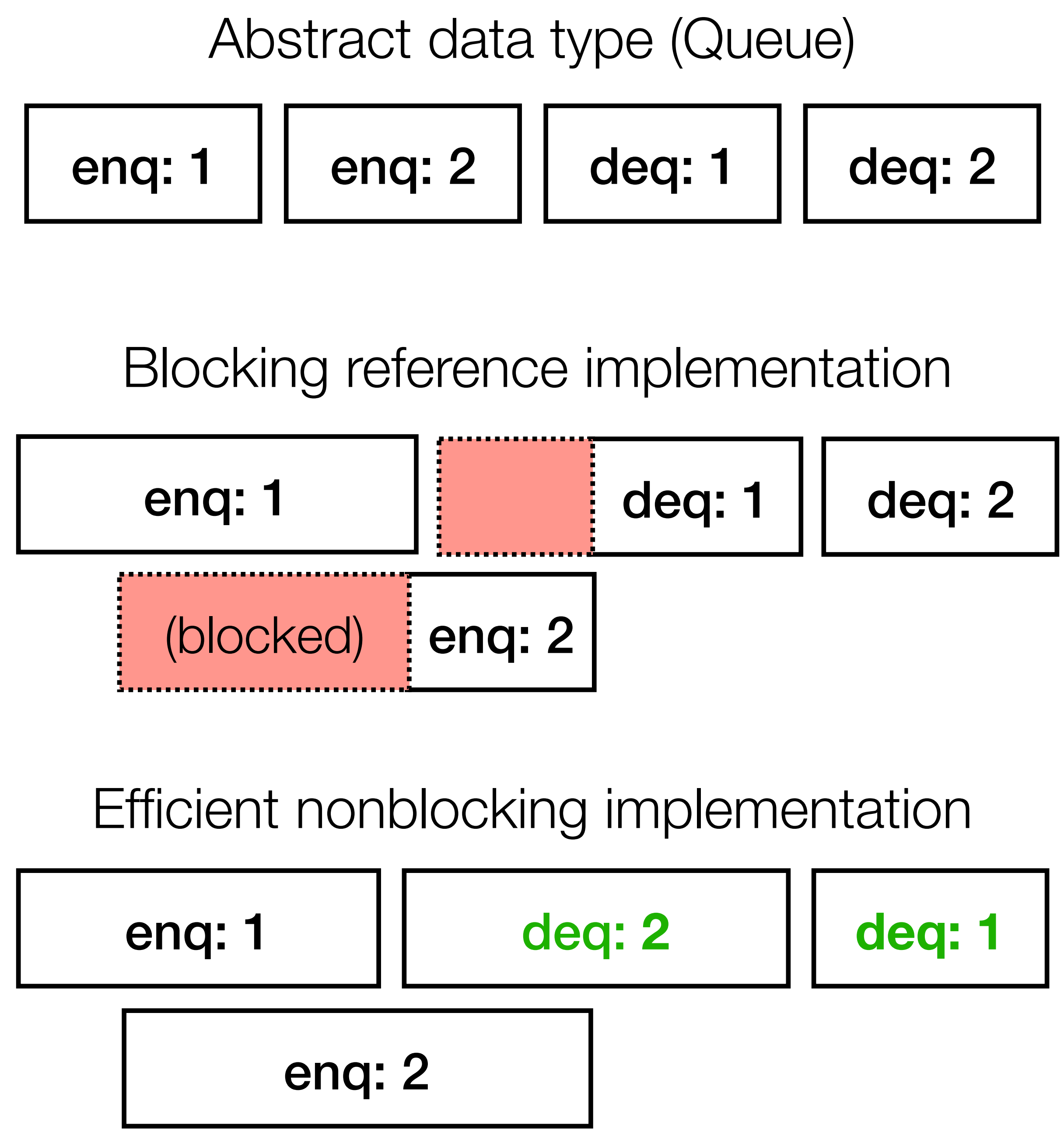
Sound, Complete, and Tractable Linearizability Monitoring for Concurrent Collections

