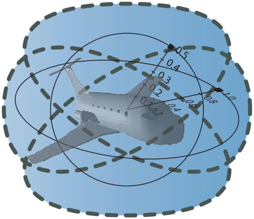
15-819/18-879: Hybrid Systems Analysis & Theorem Proving

10: d$\mathcal{L}$ Tableaux Procedures Modulo Theories

André Platzer

aplatzer@cs.cmu.edu
Carnegie Mellon University, Pittsburgh, PA



Outline

1. Differential Dynamic Logic d$\mathcal{L}$
   - Syntax
   - Semantics
   - Verification Calculus
2. Analysis of the European Train Control System
3. Combining Deduction and Algebraic Constraints
   - Nondeterminisms in Branch Selection
   - Nondeterminisms in Formula Selection
   - Nondeterminisms in Mode Selection
   - Iterative Background Closure Strategy
4. Experimental Results

Differential Dynamic Logic d$\mathcal{L}$: Syntax

Definition (Hybrid program α)

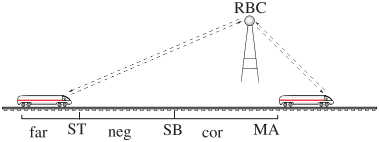
$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

Differential Dynamic Logic $d\mathcal{L}$: Syntax

Definition (Hybrid program α)

$x' = f(x)$	(continuous evolution)
$x := \theta$	(discrete jump)
$?\chi$	(conditional execution)
$\alpha; \beta$	(seq. composition)
$\alpha \cup \beta$	(nondet. choice)
α^*	(nondet. repetition)

$$
\begin{aligned}
ETCS &\equiv (ctrl\,; drive)^* \\
ctrl &\equiv (?MA - z \leq SB; a := -b) \\
&\quad \cup (?MA - z \geq SB; a := \dots) \\
drive &\equiv z'' = a
\end{aligned}
$$



Differential Dynamic Logic d$\mathcal{L}$: Syntax

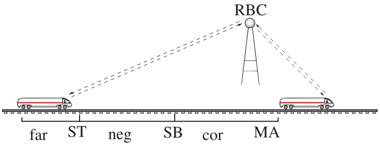
Definition (Formulas ϕ)

$\neg, \wedge, \vee, \rightarrow, \ \forall x, \exists x, \ =, \leq, \ +, \cdot$ (ℝ-first-order part)

$[\alpha]\phi, \quad \langle\alpha\rangle\phi$ (dynamic part)

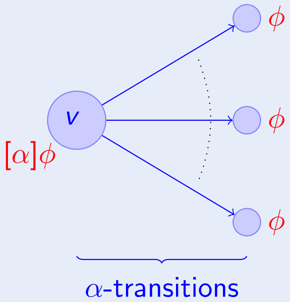
$$\psi \ \rightarrow \ [(ctrl\,; drive)^*]\, z \leq MA$$

All trains respect MA
$\Rightarrow$ system safe



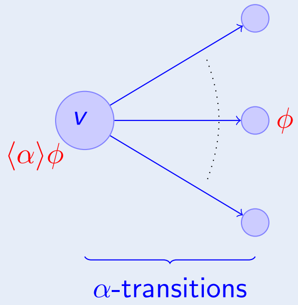
Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)



Differential Dynamic Logic d$\mathcal{L}$: Semantics

Definition (Formulas ϕ)



11 dynamic rules

(D1) $\dfrac{\phi \wedge \psi}{\langle ?\phi \rangle \psi}$ (D5) $\dfrac{\phi \vee \langle \alpha; \alpha^* \rangle \phi}{\langle \alpha^* \rangle \phi}$ (D9) $\dfrac{\exists t{\geq}0\,(\bar{\chi} \wedge \langle x := y_x(t) \rangle}{\langle x' = \theta \,\&\, \chi \rangle \phi}$

(D2) $\dfrac{\phi \rightarrow \psi}{[?\phi]\psi}$ (D6) $\dfrac{\phi \wedge [\alpha; \alpha^*]\phi}{[\alpha^*]\phi}$ (D10) $\dfrac{\forall t{\geq}0\,(\bar{\chi} \rightarrow [x := y_x(t)}{[x' = \theta \,\&\, \chi]\phi}$

(D3) $\dfrac{\langle \alpha \rangle \phi \vee \langle \beta \rangle \phi}{\langle \alpha \cup \beta \rangle \phi}$ (D7) $\dfrac{\langle \alpha \rangle \langle \beta \rangle \phi}{\langle \alpha; \beta \rangle \phi}$

(D4) $\dfrac{[\alpha]\phi \wedge [\beta]\phi}{[\alpha \cup \beta]\phi}$ (D8) $\dfrac{\phi_x^\theta}{\langle x := \theta \rangle \phi}$

(D11) $\dfrac{\vdash p \quad \vdash [\alpha^*](p \rightarrow [\alpha]p)}{\quad}$

9 propositional rules + 4 quantifier rules

(P1) $$\frac{\vdash \phi}{\neg\phi \vdash}$$

(P4) $$\frac{\phi, \psi \vdash}{\phi \land \psi \vdash}$$

(P7) $$\frac{\phi \vdash \quad \psi \vdash}{\phi \lor \psi \vdash}$$

(P2) $$\frac{\phi \vdash}{\vdash \neg\phi}$$

(P5) $$\frac{\vdash \phi \quad \vdash \psi}{\vdash \phi \land \psi}$$

(P8) $$\frac{\vdash \phi, \psi}{\vdash \phi \lor \psi}$$

(P3) $$\frac{\phi \vdash \psi}{\vdash \phi \to \psi}$$

(P6) $$\frac{\vdash \phi \quad \psi \vdash}{\phi \to \psi \vdash}$$

(P9) $$\frac{}{\phi \vdash \phi}$$

(F1) $$\frac{\mathrm{QE}(\exists x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \exists x\, \phi}$$

