftrightarrow M \models \phi$

$\Rightarrow$: $M, (0, n, 0) \models EE\phi \Rightarrow$

$M, (0, n, 0) \models K_T E\phi \Rightarrow$

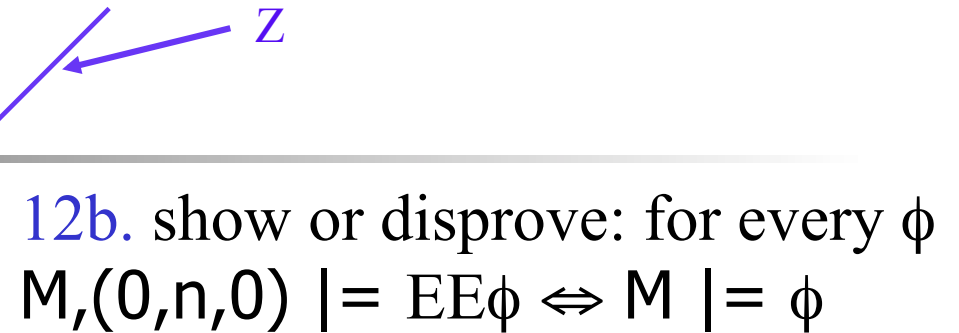
$M, x \models E\phi$ for all x in $V \Rightarrow$

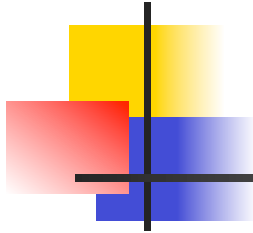
$M, (0, n, 0) \models E\phi$ and

$M, (1, n, 0) \models E\phi \Rightarrow$

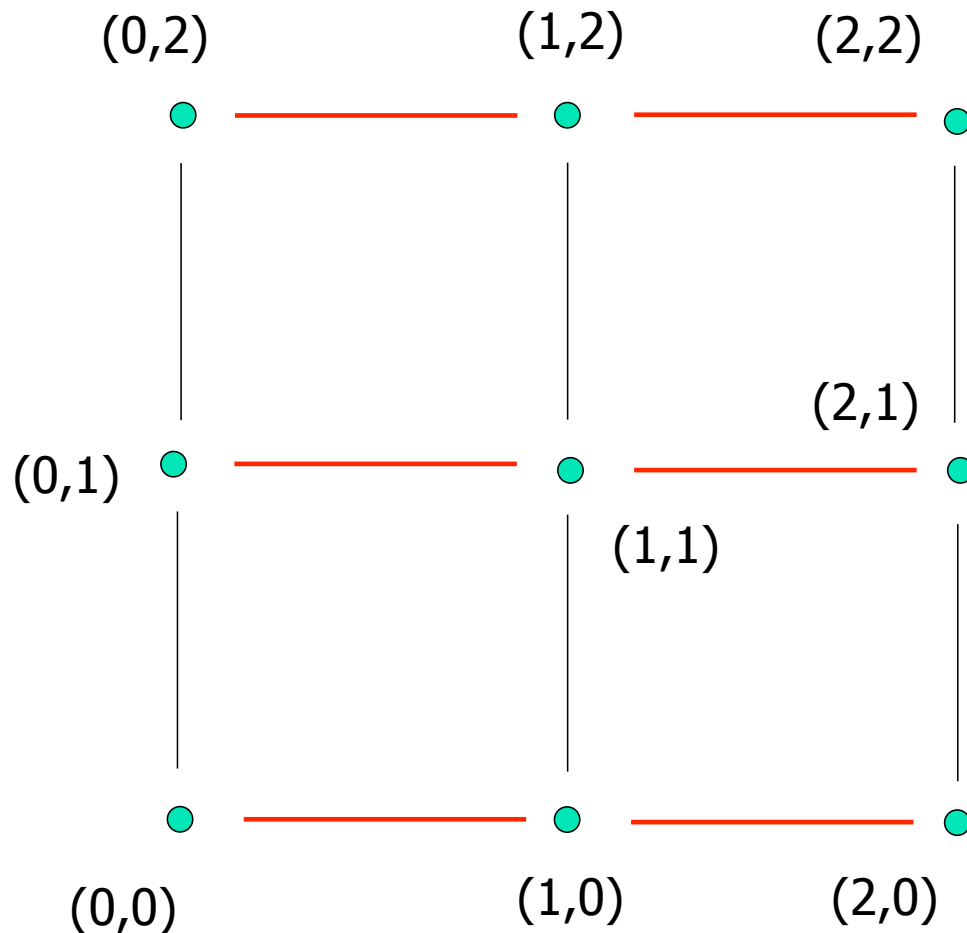
$M, (0, n, 0) \models K_F \phi$ and

$M, (1, n, 0) \models K_F \phi \Rightarrow$


$$M_r(0,n,0) = K_T E \phi \Rightarrow$$
$$\begin{array}{l} M_{\langle 0, n, 0 \rangle} \models E\phi \text{ and} \\ M_{\langle 1, n, 0 \rangle} \models E\phi \Rightarrow \end{array}$$
$$\begin{aligned} M_{\mathcal{F}}(0,n,0) &|= K_F \phi \text{ and} \\ M_{\mathcal{F}}(1,n,0) &|= K_F \phi \Rightarrow \end{aligned}$$
$$\begin{array}{l} M, y \models \phi \text{ for all } y \text{ in } Y \text{ and} \\ M, z \models \phi \text{ for all } z \text{ in } Z \Rightarrow M \models \phi \end{array}$$



