Epistemic Logic IV

from friends to couples

Yanjing Wang
Department of Philosophy, Peking University

Oct. 10th 2023

Classification of logic and action

The different levels of rationality (van Benthem):

- reason logically
- act cleverly
- interact intelligently
- everything above under uncertainty

	no knowledge	knowledge	group
no action	PL	EL	...
act/time	PDL, TL	ETL, DEL, EPDL	...
strategy	ATL, STIT	AETL, ESTIT	...

More interesting, if knowledge can be updated.

No knowledge but action or time

No knowledge but agent-based strategy

Combinations

No knowledge but action or time

Propositional dynamic logic (Pratt [76], Fischer & Ladner [79])

Propositional dynamic logic (where $a \in \mathbf{Act}$):

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid [\pi]\phi$$

$$\pi \quad ::= \quad a \mid ?\phi \mid (\pi;\pi) \mid (\pi + \pi) \mid \pi^*$$

$[\pi]\phi$ reads: ϕ holds after any successful execution of program π. $[\texttt{while}\ \phi\ \texttt{do}\ a]\psi := [(?\phi;a)^*;?\neg\phi]\psi$, $C_{\{a,b\}}\phi := [(a+b)^*]\phi$. A model is a tuple $\langle S, \{\xrightarrow{a} \mid a \in \mathbf{Act}\}, V\rangle$ the semantics is given by:

$$\boxed{\mathcal{M}, s \vDash [\pi]\phi \quad \Leftrightarrow \quad \forall t : sR_\pi t \text{ implies } \mathcal{M}, t \vDash \phi}$$

$$R_a = \xrightarrow{a}$$

$$R_{?\phi} = \{(s,s) \mid \mathcal{M}, s \vDash \phi\}$$

$$R_{\pi;\pi'} = R_\pi \circ R_{\pi'}$$

$$R_{\pi+\pi'} = R_\pi \cup R_{\pi'}$$

$$R_{\pi^*} = \bigcup_{n \in \mathbb{N}} R_{\pi^n}$$

Important axioms

- Distribution axioms and necessitation rules for $[\pi]$
- $[?\phi]p \leftrightarrow (\phi \to p)$
- $[\pi; \pi']p \leftrightarrow [\pi][\pi']p$
- $[\pi + \pi']p \leftrightarrow [\pi]p \wedge [\pi']p$
- Fixed Point: $[\pi^*]p \leftrightarrow (p \wedge [\pi][\pi^*]p)$
- Induction: $(p \wedge [\pi^*](p \to [\pi]p)) \to [\pi^*]p$
- Or the rule: form $\vdash \phi \to (\psi \wedge [\pi]\phi)$ infer $\vdash \phi \to [\pi^*]\psi$. The rule also says that $[\pi^*]\psi$ is the greatest post-fixed point.

We can understand axioms about common knowledge and other temporal operators in the similar way.

Temporal logics

Linear-time temporal logic Pnueli (1977) based on Kamp (1968):

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid X\phi \mid (\phi U \phi)$$

A model $\mathcal{M}$ is $\langle R, V \rangle$ where:

- R is a non-empty set of runs (intuitively, *infinite* sequences indexed by natural numbers, labelled by propositions);
- $V : R \times \mathbb{N} \to 2^{\mathbf{P}}$.

$$\boxed{\begin{array}{rcl} \mathcal{M}, (r,t) \vDash X\phi & \Leftrightarrow & \mathcal{M}, (r, t+1) \vDash \phi \\ \mathcal{M}, (r,t) \vDash \phi U \psi & \Leftrightarrow & \exists t' \geq t \in \mathbb{N} \text{ such that } \mathcal{M}, (r,t') \vDash \psi \\ & & \text{and } \forall t'' : t \leq t'' < t' : \mathcal{M}, (r, t'') \vDash \phi \end{array}}$$

$F\phi := \top U \phi$, $G\phi := \neg F \neg \phi$, $\phi W \psi := (\phi U \psi) \vee G\phi$.

