Mathematical Structures in Formal Methods, *MSFM*
Handout for Lecture 10 (2018/7/19)

Ichiro Hasuo, NII/SOKENDAI, Tokyo, Japan `http://group-mmm.org/~ichiro`

1 Today's Lecture

Examples of the translation of LTL formulas into Buechi automata. Section 4.2, 4.3.

Move to [Jurdzinski, STACS'00]. Parity games, progress measures.

2 Coming Up

2.1 Reactive LTL Synthesis

Theorem. *Let φ be an LTL formula over the set* AP *of atomic propositions. Let* $\mathrm{AP} = \mathrm{AP}_P \amalg \mathrm{AP}_O$ *be a partition of* AP*, into* Proponent's *and* Opponent's *atomic propositions. Then there exists a finite state machine*

$$\bigl(\, Q,\, q_0 \in Q,\, \delta\colon Q \times 2^{\mathrm{AP}_O} \longrightarrow Q \times 2^{\mathrm{AP}_P} \,\bigr)$$

such that, for any sequence $a_0 a_1 \ldots \in (2^{\mathrm{AP}_O})^\omega$ ("environmental input"), the sequence

$$(a_0 \cup b_0)\,(a_1 \cup b_1)\,\ldots$$

satisfies φ. Here b_i is defined inductively by $(q_{i+1}, b_i) := \delta(q_i, a_i)$ for each i.

The LTL synthesis workflow:

> LTL $\longrightarrow$ ABA $\longrightarrow$ BA $\xrightarrow{\text{determinization}}$ Rabin automata $\xrightarrow{\text{[Kretinsky+, TACAS'17]}}$ deterministic parity automata $\longrightarrow$ parity games.

The second last step is in

> Jan Kretinsky, Tobias Meggendorfer, Clara Waldmann, Maximilian Weininger: Index Appearance Record for Transforming Rabin Automata into Parity Automata. Proc. TACAS 2017, 443-460

The last step is as follows. Given a deterministic parity automaton $A = (2^{\mathrm{AP}}, S, s_0, \rho\colon S \times 2^{\mathrm{AP}} \to S, F)$, the resulting parity game is as follows. Note that different brackets $\langle s, a\rangle, [s, b]$ are used for distinguishing players.

- Proponents's positions: $\langle s, a\rangle \in S \times 2^{\mathrm{AP}_O}$ ("the current state is s and Opponent's action, to which I have to react, was a")
- Opponent's positions: $[s, b] \in S \times 2^{\mathrm{AP}_P}$ ("Proponent reacted with the action b, which led to the current state s")
- Transitions:
  - $[s, b] \to \langle s, a\rangle$ for each $s \in S, a \in 2^{\mathrm{AP}_O}, b \in 2^{\mathrm{AP}_P}$ (the state remains the same)
  - $\langle s, a\rangle \to [s', b]$ if and only if $s' = \rho(s, a \cup b)$. Note that $a \cup b \in 2^{\mathrm{AP}}$.
- Accepting states are: $[s, b]$ with $s \in F$.

In [Vardi, 1995] an alternative workflow is presented that relies on the emptiness check of Rabin tree automata. The above workflow is advantageous in that efficient solvers of parity games have been actively studied.

Further topics:

- Need of determinization. You cannot commit to a particular choice before observing the whole input sequence. To see the whole input, you have to wait for infinitely long!
- Safraless procedures
- GR(1) Synthesis—an efficient fragment of LTL