Capítulo 5: Sistemas Híbridos

Introdução

Sistemas ciber-físicos formam uma classe de sistemas dinâmicos cujo comportamento alia uma **componente discreta**, análoga ao de uma máquina de estados, a uma **componente contínua** análogo ao de um sistema de controlo automático.

A componente discreta traduz o nível de *comportamento de controlo* e é modelada por sistema de transições Σ definido da forma usual por um espaço de estados Q, uma relação de transição δ e um estado inicial $m_0 \in \mathrm{Q}$.

A comportamento contínua traduz o nível de *comportamento local.* Esses são comportamentos específicos de cada um dos estados $m \in \mathrm{Q}$. Os comportamentos locais usualmente são determinados por leis físicas e por isso são modelados por equações ou relações envolvendo grandezas que evoluem continuamente.

Adicionalmente o comportamento local lida explicitamente com uma ou mais grandezas que modelam o *tempo*. Ao contrário dos sistemas de transição, onde as transições de estado existem sem ligação a nenhum referencial de tempo (um "relógio"), no comportamento local existe pelo menos um "relógio mestre" em relação ao qual todos os eventos e mudanças de estado estão ligados.

Os **autómatos híbridos ("hybrid automata", HA)** são modelos particulares de sistemas ciber-físicos em que a componentes discreta é definida por uma máquina de estados finita (FSM) e a componente contínua é descrita por equações ou relações diferenciais. Nestes sistemas existe um único referencial de tempo global a todos os comportamentos locais.

A característica essencial dos HA's, que os distingue dos sistemas híbridos mais genéricos, é a ausência de concorrência interna. Como o referencial de tempo é global, existe uma única linha de tempo onde todas as transições de estado ocorrem. Por isso a semântica de um HA pode ser sempre definida por traços.

Os **sistemas híbridos ("hybrid systems", HS)** são modelos constituídos por vários HA's que, em princípio, evoluem de forma "quase-independente"; a única dependência manifesta-se no sincronismo de duas ou mais transições em autómatos distintos.

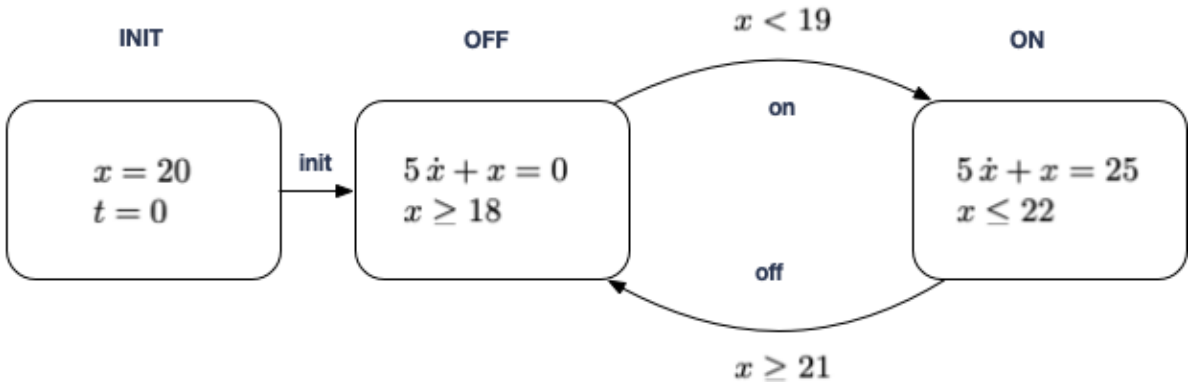
Nesses sistemas cada componente HA pode ter o seu próprio relógio mas existe sempre um referencial de tempo (“relógio mestre”) com o qual os restantes relógios sincronizam.

Antes de uma definição formal e uma análise do comportamento vamos ilustrar ambos os modelos com um exemplo simples:

> *Modelar um sistema de controlo de temperatura (de um reactor, de uma casa, etc.) efetuado por um termostato e uma fonte de calor e um contador para medir a energia consumida.*

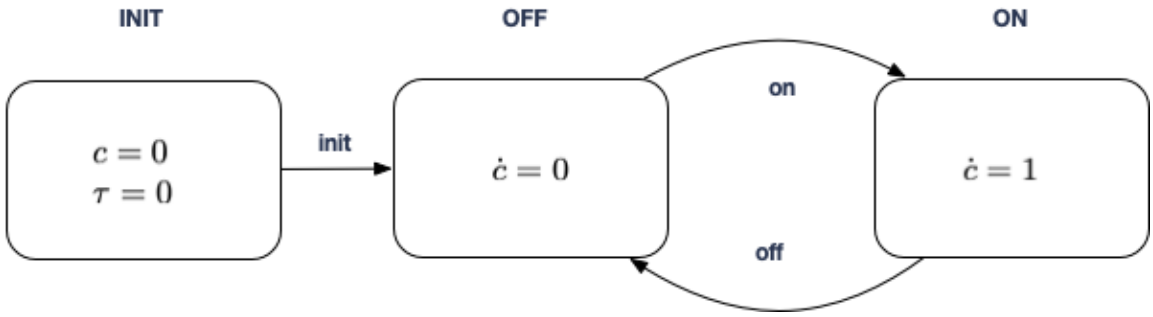
Este sistema vai ser modelado por dois autómatos híbridos: um para descrever o termostato e a fonte de calor e outro para descrever o contador.

O primeiro é representado no seguinte diagrama:



Termostato

O contador tem uma diagrama análogo mas relações mais simples



Contador

A FSM em cada um destes autómatos tem três estados identificados do mesmo modo: **INIT** , **OFF** e **ON**. Na terminologia dos autómatos híbridos os estados da FSM designam-se por **estados de controlo** ou **modos de funcionamento** (ou, simplesmente, **modos**). Numa versão mais geral de um "Control Flow Automaton" *modos* tomam a designação de **locais**.

Os autómatos têm, associados às transições, marcas designadas por **eventos**. Cada transição é marcada por um e só um evento mas transições diferentes podem ser marcadas pelo mesmo evento. Neste exemplo ambos os autómatos têm o mesmo conjunto de eventos: $\{\mathbf{init}, \mathbf{off}, \mathbf{on}\}$.

