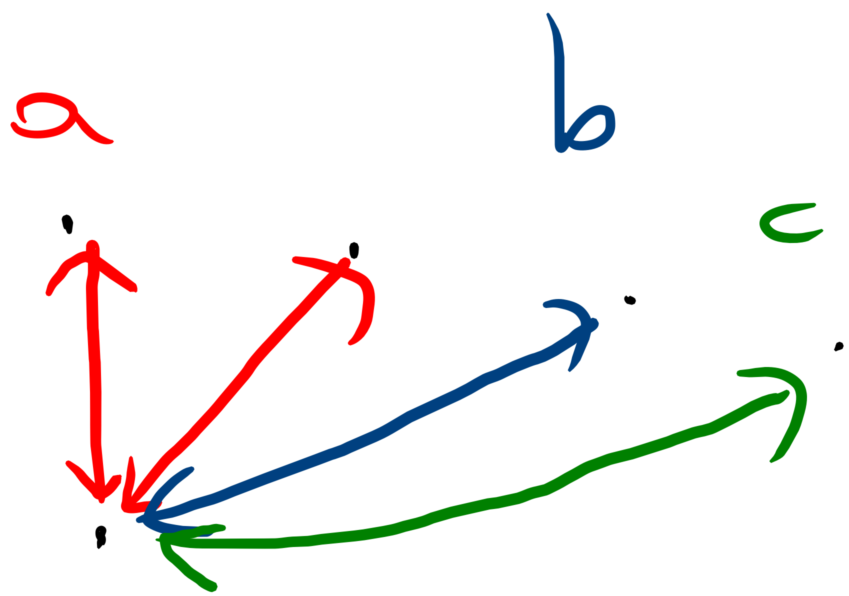
Group Notions of Knowledge

$S5_n$ Group of agents $A = \{a, b, c, \ldots\}$

$K_a \phi \; (\equiv \Box_a \phi)$ $\qquad$ $\hat{K}_a \phi \equiv \neg K_a \neg \phi$

Knowledge

it is consistent with a's knowlegde that ϕ



Let $B \subseteq A$, where B is finite

$$E_B \phi \equiv \bigwedge_{b \in B} K_b \phi$$

↑

"Everybody in B knows ϕ"

$$E_B \phi = K_{b_1} \phi \wedge \ldots \wedge K_{b_n} \phi$$

$$K_a\phi \to K_aK_a\phi \quad (4)$$

$$K_aK_a\phi \to K_a\phi$$

$$K_a\phi \leftrightarrow K_aK_a\phi$$

$$K_a\phi \leftrightarrow K_a^n\phi \quad , n \geq 1$$

$$X^0\phi = \phi \qquad X = (K_{a_1} + \dots + K_{a_n})^+$$

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

$E_\beta \phi \cancel{\overset{?}{\to}} E_\beta E_\beta \phi$

$r =$ "it rains in Otago"

