Introduction to Temporal Logic and Reactive Systems

Zohar Manna

- Verification of *sequential* programs.
  - No concurrency.
  - Programs (should) always terminate.
  - Observable at start (input) and end (output) of execution.
- Logical foundations:
  - FOL.
  - Invariants and ranking functions.
  - Verification conditions.
  - Decision procedures.
  - Induction.

- Verification of *reactive systems*.
    - Highly concurrent.
      Concept of *fairness*.
      Properties: *mutual exclusion*, *freedom from deadlock*.
    - Programs need not terminate (e.g., OS, web server).
      But some components must terminate (e.g., IO handler).
    - Observable throughout execution.
      And the environment affects execution.
- Logical foundations: Everything from CS156 *plus*
    - *temporal logics*
      linear (LTL), branching (CTL), alternating (ATL) time
    - *automata theory* and connection with temporal logics
      infinite strings (linear) and trees (branching, alternating)

PRIME

```
local $y$ : integer where $y = 1$
$\ell_0$ : loop forever do
    [ ⋮
      $\ell_5$ : print $y$
      $\ell_6$ :
      ⋮
      $\ell_{10}$ : $y \leftarrow y + 1$
      ⋮ ]
```

Output: 2,3,5,7,11,13, . . .

- only primes:

$$\Box[at\_\ell_5 \rightarrow \text{prime}(y)]$$

- all primes:

$$\forall u.\ [\text{prime}(u) \ \rightarrow\ \Diamond(at\_\ell_5 \wedge y = u)]$$

- monotonicity (correct order):

$$\forall u.\ \Box[(at\_\ell_6 \wedge y = u) \ \rightarrow\ \Box(at\_\ell_5 \rightarrow y > u)]$$

BAKERY

```
local   $y_1, y_2$   : integer where $y_1 = 0, y_2 = 0$
$P_1$ ::
  loop forever do
    $\ell_0$ : noncritical
    $\ell_1$ : $y_1 := y_2 + 1$
    $\ell_2$ : await $y_2 = 0 \vee y_1 \leq y_2$
    $\ell_3$ : critical
    $\ell_4$ : $y_1 := 0$
$||$
$P_2$ ::
  loop forever do
    $m_0$ : noncritical
    $m_1$ : $y_2 := y_1 + 1$
    $m_2$ : await $y_1 = 0 \vee y_2 \leq y_1$
    $m_3$ : critical
    $m_4$ : $y_2 := 0$
```

Requirements for BAKERY

- Mutual exclusion

$$\boxed{\Box\neg(\ell_3 \quad \wedge \quad m_3)}$$

The two processes are not in the critical section simultaneously.

- One-bounded overtaking

$$\boxed{\ell_2 \;\Rightarrow\; \neg m_3 \,\mathcal{W}\, m_3 \,\mathcal{W}\, \neg m_3 \,\mathcal{W}\, \ell_3}$$

Once P_1 waits to get access, P_2 can enter its critical section at most once.

- Progress

$$\boxed{\ell_1 \;\Rightarrow \Diamond \ell_3}$$

Once P_1 shows interest in entering its critical section, it eventually gets access to the critical section.

Administration

- Instructor: Zohar Manna

- Text:

  The Temporal Verification of Reactive Systems: Safety
  Zohar Manna and Amir Pnueli
  Springer-Verlag 1995