What can we express

X is sometimes written $\bigcirc$ (self-dual operator: both Box and Diamond).

- *Safety* properties: bad things do not happen, e.g., $G\neg p$
- *Liveness* properties: good things will happen, e.g., Fp

More complicated ones:

- FGp
- $G(p \to Fq)$
- $GFp \to GFq$ (strong fairness)
- $G(r \to X(rU(g \wedge X(gU(y \wedge X(yUr))))$? r=red

Important axioms to axiomatize the logic

- Distribution axioms and necessitation rules for X and G
- Functionality: $X\neg p \leftrightarrow \neg Xp$
- Fixed Point: $Gp \leftrightarrow (p \wedge XGp)$
- Induction rule: from $\vdash \psi \to \varphi \wedge X\psi$ infer $\vdash \psi \to G\psi$
- Fixed Point: $pUq \leftrightarrow q \vee (p \wedge X(pUq))$
- Induction rule: from $\vdash (\psi \vee (\varphi \wedge X\theta)) \to \theta$ infer $\vdash \varphi U\psi \to \theta$
- Interaction: $pUq \to Fq$

Branching-time temporal logic

Computational tree logic (CTL) Clarke and Emerson (1982):

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid EX\phi \mid EG\phi \mid E(\phi U \phi)$$

E is a path quantifier. $EF\phi := E[\top U\phi]$, $AX\phi := \neg EX(\neg\phi)$, $AG\phi := \neg EF(\neg\phi)$, etc. EG is not expressible by EU (but by AU).

It is interpreted on a transition system $\langle S, \to, V\rangle$ where $\to$ is serial. Here is the *rough* idea for the semantics for $E\phi(\phi = X\psi, G\psi, \psi_1 U\psi_2)$:

$$\boxed{\mathcal{M}, s \vDash E\phi \quad \Leftrightarrow \quad \exists r \text{ starting at } s \text{ such that } \mathcal{M}, (r, 0) \vDash_{LTL} \phi}$$

More precisely (still based on *states*, not paths) e.g.,

$$\boxed{\mathcal{M}, s_0 \vDash EG\phi \quad \Leftrightarrow \quad \exists \text{ a path } s_0 s_1 s_2 \ldots \text{ such that } \forall k \in \mathbb{N} : \mathcal{M}, s_k \vDash \phi}$$

Some important axioms and rules

Fixed point axioms:

- $E(pUq) \leftrightarrow q \vee (p \wedge EXE(pUq))$
- $A(pUq) \leftrightarrow q \vee (p \wedge AXA(pUq))$

Induction Rules:

- from $\vdash (\psi \vee (\varphi \wedge EX\theta)) \rightarrow \theta$ infer $\vdash E(\varphi U \psi) \rightarrow \theta$
- from $\vdash (\psi \vee (\varphi \wedge AX\theta)) \rightarrow \theta$ infer $\vdash A(\varphi U \psi) \rightarrow \theta$

Comparing LTL and CTL

We can also define LTL semantics over pointed Kripke models:

$$\boxed{\mathcal{M}, s \vDash \phi \quad \Leftrightarrow \quad \forall \text{ infinite path } r \text{ starting from } s : \mathcal{M}, (r, 0) \vDash \phi}$$

There is always an implicit universal path quantifier when using LTL formulas to do model checking!

- Model checking problems of LTL and CTL on finite models are decidable ($m = |\mathcal{M}|, n = |\phi|$):
  - CTL: $O(mn)$ using labelling and fixed-point computation
  - LTL: $O(m2^n)$ using emptiness checking of Büchi automata over infinite words: to check whether $\mathcal{M}, s \vDash \phi$, compute the automaton of $\neg\phi$ and the automaton of $\mathcal{M}, s$ and then check whether the product automaton can accept any path.
- LTL is more intuitive to use

- LTL and CTL are not comparable in expressivity:
  - LTL formulas implicitly start with an A path quantifier.
  - FGp is not expressible in CTL. What about $AF(AGp)$?
  - $AG(EFp)$ is not expressible in LTL.
- They are both fragments of CTL^*, e.g. $EXp \wedge AFGp$ is neither in CTL nor LTL, but in CTL*, which breaks the “bundles”.