Exercise 13



Atoms:

$x=0; x=1; x=2$ and
 $y=0; y=1; y=2$

R_A and R_B are reflexive
 and transitive

13a. show:

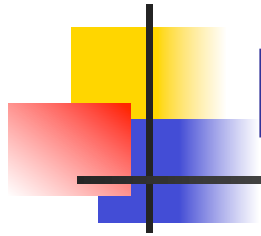
$$M, (0,0) \models E(x=0 \vee y=0)$$

13b. show:

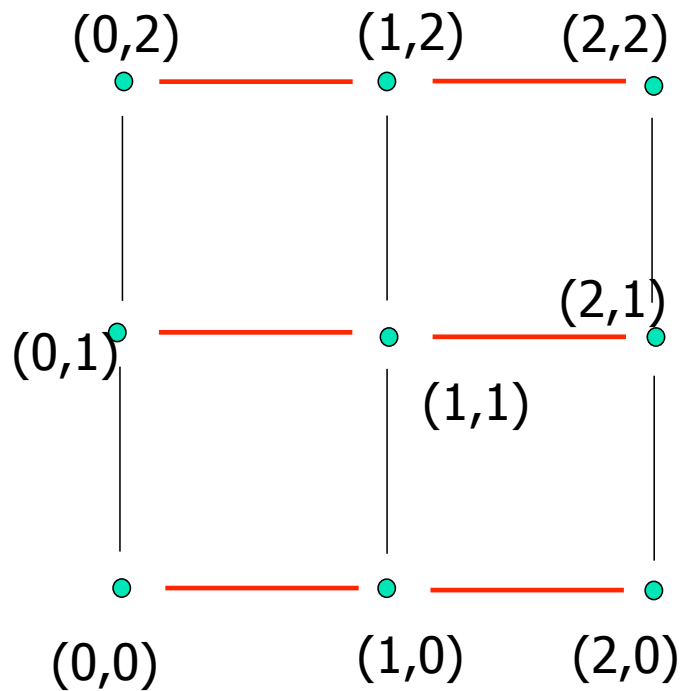
$$M, (0,0) \models I(x=0 \wedge y=0)$$

13c. show in interpreted systems:

$$M, w \models D\phi \leftrightarrow \phi$$



Exercise 13: Solution



13b. show:

$$M, (0,0) \models I(x=0 \wedge y=0)$$

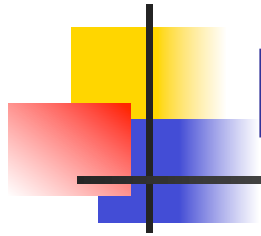
$$M, (0,0) \models I\phi \Leftrightarrow$$

$$\forall (x,y) (R_I (0,0)(x,y) \Rightarrow M, (x,y) \models \phi \Leftrightarrow$$

$$\forall (x,y) (R_A (0,0)(x,y) \text{ and } R_B (0,0)(x,y) \Rightarrow M, (x,y) \models \phi \Leftrightarrow$$

$$\forall (x,y) (x=0 \text{ and } y=0 \Rightarrow M, (x,y) \models \phi) \Leftrightarrow$$

$$M, (0,0) \models \phi \Leftrightarrow$$



Exercise 13: solution

13c. show in interpreted systems: $M, w \models D\phi \Leftrightarrow \phi$

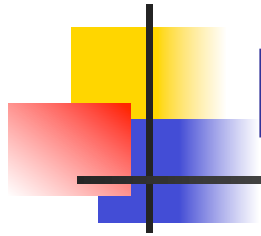
first of all: the $\rightarrow$ direction is easy:

if $M, w \models D\phi$ then

$M, v \models \phi$ for all v such that $(R_1 \cap R_2 \dots \cap \dots R_n)wv$

in interpreted systems, $R_i ww$, so $(R_1 \cap R_2 \dots \cap \dots R_n)wv$

so $M, w \models \phi$



Exercise 13: solution

13c. show in interpreted systems: $M, w \models D\phi \Leftrightarrow \phi$

now suppose : $M, w \models \phi$. To prove: $M, w \models D\phi$

recall that $w = \langle w_1, w_2, \dots, w_n \rangle$

take an arbitrary v for which $(R_1 \cap R_2 \dots \cap \dots R_n)wv$

R_1wv , so $v_1 = w_1$ and R_2wv , so $v_2 = w_2 \dots$ and R_nwv , so $v_n = w_n$

hence $v = \langle v_1, v_2, \dots, v_n \rangle = \langle w_1, w_2, \dots, w_n \rangle = w$

and so $M, v \models \phi$ for an arbitrary v with $(R_1 \cap R_2 \dots \cap \dots R_n)wv$

and hence $M, w \models I\phi$