(F3) $$\frac{\mathrm{QE}(\forall x \bigwedge_i (\Gamma_i \vdash \Delta_i))}{\Gamma \vdash \Delta, \forall x\, \phi}$$

(F2) $$\mathrm{QE}(\forall x \bigwedge_i (\Gamma_i \vdash \Delta_i))$$

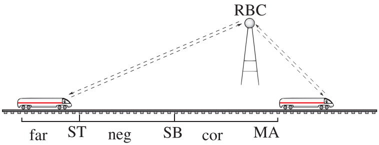
(F4) $$\mathrm{QE}(\exists x \bigwedge_i (\Gamma_i \vdash \Delta_i))$$

Concise Theory! But End of the Story?

Outline

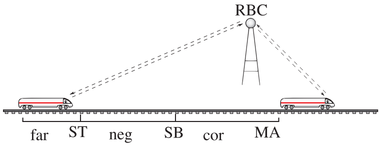
1. Differential Dynamic Logic d$\mathcal{L}$
   - Syntax
   - Semantics
   - Verification Calculus
2. Analysis of the European Train Control System
3. Combining Deduction and Algebraic Constraints
   - Nondeterminisms in Branch Selection
   - Nondeterminisms in Formula Selection
   - Nondeterminisms in Mode Selection
   - Iterative Background Closure Strategy
4. Experimental Results

$$\psi \;\rightarrow\; [(ctrl\,;drive)^*]\,z \le MA$$
$$ctrl \equiv (?MA - z < SB;\, a := -b)$$
$$\cup\,(?MA - z \ge SB;\, a := 0)$$
$$drive \equiv \tau := 0;\, z' = v, v' = a, \tau' = 1$$
$$\&\, v \ge 0 \land \tau \le \varepsilon$$



provable automatically using invariant!

$$\psi \rightarrow [(ctrl; drive)^*]\, z \leq MA$$
$$ctrl \equiv (?MA - z < SB; a := -b)$$
$$\cup\, (?MA - z \geq SB; a := 0)$$
$$drive \equiv \tau := 0; z' = v, v' = a, \tau' = 1$$
$$\&\, v \geq 0 \wedge \tau \leq \varepsilon$$



$$\dots$$
$$p, MA-z\geq SB \vdash v^2 \leq 2b(MA - \varepsilon v - z)$$
$$p, MA-z\geq SB \vdash \forall t\geq 0\, (\langle \tau := t\rangle \tau \leq \varepsilon \rightarrow \langle z := vt$$
$$p, MA-z\geq SB \vdash \langle \tau := 0\rangle \forall t\geq 0\, (\langle \tau := t + \tau\rangle \tau \leq \varepsilon$$
$$*$$
$$p, MA-z\geq SB \vdash \langle \tau := 0\rangle [z' = v, v' = 0, \tau' = 1\, \&$$
$$p \vdash \forall t\geq 0\, (\langle v := -bt + v\rangle v \geq 0 \rightarrow \langle z := -\tfrac{b}{2}t^2 + vt + z; v := -bt + v\rangle p) \quad p, MA-z\geq SB \vdash \langle a := 0\rangle \langle \tau := 0\rangle [z' = v, v' = a, \tau$$
$$p \vdash [z' = v, v' = -b\, \&\, v \geq 0]p \quad p, MA-z\geq SB \vdash \langle a := 0\rangle [drive]p$$
$$p \vdash \langle a := -b\rangle [drive]p \quad p \vdash [?MA-z\geq SB; a := 0][drive]p$$
$$p \vdash [ctrl][drive]p$$
$$p \vdash [ctrl; drive]p$$

$$
\begin{aligned}
\text{spec} &: \tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \land \tau.v \ge 0 \land \mathbf{m}.d \ge 0 \land b > 0\\
&\quad \rightarrow\ [\text{ETCS}](\tau.p \ge \mathbf{m}.e \rightarrow \tau.v \le \mathbf{m}.d)\\
\text{ETCS} &: (\text{train} \cup \text{rbc})^*\\
\text{train} &: \text{spd};\ \text{atp};\ \text{move}\\
\text{spd} &: \ (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ? - b \le \tau.a \le A)\\
&\quad \cup(?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b)\\
\text{atp} &: SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\,\tau.v\right);\\
&\quad (?(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency);\ \tau.a := -b)\\
&\quad \cup(?\mathbf{m}.e - \tau.p \ge SB \land rbc.message \ne emergency)\\
\text{move} &: t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1\,\&\,\tau.v \ge 0 \land t \le \varepsilon)\\
\text{rbc} &: \ (rbc.message := emergency)\\
&\quad \cup \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *;\\
&\qquad ?\mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0 \land \mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e)\big)
\end{aligned}
$$

not provable automatically!