Modal μ-calculus generalize these further by directly introducing greatest/least fixed points into the language.

Examples to see the tricky differences

s satisfies LTL formula FGp but not CTL formula $AF(AGp)$:

$$
\begin{tikzcd}
s:p \arrow[loop above] \arrow[r] & w \arrow[r] & t:p \arrow[loop above]
\end{tikzcd}
$$

s satisfies CTL formula $AGEFp$ but not LTL formula GFp:

$$
\begin{tikzcd}
s \arrow[loop above] \arrow[r] & t:p \arrow[loop above]
\end{tikzcd}
$$

Note that $AGAFp$ is equivalent to LTL formula GFp but $AGAFp \to AGAFq$ is not equivalent to LTL formula $GFp \to GFq$, why?

No knowledge but agent-based strategy

Alternating-time temporal logic (ATL) [Alur et al. 1997]

We want to express some agents can together make sure some properties.

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid \langle\langle A \rangle\rangle X\phi \mid \langle\langle A \rangle\rangle G\phi \mid \langle\langle A \rangle\rangle (\phi U \phi)$$

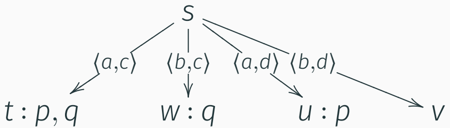
$\langle\langle A \rangle\rangle\psi$ says that the agent group A *can* *make sure* ψ by a collective strategy. $\langle\langle A \rangle\rangle$ is like a path quantifier in CTL.

The model is called *concurrent game structure* (given a set of agents **I** and a set of actions **Act**):

$$\mathcal{M} = \langle S, d, \delta, V \rangle$$

- $d : S \times \mathbf{I} \to 2^{\mathbf{Act}}$ gives available actions for each agent;
- $\delta : S \times \mathbf{Act}^{|\mathbf{I}|} \to S$ is a partial transition function coherent with d

(Simplified) Example



where $S = \{s, t, u, v\}$, $\mathbf{I} = \{1, 2\}$, $d(s, 1) = \{a, b\}, d(s, 2) = \{c, d\}$. If 1 does a and 2 does c at s then the result is t: $\delta(s, \langle a, c\rangle) = t$. Other transitions are similar.

Intuitively 1 cannot make sure q but 2 can by doing c. On the other hand, 2 cannot make sure p but 1 can by doing a. 1 and 2 together can make sure $p \wedge q$ by doing a and c respectively. The semantics of ATL will make this more precise.

Semantics for ATL

A strategy for an agent is a function: $S^+ \to \mathbf{Act}$ coherent with the available actions to the same agent, where S^+ is the set of non-empty finite sequences of the states in S (the history matters when choosing your next action). A collective strategy for a group $A \subseteq \mathbf{I}$ is a function: $S^+ \times A \to \mathbf{Act}$. Note that if A is not the set of all the agents then usually a collective strategy of A *cannot* force a single path since other agents outside A can do something to affect the resulting states of the *joint actions*.

The semantics is given by (we only show the simplest case):

$\mathcal{M}, s \vDash \langle\langle A \rangle\rangle X\phi$	$\Leftrightarrow$	there is a collective strategy η for group A such that: for *every* path r w.r.t. η: $\mathcal{M}, r[1] \vDash \phi$