A componente contínua de um HA é determinada por dois tipos de predicados: **flows** e **jumps**.
Existe um **flow** para cada modo e um **jump** para cada transição.

Ambos predicados são definidos sobre um conjunto de variáveis continuas, uma das quais denota o **tempo**. Neste exemplo, para além de dois tempos distintos (t e τ um para cada autómato), temos a variável x , que no termostato denota a temperatura que se pretende controlar, e a variável c, que no contador denota o valor acumulado dos custos de energia.
Genericamente, em cada autómato híbrido, denotemos por X o vetor contendo todas as variáveis contínuas. No termostato tem-se $\mathrm{X} \equiv (x, t)$ e no contador $\mathrm{X} \equiv (c, \tau)$.

O **flow** de um determinado modo de funcionamento é um conjunto de relações envolvendo a variável X e o vetor $\dot{\mathrm{X}}$ das suas derivadas em ordem ao tempo. Este predicado estabelece restrições na forma como os valores das variáveis evoluem com o tempo.

Os **jumps**, tal como os eventos, estão associados às transições. São predicados onde ocorrem as variáveis X (antes da transição) e X' (após a transição). Quando uma variável $x' \in \mathrm{X}'$ não aparece no "jump" está implícita uma equação $x' = x$ indicando que o valor da variável x não é modificado no acto de transição.

Neste modelo o papel dos eventos tem duas facetas:

- servem para caracterizar os traços do sistema e definir propriedades temporais nesses traços.
- servem para sincronizar as transições de um autómato com as transições de outro qualquer autómato que pertença ao mesmo sistema híbrido.

Os eventos são a única informação que é global a todos o sistema híbrido. Toda a outra informação tal como as variáveis de estado ou os modos são locais a cada autómato dentro do sistema.

Em particular, algo que é importante referir, é o facto de cada autómato híbrido ter o seu tempo próprio e as derivadas nesse autómato serem feitas em ordem a esse tempo. Todo o sincronismo entre os relógios internos de cada autómato tem de ser feito através do sincronismo de eventos.
Por isso os dois tempos podem avançar a "velocidades" diferentes; de facto é a "velocidade" do tempo τ em relação a t que estabelece quantas unidades de energia são acrescentadas a c por cada unidade e tempo t no modo **ON**.

Neste sistema cada um dos relógios locais t, τ pode servir de "relógio mestre"; a escolha de um deles vais depender da forma como este sistema interage com outros sistemas fora deste modelo.

Alguns comentários sobre este exemplo

1. No autómato **termostato** os fluxos ("flows") associados a cada um dos seus modos são baseados em uma variável x que represente a temperatura controlada e uma variavel t que denota o tempo.

Neste modelo assume-se que, por arrefecimento natural, a temperatura controlada decresce em 20% (isto é $\frac{1}{5}$) por cada unidade de tempo. Quando o sistema está no estado ON a temperatura controlado sobe, como causa exclusiva desse facto, 5 unidades de temperatura por cada unidade de tempo.

   a. O modo **INIT** existe para inicializar as variáveis através do fluxo $(t = 0) \wedge (x = 20)$.
   b. No modo **OFF** o recipiente controladoo fluxo é $(\dot{x} = -\frac{1}{5}x) \wedge (x \geq 18)$. O primeiro termo indica que a temperatura decresce proporcionalmente à temperatura: 20% em cada unidade de tempo. O segundo termo indica um limite mínimo de 18 unidades de temperatura: se o limite for ultrapassado o modo deixa de evoluir.
   c. No modo **ON** o fluxo é $(\dot{x} = 5 - \frac{1}{5}x) \wedge (x \leq 22)$. No primeiro predicado o acréscimo de temperatura por unidade de tempo é 5 menos 20% da temperatura; estes termos cancelam-se quando a temperatura for 25. Porém o segundo predicado do fluxo impõe um limite superior de 22 e, se o limite for ultrapassado, o modo deixa de evoluir.
   d. Note-se que, quando um modo deixa de evoluir, todas as variáveis deixam de evoluir, incluindo o tempo, e por isso o autómato fica bloqueado.

2. No autómato **contador** existem três modos que, por acaso têm o mesmo nome que os modos do autómato "termostato" mas isso não indica nenhuma ligação entre as duas classes de modos.
   a. No modo **INIT** inicializam-se as variáveis com o fluxo $(c = 0) \wedge (\tau = 0)$.
   b. No modo **OFF** o tempo τ evolui mas o contador está parado (já que o fluxo é $\dot{c} = 0$).
   c. No modo **ON** o tempo e o contador evoluem exatamente do mesmo modo ($\dot{c} = 1$).

3. Os "jumps" , em qualquer dos autómatos, não modificam o valor das variáveis: no "termoestato" está implícito um predicado $(x = x') \wedge (t = t')$ em cada transição e no "contador" está igualmente implícito $(c = c') \wedge (\tau = \tau')$ em cada transição.

4. As transições no "termoestato" são ativadas ("triggered") por predicados. O predicado $(x < 19)$ ativa a transição $\mathrm{OFF} \rightarrow \mathrm{ON}$ enquanto que $(x \geq 21)$ ativa a transição $\mathrm{ON} \rightarrow \mathrm{OFF}$. As transições no autómato "contador" são activadas pelo sincronismo com os eventos que partilham com o "termoestato".

5. O sistema é ativado pelo evento $\mathbf{init}$; esse evento é partilhado também com um agente/autómato externo (um "switch") que controla o início do seu funcionamento.

Dissemos que os eventos são a única informação global de um sistema híbrido e, por isso, partilhada pelos diferentes autómatos que o constituem. Neste exemplo o conjunto $\{\mathbf{init}, \mathbf{on}, \mathbf{off}\}$ é essa informação global; ao contrário dos identificadores dos modos, os identificadores dos eventos identificam a mesma entidade em qualquer dos autómatos do sistema.
O significado que se pretende capturar é o do simultaneidade:

> *todas as transições, nos diferentes autómatos do sistema, marcadas com o mesmo evento ocorrem simultaneamente.*

Como resultado de transições diferentes para o mesmo evento, em cada autómato as variáveis alteram os valores de forma distinta.

