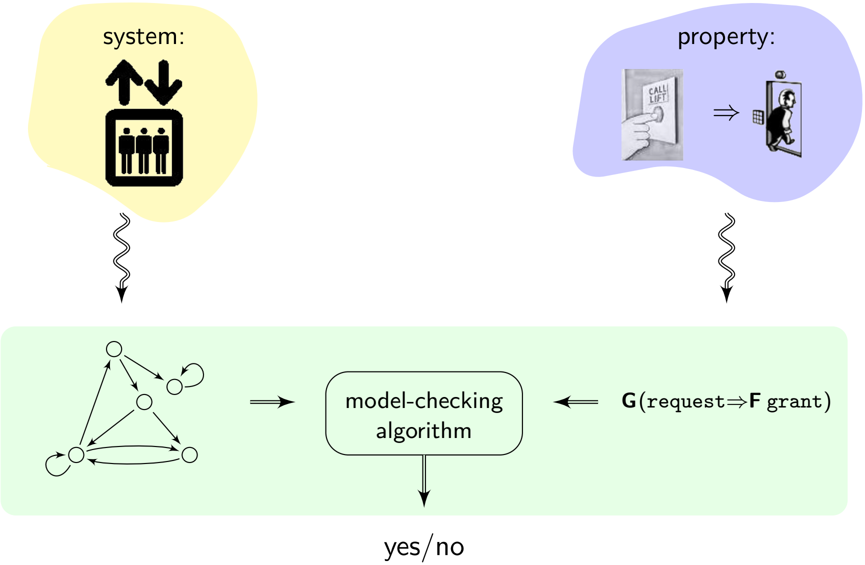
ATL and extensions

Thomas Brihaye[1], Arnaud Da Costa[2], François Laroussinie[3], Nicolas Markey[2]

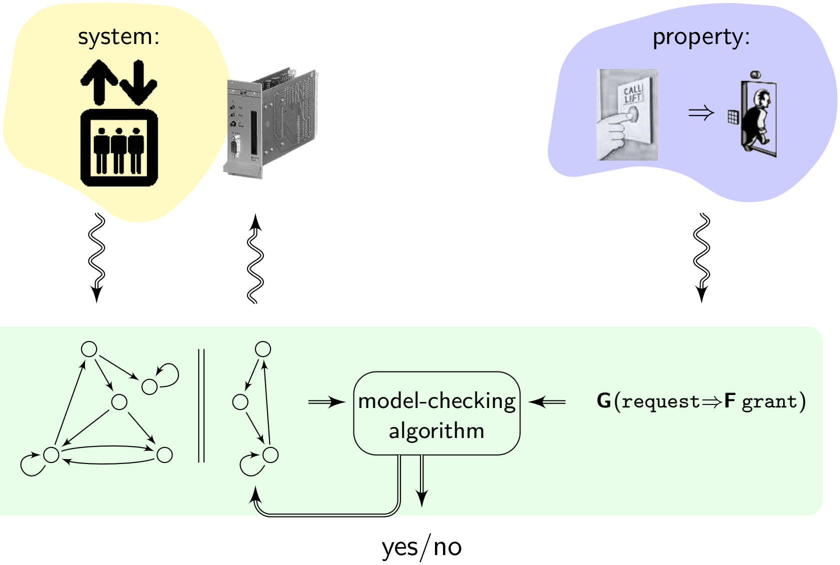
[1] U. Mons, Belgium
[2] LSV, CNRS & ENS Cachan, France
[3] LIAFA, CNRS & Univ. Paris7-Diderot, France

LogICCC final conference – Berlin, Sep. 2011

Model checking



Model checking and control



Computation-Tree Logic (CTL) [CE81,QS82]

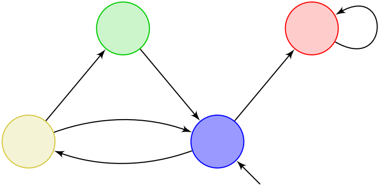
Definition

$$\mathrm{CTL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg \varphi \mid \mathbf{E}\,\mathbf{X}\,\varphi \mid \mathbf{E}\,\mathbf{G}\,\varphi \mid \mathbf{E}\varphi\;\mathbf{U}\;\varphi$$

Computation-Tree Logic (CTL) [CE81,QS82]