56 user interactions!

$$
\begin{aligned}
\text{spec} &: \tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \wedge \tau.v \ge 0 \wedge \mathbf{m}.d \ge 0 \wedge b > 0 \\
&\quad \rightarrow \; [\text{ETCS}](\tau.p \ge \mathbf{m}.e \rightarrow \tau.v \le \mathbf{m}.d) \\
\text{ETCS} &: (\text{train} \cup \text{rbc})^* \\
\text{train} &: \text{spd};\ \text{atp};\ \text{move} \\
\text{spd} &: \ (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ? - b \le \tau.a \le A) \\
&\quad \cup (?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
\text{atp} &: SB := \tfrac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\tfrac{A}{b} + 1\right)\left(\tfrac{A}{2}\varepsilon^2 + \varepsilon\,\tau.v\right); \\
&\quad \ (?(\mathbf{m}.e - \tau.p \le SB \vee rbc.message = emergency);\ \tau.a := -b) \\
&\quad \cup (?\mathbf{m}.e - \tau.p \ge SB \wedge rbc.message \ne emergency) \\
\text{move} &: t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \,\&\, \tau.v \ge 0 \wedge t \le \varepsilon) \\
\text{rbc} &: \ (rbc.message := emergency) \\
&\quad \cup \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
&\qquad ?\mathbf{m}.r \ge 0 \wedge \mathbf{m}.d \ge 0 \wedge \mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e)\big)
\end{aligned}
$$

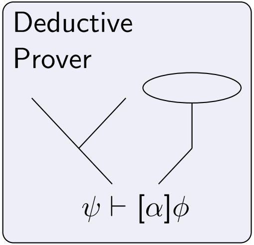
Full European Train Control System (ETCS)

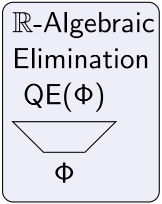
```
 state = 0,
 2 * b * (m - z) >= v ^ 2 - d ^ 2,
 v >= 0, d >= 0, v >= 0, ep >  0, b >  0, amax >  0, d >= 0
==>
    v <= vdes
 -> \forall R a_3;
      (   a_3 >= 0 & a_3 <= amax
       ->   (      m - z
               <= (amax / b + 1) * ep * v
                + (v ^ 2 - d ^ 2) / (2 * b)
                + (amax / b + 1) * amax * ep ^ 2 / 2
            -> \forall R t0;
                 (   t0 >= 0
                  -> \forall R ts0;  (0 <= ts0 & ts0 <= t0 -> -b * ts0 + v >= 0 & ts0 + 0 <= ep)
                  ->      2 * b * (m - 1 / 2 * (-b * t0 ^ 2 + 2 * t0 * v + 2 * z))
                       >= (-b * t0 + v) ^ 2
                        - d ^ 2
                     & -b * t0 + v >= 0
                     & d >= 0))
         & (      m - z
               >  (amax / b + 1) * ep * v
                + (v ^ 2 - d ^ 2) / (2 * b)
                + (amax / b + 1) * amax * ep ^ 2 / 2
            -> \forall R t2;
                 (   t2 >= 0
                  -> \forall R ts2;  (0 <= ts2 & ts2 <= t2 -> a_3 * ts2 + v >= 0 & ts2 + 0 <= ep)
                  ->      2 * b * (m - 1 / 2 * (a_3 * t2 ^ 2 + 2 * t2 * v + 2 * z))
                       >= (a_3 * t2 + v) ^ 2
                        - d ^ 2
                     & a_3 * t2 + v >= 0
                     & d >= 0)))
```

Practice Seems Quite Tricky!

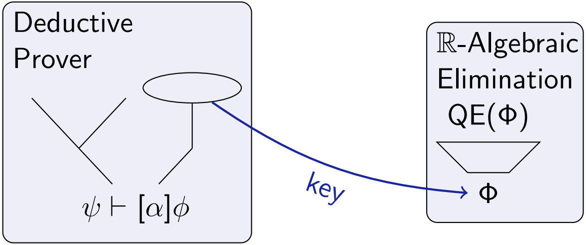
Outline

1. Differential Dynamic Logic $d\mathcal{L}$
   - Syntax
   - Semantics
   - Verification Calculus
2. Analysis of the European Train Control System
3. Combining Deduction and Algebraic Constraints
   - Nondeterminisms in Branch Selection
   - Nondeterminisms in Formula Selection
   - Nondeterminisms in Mode Selection
   - Iterative Background Closure Strategy
4. Experimental Results

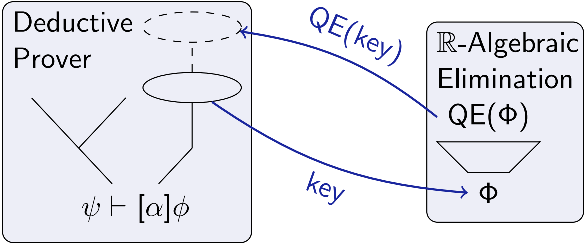

Deductive
Prover
$\psi \vdash [\alpha]\phi$


$\mathbb{R}$-Algebraic
Elimination
QE(Φ)
Φ

Modular Combination of Provers



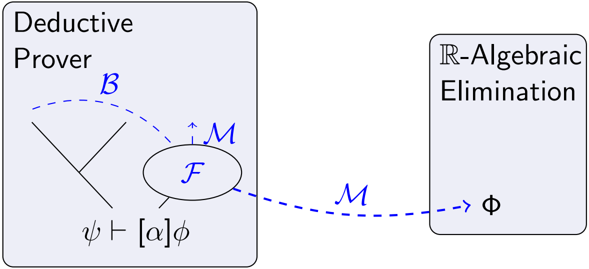
Modular Combination of Provers



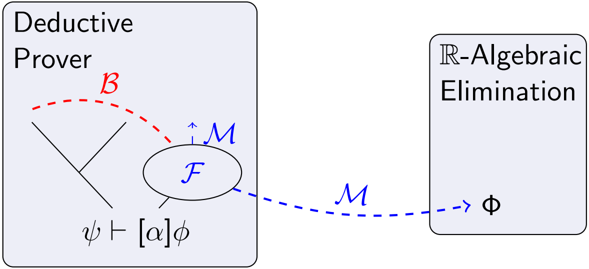
Tableaux Procedure for d$\mathcal{L}$

```
while tableaux T has open branches do
  B := selectBranch(T)              (* B-nondeterminism *)
  M := selectMode(B)                (* M-nondeterminism *)
  F := selectFormulas(B,M)          (* F-nondeterminism *)
  if M = foreground then
    B2 := result of applying D-rule/P-rule to F in B
    replace B by B2 in T
  else
    send key F to background decision procedure QE
    receive result R from QE
    apply a rule F3-F4 to T with QE-result R
  end if
end while
```