h w b

o $\cdot$ $\cdot$ g

$\cdot$ ℓ

$E_{hwb}\, r$

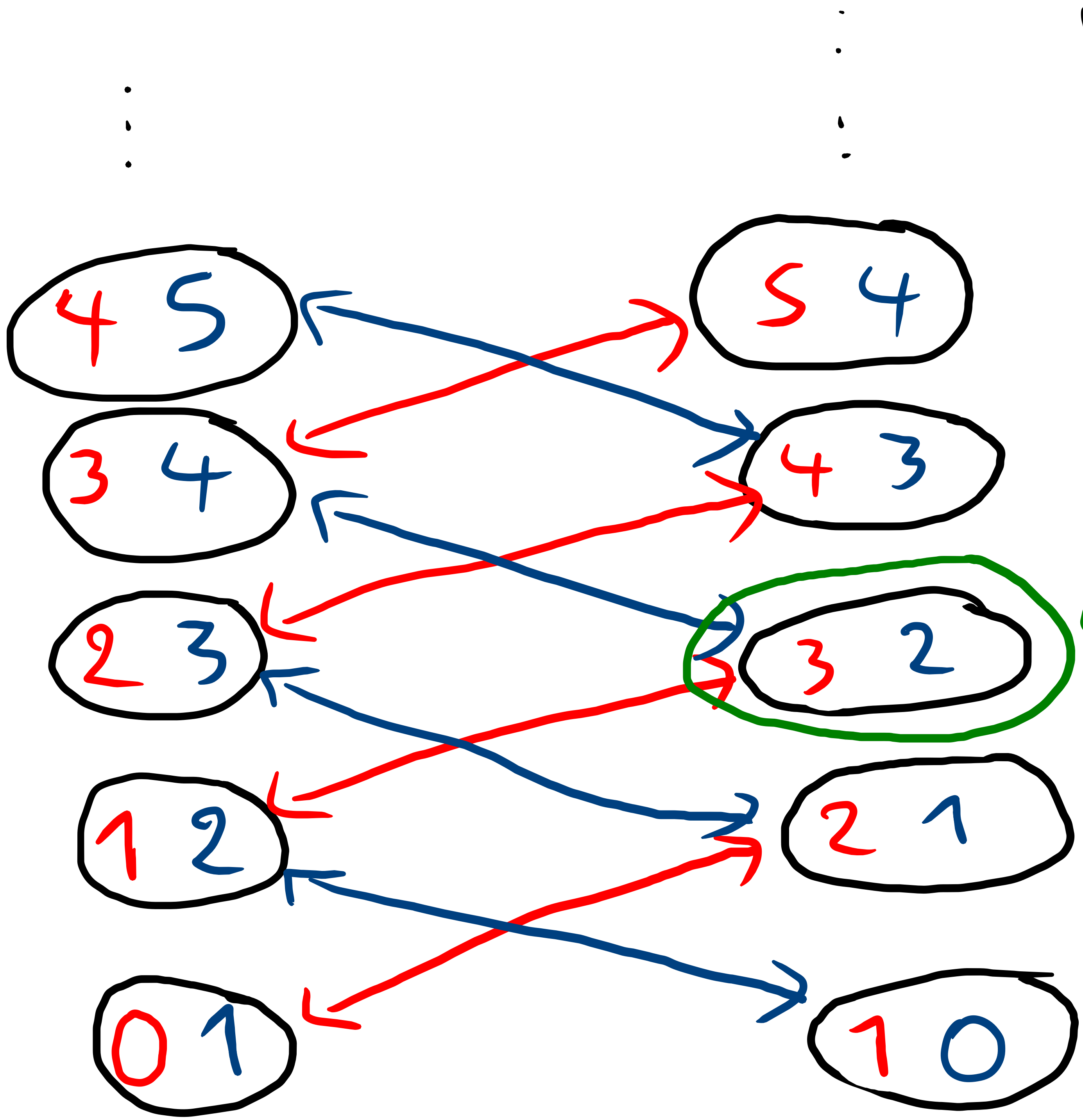
$\neg E_{hwb} E_{hwb}\, r$

Ex. 2.4 (Consecutive Numbers)

a b

$E_{ab} \neg a_5 \wedge$

$\neg E_{ab} E_{ab} \neg a_5$



actual word

$$B = \{b_1, b_2, \ldots, b_n\}$$

$$E_B \phi \rightarrow K_{b_1}\phi \wedge \ldots K_{b_n}\phi$$

$$E_B E_B \phi \rightarrow K_{b_1} E_B \phi \wedge \ldots \wedge K_{b_n} E_B \phi \rightarrow$$

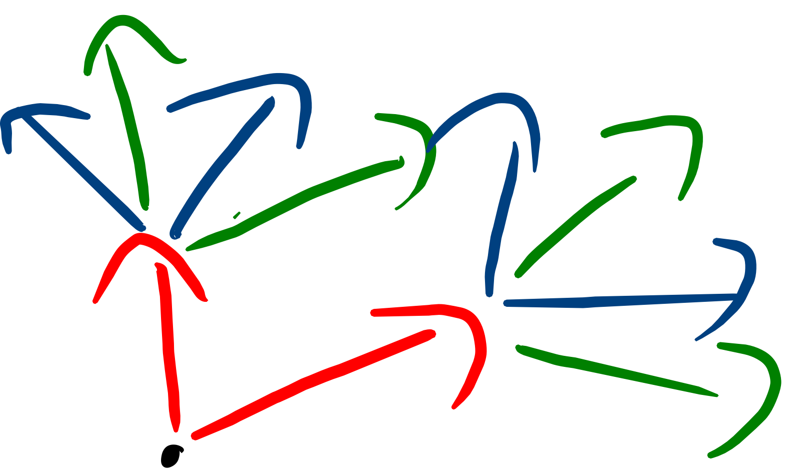
$$K_{b_1}(K_{b_1}\phi \wedge \ldots \wedge K_{b_n}\phi) \wedge \ldots \wedge$$