É importante referir que a classe dos sistemas dinâmicos referidos como ciber-físicos contém outros tipos de modelos de comportamento que não podem ser descritos por autómatos/sistemas híbridos. Normalmente são modelos que contêm algumas das componentes dos sistema híbridos mas adicionalmente definem uma lógica específica para modelar o comportamento.

O modelo autómato/sistema híbrido, que iremos apresentar neste capítulo, não usa lógicas específicas e é uma extensão simples dos modelos FOTS/CFA's que estudámos anteriormente.
Porém, para isso a componente contínua do comportamento necessita de ser integrada na abordagem FOTS/CFA's através de um mecanismo que designamos por **discretização**. A função deste mecanismo é o de transformar comportamentos contínuos, descritos por variáveis continuas (incluindo o tempo) e equações diferenciais, em sistemas discretos do tipo FOTS/CFA's que usam relações de transição de estados para descrever as trajetórias definidas por equações diferenciais.

Definição e descrição dos autómatos híbridos

Para ser possível verificar propriedades temporais nestes sistemas dinâmicos vamos apresentar um processo sistemático para converter um autómato ou um sistema híbrido num FOTS e transferir para tal modelo as propriedades que se pretendem verificar.

Definiçao

Um **autómato híbrido** $\mathrm{A} \equiv \langle \mathrm{X}, \Sigma, F, J, E \rangle$ consiste nas seguinte componentes:

- Um conjunto de variáveis contínuas X, uma das quais designa o tempo. Clones $\dot{\mathrm{X}}$ e X' denotam, respetivamente, o conjunto das respetivas derivadas em ordem ao tempo, nas transições contínuas, e "no próximo estado" nas transições discretas. O conjunto X contém sempre uma variável (normalmente representada por t, τ ou T) que designa o *tempo*.
- Uma máquina de estados finita $\Sigma \equiv \langle Q, \delta, I \rangle$ cujos estados $m \in Q$ se designam por **modos** ou **locais** e cujas transições $\sigma \in \delta$ se designam por **"jumps"** . Como em qualquer FSM, a definição completa-se com o conjunto de estados iniciais I .
- Um dicionário F que associa cada modo $m \in Q$ a um predicado flow_m cujas variáveis livres pertencem a $\mathrm{X} \cup \dot{\mathrm{X}}$.
- Um dicionário J que associa cada $\sigma \in \delta$ a um predicado switch_σ cujas variáveis livres pertencem a $\mathrm{X} \cup \mathrm{X}'$.
- Um conjunto finito E de símbolos, designados por "eventos" e uma função $\mathrm{ev}: \delta \to E$ que associa cada "jump" a um evento.

Restrições

1. O conjunto de estados iniciais I tem um único elemento INIT .

2. O conjunto de eventos E contém o evento init, que marca todas as transições com origem INIT, e o evento blocked que marca todas as pseudo-transições bloqueadas.
3. O fluxo $\text{flow}_{\text{INIT}}$ tem apenas as variáveis livres em X.

Nota
As definições de autómato híbrido diferem em alguns pormenores dependendo das fontes. A versão aqui apresentada parece-me a mais simples que capta todos os comportamentos que tipicamente estão associados a estes sistemas dinâmicos.

Descrição do autómato híbrido através de um FOTS

Um modelo de comportamento de um autómato híbrido deve ser um sistema de transições de 1ª ordem (FOTS)

$$\text{H} \equiv \langle Z, \mathbf{T}, \mathbf{I} \rangle$$

1. As variáveis de estado Z têm valores com a forma de um triplo
   $$z = (m, x, t)$$
   em que $m \in Q$ é o modo ativo neste estado, x é o estado das variáveis contínuas (com excepção do tempo) e t denota o estado do relógio local.

Como primeira aproximação vamos considerar o autómato isolado sem sincronismo com qualquer outro autómato. Por isso, por enquanto, vamos ignorar o papel dos eventos.

2. A relação $\mathbf{I}$, dadas as restrições impostas na inicialização do autómato híbrido é
   $$\mathbf{init}(m, x, t) \equiv (m = \text{INIT}) \wedge \text{flow}_{\text{INIT}}(x) \wedge (t = t_0)$$
   sendo t_0 uma constante que define o valor inicial do relógio local.

1. A relação de transição $\mathbf{T}$ é um predicado nas variáveis Z e Z' que agrega três tipos de transições:
   a. **transições contínuas** dentro de um mesmo modo m, designadas por $\mathbf{timed}_m$, e determinados pelas relações de fluxo flow_m.
   b. **transições discretas** entre dois modos m, m', designadas por $\mathbf{untimed}_{(m,m')}$, e determinadas pelos "jumps" $\text{jump}_{(m,m')}$.
   c. pseudo-transições $\mathbf{blocked}_m$ que corresponde ao bloqueio (não evolução) de todas as componentes do estado excepto o tempo.

Concretamente

a. As transições $\mathbf{timed}_m$ indexadas pelos modos $m \in Q$ têm a forma

$$(m, x, t) \xrightarrow{\tau} (m, x', t')$$

e estão associadas a uma duração temporal $\tau \equiv t' - t > 0$.

A transição ocorre sse existe uma função diferenciável y que verifica $\text{flow}_m(y, \dot{y})$ no intervalo de tempo $[0, \tau]$, com $y(0) = x$ e $y(\tau) = x'$.

b. As transições $\mathbf{untimed}^{(e)}_{(m,m')}$ indexadas pelos "jumps" $(m, m') \in \delta$

$$(m, x, t) \xrightarrow{e,\tau} (m', x', t')$$

estão associadas a um evento $e \in E$ e a uma duração temporal $\tau \equiv t' - t \geq 0$.

As transições são agrupadas por eventos

$$\mathbf{untimed}^{(e)}_{m,m'}(x, x') \equiv \text{switch}_{(m,m')}(x, x')$$

sendo $e = \text{ev}(m, m')$

c. As transições $\mathbf{blocked}_m$ indexadas pelos modos $m \in Q$ têm a forma

$$(m, x, t) \xrightarrow{b,\infty} (m, x, \infty)$$

em que b é o evento blocked.

