A Real-Time, Flexible Logging Infrastructure for MonPoly

Bachelor's Thesis

Jonas Degelo

ETH Zürich

February 24, 2023

MonPoly

- Runtime Monitor
- Metric First Order Temporal Logic (MFOTL)
  - $\bigcirc$ ("Next")
  - $\bullet$ ("Previous")
  - $\mathcal{S}$ ("Since")
  - $\mathcal{U}$ ("Until")

Time-Series Databases

A time-series database is optimized for the insertion and retrieval of temporal data.

Motivation

- Combining logging and monitoring.
- Missing policy change in MonPoly

Signature to Database Schema 1

```
loc_accessed(user_id: int, purpose: string)
perm_granted(user_id: int)
perm_revoked(user_id: int)
```

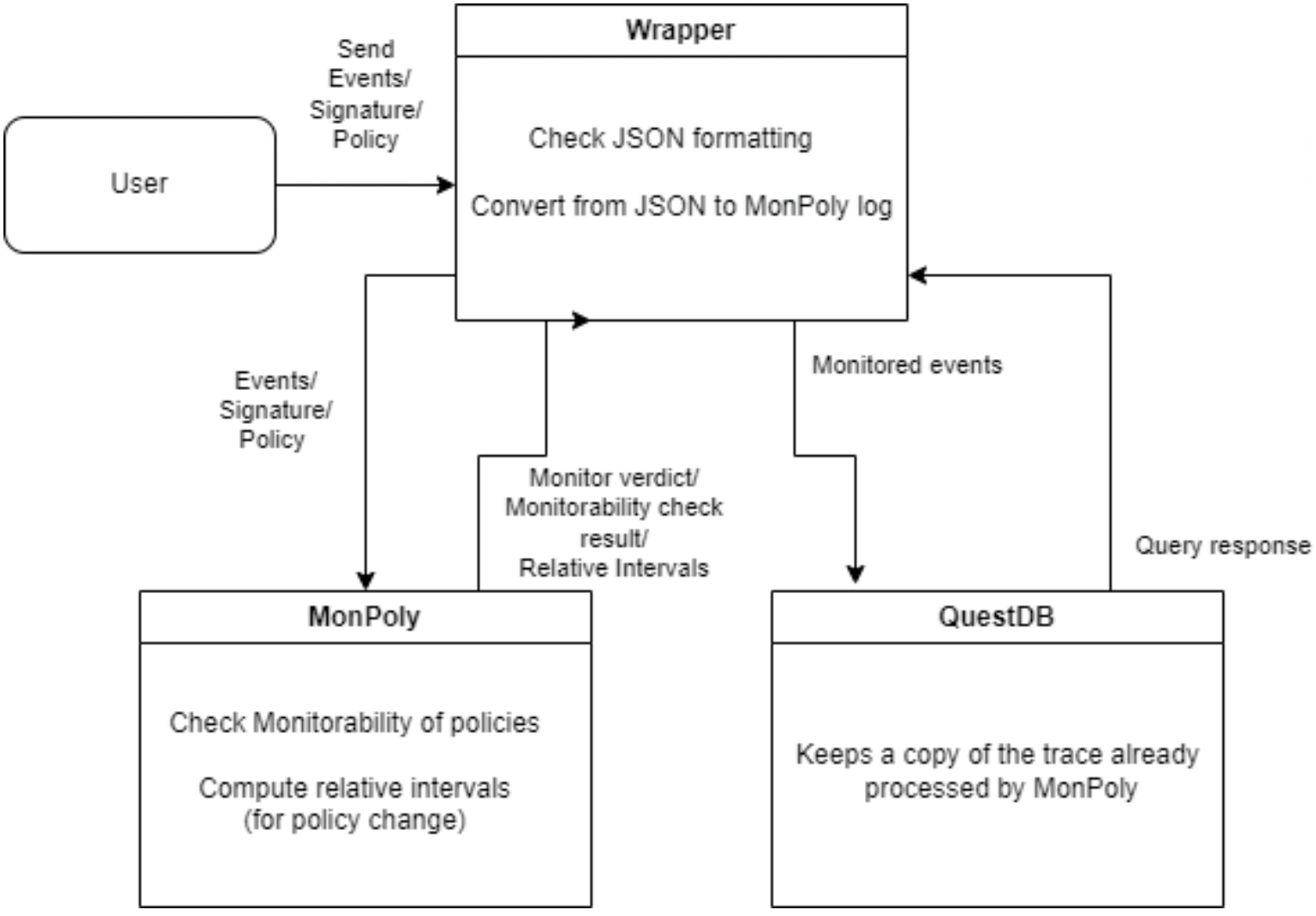
Figure: Sample MonPoly Signature

Signature to Database Schema 2

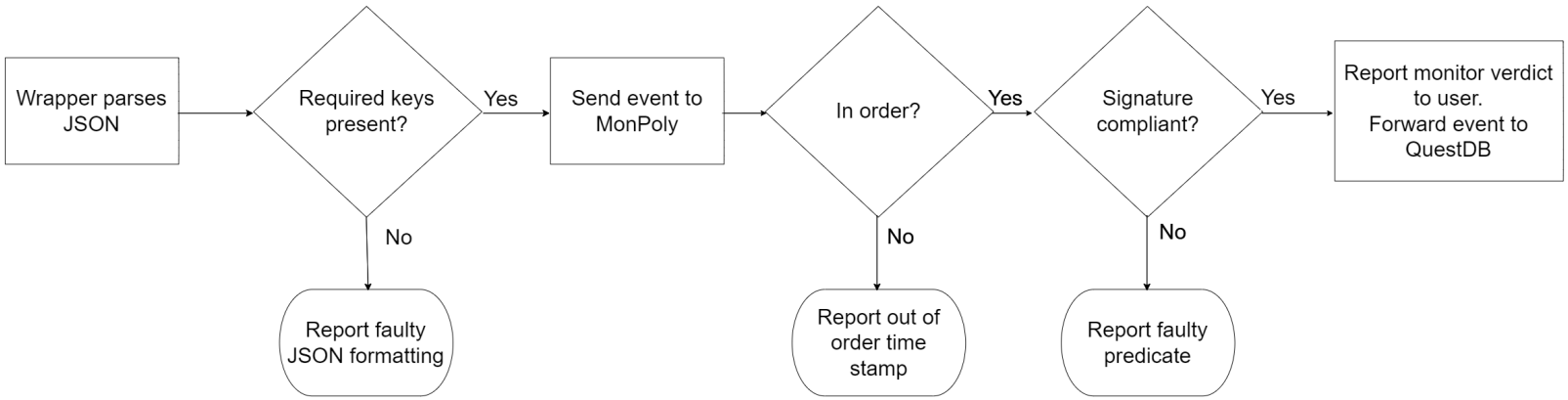
```
CREATE TABLE perm_revoked(x1 INT,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE perm_granted(x1 INT,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE loc_accessed(x1 INT, x2 STRING,
                          time_stamp TIMESTAMP,
                          time_point INT)
                          timestamp(time_stamp);
CREATE TABLE ts( time_stamp TIMESTAMP,
                 time_point INT)
                 timestamp(time_stamp);
```

Figure: SQL Schema for Sample Policy

The Wrapper


Wrapper
Send
Events/
Signature/
Policy
User
Check JSON formatting
Convert from JSON to MonPoly log
Events/
Signature/
Policy
Monitor verdict/
Monitorability check
result/
Relative Intervals
Monitored events
Query response
MonPoly
Check Monitorability of policies
Compute relative intervals
(for policy change)
QuestDB
Keeps a copy of the trace already
processed by MonPoly

The Wrapper


Wrapper parses JSON
Required keys present?
Yes
No
Report faulty JSON formatting
Send event to MonPoly
In order?
Yes
No
Report out of order time stamp
Signature compliant?
Yes
No
Report faulty predicate
Report monitor verdict to user.
Forward event to QuestDB

Policy Change

- Start a new monitor with the new policy
- **Goal:** Our monitor evaluates the new policy at the current time point just as if it had seen the same trace as the old monitor
- **Naive approach:** Read entire trace again
- **Idea:** Reduce the size of the trace by removing events that do not influence how the new policy gets evaluated

