The opacity of real-time automata (实时自动机的不透明性)

Lingtai Wang, Naijun Zhan, and Jie An

The Opacity of Real-Time Automata. IEEE Trans. on CAD of Integrated Circuits and Systems 37(11): 2845-2856 (2018)
(Special issue of EMSOFT 2018)

Lingtai Wang, wanglt@ios.ac.cn, 18810516096; Naijun Zhan, znj@ios.ac.cn, 13810460251

Opacity is an information flow property aiming at keeping the “secret” of a system opaque to its intruder with partial observability. We mainly focus on the dicidability of language-opacity cases on a timed model on real-time automata (RTA). The main idea is to reduce the language-opacity problem of RTA to the language-inclusion problem of FA, with the help of trace-equivalence relation, partitioned alphabets and languages, as well as the projection operation of FA onto a given alphabet.

1. Real-time Automata (RTA)

A real-time automaton (RTA) is a 6-tuple $\mathcal{A}=(S,\Sigma,\Delta,Init,F,\mu)$, where

- S is a finite set of states;
- Σ is a finite alphabet;
- $\Delta\subseteq S\times\Sigma\times S$ is the transition relation;
- $Init\subseteq S$ is the set of initial states;
- $F\subseteq S$ is the set of accepting states;
- $\mu:\Delta\to 2^{R_{\geq 0}}\setminus\{\phi\}$ is the time labelling function.

2. Language-opacity and Initial-state Opacity of RTA

Given an RTA $\mathcal{A}=(S,\Sigma,\Delta,Init,F,\mu)$,
an observable alphabet Σ_o,
a secret timed language L_{secret} over Σ,
a secret set of states S_{secret},
$\mathcal{A}$ is

- language-opaque with respect to L_{secret} and Σ_o iff $P_{\Sigma_o,t}(L(\mathcal{A}))\subseteq P_{\Sigma_o,t}(L(\mathcal{A})\setminus L_{secret})$
- initial-state opaque with respect to S_{secret} and Σ_o iff $P_{\Sigma_o,t}(L(\mathcal{A}))\subseteq P_{\Sigma_o,t}(Tr(Init\setminus S_{secret}))$

3. Decidability of Language-Opacity

We focus on the language-opacity problem, because initial-state opacity can be reduced to language-opacity.

Trace-equivalence Relation

The *trace-equivalence* relation requires that all the timed words accepted by an RTA are covered by an corrsponding FA and vice versa.
So we can translate an RTA into an FA by integrating time labels in the RTA into actions.

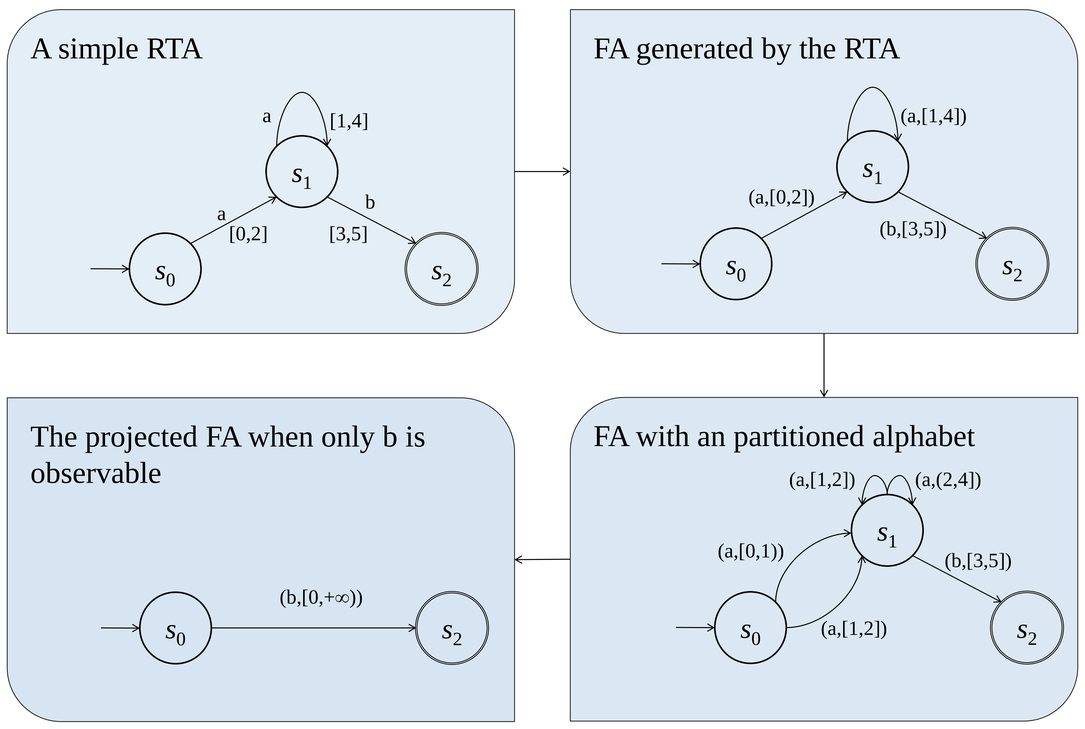
Partitioned Alphabet and Languages

An alphabet is called a *partitioned alphabet* if the time labels of each symbol forms a partition of $R_{\geq 0}$. And a language is called a *partitioned language* if it is over a partitioned alphabet.
By splitting overlapping durations, the trace-equvalence relation is preserved under the complement and product operations.

Projection of FA

The *projection* of an FA over a timed alphabet is another FA over a new timed alphabet accepting the projection of the original FA's accepting language. Only observable symbols and their occurring time will be retained after projection.
There are two steps:

- Summing up the possible elapsed time by a successive sequence of unobservable symbols (by following the well-known Floyd-Warshall algorithm proving the Kleene's Theorem)
- Merging the sum into the time label of corresponding observable transitions



The Whole Progress

Step 1
Calculating the FA “accepting” $L(\mathcal{A})$ and L_{secret} respectively

Step 2
Calculating the FA “accepting” $L(\mathcal{A})\setminus L_{secret}$

Step 3
Calculating the FA “accepting” $P_{\Sigma_o,t}(L(\mathcal{A}))$ and $P_{\Sigma_o,t}(L(\mathcal{A})\setminus L_{secret})$ respectively;

Step 4
Deciding whether $P_{\Sigma_o,t}(L(\mathcal{A}))\subseteq P_{\Sigma_o,t}(L(\mathcal{A})\setminus L_{secret})$

Here “accepting” means the accepting language of the FA is trace-equivalent to the corresponding timed language.

4. Theoretical Results

Theorem 1. The language-opacity problem of RTA is decidable.
Corollary 1. The initial-state opacity problem of RTA is decidable.

5. Implementation

A prototypical tool is developed for deciding the language-opacity problem of RTA, which can be found at https://github.com/Leslieaj/RTAOpacity.

6. Conclusions

- ✓ We investigate the opacity problems of RTA, mainly focussing on language-opacity, which can be reduced to the language-inclusion problem of FA.
- ✓ Trace-equivalence and partitioned alphabets and languages are proposed in order to translate RTA into FA, such that trace-equivalence is preserved under complement and product.
- ✓ The projection of FA onto a given observable alphabet is also defined.
- ✓ The result is that language-opacity problem and initial-state opacity problem of RTA are both decidable.