Definition

$$\mathrm{CTL} \ni \varphi ::=$$  $$\mid \varphi \vee \varphi \mid \neg \varphi \mid \mathbf{E\,X}\,\varphi \mid \mathbf{E\,G}\,\varphi \mid \mathbf{E}\varphi\ \mathbf{U}\ \varphi$$

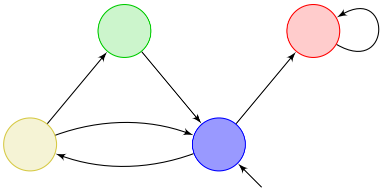


✓ $\mathbf{E}(\mathtt{true}\ \mathbf{U}$  $) \equiv \mathbf{E\,F}$ 

Computation-Tree Logic (CTL) [CE81,QS82]

Definition

$$\text{CTL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\varphi \mid \mathbf{EX}\,\varphi \mid \mathbf{EG}\,\varphi \mid \mathbf{E}\varphi\,\mathbf{U}\,\varphi$$

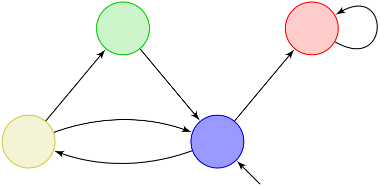


- ✓ $\mathbf{E}(\texttt{true}\ \mathbf{U}\ \bigcirc) \equiv \mathbf{EF}\ \bigcirc$
- ✓ $\mathbf{EG}\ \neg\bigcirc \equiv \neg(\mathbf{AF}\ \neg\bigcirc)$

Computation-Tree Logic (CTL) [CE81,QS82]

Definition

$$\mathrm{CTL} \ni \varphi ::= {\color{red}\bigcirc} \mid \varphi \vee \varphi \mid \neg\varphi \mid \mathbf{E\,X}\,\varphi \mid \mathbf{E\,G}\,\varphi \mid \mathbf{E}\varphi\ \mathbf{U}\ \varphi$$

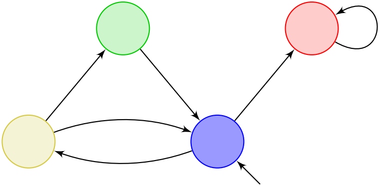


- ✓ $\mathbf{E}(\mathtt{true}\ \mathbf{U}\ {\color{red}\bigcirc}) \equiv \mathbf{E\,F}\,{\color{red}\bigcirc}$
- ✓ $\mathbf{E\,G}\,\neg{\color{green}\bigcirc} \equiv \neg(\mathbf{A\,F}\,\neg{\color{green}\bigcirc})$
- × $\mathbf{E}(\neg{\color{olive}\bigcirc}\ \mathbf{U}\ {\color{green}\bigcirc})$

Computation-Tree Logic (CTL) [CE81,QS82]

Definition

$$\text{CTL} \ni \varphi ::= {\color{red}\bigcirc} \mid \varphi \vee \varphi \mid \neg\varphi \mid \mathbf{EX}\,\varphi \mid \mathbf{EG}\,\varphi \mid \mathbf{E}\varphi\,\mathbf{U}\,\varphi$$

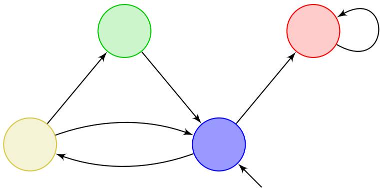


- ✓ $\mathbf{E}(\texttt{true}\ \mathbf{U}\ {\color{red}\bigcirc}) \equiv \mathbf{EF}\,{\color{red}\bigcirc}$
- ✓ $\mathbf{EG}\,\neg{\color{green}\bigcirc} \equiv \neg(\mathbf{AF}\,\neg{\color{green}\bigcirc})$
- × $\mathbf{E}(\neg{\color{olive}\bigcirc}\ \mathbf{U}\ {\color{green}\bigcirc})$
- ✓ $\mathbf{EG}(\neg{\color{green}\bigcirc} \wedge \mathbf{EF}\,{\color{green}\bigcirc})$

Computation-Tree Logic (CTL) [CE81,QS82]

Definition

$$\mathsf{CTL} \ni \varphi ::= {\color{red}\bigcirc} \mid \varphi \vee \varphi \mid \neg \varphi \mid \mathbf{EX}\,\varphi \mid \mathbf{EG}\,\varphi \mid \mathbf{E}\varphi\,\mathbf{U}\,\varphi$$