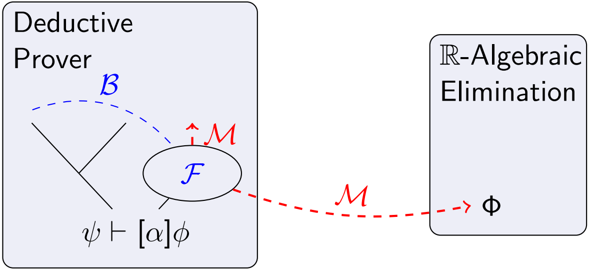
$\mathcal{R}$ Tableaux Procedure for d$\mathcal{L}$: Nondeterminisms



$\mathcal{R}$ Tableaux Procedure for d$\mathcal{L}$: Nondeterminisms

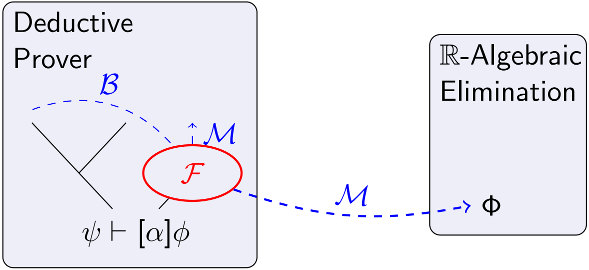


$\mathcal{B}$ branch selection



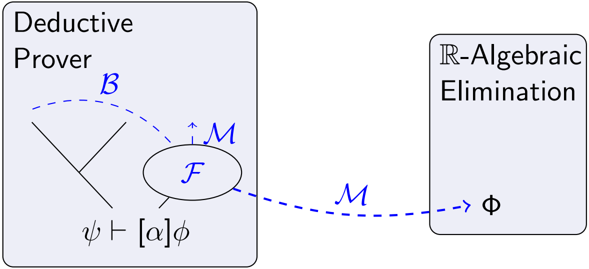
$\mathcal{M}$ mode selection

Tableaux Procedure for d$\mathcal{L}$: Nondeterminisms



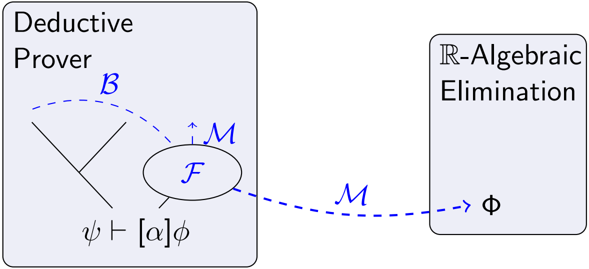
$\mathcal{F}$ formula selection

Tableaux Procedure for d$\mathcal{L}$: Nondeterminisms



no nondeterminism from closing substitutions

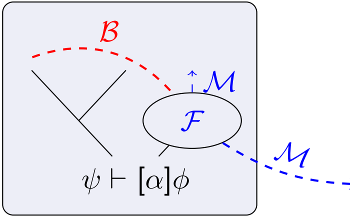
$\mathcal{R}$ Tableaux Procedure for d$\mathcal{L}$: Nondeterminisms

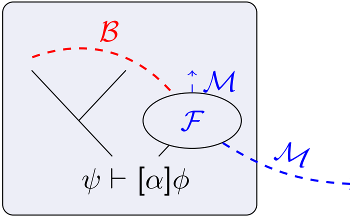


uninterpreted FOL	interpreted d$\mathcal{L}$
uninterpreted symbols	interpreted symbols
close by substitution	close by arithmetic
close needs backtracking	equivalent QE elimination
closing is cheap	arithmetic is $O(2^{2^n})$

Nondeterminisms in Branch Selection

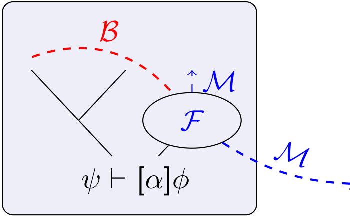
- harmless
  because no closing substitutions





$$\dfrac{\dfrac{\dfrac{\mathrm{QE}(\forall x\,(\ldots bx^2 \geq 0))}{\Gamma, b > 0 \vdash bx^2 \geq 0} \qquad \dfrac{\mathrm{QE}(\forall x\,(\ldots bx^4 + x^2 \geq 0))}{\Gamma, b > 0 \vdash bx^4 + x^2 \geq 0}}{\Gamma, b > 0 \vdash bx^2 \geq 0 \land bx^4 + x^2 \geq 0}}{\Gamma, b > 0 \vdash \forall x\,(bx^2 \geq 0 \land bx^4 + x^2 \geq 0)}$$