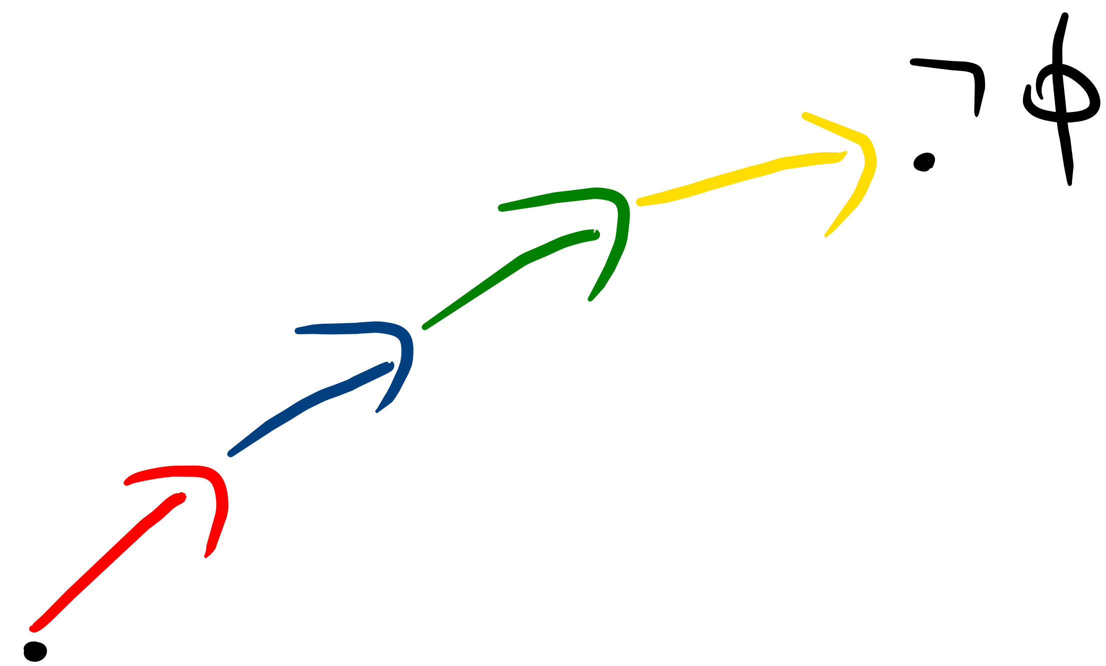
$$K_{b_n}(K_{b_1}\phi \wedge \ldots \wedge K_{b_n}\phi) \rightarrow$$

$$K_{b_1}K_{b_1}\phi \wedge K_{b_1}K_{b_2}\phi \wedge \ldots \wedge K_{b_1}K_{b_n}\phi$$

$$\neg E_B^n \phi \equiv \hat{K}_{b_1} \cdots \hat{K}_{b_n} \neg\phi \vee \cdots$$

$$\hat{K}_{b_2} \cdots \hat{K}_{b_n} \neg\phi \vee \cdots \vee$$





Common Knowledge

$C_B\phi$ = "it is common Knowledge among the group of agents B that ϕ" = "for every $n \geq 0$, it holds that $E_B^n\phi$"

$$C_B\phi \approx \bigwedge_{n\in\mathbb{N}} E_B^n\phi$$

<u>Ex. 2.24</u> p = "Saint Nicholas does not exist"

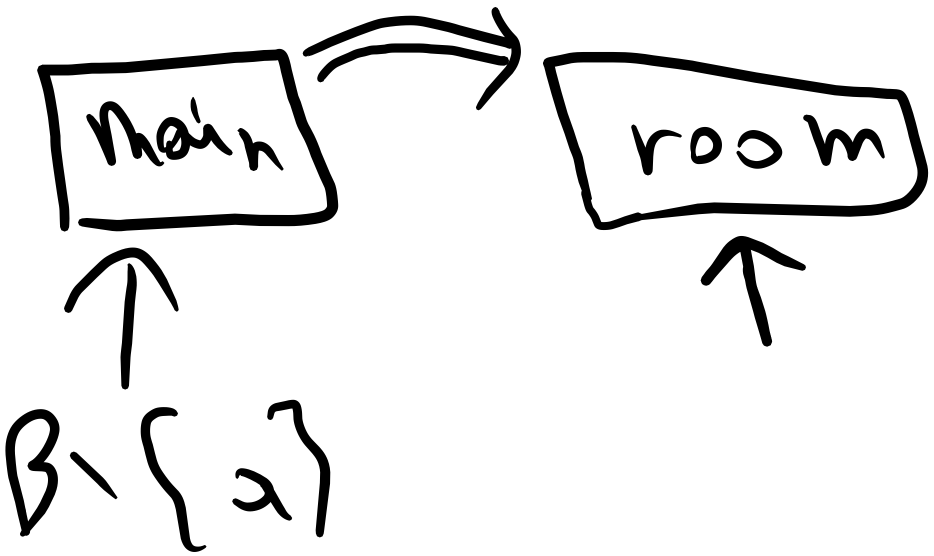
$$F = \{a, b, c, \ldots\}$$

$$K_a p \wedge \neg E_F p$$

$$E_F p \wedge \neg E_F E_F p$$

Ex. 2.26 (Alco at the conference)

