An Application of Separation in Discrete Time ITL to Branching Time

Dimitar P. Guelev

http://www.math.bas.bg/~gelevdp

Plan of Talk

Preliminaries

- LTL with Past and Gabbay's theorem
- propositionally quantified CTL^* (QCTL^*)
- expressing strategic ability in QCTL^*
- Interval Temporal Logic (ITL)

An Interval-based CTL^* (ICTL)

The neighbourhood modalities $\Diamond_l$ and $\Diamond_r$ in ICTL:

- eliminating $\Diamond_l$ and $\Diamond_r$ using ITL separation

Eliminating propositional quantification in ICTL

LTL **with Past** (PLTL)

Set of atomic propositions AP. An interval $I \subseteq \mathbb{Z}$; $\sigma : I \to \mathcal{P}(AP)$, $i \in I$.

$$A ::= \mathit{false} \mid \underbrace{p}_{\in AP} \mid A \supset A \mid \underbrace{\bigcirc A \mid A \,\mathsf{U}\, A}_{\text{not allowed in past formulas}} \mid \underbrace{\ominus A \mid A \,\mathsf{S}\, A}_{\text{not allowed in future formulas}}$$

$$\sigma, k \models \bigcirc A \quad \text{iff} \quad \sigma, k+1 \models A, \qquad \sigma, k \models \ominus A \quad \text{iff} \quad \sigma, k-1 \models A$$

$$\sigma, k \models A \,\mathsf{U}\, B \quad \text{iff} \quad \exists k(\sigma, k+i \models B \wedge \bigwedge_{j=0}^{i-1} \sigma, k+j \models A)$$

$$\sigma, k \models A \,\mathsf{S}\, B \quad \text{iff} \quad \exists k(\sigma, k-i \models B \wedge \bigwedge_{j=0}^{i-1} \sigma, k-j \models A)$$

Strictly future (past) formulas: $\bigcirc F$ ($\ominus P$).

Theorem 1 (Gabbay, 1989) *Every* LTL *formula is equivalent to a boolean combination of past formulas, strictly future formulas and atomic propositions.*

Expressive power of LTL and propositionally quantified LTL

Every first order definable unary predicate in a vocabulary $P_1, \ldots, P_n$ of unary predicate symbols on $\langle \omega, < \rangle$ can be expressed by an LTL formula, if given atomic propositions $p_1, \ldots, p_n$ such that $\sigma, k \models p_i$ is equivalent to $\sigma \models P_i(k)$ in the f.o. sense.

Propositional Quantification:

Given $X \subseteq \mathrm{dom}\sigma$, $(\sigma_p^X)^i \hat{=} \sigma^i \cup \{p\}$ for $i \in X$ and $(\sigma_p^X)^i \hat{=} \sigma^i \setminus \{p\}$, otherwise.

$$\sigma, i \models \exists p A \text{ iff } \sigma_p^X, i \models A \text{ for some } X \subseteq \mathrm{dom}\sigma.$$

Every monadic second order unary predicate can be expressed by a formula in LTL with propositional quantification.

Propositionally Quantified CTL^*: Kripke Models

Kripke models $M \mathrel{\hat{=}} \langle W, w_I, R, V\rangle$ with (total) transition relation $R \subseteq W \times W$ and valuation $V \subseteq AP \times W$.

The infinite continuations of $\mathbf{w}$:

$$R_M^{\inf}(\mathbf{w}) \mathrel{\hat{=}} \{\mathbf{v} \in W^\omega : \mathbf{v}^0 \ldots \mathbf{v}^{|\mathbf{w}|-1} = \mathbf{w}, (\forall k < \omega) R(\mathbf{v}^k, \mathbf{v}^{k+1})\}.$$

$R_M^{\mathrm{fin}}(\mathbf{w}) \subseteq W^+$ is defined similarly.

$R_M^{\inf}(w_I) \quad (R_M^{\mathrm{fin}}(w_I))$ - all the infinite (finite) runs in M.

Given a $p \in AP$ and an $X \subseteq W$, $M_p^X \mathrel{\hat{=}} \langle W, w_I, R, V_p^X\rangle$ where

$V_p^X(p, w) \mathrel{\hat{=}} p \in X$ and $V_p^X(q, w) \mathrel{\hat{=}} V(q, w)$ for $q \in AP \setminus \{p\}$.