Interval Operators

Let I and J be two intervals, then

- $I \oplus J = \{i + j \mid i \in I, j \in J\}$
  - $[0, 3] \oplus [-2, 4] = [-2, 7]$
- $I \Cup J$ is the smallest interval that contains all elements that are in at least one of the intervals I and J.
  - $[-4, 1] \Cup [4, 5] = [-4, 5]$

Relative Intervals

Definition

The relative interval of the formula ϕ, $\mathsf{RI}(\phi) \subseteq \mathbb{Z}$ is defined recursively over the formula structure: $\mathsf{RI}(\phi) =$

$$
\begin{cases}
\{0\} & \text{atomic formula,} \\
\mathsf{RI}(\psi) & \neg\psi,\ \exists x.\psi, \\
 & \text{or } \forall x.\psi, \\
\mathsf{RI}(\psi) \uplus \mathsf{RI}(\chi) & \psi \vee \chi, or \psi \wedge \chi, \\
(-b, 0] \uplus ((-b, -a] \oplus \mathsf{RI}(\psi)) & \bullet_{[a,b)}\psi, \\
[0, b) \uplus ([a, b) \oplus \mathsf{RI}(\psi)) & \bigcirc_{[a,b)}, \\
(-b, 0] \uplus ((-b, 0] \oplus \mathsf{RI}(\psi)) \uplus ((-b, -a] \oplus \mathsf{RI}(\chi)) & \psi\, \mathcal{S}_{[a,b)} \chi, \\
[0, b) \uplus ([0, b) \oplus \mathsf{RI}(\psi)) \uplus ([a, b) \oplus \mathsf{RI}(\chi)) & \psi\, \mathcal{U}_{[a,b)}\, \chi,
\end{cases}
$$

Basin et al. [1]

Relative Intervals Example

$$\neg(\texttt{loc\_accessed(i, "advertising")})\,\mathcal{S}_{[0,30\text{d})}\,\texttt{perm\_revoked(i)}$$

Extended Relative Intervals

Definition

Let M and N be two masked predicate maps and T a positive interval, then

$$
\begin{aligned}
M \ddot{\Cup} N =& \{p(I) \to (I \Cup J) \mid p(I) \to I \in m \text{ and } p(I) \to J \in n\} \\
&\cup \{p(I) \to I \mid (p(I) \to I \in m \text{ and } p(I) \in \mathrm{k}(M) \setminus \mathrm{k}(N))\} \\
&\cup \{p(I) \to I \mid (p(I) \to I \in n \text{ and } p(I) \in \mathrm{k}(N) \setminus \mathrm{k}(M))\} \\
T \dot{\Cup} M =& \{p(I) \to (T \Cup I) \mid p(I) \to I \in M\} \\
T \dot{\oplus} M =& \{p(I) \to (T \oplus I) \mid p(I) \to I \in M\}
\end{aligned}
$$

Extended Relative Intervals

Definition

The extended relative interval of the formula φ, $\mathrm{ERI}(\varphi)$ is defined recursively over the formula structure: $\mathrm{ERI}(\varphi) =$

$$\begin{cases} \{\} & \text{if } \varphi \text{ is an atomic formula} \\ & \text{and not a predicate,} \\ \{p(m) \to [0,0]\} & \text{if } \varphi \text{ is a predicate with name} \\ & p \text{ and mask } m, \\ \mathrm{ERI}(\psi) & \text{if } \varphi \text{ is of the form } \neg\psi, \exists x.\psi, \\ & \text{or } \forall x.\psi, \\ \ldots & \end{cases}$$

Extended Relative Intervals Example

Partial Policy Change in MonPoly (Work in Progress)