$B = \{a, \ldots\}$



$$E_B \phi \wedge \neg E_B E_B \phi$$

$$\neg C_B \phi$$

$$E_B \phi \wedge E_B E_B \phi \wedge \neg E_B E_B E_B \phi$$

$$\neg C_B \phi$$

Language with common Knowledge

L_{KC}

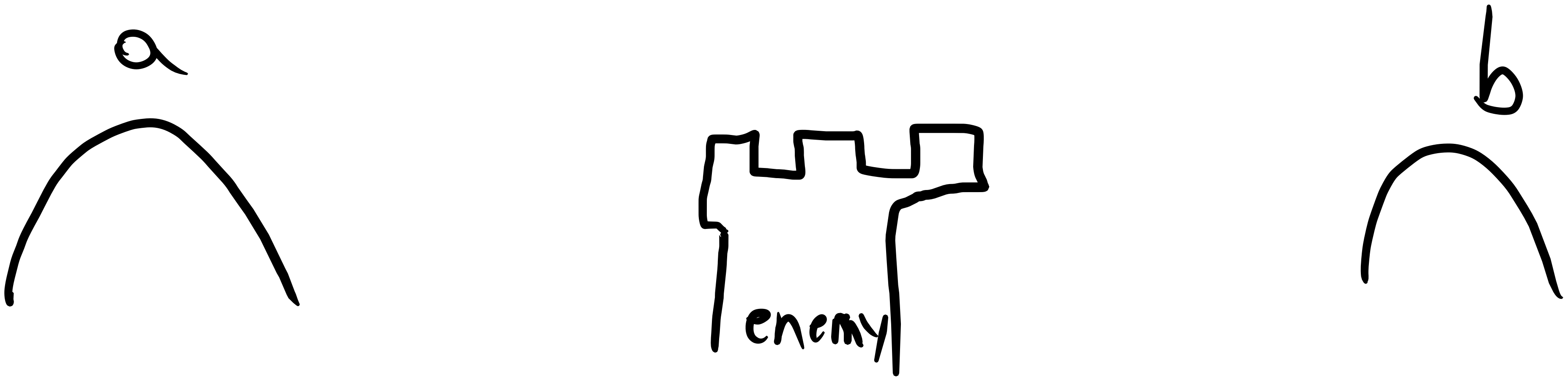
$$\phi ::= p \mid \neg\phi \mid (\phi \wedge \phi) \mid K_a\phi \mid C_B\phi$$

$p \in \Phi = \{\text{atomic prop}\}$, $a \in A$, $B \subseteq A$

$E_B\phi$ is a shortcut, so it is not necessary to add it in L_{KC}

However $C_B\phi$ must belong in L_{KC}

Ex 2.27 (Byzantine Generals)



a and b <u>together</u> can beat the enemy but only one of them will certainly loose

Assume that a wants to sent to b the message m="I propose that we attack together at 1/4/2021, 8:00pm" a b

- If m successfully arrives to b then $K_b m$ and $K_b K_a m$, but $\neg K_a K_b m$
- Assume that b, after receiving m sents an acknowledgement to a and assume that the acknowledgement successfully arrives

$K_a K_b m$ but $\neg K_b K_a K_b m$

By induction on n we cas show the following: ($n \in \mathbb{N}$)

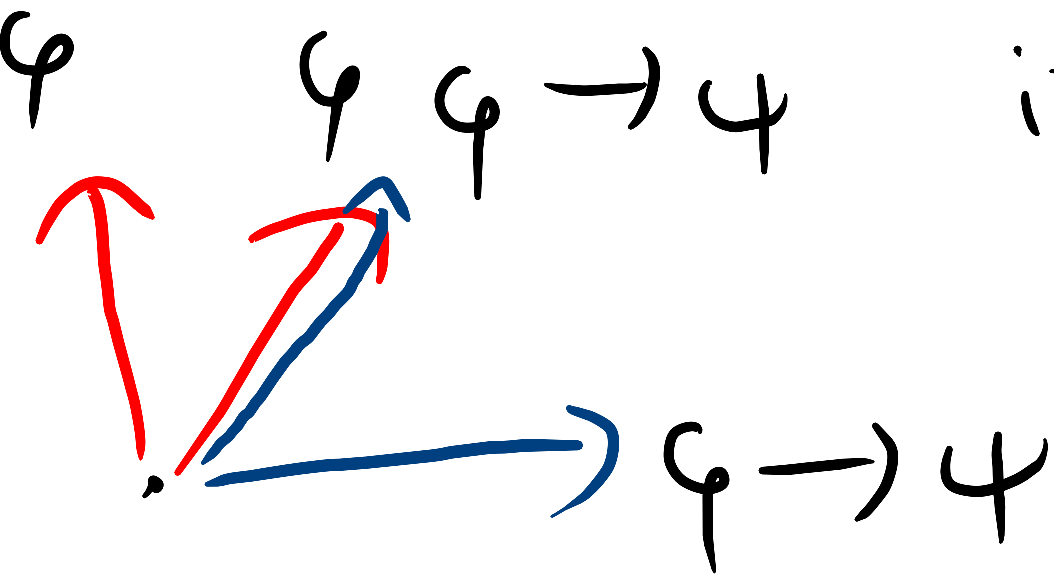
<u>odd rounds</u>: After $2n+1$ successful messages (all but the first are acknowledgements) $K_b (K_a K_b)^n m$ but $\neg (K_a K_b)^{n+1} m$

<u>even rounds</u>: After $2n+2$ successful messages (all but the first are acknowledgements) $(K_a K_b)^{n+1} m$ is true but $\neg K_b (K_a K_b)^{n+1} m$ is also true

Hence, common knowlege cannot be established this way.