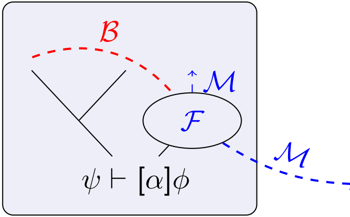
- branches close independently



$$\dfrac{\dfrac{\mathrm{QE}(\forall x\,(\dots bx^2 \geq 0))}{\Gamma, b>0 \vdash bx^2 \geq 0} \qquad \dfrac{\mathrm{QE}(\forall x\,(\dots bx^4 + x^2 \geq 0))}{\Gamma, b>0 \vdash bx^4 + x^2 \geq 0}}{\dfrac{\Gamma, b>0 \vdash bx^2 \geq 0 \land bx^4 + x^2 \geq 0}{\Gamma, b>0 \vdash \forall x\,(bx^2 \geq 0 \land bx^4 + x^2 \geq 0)}}$$

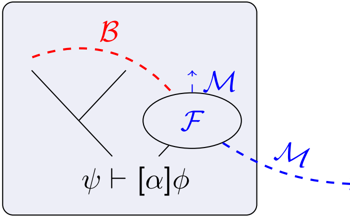
Nondeterminisms in Branch Selection: $\forall$ quantifiers

- branches close independently
- order not important



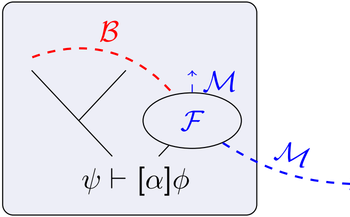
$$\cfrac{\cfrac{\cfrac{\mathrm{QE}(\forall x\,(\ldots bx^2 \geq 0))}{\Gamma, b > 0 \vdash bx^2 \geq 0} \qquad \cfrac{\mathrm{QE}(\forall x\,(\ldots bx^4 + x^2 \geq 0))}{\Gamma, b > 0 \vdash bx^4 + x^2 \geq 0}}{\Gamma, b > 0 \vdash bx^2 \geq 0 \land bx^4 + x^2 \geq 0}}{\Gamma, b > 0 \vdash \forall x\,(bx^2 \geq 0 \land bx^4 + x^2 \geq 0)}$$

$\mathcal{R}$ Nondeterminisms in Branch Selection: $\exists$ quantifiers



$$\dfrac{\dfrac{\text{QE}(\exists v \ldots)}{\dfrac{\dfrac{b > 2 \vdash b(V-1) > 0}{b > 2 \vdash [v := V-1]bv > 0} \quad \dfrac{b > 2 \vdash (V+1)^2 + b\epsilon(V+1) > 0}{b > 2 \vdash [v := V+1]v^2 + b\epsilon v > 0}}{b > 2 \vdash [v := V-1]bv > 0 \land [v := V+1]v^2 + b\epsilon v >}}}{b > 2 \vdash \exists v\,([v := v-1]bv > 0 \land [v := v+1]v^2 + b\epsilon v}$$

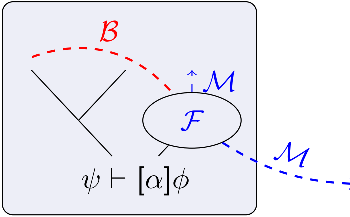
- existential dependency synchronization



$$\dfrac{\dfrac{\dfrac{b>2 \vdash b(V-1)>0}{b>2 \vdash [v:=V-1]bv>0} \qquad \dfrac{\dfrac{\text{QE}(\exists v\ \ldots)}{b>2 \vdash (V+1)^2+b\epsilon(V+1)>0}}{b>2 \vdash [v:=V+1]v^2+b\epsilon v>0}}{b>2 \vdash [v:=V-1]bv>0 \land [v:=V+1]v^2+b\epsilon v>}}{b>2 \vdash \exists v\,([v:=v-1]bv>0 \land [v:=v+1]v^2+b\epsilon v}$$

Nondeterminisms in Branch Selection: $\exists$ quantifiers

- existential dependency synchronization
- order of intermediate steps has not impact

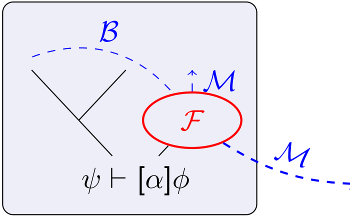


$$\dfrac{\dfrac{\dfrac{\dfrac{\text{QE}(\exists v \ldots)}{b > 2 \vdash b(V-1) > 0}}{b > 2 \vdash [v := V-1]bv > 0} \qquad \dfrac{b > 2 \vdash (V+1)^2 + b\epsilon(V+1) > 0}{b > 2 \vdash [v := V+1]v^2 + b\epsilon v > 0}}{b > 2 \vdash [v := V-1]bv > 0 \land [v := V+1]v^2 + b\epsilon v >}}{b > 2 \vdash \exists v\,([v := v-1]bv > 0 \land [v := v+1]v^2 + b\epsilon v}$$

Nondeterminisms in Formula Selection

- In principle: simple

$$\Phi \text{ closes} \;\Rightarrow\; \Psi \supseteq \Phi \text{ closes}$$



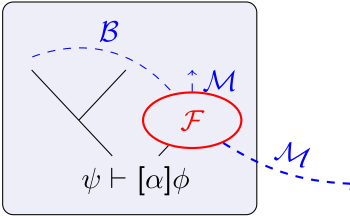
Nondeterminisms in Formula Selection

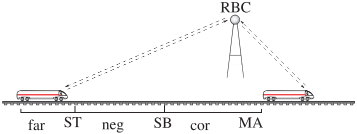
- In principle: simple

$$\Phi \text{ closes} \;\Rightarrow\; \Psi \supseteq \Phi \text{ closes}$$

- In practice: irrelevant formulas distract QE considerably
- Partially necessary ETCS constraint:

$$SB \geq \frac{v^2}{2b} + \left(\frac{a}{b} + 1\right)\left(\frac{a}{2}\varepsilon^2 + \varepsilon v\right)$$