Michael Emmi SRI International

Constantin Enea Université Paris 7

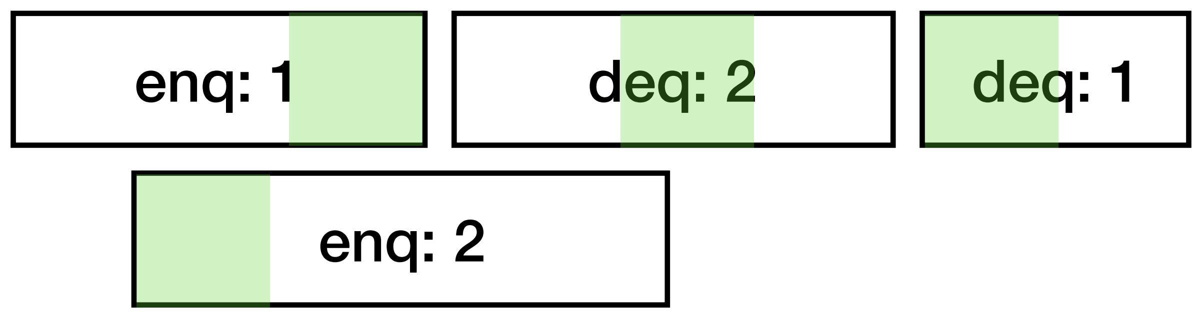
Concurrent Objects



Linearizability

Effects of each invocation appear to occur instantaneously

Execution history



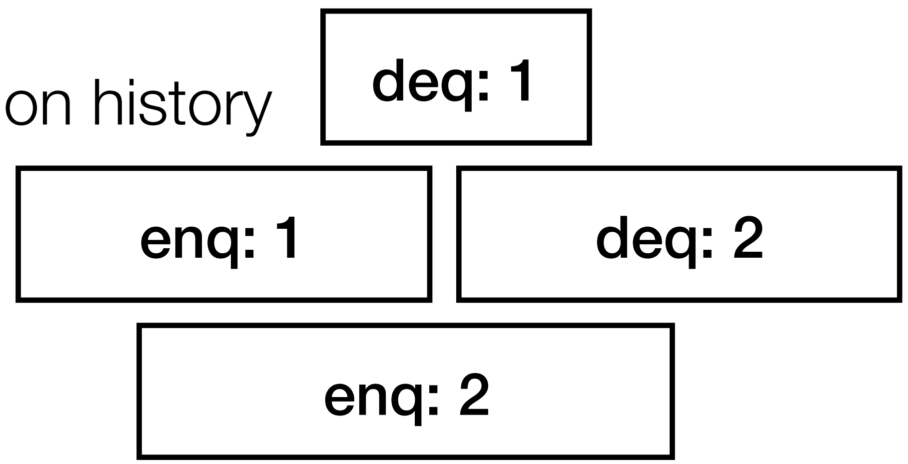
Linearization admitted by Queue type

Theorem (Herlihy and Wing, 1990)
Linearizability implies observational refinement

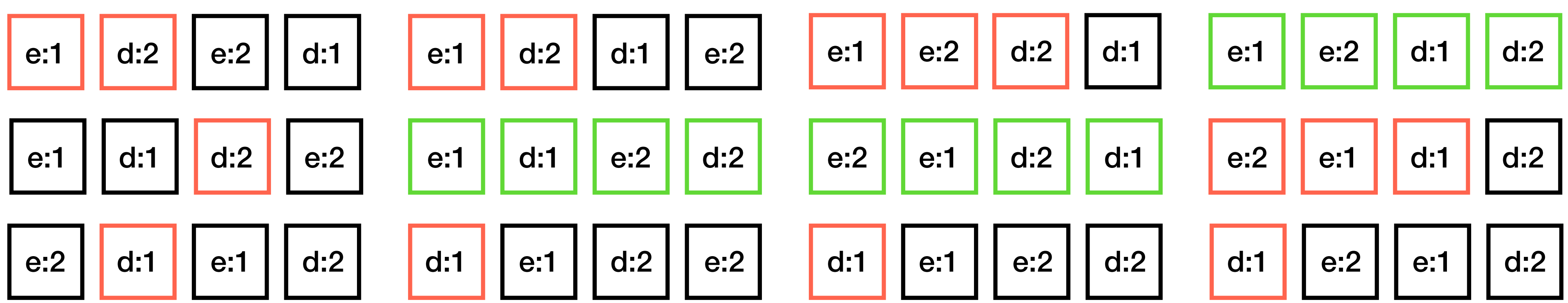
Theorem (Filipovic et al, 2010)
Observational refinement implies linearizability