- ✓ $\mathbf{E}(\mathtt{true}\ \mathbf{U}\ {\color{red}\bigcirc}) \equiv \mathbf{EF}\,{\color{red}\bigcirc}$
- ✓ $\mathbf{EG}\,\neg{\color{green}\bigcirc} \equiv \neg(\mathbf{AF}\,\neg{\color{green}\bigcirc})$
- × $\mathbf{E}(\neg{\color{yellow}\bigcirc}\ \mathbf{U}\ {\color{green}\bigcirc})$
- ✓ $\mathbf{EG}(\neg{\color{green}\bigcirc} \wedge \mathbf{EF}\,{\color{green}\bigcirc})$

Theorem

CTL model checking is PTIME*-complete.*

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

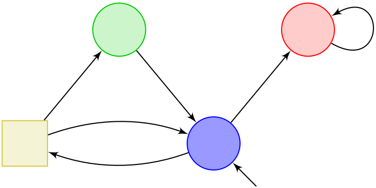
$$\mathrm{ATL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

$$\text{ATL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$



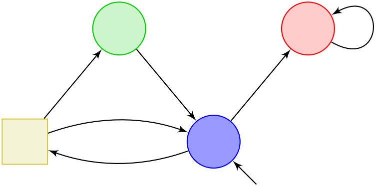
✓ $\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{F}\, \bigcirc$

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

$$\mathsf{ATL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$



✓ $\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{F}\, \bigcirc$

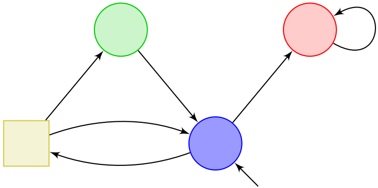
× $\langle\!\langle \square \rangle\!\rangle\, \mathbf{F}\, \bigcirc$

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

$$\text{ATL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\,\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$



✓ $\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{F}\, \bigcirc$

× $\langle\!\langle \square \rangle\!\rangle\, \mathbf{F}\, \bigcirc$

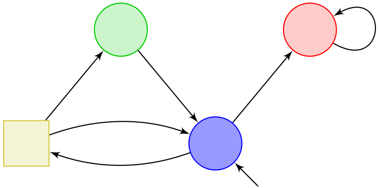
$\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{G}(\, \langle\!\langle \square \rangle\!\rangle\, \mathbf{F}\, \bigcirc)$

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

$$\mathsf{ATL} \ni \varphi ::= {\color{red}\bigcirc} \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$



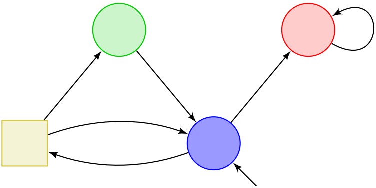
- ✓ $\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{F}\, {\color{red}\bigcirc}$
- × $\langle\!\langle \square \rangle\!\rangle\, \mathbf{F}\, {\color{green}\bigcirc}$
- × $\langle\!\langle \bigcirc \rangle\!\rangle\, \mathbf{G}(\langle\!\langle \square \rangle\!\rangle\, \mathbf{F}\, {\color{green}\bigcirc})$

Alternating-time Temporal Logic (ATL) [AHK97]

Definition

ATL extends CTL with *strategy quantifiers*:

$$\text{ATL} \ni \varphi ::= \bigcirc \mid \varphi \vee \varphi \mid \neg\varphi \mid \langle\!\langle A \rangle\!\rangle\, \mathbf{X}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \varphi\, \mathbf{U}\, \varphi \mid \langle\!\langle A \rangle\!\rangle\, \neg(\varphi\, \mathbf{U}\, \varphi)$$



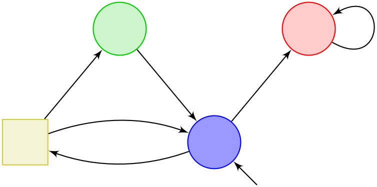
- ✓ $\langle\!\langle \bigcirc \rangle\!\rangle\ \mathbf{F}\ \bigcirc$
- × $\langle\!\langle \square \rangle\!\rangle\ \mathbf{F}\ \bigcirc$
- × $\langle\!\langle \bigcirc \rangle\!\rangle\ \mathbf{G}(\langle\!\langle \square \rangle\!\rangle\ \mathbf{F}\ \bigcirc)$

Theorem

ATL model checking is PTIME*-complete.*

ATL with strategy contexts [BDLM09]

