Timed Automata

TA 用于为实时系统建模，常见的有两种模型

- discrete time domain
- continuous time domain

Discrete Time Domain

基本思想是时钟每隔一个固定的时间间隔后发出信号，且系统在时钟发出信号后做出改变，在两次信号间的时候系统等待

选定一个基本的时间段 ε ，则任何事件发生的时间点只能是 ε 的整数倍

挑战在于 ε 的选取，常常用于建模同步系统，如硬件电路的建模

Continuous Time Domain

模型中时间以实数表示，而 delay 可以为任意小。这样建模的结果是状态空间往往是无限甚至不可数的，不能以遍历状态空间的方式解决问题

Timed Automata

TA 是对于 FA 的扩展（添加了 clock），但是对于能对 clock 做的操作有限制

- 能将 clock 的值与一个实数比较
- 能将一个 clock reset 为 0
- uniform flow of time：所有 clock 变化的速率是相同的

Definition

TA 的图形表示是一个二元图，节点为 location，边为 transition

- 系统中有多个 clock，以相同速率运行
- 时间只会在 location 消耗
- 在边上有限制 clock 的 constraints，称为 guards。只有满足 guards 才能经由此边迁移到下一个 location
- 在边上同样可以进行 clock 的 reset 操作
- 在 location 上有限制 clock 的 invariants，只有满足 invariants 才能留在当前 location，否则必须进行 transition

Clock Constraints: 设 X 为 clock 的集合，则 $C(X)$ 为 clock constraints 的集合，其中的元素为

$$\varnothing = x \leqslant k \mid k \leqslant x \mid x < k \mid k < x \mid \varnothing \wedge \varnothing$$

满足 $x \in X, k \in \mathbb{N}$

则一个 TA 是一个 4-tuple $A = (L, X, I_0, E)$ ，其中

- L 是有限的 location 集合
- X 是有限的 clock 集合
- $I_0 \in L$ 是初始的 location
- $E \subseteq L \times C(X) \times 2^X \times L$ 是边的集合，即边为一个 4-tuple (source location, clock constraints, set of clocks to be reset, target location)

Semantics

TA 的语义是基于 TS 的，其中

- state 为 location + clock valuation
- transition 可分为两种
  - wait，此时仅有 clock valuation 变化
  - action，location 的变化

clock valuation 是一个函数 $v : X \to \mathbb{R}^+$，代表当前的 clock 的值

- $v[Y := 0]$ 代表将 Y 中的 clock 置为 0 后的 valuation，即

$$v[Y := 0](x) = \begin{cases} 0 & x \in Y \\ x & o.t. \end{cases}$$

- $v + d$ 代表 flow of time，即 $(v + d)(x) = v(x) + d$
- $v \models c$ 代表 v 满足 constraint c

则可以给出 TA 语义的定义，TA 的语义是一个 TS $S_A = (S, s_0, \to)$

- $S = L \times (X \to \mathbb{R}^+)$ 是状态集合
- $s_0 = (I_0, v_0), \forall x \in X, v_0(x) = 0$ 是初始状态
- $\to$: $S \times S$ 是迁移
  - delay action: $(I, v) \xrightarrow{\delta} (I, v + \delta)$
  - discrete action: $(I, v) \to (I', v') \iff \exists (I, c, Y, I') \in E$ s. t. $v \models c, v' = v[Y := 0]$

上述定义未涵盖 invariants 的部分

> invariants 可以看作一个从 location 到 constraint 的函数

Reachability Problem

TA 的某个 location I 的可达性是一个 PSPACE-complete 的问题

其可判定性通过 region construction 得出，其基本思想为某些 clock valuation 是等价的，故可以将不可数的 clock valuation 划分为有限个等价类，基于等价类判断可达性

首先考虑 $d \in \mathbb{R}$ ，则可定义 $\lfloor d \rfloor$ 为 d 的整数部分，$fr(d)$ 为 d 的小数部分

则两个 clock valuation $v \cong v'$ 表示对于 TA 来说其不可区分（bisimulation）

令 c_x 为 constraints 中与 clock x 所比较的常数中最大的一个，则 $v \cong v'$ 表示对所有 x, y 满足

- $v(x) \geqslant c_x \wedge v'(x) \geqslant c_x$ 或是 $\lfloor v(x) \rfloor = \lfloor v'(x) \rfloor$
- $v(x) \leqslant c_x \Rightarrow fr(v(x)) = 0 \iff fr(v'(x)) = 0$
- $v(x) \leqslant c_x \wedge v(y) \leqslant c_y \Rightarrow fr(v(x)) \leqslant fr(v(y)) \iff fr(v'(x)) \leqslant fr(v'(y))$

则所有等价的 v 组成等价类 $[v]$ ，称为 region，其数量最多为

$$|X|! \times 2^{|X|} \times \prod_{x \in X} (2c_x + 2)$$

Hybrid System

HS 是既有 discrete 部分又有 continuous 部分的系统