Implicit/Distributed Knowledge

What all the agents in B know
"together"



it does not hold $K_a \psi$

it does not hold $K_b \psi$

it holds $K_a \phi$

it holds $K_b\, \phi \to \psi$

it holds $D_{ab} \phi$

$K_a\phi$ = "a Knows ϕ"

$E_B\phi$ = "everybody in B Knows ϕ"

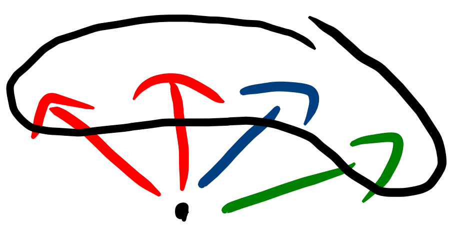
$D_B\phi$ = "a wise man Know ϕ" = "all together in B Know ϕ"

$C_B\phi$ = "it is common Knowledge among the agents in B that ϕ" = "every Fool in B Knows that ϕ"

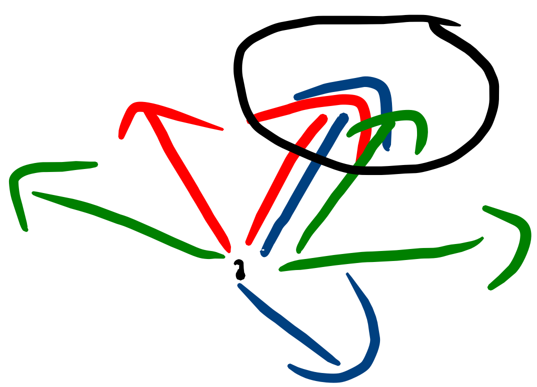
Semantics: We continue to have the same S5 epistemic modes, i.e. $\langle S, \sim, V \rangle$

Definition. Let S be a set and $\{R_b\}_{b \in B}$ is a set of binary relations in S.

- $R_{E_b} = \bigcup_{b \in B} R_b$



- $R_{D_b} = \bigcap_{b \in B} R_b$



- The transitive closure of a relation R, is a relation R^+ such that

1. $R \subseteq R^+$
2. $(\forall x,y,z)(xR^+y \wedge yR^+z \Rightarrow xR^+z)$
3. R^+ is the smallest relation that satisfies 1 and 2

- The reflexive transitive closure of a relation R, is a relation R^* that satisfies 1–3 and also $(\forall x)(xR^*x)$