Hardness

Execution history



Exponentially many linearizations to consider



Theorem (Gibbons and Korach, 1997)
Checking linearizability is NP-hard

Result

Replace enumeration by monotonic deductive inference

Execution history / partial linearization

enq: 1 deq: 2 deq: 1

enq: 2

Queue rule

if d:X d:Y

then e:X e:Y

(partial) linearization

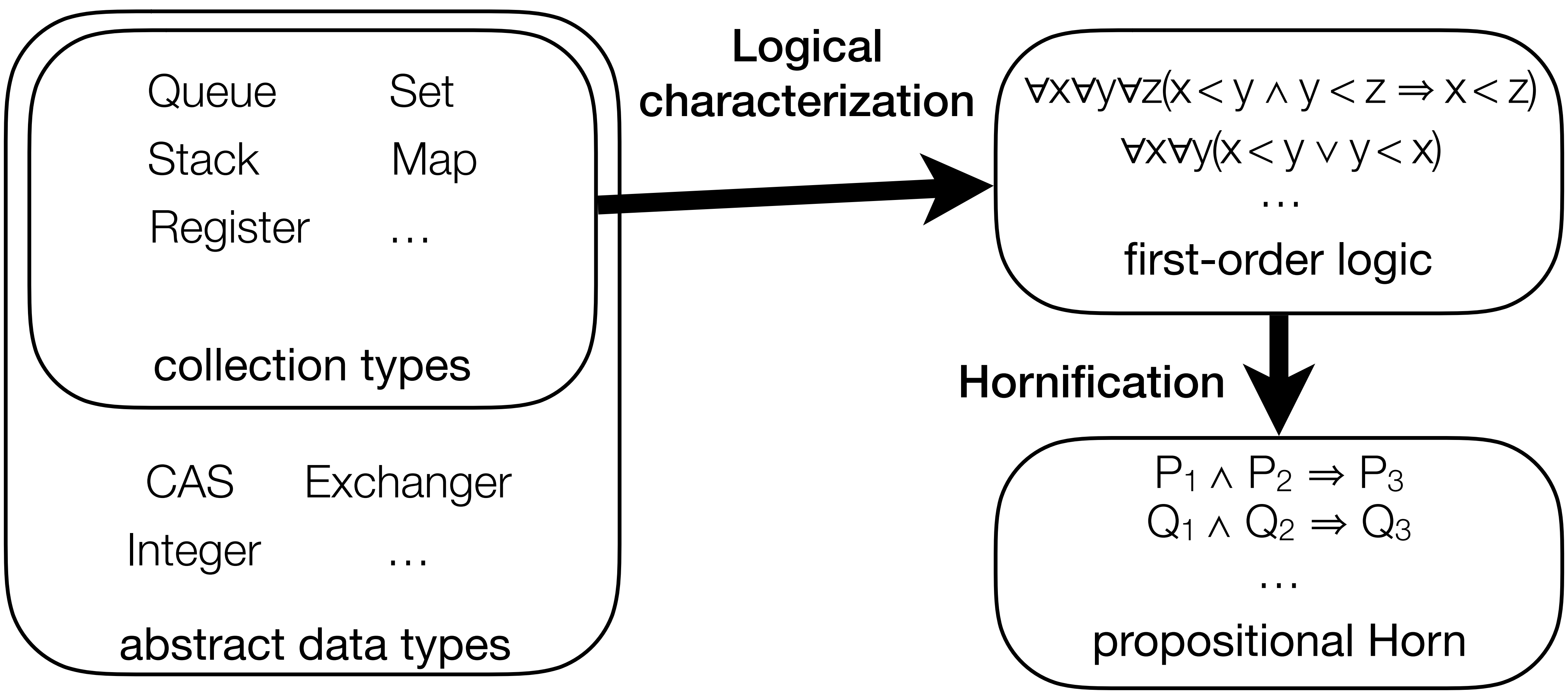
enq: 2 enq: 1 deq: 2 deq: 1

Theorem

Checking linearizability is polynomial-time for *collection types*

Approach

Reduction to logical satisfiability problem



Theorem (Dowling and Gallier, 1984)
Horn satisfiability is solvable in linear time

Logical Characterization

Queue rules

$$\frac{\text{if} \ \boxed{\text{d:X}} \ \boxed{\text{d:Y}}}{\text{then} \ \boxed{\text{e:X}} \ \boxed{\text{e:Y}}}$$

Execution history

$\boxed{\text{e:1}}$ $\boxed{\text{d:2}}$ $\boxed{\text{d:1}}$

$\boxed{\text{e:2}}$

Total order axioms

$\forall x \forall y \forall z (x < y \wedge y < z \Rightarrow x < z)$

$\forall x \forall y (x = y \vee x < y \vee y < x)$

$\ldots$

Queue axioms

$\forall x_1 \forall x_2 \forall y_1 \forall y_2 (\textbf{match}(x_1, x_2) \wedge \textbf{match}(y_1, y_2) \wedge x_1 < y_1 \Rightarrow x_2 < y_2)$