4. Uma vez definidas todas estas transições, a relação de transição global é

$$\mathbf{T} \equiv (\bigvee_{m \in Q} \mathbf{timed}_m) \vee (\bigvee_{m \in Q} \mathbf{blocked}_m) \vee (\bigvee_{e \in E} \bigvee_{(m,m') \in \delta} \mathbf{untimed}^{(e)}_{(m,m')})$$

Para a análise do comportamento individual de um único autómato híbrido esta é a forma usual de construir a relação de transição no FOTS. Porém, quando se descreve um sistema híbrido formado por vários autómatos é necessário lidar diretamente com as transições $\mathbf{untimed}^{(e)}$ para os diferentes eventos.

Como sempre, um traço é uma sequência infinita de estados $z \equiv \langle z_0, \cdots, z_i, \cdots \rangle$ que definem transições

$$\alpha_i \xrightarrow{-,\tau_i} \alpha_{i+1}$$

de um dos dois primeiros tipos acima. O traço é **não-nulo** quando a série $\sum_{i \geq 0} \tau_i$ diverge; equivalentemente, quando a série não for limitada.

No estudo de sistemas ciber-físicos realistas só são relevantes os traços não-nulos. Um traço em que a série $\sum_{i \geq 0} \tau_i$ converge ou quase (no sentido em que cresce muito

lentamente) não é um bom modelo porque indica "que há um fim do tempo". Computacionalmente as transições de estado vão-se tornando cada vez mais frequentes sem que exista uma evolução realistas do relógio

Discretização das transições continuas

Para codificar as transições "timed" recordemos que, para uma duração temporal $\tau > 0$ num modo m, com $z = (m, x, t)$ e $z' = (m, x', t + \tau)$, existe a transição

$$\mathbf{timed}_m(z, z')$$

se e só se existe uma função y diferenciável no intervalo $[0, \tau]$ tal que $y(0) = x$, $y(\tau) = x'$
e, para todo $s \in [0, \tau]$ é válida $\mathrm{flow}_m(y(s), \dot{y}(s))$.

Construir uma forma explícita para $\mathbf{timed}_m(z, z')$ é a parte crítica desta codificação; designa-se tal construção por **discretização** da relação flow_m.

Não existe uma forma universal de a realizar: de facto discretizar uma relação diferencial vai sempre depender da forma dessa relação. Na secção seguinte analisaremos algumas formas comuns (e simples) de relações diferenciais e as respetivas discretizações.

Por simplicidade vamos considerar relações de fluxo em que o estado tem apenas duas componentes contínuas: o tempo t e uma outra quantidade x, ambas tomam valores nos números racionais. O mecanismo é facilmente generalizável para casos em que x é vetorial.

Vamos ver algumas formas particulares de relações diferenciais $f(x, \dot{x})$, onde o tempo não aparece explicitamente. Porém na discretização $\hat{f}(x, t, x', t')$ é necessário referir explicitamente o tempo. Assim, as variáveis x, x' contêm os valores inicial e final da solução e as variáveis t, t' contêm os valores inicial e final do intervalo da solução.

1. $f(x, \dot{x}) \equiv (\dot{x} = c)$ sendo c uma qualquer constante racional.

   Neste caso a solução $y(t)$ é uma função linear $y(s) = x + c * (s - t)$. Por isso a relação discretizada será

$$\hat{f}(x,t,x',t') \equiv (x'-x) = c * (t'-t)$$

Note-se que as variáveis x, x', t, t' nesta relação aparecem sempre em somas e multiplicações escalares. Por isso a relação pode ser decidível.

Esta relação não está completa porque falta impor restrições que assegurem que os traços são não-nulos: temos de assegurar que se verifica $t' \geq t$.
Aliás, para maior segurança, pode-se fixar (como constante da codificação) um limite mínimo à duração das transições "timed". Seja $\lambda > 0$ tal limite; então a codificação será

$$\hat{f}(x,t,x',t') \equiv ((x'-x) = c * (t'-t)) \wedge (t'-t \geq \lambda)$$

2. $f(x,\dot{x}) \equiv (\dot{x} = c) \wedge (x \leq b)$ sendo c, b constantes racionais arbitrárias.

A discretização é análoga ao caso anterior impondo uma restrição $\forall\, s \in [t,t'] \cdot y(s) \leq b$. Para traduzir essa restrição basta impor $(x' \leq b)$ e $(x \leq b)$.
A discretização será

$$\hat{f}(x,t,x',t') \equiv ((x'-x) = c * (t'-t)) \wedge (x \leq b) \wedge (x' \leq b) \wedge (t'-t \geq \lambda)$$

3. $f(x,\dot{x}) \equiv (\dot{x} = c) \wedge (a \leq x \leq b)$ sendo c, b, a constantes.

A discretização é análoga à anterior mas introduzindo um limite inferior nos valores da solução

$$\hat{f}(x,t,x',t' \equiv ((x'-x) = c * (t'-t)) \wedge (a \leq x \leq b) \wedge (a \leq x' \leq b)) \wedge (t'-t \geq \lambda)$$

4. $f(x,\dot{x}) \equiv (\dot{x} + x = c)$ sendo c uma qualquer constante racional.

Esta equação diferencial não pode ser codificada da forma usada no caso anterior.
Uma pseudo-solução passaria por aproximar a derivada por um quociente de diferenças

$$\dot{x} \equiv \lim_{\tau \to 0} (x(t+\tau) - x(t))/\tau$$

o que levava à aproximação

$$\dot{x} \simeq (x'-x)/(t'-t)$$

Substituindo na equação diferencial obtém-se

$$(x'-x) + x * (t'-t) = c * (t'-t)$$

Nesta equação ocorre um produto não-escalar $x * (t' - t)$ e, por isso, mesmo nos inteiros ela não vai ser decidível.

Quase sempre esta equação diferencial não ocorre isoladamente no fluxo. Tomando como exemplo o termostato, a equação aparece acompanhada por restrições nos valores de x. São frequentes fluxos de uma das formas

- $f \equiv (\dot{x} + x = c) \wedge (x \leq b)$
- $f \equiv (\dot{x} + x = c) \wedge (a \leq x \leq b)$

com a, b, c constantes.

Cada uma destas formas sugere uma forma de substituir, na equação diferencial, o valor da variável x por uma constante.

No primeiro caso pode-se substituir $f \equiv (\dot{x} + x = c) \wedge (x \leq b)$ por uma relação

$$g \equiv (\dot{x} + b \geq c) \wedge (x \leq b)$$

Obviamente, uma solução de f também é uma solução de g e, por isso, uma eventual discretização de f será sempre mais forte que uma discretização de g. No entanto, a primeira não é possível realizar enquanto que a segunda é.