$x \xrightarrow{R^*} y$ iff y is reachable from x using only R-steps

$$x \xrightarrow{R} x_1 \xrightarrow{R} x_2 \to \dots \xrightarrow{R} y$$

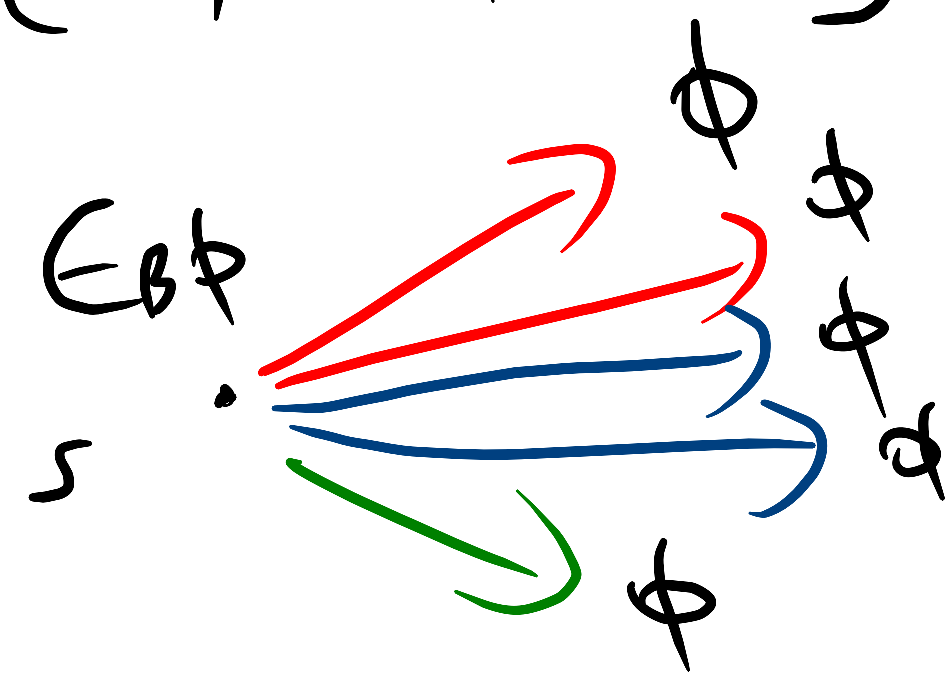
or

$x = y$

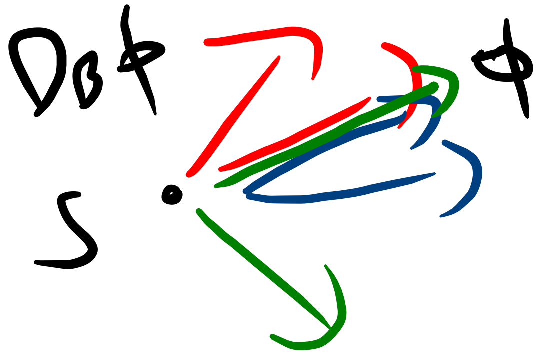
Definition 2.30 (Truth for L_{KC}-formulas)

Let $M = \langle S, \sim, V \rangle$ be an S5-model and $s \in S$

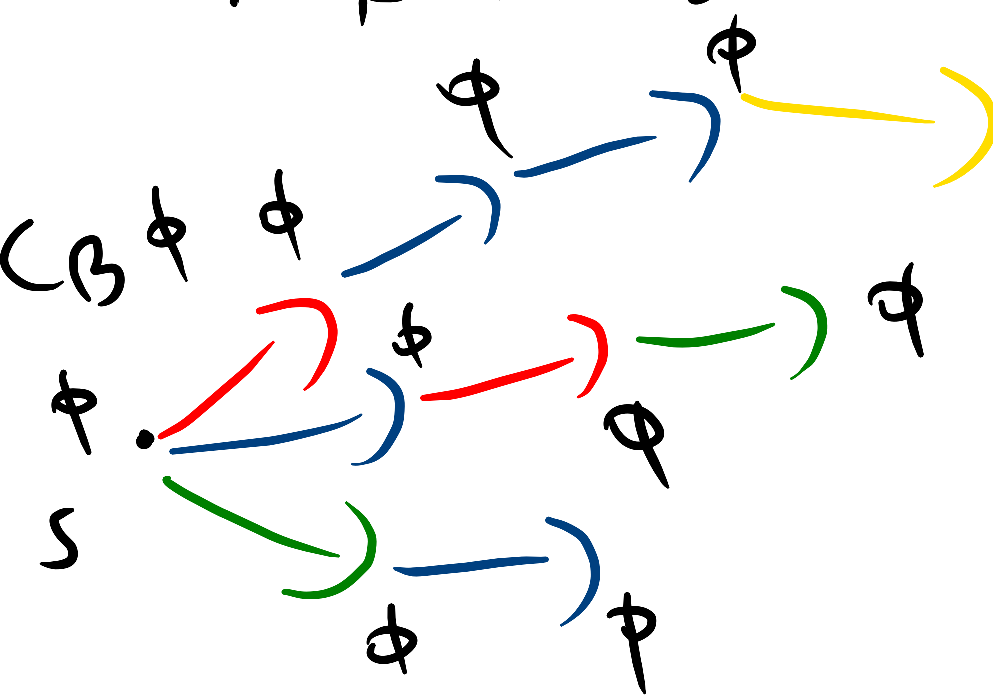
- $M, s \models E_B \phi \iff (\forall t)\left(s R_{E_B} t \Rightarrow (M, t) \models \phi\right]$



- $M, s \models D_B \phi \iff (\forall t)\left[s R_{D_B} t \implies M, t \models \phi \right]$



- $M, s \models C_B \phi \iff (\forall t)\left[s R^{*}_{E_B} t \implies M, t \models \phi \right]$