$\wedge \ldots$

Ground formula

$\text{e:1} < \text{d:2} \wedge \text{d:2} < \text{d:1} \wedge \textbf{match}(\text{e:1}, \text{d:1}) \wedge \textbf{match}(\text{e:2}, \text{d:2})$

$\wedge \ldots$

Theorem
Linearizability equivalent to satisfiability for *unambiguous* histories

ambiguous

$\boxed{\text{e:1}}$ $\boxed{\text{d:1}}$ $\boxed{\text{e:1}}$ $\boxed{\text{d:1}}$

unambiguous

$\boxed{\text{e:1}}$ $\boxed{\text{d:1}}$ $\boxed{\text{e:2}}$ $\boxed{\text{d:2}}$

Hornification

Original clause

$A < B \lor B < C \lor \neg(A < B)$

Translated clauses

$A < B \lor \boldsymbol{\neg(C < B)} \lor \neg(A < B)$

$\boldsymbol{\neg(B < A)} \lor B < C \lor \neg(A < B)$

$\boldsymbol{\neg(B < A)} \lor \boldsymbol{\neg(C < B)} \lor \neg(A < B)$

$\boldsymbol{\neg(B < A)} \lor \boldsymbol{\neg(C < B)} \lor \boldsymbol{B < A}$

Theorem
Translation is equisatisfiable and polynomial-time computable

Collection Types

<u>Parametricity</u>

{**3**,5} deq:**3** {5}

{**7**,5} deq:**7** {5}

<u>Locality</u>

{**3**,5} deq:**3** {5}

{**3**,**5**} size:**2** {3,5}

<u>Value invariance</u>

{**3**,5} deq:**3** {5}

{**3**,**5**} sum:**8** {}

<u>Reducibility</u>

{3,5,7} d:3; d:5; d:7 {} $\xrightarrow{\text{2-reducibility}}$

{3,5} d:3; d:5 {}

{3,7} d:3; d:7 {}

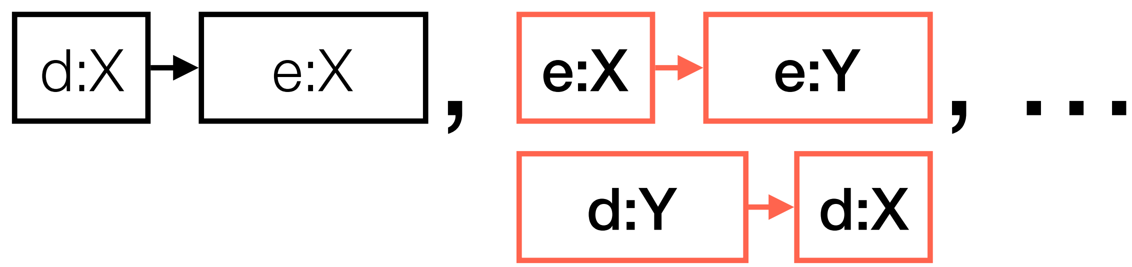
{5,7} d:5; d:7 {}

Theorem

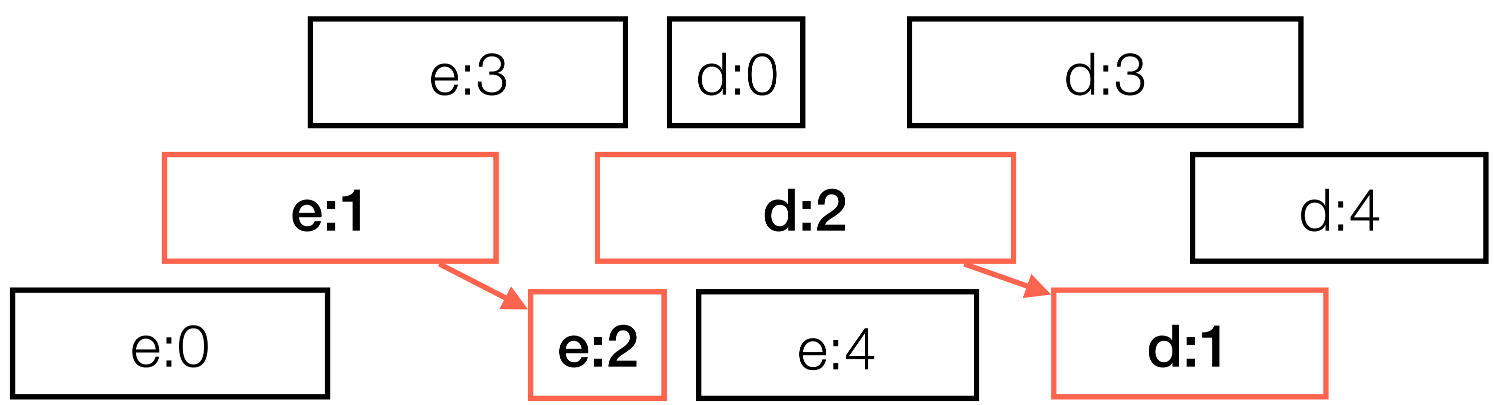
Restriction to unambiguous histories is sound for collections