De facto g tem a forma similar à do exemplo 2. com a diferença que a equação diferencial é substituída por uma relação diferencial $(\dot{x} \geq c - b)$.
Na discretização basta substituir o 1º termo, a equação $(x' - x) = c * (t' - t)$ por $(x' - x) \geq (c - b) * (t' - t)$.

Na forma mais geral $f \equiv (\dot{x} + x = c) \wedge (a \leq x \leq b)$, pelos mesmo motivos indicados acima, começamos por substituir f por

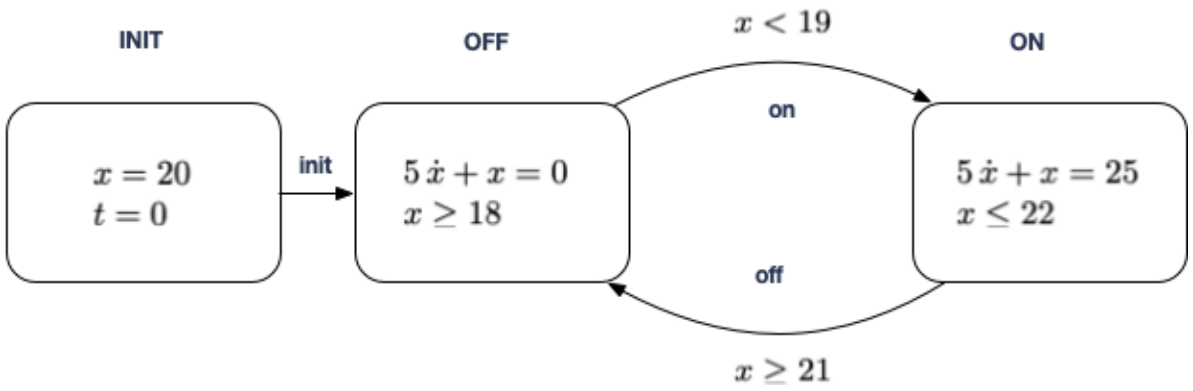
$$g(x, \dot{x}) \equiv (\dot{x} + b \geq c) \wedge (\dot{x} + a \leq c) \wedge (a \leq x \leq b)$$

A discretização desta relação será

$$\hat{g}(x, t, x', t') \equiv \begin{cases} ((x' - x) \leq (c - a) * (t' - t)) & \wedge \\ ((x' - x) \geq (c - b) * (t' - t)) & \wedge \\ (a \leq x \leq b) \wedge (a \leq x' \leq b) & \wedge \\ (t' - t \geq \lambda) \end{cases}$$

Exemplo

Vamos analisar de novo os autómatos híbridos descrevendo o termostado e o contador e criar, para cada um, a sua descrição num FOTS



Descrição FOTS do "Termostato"

Teoria T

Uma SMT que agrupe inteiros e números racionais

Estado: $\mathrm{X} \equiv (m, x, t)$

O estado é determinado por uma variável discreta m, que regista os modos, e por variáveis racionais t e x que registam o tempo e a temperatura.

Predicado $\mathbf{init}(\mathrm{X})$

O estado inicial é formado pelo modo INIT e pelo fluxo associado a esse modo.

$\mathbf{init}(m, t, x) \equiv (m = \mathrm{INIT}) \wedge (t = 0) \wedge (x = 20)$

Predicado $\mathbf{trans}(\mathrm{X}, \mathrm{X}')$

As transições **"untimed"** estão associadas aos eventos $e \in \{\mathrm{init}, \mathrm{on}, \mathrm{off}\}$

$\mathbf{untimed}_{\mathrm{init}}(\mathrm{X}, \mathrm{X}') \equiv (m = \mathrm{INIT}) \wedge (m' = \mathrm{OFF}) \wedge (t' = t) \wedge (x' = x)$

$\mathbf{untimed}_{\mathrm{on}}(\mathrm{X}, \mathrm{X}') \equiv (m = \mathrm{OFF}) \wedge (m' = \mathrm{ON}) \wedge (x < 19) \wedge (t' = t) \wedge (x' = x)$

$\mathbf{untimed}_{\mathrm{off}}(\mathrm{X}, \mathrm{X}') \equiv (m = \mathrm{ON}) \wedge (m' = \mathrm{OFF}) \wedge (x \geq 21) \wedge (t' = t) \wedge (x' = x)$

As transições "timed" estão associadas aos modos $m \in \{\mathrm{OFF}, \mathrm{ON}\}$

$$\mathbf{timed}_{\mathrm{OFF}}(\mathrm{X},\mathrm{X}') \equiv \begin{cases} 5\,(x'-x) \le -18\,(t'-t) & \wedge \\ (x' \ge 18) \wedge (x \ge 18) & \wedge \\ t' > t \end{cases} \quad \text{com} \quad \mathrm{X} \equiv (m,x,t)$$

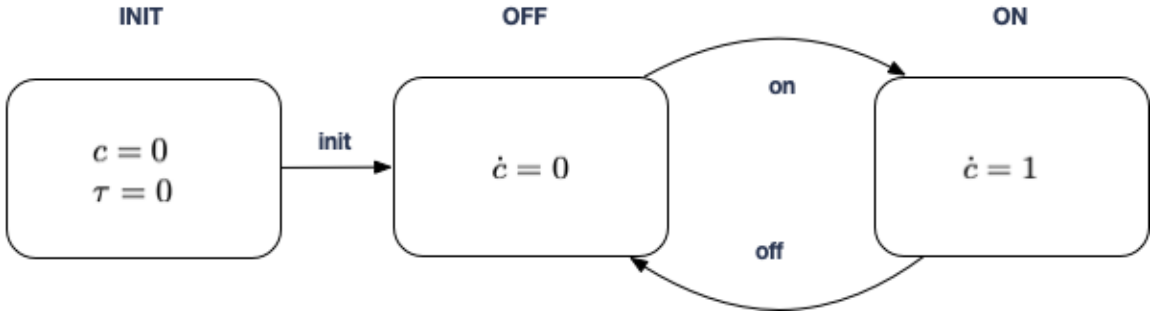
$$\mathbf{timed}_{\mathrm{ON}}(\mathrm{X},\mathrm{X}') \equiv \begin{cases} 5\,(x'-x) \ge 3\,(t'-t) & \wedge \\ (x \le 22) \wedge (x' \le 22) & \wedge \\ t' > t \end{cases} \quad \text{com} \quad \mathrm{X} \equiv (m,x,t)$$

No modo OFF o fluxo é $(5\,\dot{x}+x=0) \wedge (x \ge 18)$ que força $(5\,\dot{x}+18 \le 0) \wedge (x \ge 18)$. Esta aproximação discretiza-se como apresentado acima.
No modo ON o fluxo é $(5\,\dot{x}+x=25) \wedge (x \le 22)$ que força $(5\,\dot{x}+22 \ge 25) \wedge (x \le 22)$.