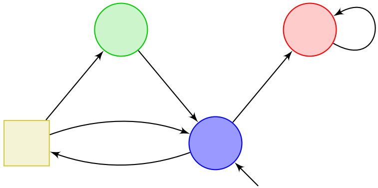
ATL$_{sc}$ has the same syntax as ATL, but different semantics:



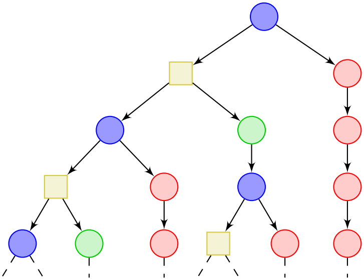
$\langle\cdot\bigcirc\cdot\rangle\ \mathbf{G}(\ \langle\cdot\square\cdot\rangle\ \mathbf{F}\ \bigcirc)$

ATL with strategy contexts [BDLM09]

ATL_{sc} has the same syntax as ATL, but different semantics:



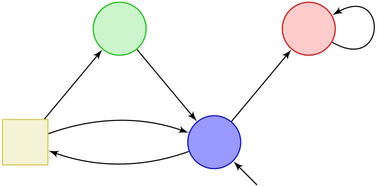
$\langle\cdot\bigcirc\cdot\rangle$ $\mathbf{G}$($\langle\cdot\Box\cdot\rangle$ $\mathbf{F}$ $\bigcirc$)



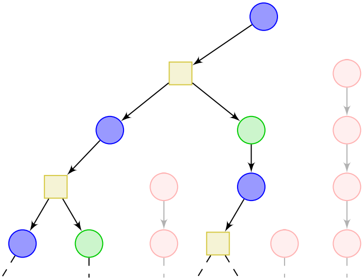
Evaluate the formula on the execution tree:

ATL with strategy contexts [BDLM09]

ATL$_{sc}$ has the same syntax as ATL, but different semantics:



$\langle\cdot\bigcirc\cdot\rangle\ \mathbf{G}(\ \langle\cdot\square\cdot\rangle\ \mathbf{F}\ \bigcirc)$

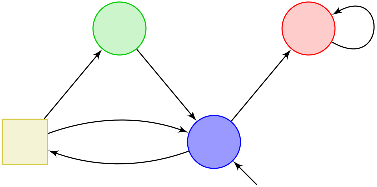


Evaluate the formula on the execution tree:

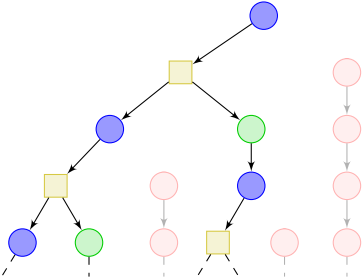
- apply a strategy of Player $\bigcirc$;

ATL with strategy contexts [BDLM09]

ATL_{sc} has the same syntax as ATL, but different semantics:



$$\langle\cdot\bigcirc\cdot\rangle\ \mathbf{G}(\ \langle\cdot\square\cdot\rangle\ \mathbf{F}\ \bigcirc)$$

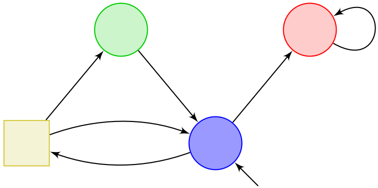


Evaluate the formula on the execution tree:

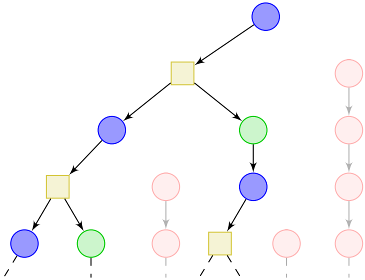
- apply a strategy of Player $\bigcirc$;
- in the remaining tree, check that Player $\square$ can always enforce a visit to $\bigcirc$.

ATL with strategy contexts [BDLM09]

ATL_{sc} has the same syntax as ATL, but different semantics:



✓ $\langle\cdot\bigcirc\cdot\rangle$ $\mathbf{G}(\langle\cdot\square\cdot\rangle$ $\mathbf{F}$ $\bigcirc)$



Evaluate the formula on the execution tree:

- apply a strategy of Player ○;
- in the remaining tree, check that Player □ can always enforce a visit to ○.