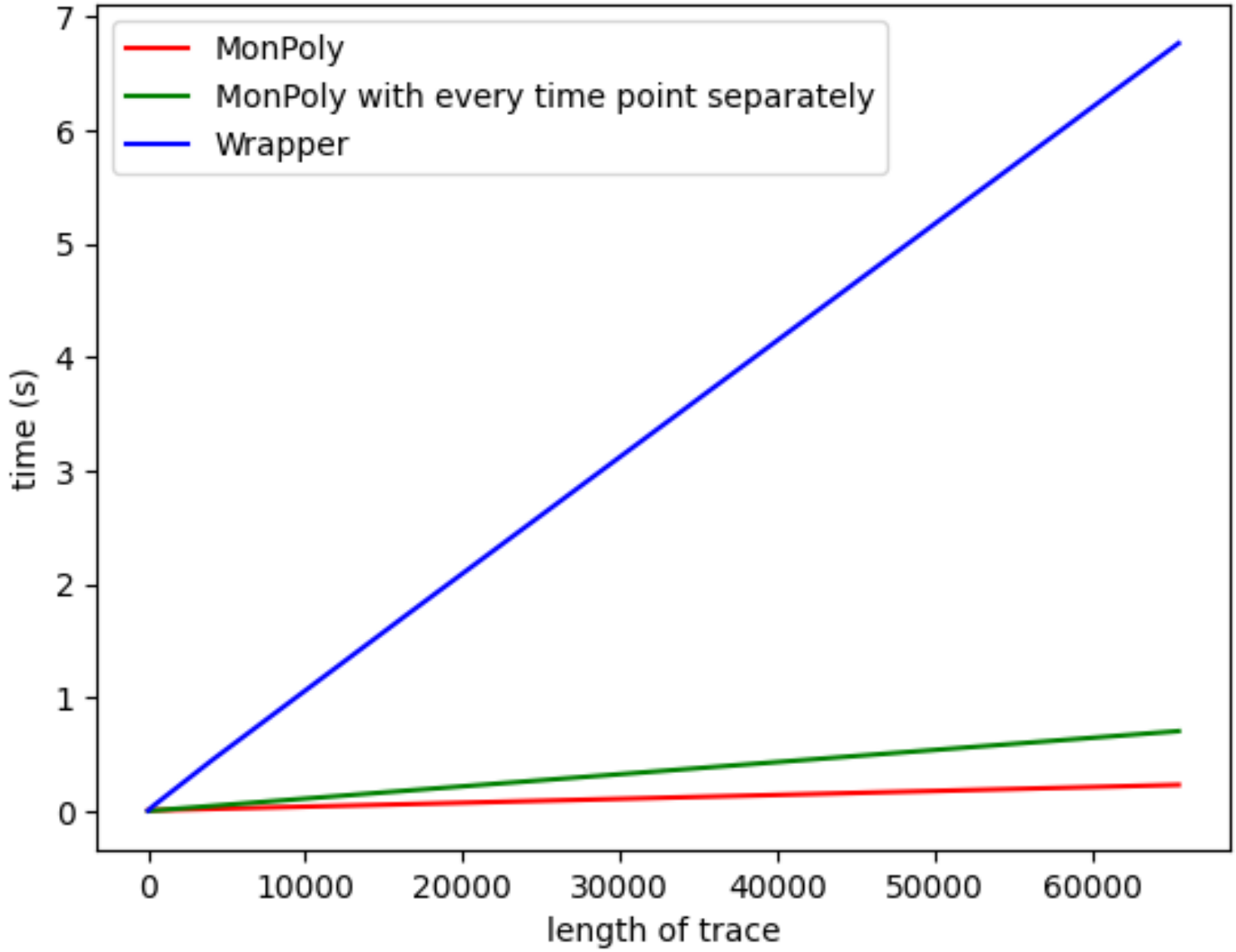
- Named formulas
- `NAME[f1, name1] OR NAME[f2 and f3, name2]`
- Commands to add or remove conjuncts or disjuncts
- Added data types for `NAME` in MonPoly
- Updated formula parser for `NAME` constructs
- Started work on commands for adding and removing parts of formulas.

