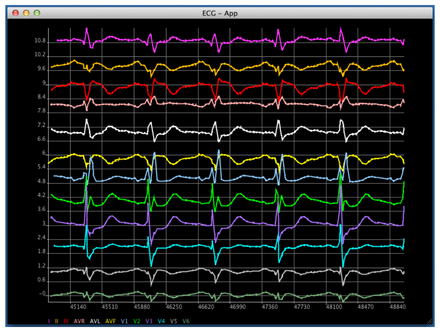
LIFE DATA RECORDER AND THREE-VALUED RUNTIME CHECKING SEMANTICS

Shaohui Wang, Anaheed Ayoub, Oleg Sokolsky, and Insup Lee (University of Pennsylvania)

› Motivation

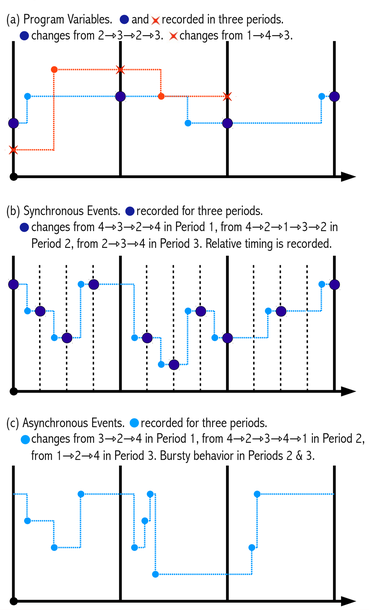
- Data recording for medical devices plays a central role in the verification, analysis, and diagnosis in safety-critical applications.
- Ideally, recorded data should be time-stamped at the exact time an event occurs.
- This results in huge amount of recorded data.
- E.g., a typical waveform (shown on right) data file is several gigabytes!



- An efficient and compact recording scheme should be designed.
- **Life Data Recorder (LDR).**

› Background—LDR Recording

- A highly configurable recording scheme, either co-designed with new medical devices, or pluggable to existing ones.
- Trades off accuracy of timing information of events recorded for efficiency in recording.
- Periodically records three types of events
  - —Program Variables
    - · At most one change in each period
  - —Synchronous Events
    - · multiple occurrences
    - · recorded by relative time to the start of the period
  - —Asynchronous Events
    - · multiple occurrences
    - · exhibit bursty behaviors
    - · bounded number in each period



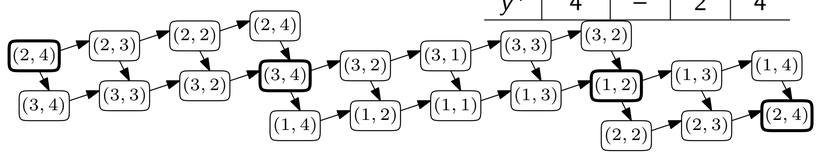
Problem Statement

- Lost information on event interleavings is exhibited in LDR recorded traces.
- Given a system trace *Tr* from an LDR recording session and a system property ϕ, how to check if the trace *Tr* satisfies ϕ?

› Three-Valued Semantics

- An LDR recorded trace (right) essentially defines a Kripke structure (below).

	Init	F1	F2	F3
x	2	3	1	2
y^1		3	2	–
y^2		2	1	3
y^3		4	3	–
y^4	4	–	2	4



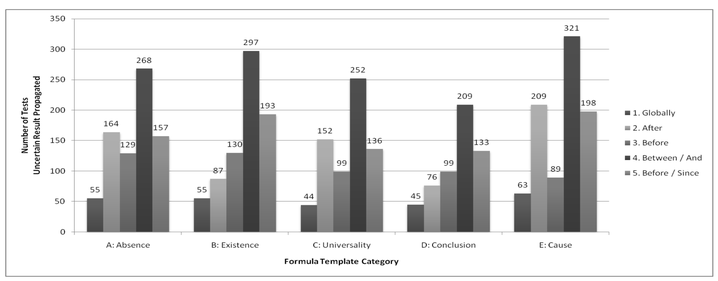
- Any one possible interleaving of events is captured as a concrete trace from beginning (leftmost ⟨x=2, y=4⟩) to end (rightmost ⟨x=2, y=4⟩).
- It is known that for concrete traces, the satisfiability problem is well defined.
- We defined a **three-valued semantics** for **Linear Temporal Logic (LTL)** properties.
  - —If all concrete traces corresponding to an LDR recorded trace *Tr* satisfy property ϕ, then [*Tr* satisfies ϕ] is true.
  - —If none of the concrete traces corresponding to *Tr* satisfies ϕ, then [*Tr* satisfies ϕ] is false.
  - —Otherwise, [*Tr* satisfies ϕ] is undecided due to loss of information in recording.
- In addition, a recursive semantics equivalent to the above was defined.
- Fast iterative algorithms for runtime checking of LTL formulas on LDR recorded traces developed.
- Efficient checker / testbed implemented.

› Evaluation—Purpose and Techniques

- Study reasonableness of the three-valued semantics: how often would the uncertain outcome occur? Do they persist?
- Gain insight into the utility of the three-valued semantics: are there patterned checking results for commonly used formula patterns? using three-valued semantics for system property specification.
- 25 common formula templates investigated, using random formula generation techniques.
- Checking the formula instances on semi-random traces. Results recorded.

› Evaluation Results

- Uncertain results do not occur as much—only 12%~15% compared to an expected ⅓ if true, false, and uncertain results were equally distributed.
- Once an uncertain outcome appears on a trace, it tends to persists on that trace.
- As shown below, certain property formats (*P* happens between *Q* and *R*, where *P* could be "always *A*", "sometimes *A*", "*A* causes *B*", "*A* prevents *B*", etc.) are sensitive to uncertain outcomes.



› Conclusion and Future Work

- The LDR data recording scheme for medical device was implemented.
- Three-valued semantics for LTL formula was defined and evaluated.
- Applications to projects in the real world?