Para construir a relação de transição, no contexto de um só autómato híbrido, basta fazer a disjunção de todas estas transições específicas

$$\mathbf{trans}(\mathrm{X},\mathrm{X}') \equiv \bigvee_{e \in \{\mathrm{init},\mathrm{on}\,\mathrm{off}\}} \mathbf{untimed}_e(\mathrm{X},\mathrm{X}') \vee \bigvee_{m \in \{\mathrm{OFF},\mathrm{ON}\}} \mathbf{timed}_m(\mathrm{X},\mathrm{X}')$$

Descrição FOTS do "Contador"



Teoria T

Uma SMT que agrupe inteiros e números racionais; a mesma que no "termostato"

Estado: $\mathrm{Y} \equiv (n,c,\tau)$

O estado é determinado por uma variável discreta n, que regista os modos, e por variáveis racionais τ e c que registam o tempo e a contagem.

Predicado $\mathbf{init}(\mathrm{Y})$

O estado inicial é formado pelo modo INIT e pelo fluxo associado a esse modo.

$$\mathbf{init}(\mathrm{Y}) \equiv (n = \mathrm{INIT}) \wedge (\tau = 0) \wedge (c = 0) \qquad \text{com } \mathrm{Y} \equiv (n, \tau, c)$$

Predicado $\mathbf{trans}(\mathrm{X}, \mathrm{X}')$

As transições **"untimed"** estão associadas aos eventos $e \in \{\mathrm{init}, \mathrm{on}, \mathrm{off}\}$

$$\mathbf{untimed}_{\mathrm{init}}(\mathrm{Y}, \mathrm{Y}') \equiv (n = \mathrm{INIT}) \wedge (n' = \mathrm{OFF}) \wedge (\tau' = \tau) \wedge (c' = c)$$

$$\mathbf{untimed}_{\mathrm{on}}(\mathrm{Y}, \mathrm{Y}') \equiv (n = \mathrm{OFF}) \wedge (n' = \mathrm{ON}) \wedge (\tau' = \tau) \wedge (c' = c)$$

$$\mathbf{untimed}_{\mathrm{off}}(\mathrm{Y}, \mathrm{Y}') \equiv (n = \mathrm{ON}) \wedge (n' = \mathrm{OFF}) \wedge (\tau' = \tau) \wedge (c' = c)$$

As transições **"timed"** estão associadas aos modos $m \in \{\mathrm{OFF}, \mathrm{ON}\}$

$$\mathbf{timed}_{\mathrm{OFF}}(\mathrm{Y}, \mathrm{Y}') \equiv (c' - c = 0) \wedge (\tau' - \tau > 0)$$

$$\mathbf{timed}_{\mathrm{ON}}(\mathrm{Y}, \mathrm{Y}') \equiv (c' - c = \tau' - \tau) \wedge (\tau' - \tau > 0)$$

Por si só o autómato "contador" tem um comportamento trivial: o estado alterna entre ON e OFF mantendo sempre o contador c igual a zero e a duração da transição $\tau' - \tau$ sempre 0.

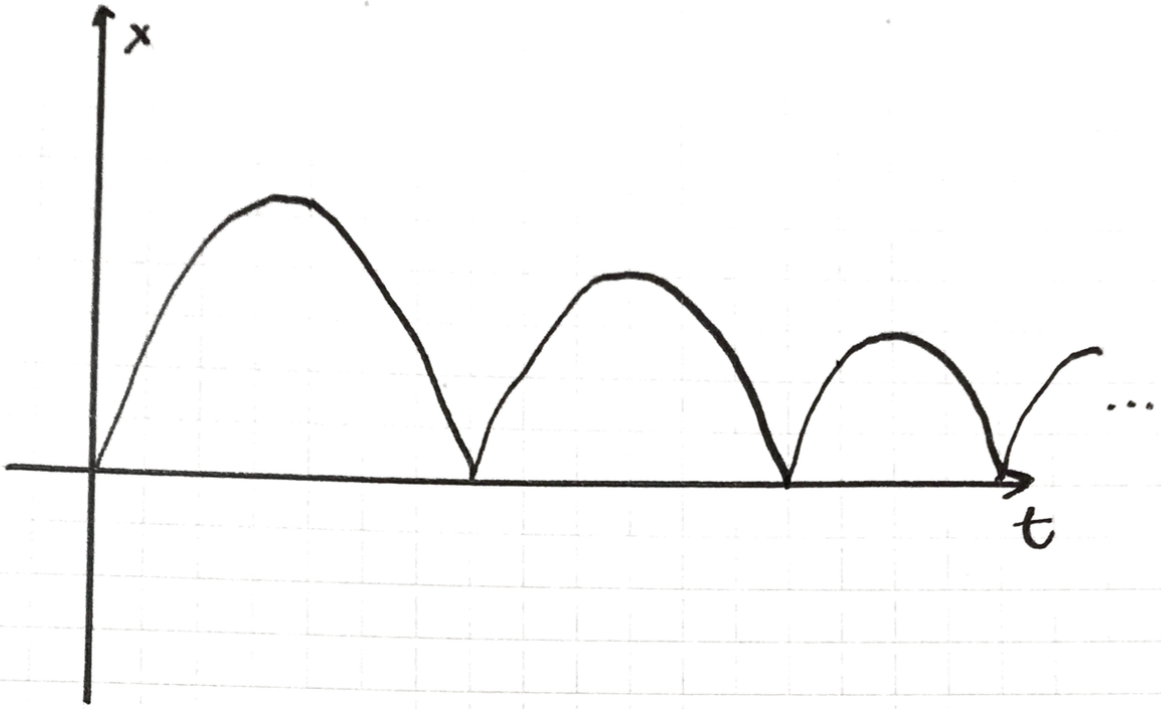
Este autómato so desempenha o seu papel quando sincroniza com o autómato "termostato" através dos eventos comuns. Esta noção de "sincronização" é o mecanismo essencial que serve para construir sistemas híbridos a partir de autómatos híbridos; designa-se por **composição** de autómatos e vamos estudá-la em seguida.