Partial Policy Change in MonPoly (Work in Progress)

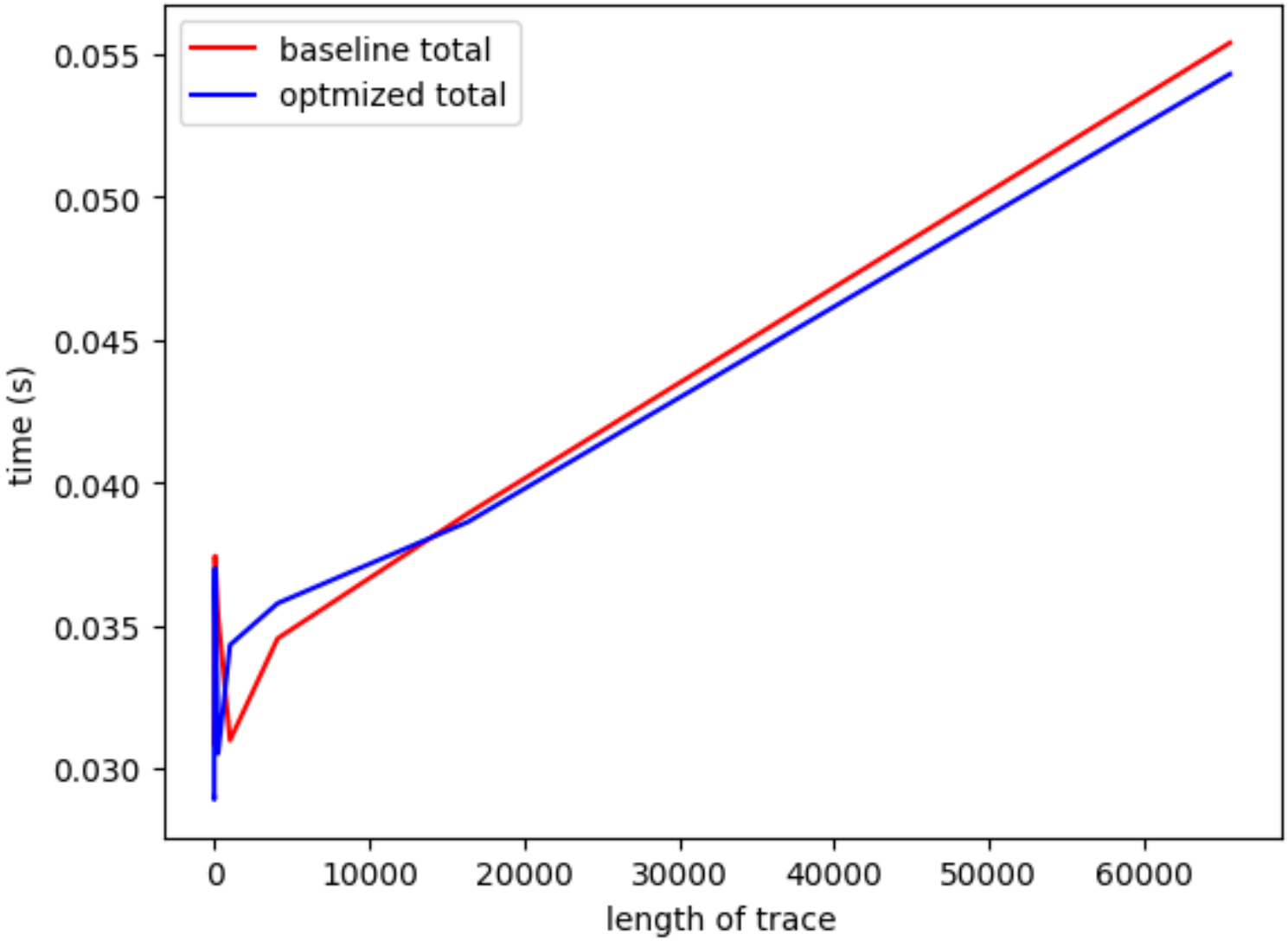
Next up:

- Compute the internal state for formula parts that will be added.
- Combine existing state with the state of the new formula.
- Update state when a formula part gets removed

Performance Overhead



Policy Change Optimization



Outlook

- Reduce overhead of the wrapper
  - Send time points asynchronously (don't wait for response before sending the next time point)
  -
- Speed up policy change
  -

References

[1] David Basin et al. “Scalable Offline Monitoring of Temporal Specifications”. In: *Formal Methods in System Design* 49 (1 2016), pp. 75–108. ISSN: 1572-8102.