Unwinding Kripke Models

$M^T \hat{=} \langle W^T, w_I^T, R^T, V^T \rangle$ - the unwinding of Kripke model $M = \langle W, w_I, R, V \rangle$:

$W^T \hat{=} R_M^{\mathrm{fin}}(w_I)$, $w_I^T = w_I$, $R^T(\mathbf{w}, \mathbf{v}) \hat{=} \mathbf{v} = \mathbf{w} \cdot \mathbf{v}^{|\mathbf{v}|-1}$ and $V^T(p, \mathbf{w}) \hat{=} V(p, \mathbf{w}^{|\mathbf{w}|-1})$.

Given $\mathbf{w} = w_I w^1 w^2 \ldots \in R_M^{\mathrm{fin}}(w_I) \cup R_M^{\mathrm{inf}}(w_I)$,

$$\mathbf{w}^T \hat{=} w_I \;\; w_I w^1 \;\; w_I w^1 w^2 \;\; \ldots$$

$$R_{M^T}^{\mathrm{fin}}(w_I^T) \cong R_M^{\mathrm{fin}}(w_I), \qquad R_{M^T}^{\mathrm{inf}}(w_I^T) \cong R_M^{\mathrm{inf}}(w_I), \qquad (M^T)^T \cong M^T.$$

Every state in the unwinding of a model is the last state of a unique finite run (and indeed is a finite run in M).

Varying $X \subseteq W^T$ allows $(M^T)_p^X$ to have different values for p at M^T states that originate from the same M state.

Propositionally Quantified CTL^* (QCTL^*)

$$A ::= \mathit{false} \mid p \mid A \supset A \mid \bigcirc A \mid A \mathsf{U} A \mid \ominus A \mid A \mathsf{S} A \mid \exists A \mid \exists p A$$

$M \mathrel{\hat{=}} \langle W, w_I, R, V \rangle$, $\mathbf{w} \in R_M^{\mathrm{inf}}(w_I)$, $k < \omega$

$M, \mathbf{w}, k \models p$	iff	$V(p, \mathbf{w}^k)$;
$M, \mathbf{w}, k \models \mathit{false},\ A \supset B$		as in classical propositional logic;
$M, \mathbf{w}, k \models \bigcirc A, A \mathsf{U} B\ \ominus A, A \mathsf{S} B$		as in LTL;
$M, \mathbf{w}, k \models \exists A$	iff	$M, \mathbf{v}, k \models A$ for some $\mathbf{v} \in R_M^{\mathrm{inf}}(\mathbf{w}^0 \dots \mathbf{w}^k)$;
$M, \mathbf{w}, k \models \exists p A$	iff	$(M^T)_p^X, \mathbf{w}^T, k \models A$ for some $X \subseteq W^T = R_M^{\mathrm{fin}}(w_I)$.

CTL^* subsumes LTL; QCTL^* subsumes propositionally quantified LTL.

Expressing Strategic Ability in QCTL^*

Concurrent Game Models (CGMs) $M \hat{=} \langle W, w_I, \langle Act_i : i \in Ag\rangle, o, V\rangle$ where Ag is a set of players.

$Act_\Gamma \hat{=} \prod\limits_{i\in\Gamma} Act_i$ for $\Gamma \subseteq Ag$

Instead of transition relation $R \subseteq W \times W$ we have outcome function $o : W \times Act_{Ag} \to W$.

Instead of the $R(w, w')$, we have $w' = o(w, \mathbf{a})$, $\mathbf{a} \in Act_{Ag}$.

Strategic ability is about the existence of strategies for achieving things.

A strategy for $i \in Ag$ is a function of type $R_M^{\mathrm{fin}}(w_I) \to Act_i$.

There exist dedicated logical notations for CGMs, but CTL^* can be interpreted too by

(1) putting $R(w, w') \hat{=} \exists \mathbf{a}(o(w, \mathbf{a}) = w')$ and

(2) extending the vocabulary to allow identifying actions.