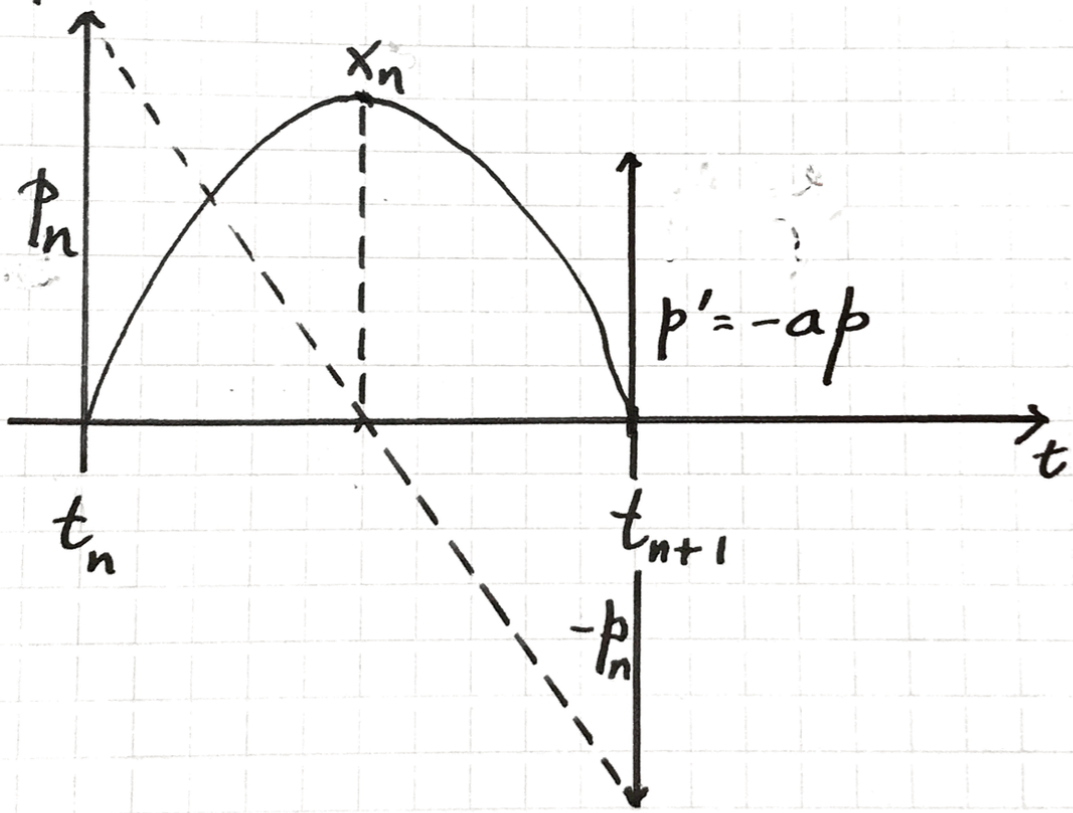
Trajetórias de Zenão/Zeno

O Paradoxo de Achiles e a Tartaruga é um dos clássicos paradoxos apresentados por Aristóteles como fundamentais à noção de contínuo. Na análise de autómatos híbridos este paradoxo pode ser ilustrado pelos traços de um autómato que comuta entre dois estados um número infinito de vezes em um qualquer intervalo de tempo não nulo mas arbitrariamente pequeno.

Um exemplo paradigmático de um tal autómato é genericamente conhecido por **“bouncing ball”** . Para além de um local de inicialização, o autómato tem dois locais: B (“bouncing”) e F (“floor”)

- No modo B uma bola elástica move-se sob o efeito da gravidade sem qualquer perda de energia devido a atritos.
- No modo F a bola tem impacto com o solo; o momento inverte o sentido e a grandeza do momento perde alguma velocidade.





$$m \frac{dx}{dt} = p$$

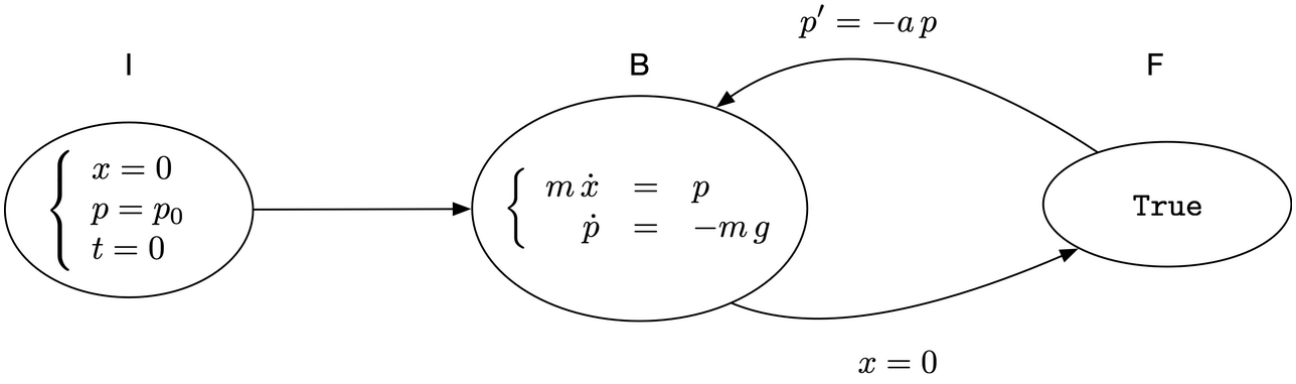
$$\frac{dp}{dt} = -mg$$

Para além da variável tempo t o sistema físico é caracterizado por outras duas grandezas contínuas: a **posição** x e o **momento** p.
Adicionalmente a relação entre estas grandezas é controlada por duas constantes: a **massa** da bola m, e a aceleração da gravidade g.