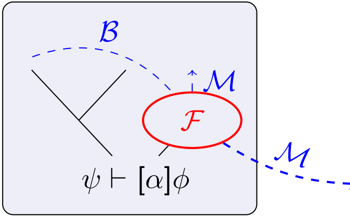


Nondeterminisms in Formula Selection

- In principle: simple

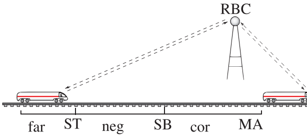
$$\Phi \text{ closes} \quad \Rightarrow \quad \Psi \supseteq \Phi \text{ closes}$$

- In practice: irrelevant formulas distract QE considerably



$\gg 24h$

$$\begin{aligned}
&t > 0,\ a + 1/tv \geq 0,\ \varepsilon \geq t,\ t \geq 0,\\
&m - z \geq v^2/(2b) + (a/b+1)(a/2\varepsilon^2 + \varepsilon v),\\
&2b(m-z) \geq v^2,\ v \geq 0,\\
&2b(m-z_0) \geq v_0^2,\ v_0 \geq 0,\\
&\varepsilon \geq 0,\ b > 0,\ a \geq 0\\
\vdash\ &(at+v)^2 \leq 2b(m - 1/2(at^2 + 2tv + 2z))
\end{aligned}$$

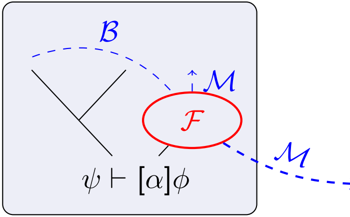


Nondeterminisms in Formula Selection

- In principle: simple

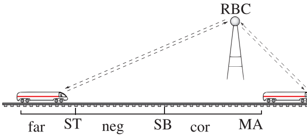
$$\Phi \text{ closes} \quad \Rightarrow \quad \Psi \supseteq \Phi \text{ closes}$$

- In practice: irrelevant formulas distract QE considerably



$\gg 24h$

$$\begin{aligned}
& t > 0,\ a + 1/tv \geq 0,\ \varepsilon \geq t,\ t \geq 0, \\
& m - z \geq v^2/(2b) + (a/b+1)(a/2\varepsilon^2 + \varepsilon v), \\
& 2b(m-z) \geq v^2,\ v \geq 0, \\
& 2b(m-z_0) \geq v_0^2,\ v_0 \geq 0, \qquad \text{(initial state)} \\
& \varepsilon \geq 0,\ b > 0,\ a \geq 0 \\
\vdash\ & (at+v)^2 \leq 2b(m - 1/2(at^2 + 2tv + 2z))
\end{aligned}$$

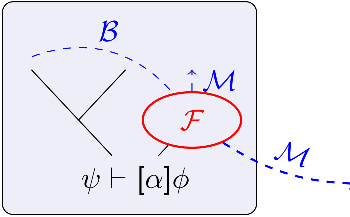


Nondeterminisms in Formula Selection

- In principle: simple

$$\Phi \text{ closes} \quad \Rightarrow \quad \Psi \supseteq \Phi \text{ closes}$$

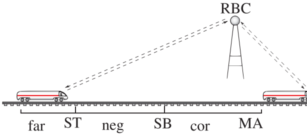
- In practice: irrelevant formulas distract QE considerably



$\ll 1s$

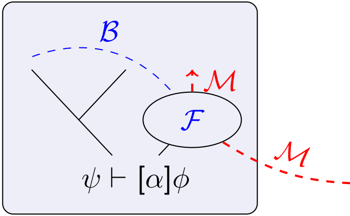
$$t > 0,\ a + 1/tv \geq 0,\ \varepsilon \geq t,\ t \geq 0,$$
$$m - z \geq v^2/(2b) + (a/b + 1)(a/2\varepsilon^2 + \varepsilon v),$$
$$2b(m - z) \geq v^2,\ v \geq 0,$$

$$\varepsilon \geq 0,\ b > 0,\ a \geq 0$$
$$\vdash (at + v)^2 \leq 2b(m - 1/2(at^2 + 2tv + 2z))$$



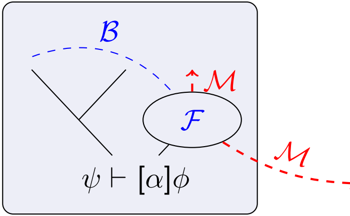
Nondeterminisms in Mode Selection

- In principle: only background closure, anything could close



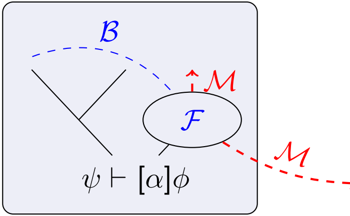
Nondeterminisms in Mode Selection

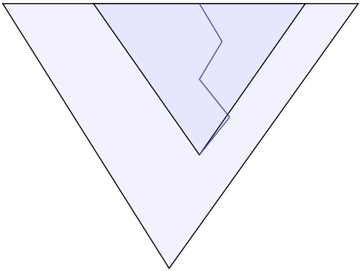
- In principle: only background closure, anything could close
- In practice: some QE “never” terminate



Nondeterminisms in Mode Selection

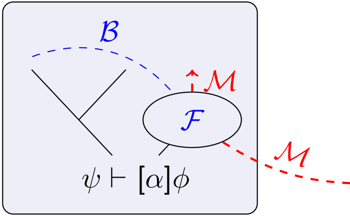
- In principle: only background closure, anything could close
- In practice: some QE "never" terminate

