A Dynamic Logic for Verification of Synchronous Models based on Theorem Proving

Yuanrui ZHANG, Frederic MALLET, Zhiming LIU

Frontiers of Computer Science, DOI: 10.1007/s11704-022-1374-4

Problems & Ideas

- Reasoning about and verifying synchronous models is a big challenge
  - It lacks a suitable formalism to correctly specify synchronous programs
  - It lacks a calculus to formally reason about and verify synchronous programs
- Ideas: A novel dynamic logic for sycnrhonous models
  - It extends first-order dynamic logic with additional special primitives and temporal formulas to support the specification of synchronous programs
  - Its proof calculus allows verification of synchronous programs through semi-automatic deduction in Floyd-Hoare style

Main Contributions

- **Defining Synchronous Dynamic Logic**

$$p ::= \mathbf{1} \mid \mathbf{0} \mid \alpha \mid p\,;p \mid p \cup p \mid p^* \mid \cap(p, ..., p),$$

where α is defined as:

$$\alpha ::= \epsilon \mid evt\,.\,\alpha,$$
$$evt ::= \psi? \mid \varrho? \mid \varsigma!e \mid x := e,$$
$$\varrho ::= \hat{\varsigma}(x) \mid \bar{\varsigma}.$$

$$\phi ::= tt \mid \theta(e,e) \mid \neg\phi \mid \phi \wedge \phi \mid \forall x.\phi \mid [p]\phi \mid [p]\Box\phi$$

- **Building Sound Proof System for SDL**

$$\frac{\phi \wedge [\alpha]\phi}{[\alpha]\Box\phi}\ (\alpha,\Box\phi) \qquad \frac{\psi \to [\alpha]\phi}{[\psi?\,.\,\alpha]\phi}\ (\psi?) \qquad \frac{([\alpha]\phi)[e/x]}{[x := e\,.\,\alpha]\phi}\ (x{:=}e) \qquad \frac{\phi}{[\epsilon]\phi}\ (\epsilon) \qquad \frac{\phi}{[\mathbf{1}]\phi}\ 1\ (\mathbf{1}) \qquad \frac{tt}{[\mathbf{0}]\phi}\ (\mathbf{0})$$

$$\frac{[p][q]\phi}{[p\,;q]\phi}\ (;,\phi) \qquad \frac{[p]\Box\phi \wedge [p][q]\Box\phi}{[p\,;q]\Box\phi}\ (;,\Box\phi) \qquad \frac{[p]\xi \wedge [q]\xi}{[p \cup q]\xi}\ (\cup) \qquad \frac{[p^*][p]\Box\phi}{[p^*]\Box\phi}\ (*,\Box\phi) \qquad \frac{[\mathbf{1} \cup p\,;p^*]\xi}{[p^*]\xi}\ (*)$$

$$\frac{\forall(\phi \to [p]\phi)}{\phi \to [p^*]\phi}\ 2\ (ind) \qquad \frac{\forall((v > 0 \wedge \phi(v)) \to \langle p\rangle\phi(v-1))}{(\exists v \geq 0.\phi(v)) \to \langle p^*\rangle\phi(0)}\ 3\ (con) \qquad \frac{\forall(\phi \to \psi)}{[p]\phi \to [p]\psi}\ ([],gen) \qquad \frac{\forall(\phi \to \psi)}{\langle p\rangle\phi \to \langle p\rangle\psi}\ (\langle\rangle,gen)$$

$$\frac{\psi \quad \forall(\psi \to [p]\psi) \quad \forall(\psi \to \phi)}{[p^*]\phi}\ ([*]) \qquad \frac{\exists v \geq 0.\psi(v) \quad \forall((v > 0 \wedge \psi(v)) \to \langle p\rangle\psi(v-1)) \quad \forall(\psi(0) \to \phi)}{\langle p^*\rangle\phi}\ (\langle*\rangle)$$

$$\frac{\phi\{q\}}{\phi\{p\}}\ \text{if } p \rightsquigarrow q\ ^1\ (r1) \qquad p\{q\} \rightsquigarrow p\{r\}\ \text{if } q \rightsquigarrow r\ ^2\ (r2)$$