Bounded Violations

Minimal violations



Minimal violation embedding



Theorem
Collections have bounded minimal violations

Logical Representation

Minimal violations

$$\boxed{d{:}X} \to \boxed{e{:}X}\;,\quad \begin{array}{l} \boxed{e{:}X} \to \boxed{e{:}Y} \\ \boxed{d{:}Y} \to \boxed{d{:}X} \end{array}\;,\;\ldots$$

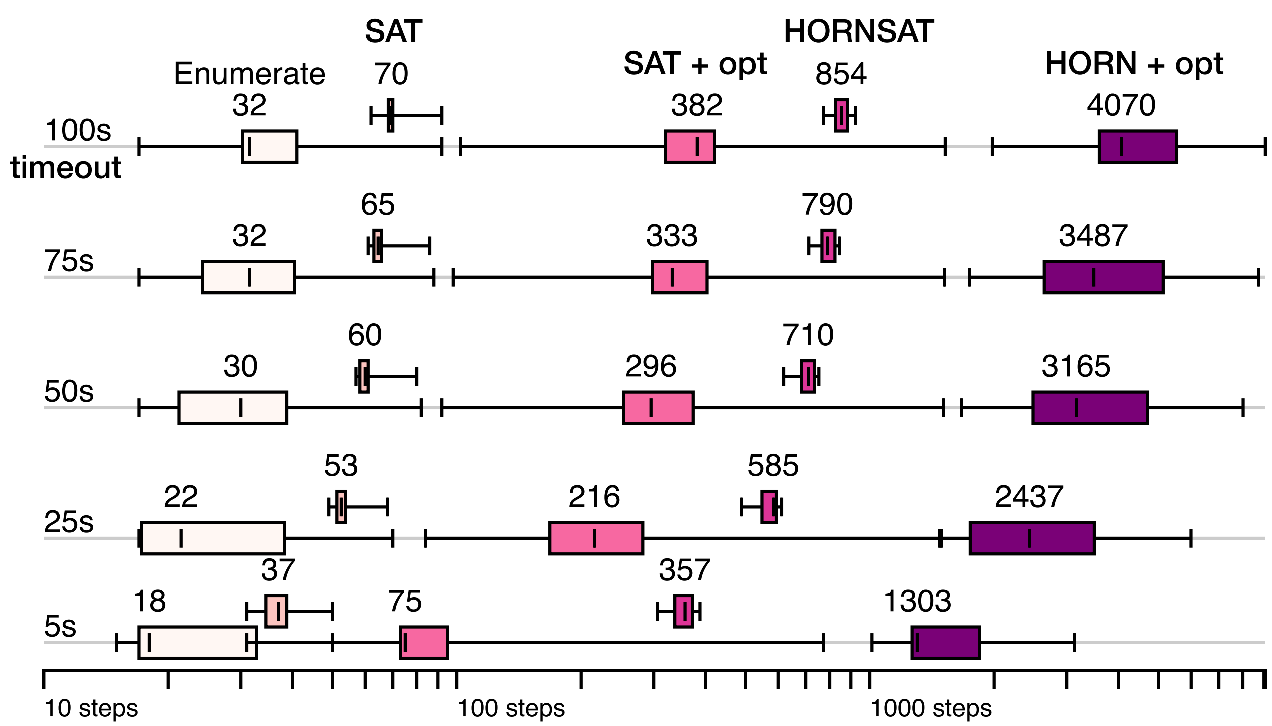
Quantified conjunction of negations

$$\begin{aligned}
&\forall x_1 \forall x_2 \forall y_1 \forall y_2\\
&\ \neg(\mathbf{m}(x_1,x_2) \wedge x_2 < x_1)\\
&\ \ \wedge \neg(\mathbf{m}(x_1,x_2) \wedge \mathbf{m}(y_1,y_2) \wedge x_1 < y_1 \wedge y_2 < x_2)\\
&\ \ \wedge \ldots
\end{aligned}$$