Important axioms

- $\neg\langle\langle A\rangle\rangle X\bot$
- $\langle\langle A\rangle\rangle X\top$
- $\neg\langle\langle\varnothing\rangle\rangle X\neg p \to \langle\langle \mathbf{I}\rangle\rangle Xp$
- $\langle\langle A_1\rangle\rangle Xp \wedge \langle\langle A_2\rangle\rangle Xq \to \langle\langle A_1 \cup A_2\rangle\rangle X(p \wedge q)$ (disjoint A_1 and A_2)
- $\langle\langle A\rangle\rangle Gp \leftrightarrow (p \wedge \langle\langle A\rangle\rangle X\langle\langle A\rangle\rangle Gp)$
- $\langle\langle\varnothing\rangle\rangle G(q \to (p \wedge \langle\langle A\rangle\rangle Xq)) \to \langle\langle\varnothing\rangle\rangle G(q \to \langle\langle A\rangle\rangle Gp)$
- $\langle\langle A\rangle\rangle pUq \leftrightarrow q \vee (p \wedge \langle\langle A\rangle\rangle X\langle\langle A\rangle\rangle pUq)$
- $\langle\langle\varnothing\rangle\rangle G((q \vee (p \wedge \langle\langle A\rangle\rangle Xr)) \to r) \to \langle\langle\varnothing\rangle\rangle G(\langle\langle A\rangle\rangle pUq \to r)$

- ATL can be viewed as an extension of CTL, $\langle\langle A\rangle\rangle$ can be viewed as a path quantifier: A in CTL is $\langle\langle\varnothing\rangle\rangle$, and $E := \langle\langle \mathbf{I}\rangle\rangle$.
- The model-checking problem for ATL is PTIME-complete, and can be solved in time $O(|\mathcal{M}| \cdot |\phi|)$ by fixed-point computation
- Strategy for ATL can be synthesized incrementally.
- Model checking ATL formulas $\langle\langle A\rangle\rangle\phi$ corresponds to solving concurrent extensive games.

Problem: $\langle\langle i\rangle\rangle G(\mathit{married} \wedge \langle\langle i\rangle\rangle X\neg \mathit{married})$ is satisfiable! (strategy may be changed at a later stage)

See to it that (STIT) logic, Belnap (2001)

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid \Box\phi \mid [i : \mathtt{stit}]\phi$$

$\Box\phi$: necessarily ϕ (no matter what agents choose). $[i : \mathtt{stit}]\phi$: i sees to it that ϕ (given the current choice, i makes sure ϕ).

A model is $\langle T, <, C, V\rangle$ where $\langle T, <\rangle$ is a tree (paths are histories)

- C gives for each i each $m \in T$ a *partition* over histories through m, representing the choices i can make at m. Call the induced equivalence relation R_i^m. We require that the choices of the agents at a moment always intersect.
- V assigns to each (h, m) a set of basic propositions

$$\boxed{\begin{array}{rcl} \mathcal{M}, (h, m) \vDash \Box\phi & \Leftrightarrow & \forall h' : m \in h' \text{ implies } \mathcal{M}, (h', m) \vDash \phi \\ \mathcal{M}, (h, m) \vDash [i : \mathtt{stit}]\phi & \Leftrightarrow & \forall h' : (h, m) R_i^m (h', m) \Rightarrow \mathcal{M}, (h', m) \vDash \phi \end{array}}$$

Important axioms

- S5 for $\Box$
- S5 for $[i\ \mathtt{stit}]$
- $\Box\phi \to [i\ \mathtt{stit}]\phi$
- $\Diamond[i_1\ \mathtt{stit}]\phi_1 \wedge \cdots \wedge \Diamond[i_n\ \mathtt{stit}]\phi_n \to \Diamond([i_1\ \mathtt{stit}]\phi_1 \wedge \cdots \wedge [i_n\ \mathtt{stit}]\phi_n)$: the agents' choices are independent.

$\Diamond$ is used to jump to other history (passing the same moment) to represent the outcome of the choices). The ATL formula $\langle\langle\{i\}\rangle\rangle\phi$ can be compared to $\Diamond[i\ \mathtt{stit}]\phi$.

Deliberative STIT: $[i\ \mathtt{stit}]\phi \wedge \neg\Box\phi$. It can be extended to $[A : \mathtt{stit}]\phi$ where we consider the intersection of R_i^m.