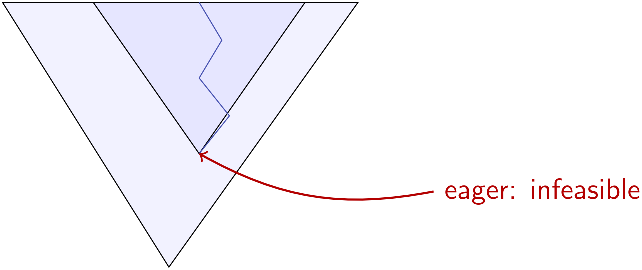




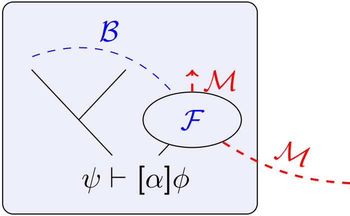
Nondeterminisms in Mode Selection

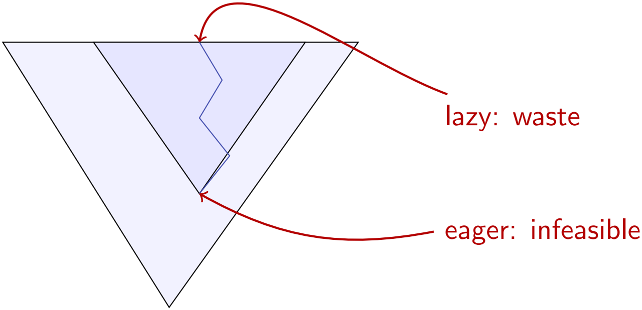
- In principle: only background closure, anything could close
- In practice: some QE "never" terminate





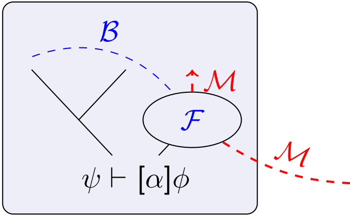
- In principle: only background closure, anything could close
- In practice: some QE "never" terminate

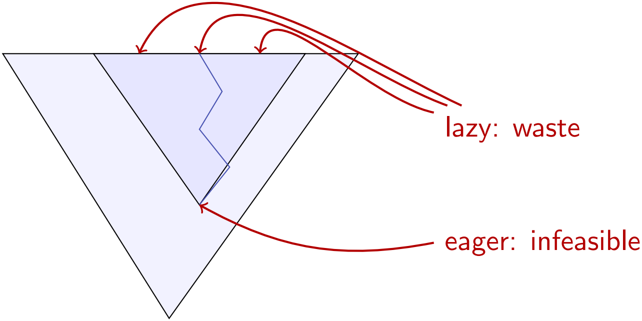




Nondeterminisms in Mode Selection

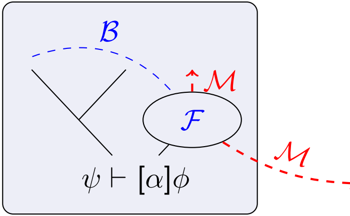
- In principle: only background closure, anything could close
- In practice: some QE "never" terminate





Nondeterminisms in Mode Selection

- In principle: only background closure, anything could close
- In practice: some QE "never" terminate
- Syntactic representational redundancy

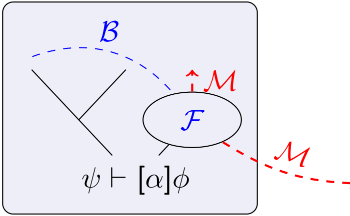


$$\frac{\psi \vdash v^2 \leq 2b(m-z) \quad \psi \vdash (z \geq 0 \rightarrow v \leq 0)}{\psi \vdash v^2 \leq 2b(m-z) \wedge (z \geq 0 \rightarrow v \leq 0)}$$

redundant duplication or case distinction improvement?

Nondeterminisms in Mode Selection

- In principle: only background closure, anything could close
- In practice: some QE "never" terminate
- Syntactic representational redundancy
- Semantic representational redundancy



$$\frac{\vdash b \geq v^2/(2m-2z) \lor m \leq z}{z < m \vdash v^2 \leq 2b(m-z)}$$

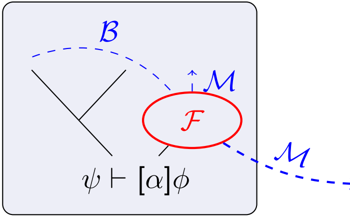
valid "reduction" but perfectly useless ($\Rightarrow$ proof loops)

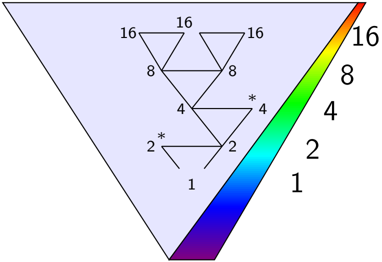
How to Navigate among Nondeterminisms?