Expressing Strategic Ability in QCTL^*

Upon unwinding a CGM, $w, \mathbf{a} \mapsto o(w, \mathbf{a})$ can be made injective wrt $\mathbf{a}$:

$M^T \hat{=} \langle W^T, w_I^T, \langle Act_i : i \in Ag\rangle, o^T, V^T\rangle$ where

$W^T \hat{=} R_M^{\mathrm{fin}}(w_I) \times Act_{Ag} \cup \{*\},\ w_I^T = w_I$

$o^T(\langle \mathbf{w}, \mathbf{b}\rangle, \mathbf{a}) \hat{=} \langle \mathbf{w} o(\mathbf{w}^{|\mathbf{w}|-1}, \mathbf{a}), \mathbf{a}\rangle$

Finite run $w_I \xrightarrow{\mathbf{a}^1} \underbrace{w^1}_{=o(w_I,\mathbf{a}^1)} \xrightarrow{\mathbf{a}^2} \underbrace{w^2}_{=o(w_1,\mathbf{a}^2)} \cdots w^{k-1} \xrightarrow{\mathbf{a}^k} \underbrace{w^k}_{=o(w^{k-1},\mathbf{a}^k)}$

corresponds to state

$$\langle w_I w^1 w^2 \ldots w^k, \mathbf{a}^k\rangle \in W^T$$

in M^T with all the previous states and the latest action $\mathbf{a}^k$ stored.

Vocabulary $AP' \hat{=} AP \cup \bigcup_{i \in Ag} Act_i$ can be used to identify latest actions:

$V^T(p, \langle \mathbf{w}, \mathbf{a}\rangle) \hat{=} V(p, \mathbf{w}^{|\mathbf{w}|-1})$ and, for $a \in Act_i,\ V^T(a, \langle \mathbf{w}, \mathbf{a}\rangle) \hat{=} a = \mathbf{a}_i$.

Expressing Strategic Ability in QCTL^*

$M^T \hat{=} \langle W^T, w_I^T, \langle Act_i : i \in Ag \rangle, o^T, V^T \rangle$ where

$W^T \hat{=} R_M^{\mathrm{fin}}(w_I) \times Act_{Ag} \cup \{*\}$, $w_I^T = w_I$, $o^T(\langle \mathbf{w}, \mathbf{b} \rangle, \mathbf{a}) \hat{=} \langle \mathbf{w} o(\mathbf{w}^{|\mathbf{w}|-1}, \mathbf{a}), \mathbf{a} \rangle$

$V^T(p, \langle \mathbf{w}, \mathbf{a} \rangle) \hat{=} V^T(p, \mathbf{w}^{|\mathbf{w}|-1})$ and $V^T(a, \langle \mathbf{w}, \mathbf{a} \rangle) \hat{=} a = \mathbf{a}_i$ for $a \in Act_i$.

In M^T, a strategy profile $\mathbf{s} \hat{=} \langle s_i : i \in \Gamma \rangle$ for $\Gamma \subseteq Ag$ defines the set

$$W_{\mathbf{s}}^T \hat{=} \{ \langle \mathbf{w} \cdot o(\mathbf{w}^{|\mathbf{w}|-1}, \mathbf{s}(\mathbf{w}) \cup \mathbf{b}), \mathbf{s}(\mathbf{w}) \cup \mathbf{b} \rangle : \mathbf{w} \in R_M^{\mathrm{fin}}(w_I), \mathbf{b} \in Act_{Ag \setminus \Gamma} \}$$

of M^T states ($=$ finite runs of M, with the last action recorded).

$$\delta_\Gamma(s) \hat{=} \bigvee_{\mathbf{a} \in Act_\Gamma} \forall \bigcirc (\hat{\mathbf{a}} \Leftrightarrow s) \quad \text{where} \quad \hat{\mathbf{a}} \hat{=} \bigwedge_{i \in \mathrm{dom}\, \mathbf{a}} \mathbf{a}_i.$$

$\forall \Box \delta_\Gamma(s)$ constrains $s \in AP$ to define a set of the form $W_{\mathbf{s}}^T$.

Γ can enforce A in the continuations of $\mathbf{w}^0 \ldots \mathbf{w}^k$, if

$$M, \mathbf{w}, k \models \exists s (\forall \Box \delta_\Gamma(s) \wedge \forall (\Box \bigcirc s \Rightarrow A)).$$

How about writing $\exists s(\forall \Box \delta_\Gamma(s) \wedge \forall(\Box \bigcirc s \Rightarrow A))$ for ITL conditions A?

Motivation:

ITL's expressive power is equal to that of the monadic second-order theory of $\langle \omega, < \rangle$:

Every MSO predicate $a(i,j)$ on $\sigma^i \ldots \sigma^j$ can be expressed as $\sigma, i, j \models A$ for some appropriate ITL formula A. (Mind that j can be ω.)

There are (ω-)automata and numerous other temporal logics which have the same expressive power: quantified LTL, the (linear time) μ-calculus, etc.