Combinations

Combinations

Knowledge comes in if there is uncertainty:

- Epistemic temporal logic (ETL: **linear** /branching)
- Dynamic epistemic logic (with PDL program) (**next lecture**)
- Alternating-time temporal epistemic logic (ATEL)
- Epistemic see-to-it-that logic (ESTIT)

Epistemic (linear-time) temporal logic, Halpern & Moss et al.

$$\phi \quad ::= \quad \top \mid p \mid \neg\phi \mid (\phi \wedge \phi) \mid X\phi \mid (\phi U \phi) \mid K_i\phi$$

We can express: $F(K_1 p \wedge G\neg(K_2 p \vee K_2 \neg p))$.

A model is $\langle R, \sim, V \rangle$ where:

- R is a non-empty set of runs;
- $\sim : \mathbf{I} \to 2^{Points \times Points}$ where $Points = R \times \mathbb{N}$ such that $\sim_i$ is an equivalence relation;
- $V : Points \to 2^{\mathbf{P}}$.

$$\boxed{\mathcal{M}, (r,t) \vDash K_i\phi \quad \Leftrightarrow \quad \forall (r', t') \sim_i (r,t) : \mathcal{M}, (r', t') \vDash \phi}$$

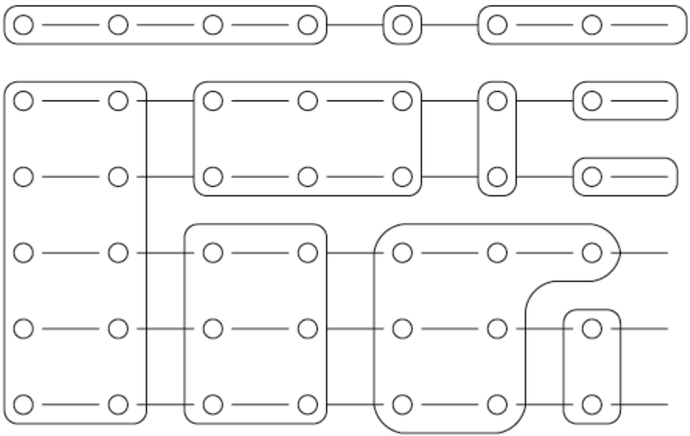
Different properties about knowledge and time

- Synchrony: for all points (r, m) and (r', n) if $(r, m) \sim_i (r', n)$ then $m = n$;
- Perfect recall: for all points $(r, m) \sim_i (r', n)$, if $m > 0$ then either $(r, m-1) \sim_i (r', n)$ or there exists $l < n$ such that $(r, m-1) \sim_i (r', l)$ and for all $l < k \leq n$: $(r, m) \sim_i (r', k)$.
- No learning: for all points $(r, m) \sim_i (r', n)$, either $(r, m+1) \sim_i (r', n)$ or there exists $l > n$ such that $(r, m+1) \sim_i (r', l)$ and for all $n \leq k < l$: $(r, m) \sim_i (r', k)$.

Try to see what PR and NL say under the synchrony condition.

Idea: PR agents can only *refine* the information cells, NL agents can only make them more coarse (not learning).

Example of perfect recall



Complexity: depending on the assumptions

The logics are computationally quite different (multi-agent no CK):

- PSPACE-complete (none, sync, sync+uis, uis)
- EXPSPACE-complete (nl+sync+uis, nl+pr+sync+uis)
- non-elementary time (pr, pr+sync, pr+uis, pr+sync+uis)
- non-elementary space (nl, nl+pr, nl+pr+sync, nl+sync)
- not decidable (nl+uis, nl+pr+uis)

Model checking is usually given by finitely generated interpreted systems using local states.