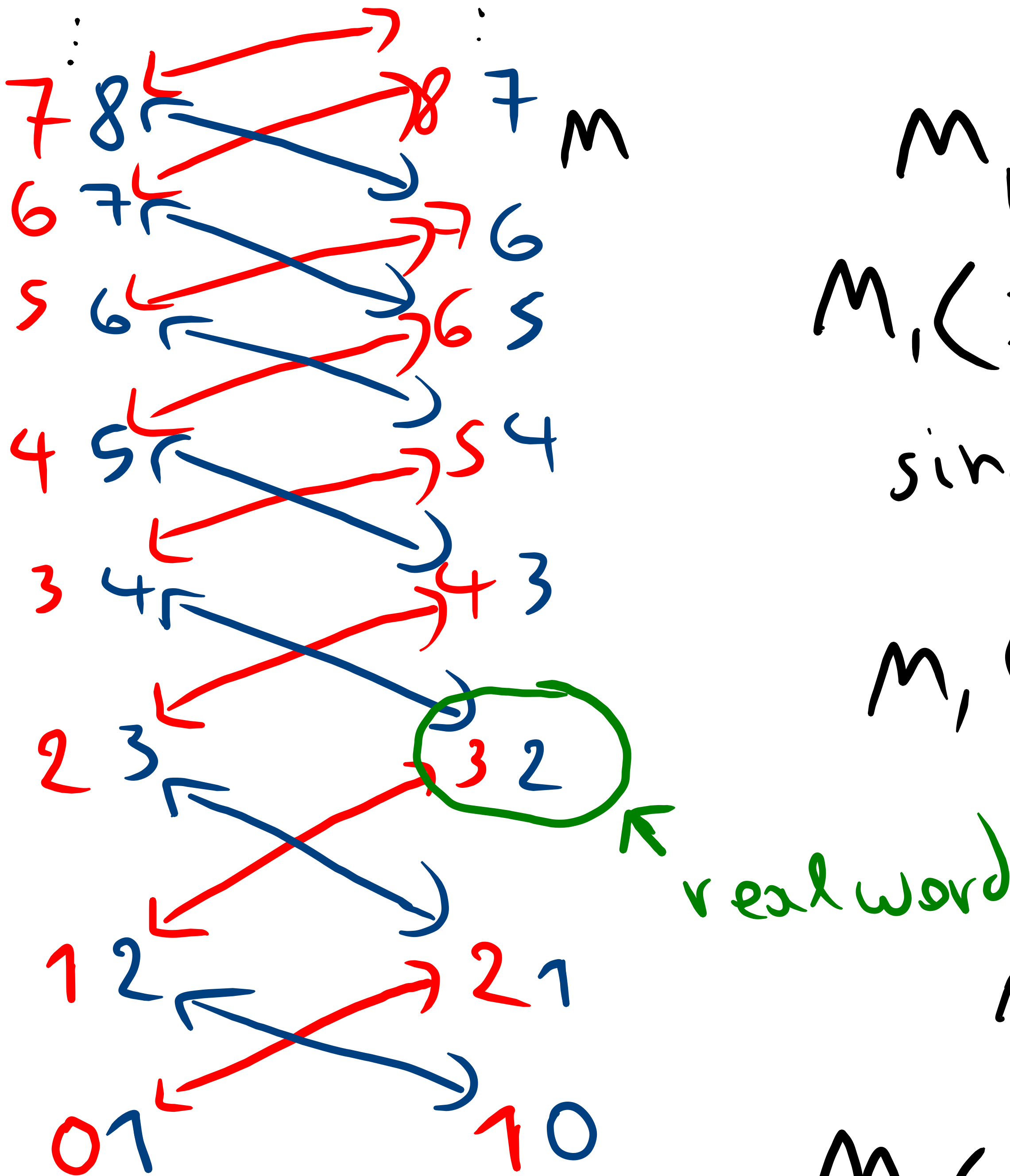


$$C_B\phi \Rightarrow E_B\phi \Rightarrow K_a\phi \Rightarrow D_B\phi \Rightarrow \phi$$

$$a \in B \subseteq A$$

S5C is the class of S5 models equiped with the definition of common knowledge truth

Ex. 2.32 (Common Knowledge in Cons. Numbers)



a b

$$M,\langle 3,2\rangle \models \neg b_4 \wedge \neg E_{ab}\neg b_4$$

$$M,\langle 3,2\rangle \models E_{ab}\neg a_5 \wedge \neg E_{ab}E_{ab}\neg a_5$$

since

$$\langle 3,2\rangle \longrightarrow \langle 3,4\rangle \longrightarrow \langle 5,4\rangle$$

$$M,\langle 3,2\rangle \models K_b K_a a_5$$

$$M,\langle 3,2\rangle \models E_{ab}E_{ab}\neg b_6 \wedge \neg E_{ab}E_{ab}E_{ab}\neg b_6$$

$$M,\langle 3,2\rangle \models \neg C_{ab}\neg a_{1235}$$

$$M,\langle 3,2\rangle \models C_{ab}\neg b_{1235}$$

$$M \models (a_3 \wedge b_2) \longrightarrow (\neg C_{ab}\neg a_{1235} \wedge C_{ab}\neg b_{1235})$$

Example 2.33 (Possible Delay). It is a generalization of Byzantine Generals.

S : sender

R : receiver

$S = R$

when a message is sent it either arrives immediately or in the next time step

No beginning or end of time

m = "the message that was sent was delivered"

"Wen will S and R have common Knowledge of m?"