$$\mathbf{1}\,;p \rightsquigarrow p\ (\mathbf{1},;) \qquad \mathbf{1}^* \rightsquigarrow \mathbf{1}\ (\mathbf{1},*) \qquad \mathbf{0}\,;p \rightsquigarrow \mathbf{0}\ (\mathbf{0},;)$$
$$\mathbf{0}^* \rightsquigarrow \mathbf{1}\ (\mathbf{0},*) \qquad (p\,;q)\,;r \rightsquigarrow p\,;(q\,;r)\ (;,ass) \qquad p\,;(q \cup r) \rightsquigarrow (p\,;q) \cup (p\,;r)\ (;,dis1)$$
$$(q \cup r)\,;p \rightsquigarrow (q\,;p) \cup (r\,;p)\ (;,dis2) \qquad (p \cup q) \cup r \rightsquigarrow p \cup (q \cup r)\ (\cup,ass) \qquad p^* \rightsquigarrow \mathbf{1} \cup p;\,p^*\ (*,exp)$$
$$\cap(..., p, \mathbf{1}, q, ...) \rightsquigarrow \cap(..., p, q, ...)\ (\cap,\mathbf{1}) \qquad \cap(..., p, \mathbf{0}, q, ...) \rightsquigarrow \mathbf{0}\ (\cap,\mathbf{0}) \qquad \cap(..., p \cup q, ...) \rightsquigarrow \cap(..., p, ...) \cup \cap(..., q, ...)\ (\cap,dis)$$
$$\cap(\alpha_1\,;q_1, ..., \alpha_n\,;q_n) \rightsquigarrow \alpha\,;\cap(q_1', ..., q_n')\ \text{if } (b, \alpha, (q_1' \mid ... \mid q_n')) = Mer(\alpha_1\,;q_1 \mid ... \mid \alpha_n\,;q_n) \text{ and } b = tt\ (\cap,mer)$$
$$\cap(p_1, ..., p_n) \rightsquigarrow Brz(\cap(p_1, ..., p_n))\ \text{if } \cap(p_1, ..., p_n) \text{ is well defined}\ (\cap,seq)$$

- **Analyzing and Proving Relative Completeness of SDL**
- **A Case Study**

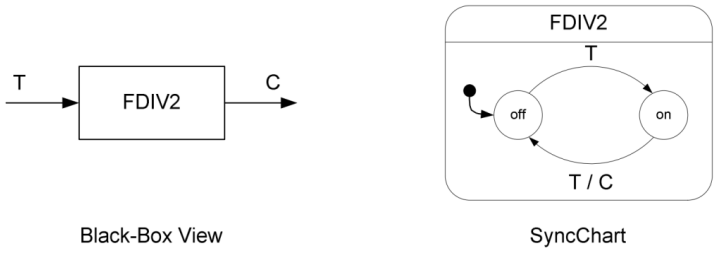

Fig. 1: A Frequency Divider

$$\dfrac{\dfrac{\dfrac{\surd}{\phi_1, \psi_1 \Rightarrow \psi_2} \quad \dfrac{\surd}{\phi_1, \psi_1, \psi_2 \Rightarrow \psi_2}}{\phi_1, \psi_1 \Rightarrow \forall x.\forall y.(\psi_2 \to [p_2]\psi_2)}\ (\forall r),(\to r),(x{:=}e) \quad \dfrac{\ldots}{\phi_1, \psi_1 \Rightarrow \forall x.\forall y.(\psi_2 \to [p_2]\Box\phi_2)}}{(1):\ \phi_1, \psi_1 \Rightarrow [p_2^*][p_2]\Box\phi_2}$$

$$\dfrac{\dfrac{(1)}{\phi_1, \psi_1 \Rightarrow [p_2^*]\Box\phi_2}\ (*,\Box\phi) \quad \dfrac{\ldots}{\phi_1, \psi_1 \Rightarrow [p_2^*][p_3]\Box\phi_2}}{\phi_1, \psi_1 \Rightarrow [p_1]\Box\phi_2}\ (;,\Box\phi),(\wedge r)$$

$$\dfrac{\dfrac{\surd}{\phi_1 \Rightarrow \psi_1} \quad \dfrac{\ldots}{\phi_1 \Rightarrow \forall x.\forall y.(\psi_1 \to [p_1]\psi_1)}}{\phi_1 \Rightarrow \forall x.\forall y.(\psi_1 \to [p_1]\Box\phi_2)}\ (\forall r),(\to r)\ ([*])$$

$$\dfrac{\phi_1 \Rightarrow [p_1^*][p_1]\Box\phi_2}{\phi_1 \Rightarrow [P]\Box\phi_2}\ (*,\Box\phi)$$

$$\dfrac{\phi_1 \Rightarrow [P]\Box\phi_2}{\cdot \Rightarrow \phi_{FD}}\ (\to r),(\cap,seq),(r1)$$

Fig. 2: The Derivation Tree of ϕ_{FD}