Theorem
Collections have sound logical specifications

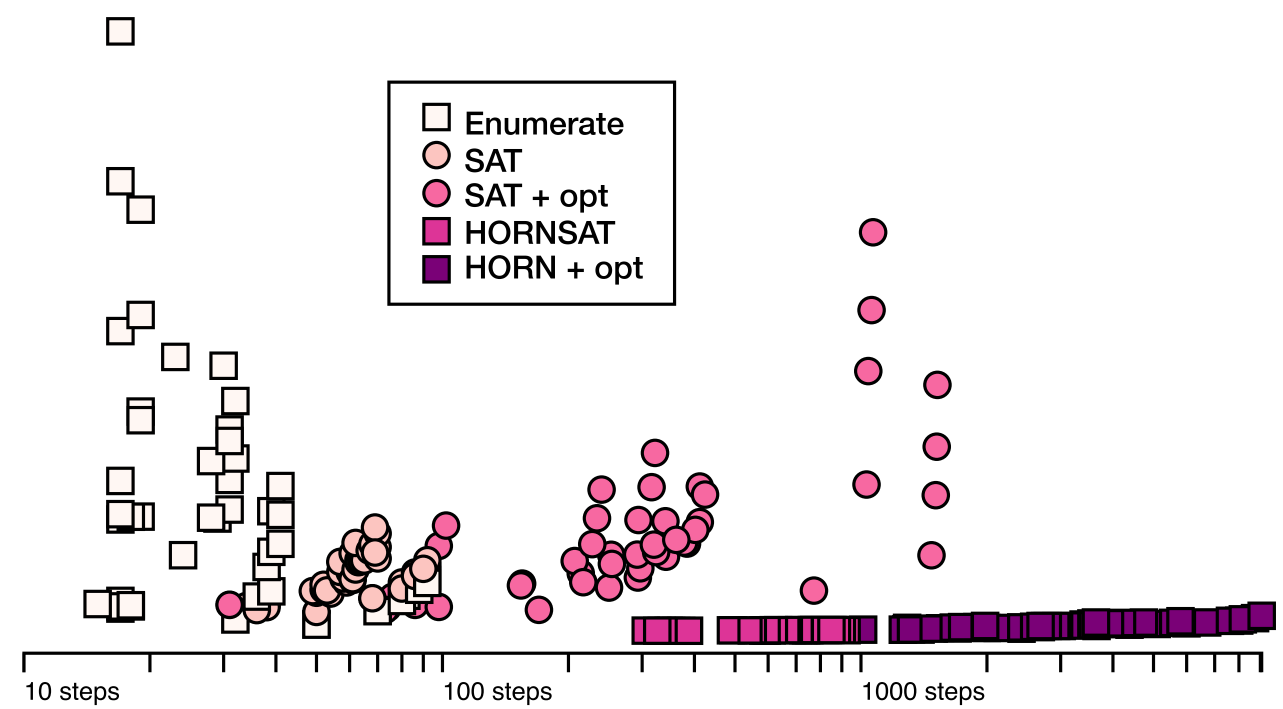
Corollary
Linearizability is PTIME computable for collections

Empirical Evaluation



Performance

Over 10 histories with 10K steps each



Scalability

Normalized by (collection size)^2

Observation

Orders of magnitude speedup

Related Work

Exponential enumeration
Wing and Gong, 1993. *Testing and Verifying Concurrent Objects*

NP Hardness
Gibbons and Korach, 1997. *Testing shared memories*

Asymptotically-equivalent optimizations
Burckhardt et al, 2010. *Line-up: a complete and automatic linearizability checker*
Shacham et al, 2011. *Testing atomicity of composed concurrent operations*
Horn et al, 2015. *Faster linearizability checking via P-compositionality*
Lowe, 2016. *Testing for linearizability*

Tractable approximation
Bouajjani et al, 2015. *Tractable refinement checking for concurrent objects*

Logical characterization
Emmi et al, 2015. *Monitoring refinement via symbolic reasoning*

Logical specification inference
Emmi et al, 2016. *Symbolic abstract data type inference*