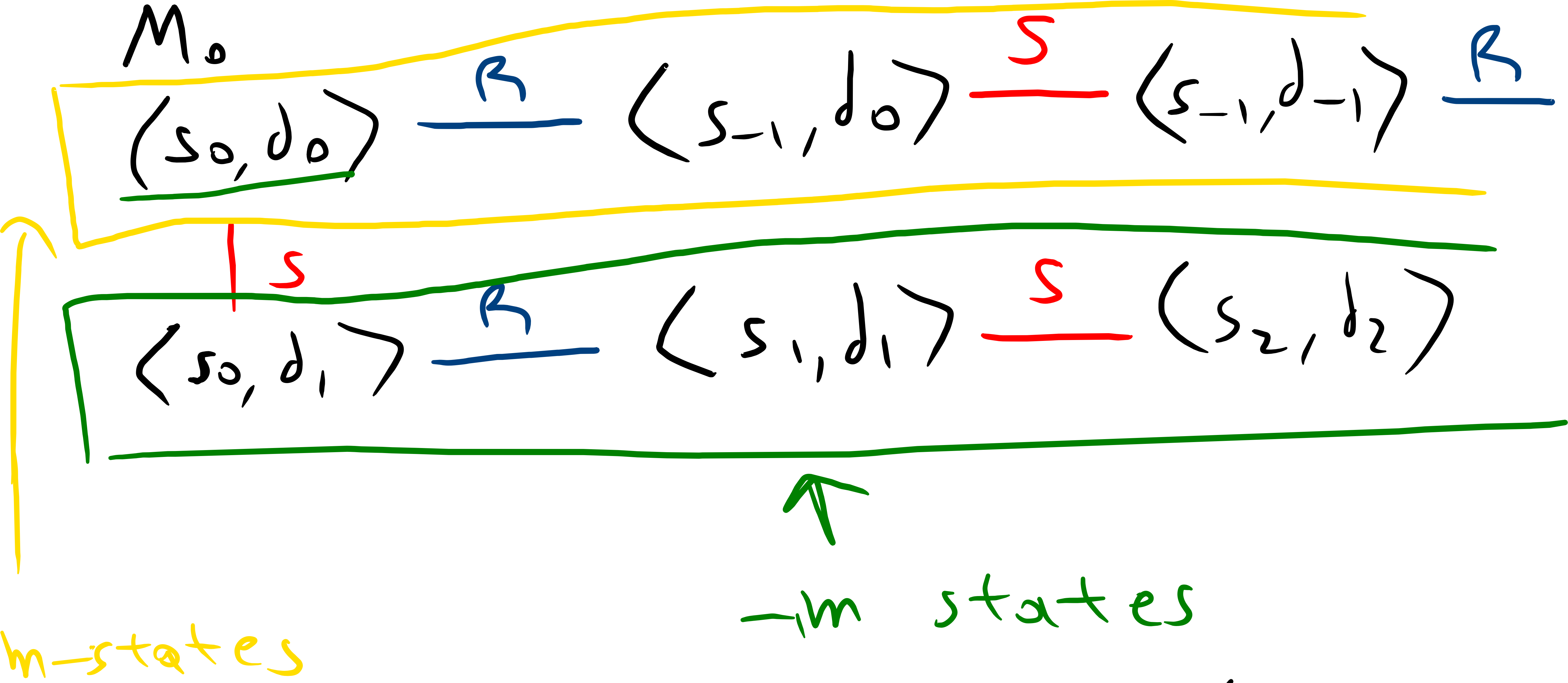
Spoiler Alert: Never!!!

states: $\langle s_i, d_j \rangle$ the message was sent at time i and delivered at time j

The model M_K describes the Knowledge after K time steps.

$$M_K, \langle s_i, d_j \rangle \models m \text{ iff } j \leq K$$

We assume that m was sent at time 0 and delivered at time 0



$$M_0, \langle s_0, d_0\rangle \models m \wedge K_R m \wedge \neg K_S m \wedge \neg C_{SR} m$$

M_1 is M_0 where $\langle s_0, d_0 \rangle$ is shifted 2 steps to the right

$$
\begin{tikzcd}
\langle s_1, d_1 \rangle \arrow[r, dash, "R"] \arrow[d, dash, "S"] & \langle s_0, d_1 \rangle \arrow[r, dash, "S"] & \langle s_0, d_0 \rangle \arrow[r, dash, "R"] & \langle s_{-1}, d_0 \rangle \arrow[r, dash, "R"] & {} \\
\langle s_1, d_2 \rangle \arrow[r, dash, "R"] & \langle s_2, d_2 \rangle \arrow[r, dash, "S"] & \langle s_2, d_3 \rangle \arrow[r, dash, "R"] & {}
\end{tikzcd}
$$

M_k is the same as M_0 with the $\langle s_0, d_0 \rangle$ shifted $k+2$ positions to the right and also $M_k, \langle s_k, d_{k+1} \rangle \models \neg m$

So, $C_{SR}\, m$ can NEVER be achieved