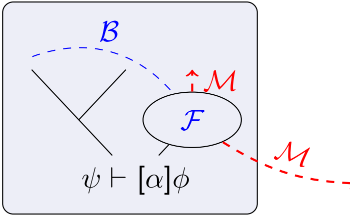
Proof Strategy Priorities for Formula Selection

"accept QE if variable eliminated"
ensures progress and termination

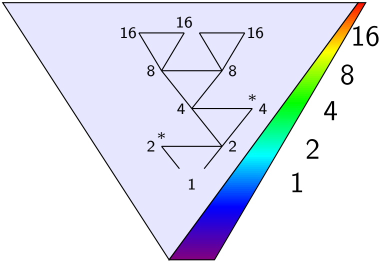
1. non-splitting propositional rules
2. *arithmetic rules* if variable eliminated
3. dynamic rules
4. splitting rules on modalities
5. *arithmetic rules* if variable eliminated
6. (in)variant global rules
7. splitting rules on first-order formulas

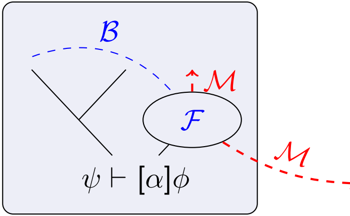



16
16
16
8
8
4
*
4
2
*
2
1
16
8
4
2
1


$\mathcal{B}$
$\mathcal{M}$
$\mathcal{F}$
$\mathcal{M}$
$\psi \vdash [\alpha]\phi$

Iterative Background Closure (IBC) Strategy





- Periodical background arithmetic with increasing timeout after split
- Avoid splitting in average case
- Split prohibitively complicated cases

Outline

1. Differential Dynamic Logic $d\mathcal{L}$
   - Syntax
   - Semantics
   - Verification Calculus
2. Analysis of the European Train Control System
3. Combining Deduction and Algebraic Constraints
   - Nondeterminisms in Branch Selection
   - Nondeterminisms in Formula Selection
   - Nondeterminisms in Mode Selection
   - Iterative Background Closure Strategy
4. Experimental Results

$$
\begin{array}{ll}
\text{spec} : & \tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \land \tau.v \ge 0 \land \mathbf{m}.d \ge 0 \land b > 0 \\
& \to \ [\text{ETCS}](\tau.p \ge \mathbf{m}.e \to \tau.v \le \mathbf{m}.d) \\
\text{ETCS:} & (\text{train} \cup \text{rbc})^* \\
\text{train} : & \text{spd};\ \text{atp};\ \text{move} \\
\text{spd} : & \ (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ?-b \le \tau.a \le A) \\
& \cup(?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
\text{atp} : & SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\,\tau.v\right); \\
& \ (?(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency);\ \tau.a := -b) \\
& \cup(?\mathbf{m}.e - \tau.p \ge SB \land rbc.message \ne emergency) \\
\text{move} : & t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1\,\&\,\tau.v \ge 0 \land t \le \varepsilon) \\
\text{rbc} : & \ (rbc.message := emergency) \\
& \cup\ \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
& \quad ?\mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0 \land \mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e)\big)
\end{array}
$$

provable automatically with IBC!

only $1 \ll 56$ user interaction + reduced verification time!

$$
\begin{aligned}
\text{spec} &: \tau.v^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \tau.p) \land \tau.v \ge 0 \land \mathbf{m}.d \ge 0 \land b > 0 \\
&\quad \to [\text{ETCS}](\tau.p \ge \mathbf{m}.e \to \tau.v \le \mathbf{m}.d) \\
\text{ETCS} &: (\text{train} \cup \text{rbc})^* \\
\text{train} &: \text{spd};\ \text{atp};\ \text{move} \\
\text{spd} &: (?\tau.v \le \mathbf{m}.r;\ \tau.a := *;\ ? - b \le \tau.a \le A) \\
&\quad \cup (?\tau.v \ge \mathbf{m}.r;\ \tau.a := *;\ ?0 > \tau.a \ge -b) \\
\text{atp} &: SB := \frac{\tau.v^2 - \mathbf{m}.d^2}{2b} + \left(\frac{A}{b} + 1\right)\left(\frac{A}{2}\varepsilon^2 + \varepsilon\, \tau.v\right); \\
&\quad (?(\mathbf{m}.e - \tau.p \le SB \lor rbc.message = emergency);\ \tau.a := -b) \\
&\quad \cup (?\mathbf{m}.e - \tau.p \ge SB \land rbc.message \ne emergency) \\
\text{move} &: t := 0;\ (\tau.p' = \tau.v, \tau.v' = \tau.a, t' = 1 \,\&\, \tau.v \ge 0 \land t \le \varepsilon) \\
\text{rbc} &: (rbc.message := emergency) \\
&\quad \cup \big(\mathbf{m}_0 := \mathbf{m}; \mathbf{m} := *; \\
&\qquad ?\mathbf{m}.r \ge 0 \land \mathbf{m}.d \ge 0 \land \mathbf{m}_0.d^2 - \mathbf{m}.d^2 \le 2b(\mathbf{m}.e - \mathbf{m}_0.e)\big)
\end{aligned}
$$

Experimental Results (2007)

Case Study	Interactions	IBC	No IBC
ETCS-binary	1	89s	>8h
ETCS-binary	2	<89s	1184s
ETCS-binary	3	<89s	30s
ETCS	1	3000s	∞
ETCS	2	500s	∞
ETCS	10		427s
ETCS-optimal	2	>3h	∞
ETCS-binary	1	89s	
ETCS	1	1381s	
ETCS	2	271s	
Water tank	1	4.7s	

A. Bauer, E. M. Clarke, and X. Zhao.
Analytica - an experiment in combining theorem proving and symbolic computation.
J. Autom. Reasoning, 21(3):295–325, 1998.

G. Dowek, T. Hardin, and C. Kirchner.
Theorem proving modulo.
J. Autom. Reasoning, 31(1):33–72, 2003.

A. Platzer.
Combining deduction and algebraic constraints for hybrid system analysis.
In B. Beckert, editor, *VERIFY'07 at CADE, Bremen, Germany*, volume 259 of *CEUR Workshop Proceedings*, pages 164–178. CEUR-WS.org, 2007.

C. Tinelli.
Cooperation of background reasoners in theory reasoning by residue sharing.
J. Autom. Reasoning, 30(1):1–31, 2003.