However, ITL's temporal connectives are compositional; this facilitates big-step reasoning and contract-based reasoning.

The propositional quantifier is expressible in ITL.

Interval Temporal Logic

Set of atomic propositions AP; Statepace: $\Sigma \hat{=} \mathcal{P}(AP)$;

$\sigma \in \Sigma^+ \cup \Sigma^\omega$ have been dubbed intervals, despite that their type is $[0, ..., |\sigma|] \to \Sigma$, like in LTL, not just $[0, ..., |\sigma|]$

For our purposes we consider $\models$ on infinite time lines $\sigma \in \Sigma^\omega$ with a pair of positions designating the reference interval:

$$\sigma, i, j \models_{\mathrm{ITL}} A \text{ where } i \leq j \leq \omega,\ i < \omega.$$

Interval Temporal Logic

Syntax: $A ::= \mathit{false} \mid p \mid A \supset A \mid \bigcirc A \mid A; A \mid A^*$, $p \in AP$.

$\sigma, i, j \not\models \mathit{false}$ $\quad$ $\sigma, i, j \models p$ iff $p \in \sigma^i$ $\quad$ $\sigma, i, j \models A \supset B$ iff $\sigma, i, j \models B$ or $\sigma, i, j \not\models A$

$\sigma, i, j \models \bigcirc A$ $\quad$ iff $i < j$ and $\sigma, i+1, j \models A$

$\sigma, i, j \models A; B$ $\quad$ iff $\sigma, i, k \models A$ and $\sigma, k, j \models B$ for some k s.t. $i \leq k \leq j$.

$\sigma, i, j \models A^*$ $\quad$ iff $\quad$ either $i = j$,

or there exists a finite sequence $k_0 = i < k_1 < \ldots < k_n = j$

such that $\sigma, k_i, k_{i+1} \models A$ for $i = 0, \ldots, n-1$,

or $j = \omega$ and there exists an infinite sequence

$k_0 = 0 < k_1 < \ldots$ such that $\sigma^{k_i..k_{i+1}} \models A$ for all $i < \omega$.

Interval-based CTL^* (ICTL)

$$A ::= \mathit{false} \mid p \mid A \supset A \mid \bigcirc A \mid A; A \mid A^* \mid \exists A \mid \exists p A$$

$M, \mathbf{w}, i, j \models A$ where $\mathbf{w} \in R_M^{\inf}(w_I)$, $i < \omega$, and $i \leq j \leq \omega$ where M is a Kripke model:

$M, \mathbf{w}, i, j \not\models \mathit{false}$;		
$M, \mathbf{w}, i, j \models p$	iff	$V(p, \mathbf{w}^i)$;
$M, \mathbf{w}, i, j \models A \supset B$	iff	$M, \mathbf{w}, i, j \not\models A$ or $M, \mathbf{w}, i, j \models B$;
$M, \mathbf{w}, i, j \models \bigcirc A,\ A; B,\ A^*$		as in ITL at 'interval' $V(w^i) \dots V(w^j)$
		$V(w) \mathrel{\hat{=}} \{p \in AP : V(w, p)\}$
$M, \mathbf{w}, i, j \models \exists A$	iff	$M, \mathbf{v}, i, \infty \models A$ for some $\mathbf{v} \in R_M^{\inf}(\mathbf{w}^0 \dots \mathbf{w}^i)$.

There are interval-based ATLs in the literature which subsume ICTL.

Interval-based ATLs and are in turn subsumed by propositionally quantified ICTL by virtue of the expressibility of strategic ability discussed above.

$\bigcirc A$, $A;B$, A^* are introspective as they allow reference to subintervals only:

$$\begin{array}{ll} \sigma,i,j \models \bigcirc A & \text{iff } i<j \text{ and } \sigma, i+1, j \models A \\ \sigma,i,j \models A;B & \text{iff } \sigma,i,k \models A \text{ and } \sigma,k,j \models B \text{ for some } k \text{ s.t. } i \leq k \leq j. \\ \sigma,i,j \models A^* & \text{iff } \ldots \end{array}$$

The Neighbourhood Modalities $\Diamond_l$, $\Diamond_r$, AKA $\langle \overline{A} \rangle$ and $\langle A \rangle$

$$\begin{array}{lll} \sigma,i,j \models \Diamond_l A & \text{iff} & i > -\infty \text{ and there exists a } k \leq i \text{ such that } \sigma,k,i \models A \\ \sigma,i,j \models \Diamond_r A & \text{iff} & j < \infty \text{ and there exists a } k \geq j \text{ such that } \sigma,j,k \models A \end{array}$$