What ATL_{sc} can express

- All ATL and ATL* properties;

What ATL_{sc} can express

- All ATL and ATL* properties;
- Client-server interactions for accessing a shared resource:

$$\langle\!\cdot\text{Server}\cdot\!\rangle\ \mathbf{G}\left[\begin{array}{ll} & \displaystyle\bigwedge_{c\in\text{Clients}} \langle\!\cdot c\cdot\!\rangle\ \mathbf{F}\,\text{access}_c \\ \wedge & \\ & \neg \displaystyle\bigwedge_{c\neq c'} \text{access}_c \wedge \text{access}_{c'} \end{array}\right]$$

What ATL_{sc} can express

- All ATL and ATL* properties;
- Client-server interactions for accessing a shared resource:

$$\langle\cdot \mathrm{Server} \cdot\rangle\ \mathbf{G} \left[\begin{array}{ll} & \bigwedge_{c \in \mathrm{Clients}} \langle\cdot c \cdot\rangle\ \mathbf{F}\, \mathrm{access}_c \\ \wedge & \\ & \neg \bigwedge_{c \neq c'} \mathrm{access}_c \wedge \mathrm{access}_{c'} \end{array} \right]$$

- Existence of Nash equilibria:

$$\langle\cdot A_1, \ldots, A_n \cdot\rangle \bigwedge_i \left(\langle\cdot A_i \cdot\rangle\, \varphi_{A_i} \Rightarrow \varphi_{A_i} \right)$$

What ATL_{sc} can express

- All ATL and ATL* properties;
- Client-server interactions for accessing a shared resource:

$$\langle\!\cdot \mathrm{Server} \cdot\!\rangle\ \mathbf{G} \left[\begin{array}{ll} & \bigwedge_{c \in \mathrm{Clients}} \langle\!\cdot c \cdot\!\rangle\ \mathbf{F}\, \mathrm{access}_c \\ \wedge & \\ & \neg \bigwedge_{c \neq c'} \mathrm{access}_c \wedge \mathrm{access}_{c'} \end{array} \right]$$

- Existence of Nash equilibria:

$$\langle\!\cdot A_1, \ldots, A_n \cdot\!\rangle \bigwedge_i \left(\langle\!\cdot A_i \cdot\!\rangle\, \varphi_{A_i} \Rightarrow \varphi_{A_i} \right)$$

- Existence of dominating strategy:

$$\langle\!\cdot A \cdot\!\rangle\ [\cdot B \cdot] \left(\neg \varphi \Rightarrow [\cdot A \cdot]\ \neg \varphi \right)$$

Verifying ATL$_{sc}$ properties

Theorem

Given a CGS $\mathcal{C}$, a state ℓ_0 and an ATL$_{sc}$ formula φ, we can build a Büchi tree automaton $\mathcal{A}$ s.t.

$$\mathcal{L}(\mathcal{A}) \neq \varnothing \quad \Leftrightarrow \quad \mathcal{C}, \ell_0 \models_\varnothing \varphi.$$

$\mathcal{A}$ has size d-exponential, where d is the maximal number of nested quantifiers in φ.

Checking whether $\mathcal{C}, \ell_0 \models_\varnothing \varphi$ is in d-EXPTIME*.*

Verifying ATL$_{sc}$ properties

Theorem

Given a CGS $\mathcal{C}$, a state ℓ_0 and an ATL$_{sc}$ formula φ, we can build a Büchi tree automaton $\mathcal{A}$ s.t.

$$\mathcal{L}(\mathcal{A}) \neq \varnothing \quad \Leftrightarrow \quad \mathcal{C}, \ell_0 \models_{\varnothing} \varphi.$$

$\mathcal{A}$ has size d-exponential, where d is the maximal number of nested quantifiers in φ.

Checking whether $\mathcal{C}, \ell_0 \models_{\varnothing} \varphi$ is in d-EXPTIME.

Proposition

Checking whether $\mathcal{C}, \ell_0 \models_{\varnothing} \varphi$ is (d−1)-EXPSPACE*-hard.*

Conclusions and research directions

ATL_{sc} has a natural semantics:

- it can express many interesting properties (especially non-zero-sum);
- this expressiveness comes with a cost (in terms of model-checking complexity);
- we also studied bounded-memory strategies.

Conclusions and research directions

ATL_{sc} has a natural semantics:

- it can express many interesting properties (especially non-zero-sum);
- this expressiveness comes with a cost (in terms of model-checking complexity);
- we also studied bounded-memory strategies.

We keep on exploring ATL_{sc}:

- characterize behavioural equivalence for ATL_{sc};
- randomized strategies;
- find interesting sublogics, with more efficient model-checking algorithm;
- study satisfiability of ATL_{sc}.