Important axioms

To axiomatize logics (uis is unique initial state):

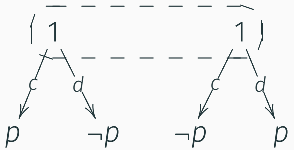
- S5+LTL (none, sync, sync+uis, uis)
- KT2: $K_i X p \to X K_i p$ (pr+sync, pr+sync+uis)
- KT3: $K_i p \wedge X(K_i q \wedge \neg K_i r) \to \neg K_i \neg (K_i p U (K_i q U \neg r))$ (pr, pr+uis)
- KT4: $(K_i p U K_i q) \to K_i (K_i p U K_i q)$ (nl)
- KT5 $X K_i p \to K_i X p$ (nl+sync)
- KT6: $K_i p \leftrightarrow K_1 p$

. Combination to axiomatize logics:

- KT2+5 (nl+pr+sync)
- KT2+5+6 (nl+sync+uis, nl+pr+uis)
- KT3+4 (nl+pr, nl+pr+uis, nl+uis)

Alternating-time epistemic logic (ATEL)

What if we just add some epistemic uncertainty in the model as in the temporal logic case? Intuitively, the agent 1 cannot make sure p in the following model with the initial uncertainty (if he is not sure which state he is, then he does not know what to choose to make sure p):



Something wrong: $K_i\langle\langle 1\rangle\rangle Xp$ holds at any state of the first level: the agent can chose c or d respectively. Know+can≠*know how*!

Possible solution in epistemic STIT

In our later know-how framework, it will become more clear: what we need is $\exists$strategy K[strategy]ϕ, but not $K\exists$strategy [strategy]ϕ (de dicto vs. de re again).

- We need to insert the knowledge operator at the right position.
- $\langle\langle i\rangle\rangle X\phi$ in temporal STIT logic is $\Diamond[i\ \mathtt{stit}]X\phi$ (*there is* a choice that i can make sure...)
- $K_i\langle\langle i\rangle\rangle Xp = K_i \Diamond [i\ \mathtt{stit}]X\phi$
- $\Diamond K_i[i\ \mathtt{stit}]X\phi$ is a better attempt.

Further extensions

- Common knowledge
- Model building methods:
  - Generated epistemic relation by local states.
  - Generated temporal structures by (knowledge-based) programs/protocols.

Model checking tools for epistemic temporal logic: MCK, MCMAS.

Epistemics in a security setting

Security protocols with three lines can still go wrong. E.g., Needham-Schroeder authentication protocol to make sure you are talking to the right guy:

$$\begin{array}{llcl} 1. & A \to B & : & \{n_A, A\}_{PK_B} \\ 2. & B \to A & : & \{n_A, n_B\}_{PK_A} \\ 3. & A \to B & : & \{n_B\}_{PK_B} \end{array}$$

Initially, only agent A *'knows'* the value of its own nonce and only B *'knows'* the value of its own nonce. In the end, we want to make sure they *'know'* that they are talking to each other (the one who *''knows'* the right private key): **mutual authentication**.

Attack!

Syntactic given BAN-logic provided a correctness proof of the above protocol, which was later proven flawed due to a man-in-the-middle attack:

$$
\begin{array}{llll|lll}
1 & A \to I & : & \{n_A, A\}_{PK_I} & & & \\
1' & & & & I(A) \to B & : & \{n_A, A\}_{PK_B} \\
2' & & & & B \to I(A) & : & \{n_A, n_B\}_{PK_A} \\
2 & I \to A & : & \{n_A, n_B\}_{PK_A} & & & \\
3 & A \to I & : & \{n_B\}_{PK_I} & & & \\
3' & & & & I(A) \to B & : & \{n_B\}_{PK_B}
\end{array}
$$

Epistemic security properties

Secrecy Intruder should not be able to *know*.

Authentication of the origin Receiver *knows* the sender of a message.

Anonymity Sender is *unknown* to an eavesdropper.

Individual verifiability: a voter can verify that her vote was really counted.

Receipt-freeness: A voter does not gain any information (a receipt) which can help a coercer to *know* to whom she voted in a certain way.

Next

Combination of knowledge and action: dynamic epistemic logic