$\Diamond_l$ and $\Diamond_r$ are expanding. ICTL can be extended by $\Diamond_l$ and $\Diamond_r$ too:

$$\begin{array}{lll} M,\mathbf{w},i,j \models \Diamond_l A & \text{iff} & M,\mathbf{w},k,i \models A \text{ for some } k \leq i \\ M,\mathbf{w},i,j \models \Diamond_r A & \text{iff} & j < \omega \text{ and } M,\mathbf{w},j,k \models A \text{ for some } k \leq \omega. \end{array}$$

The Separation Theorem in ITL

Introspective formulas C:

$$C ::= \mathit{false} \mid p \mid C \supset C \mid \bigcirc C \mid C;C \mid C^* \quad \text{indeed ITL as given so far}$$

Future formulas: $F ::= C \mid \neg F \mid F \vee F \mid \Diamond_r F$.

Stricty future formulas: $\Diamond_r(\mathit{skip}; F)$ where F is future.

$\mathit{skip} \mathrel{\hat=} \bigcirc \neg \bigcirc \mathit{true}$ provides that no state is shared with the reference interval.

Past formulas ($\Diamond_l$ instead of $\Diamond_r$): $P ::= C \mid \neg P \mid P \vee P \mid \Diamond_l P$

Strictly past formulas: $\Diamond_c(\mathit{skip}; P)$

Theorem 2 *Every ITL formula is equivalent to a boolean combination of strictly past formulas, strictly future formulas and introspective formulas.*

Eliminating The Neighbourhood Modalities in ICTL

Taking some special care for the path quantifier $\exists$ in ICTL enables applying separation there too. By separating the operands of $\exists$ in ICTL bottom up, and using the validity of equivalences of the forms

$\exists(A \vee B) \equiv \exists A \vee \exists B$ and $\exists(P \wedge C \wedge F) \equiv P \wedge \exists(C \wedge F')$

where $F' \in \{\perp, \top\}$, we prove

Theorem 3 *Let A be a formula in $\mathrm{ICTL} + \Diamond_l, \Diamond_r$. Then there exists an ICTL ($\Diamond_l$- and $\Diamond_r$-free) formula A' such that $M, \mathbf{w}, 0, \infty \models A \equiv A'$ for all Kripke models M for $AP \supseteq \mathrm{Var}(A)$ and all $\mathbf{w} \in R_M^{\mathrm{inf}}(w_I)$.*

The proof follows the example of the use of Gabbay's theorem about LTL for (its corresponding point-based) CTL^* with past, but with the use of the new separation theorem for ITL with $\Diamond_l$ and $\Diamond_r$ instead.

Propositional Quantification in ICTL

$$M, \mathbf{w}, i, j \models \exists p A \quad \text{iff} \quad (M^T)_p^X, \mathbf{w}, i, j \models A \text{ for some } X \subseteq W^T.$$

Observe that M becomes unwound 'before' a witness $X \subseteq W^T$ is considered.

Propositional quantification is known to be expressible in the underlying linear time logic ITL.

Theorem 4 *Let A be a formula in* ICTL *with propositional quantification in it. Then there exists a quantifier-free* ICTL *formula A' in* ICTL *with no propositional quantification in it such that $\models A' \equiv A$.*

Applying this statement bottom-up implies the decidability of validity in ICTL:

$\models A$ iff $\models \forall p_1 \ldots \forall p_n A$ where $\{p_1, \ldots, p_n\} \hat{=} \mathrm{Var}(A)$.

Quantifier elimination this reduces to a variable-free formula.

The decidability of point-based propositionally quantified CTL^* was established by automata-theoretic means by French (2002, 2006).

A comparison with the related results on point-based quantified CTL^*

1. Elimination of the neighbourhood modalities: the analogy with eliminating the past and eliminating $\Diamond_l$ is complete.

2. Propositional quantifiers cannot be eliminated in LTL and CTL^*; the quantified systems are strictly more expressive.

3. The main gains:

ITL's temporal connectives facilitate compositional reasoning abstraction and contract-based reasoning;

We have proven that reference to the past and propositional quantification can be enjoyed but no enhancements are needed to handle it, e.g., when model-checking.

The End