- No modo B as leis do movimento são descritas por duas equações diferencias
  - $m\dot{x} = p$; *definição de momento*: a massa vezes a velocidade é o momento
  - $\dot{p} = -mg$; *lei de Newton*: a derivada do momento é igual à força que actua na bola; isto é, a massa vezes a aceleração da gravidade.
- No modo F dá-se o impacto da bola no solo ($x = 0$) , o momento muda de direção e diminui de grandeza por perda de energia; a posição da bola e o tempo não mudam.
  - $p' = -ap$

  A constante $a < 1$ é um racional positivo que relaciona a grandeza do momento antes e depois do impacto.
- No estado inicial assume-se que a bola está no solo $(x = 0)$ mas tem um momento positivo $p_0 > 0$.

O autómato híbrido pode ser descrito no seguinte diagrama



Como é usual, as variáveis que não aparecem explicitamente nos "jumps" mantém o seu valor durante a transição de modo.

Para interpretar de forma discreta o comportamento deste autómato enumera-se os instantes de impacto numa sequência de tempos $\{t_n\}_{n\geq 0}$. Assume-se $t_0 = 0$.
O valor do momento no instante t_n é representado por p_n e a altura máxima da bola a seguir a t_n é representado por x_n. A figura anterior ajuda a interpretar estas grandezas.

A integração das equações do movimento e a relação entre momentos conduz facilmente às seguinte relações

$$\begin{cases} p_n &= a^n p_0 \\ (t_{n+1} - t_n) &= 2p_n/mg \\ x_n &= (g/8)(t_{n+1} - t_n)^2 \end{cases}$$

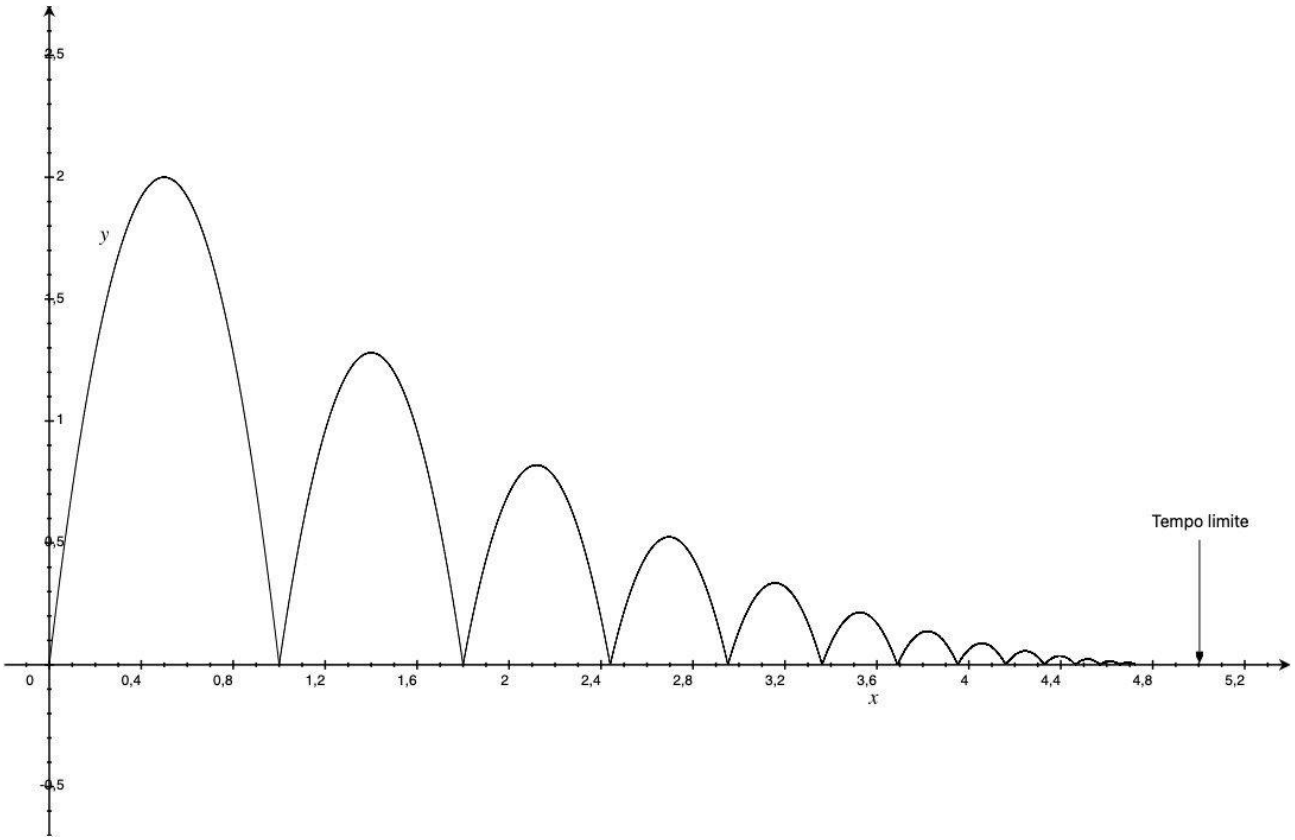
Como $0 \leq a < 1$, os momentos decrescem exponencialmente com n. O intervalo entre dois instantes de impacto são proporcionais aos momentos e portanto também decrescem exponencialmente com n. Finalmente as alturas máximas x_n decrescem exponencialmente com o dobro de n.

Tal como o paradoxo de Zenão, os momentos p_n, os intervalos $(t_{n+1} - t_n)$ entre instantes de impacto e as alturas máximas x_n vão diminuindo mas nunca chegam a zero. Aparentemente Aquiles nunca alcança a tartaruga.

Note-se que existe um limite finito para a sequência de tempos t_n: assumindo $t_0 = 0$, tem-se

$$\lim_{n\to\infty} t_n = \sum_{n=0}^{\infty} (t_{n+1} - t_n) = (2p_0/mg)\left(\sum_{n=0}^{\infty} a^n\right) = (2p_0/mg)(1-a)^{-1} < \infty$$

Temos aqui a essência do **paradoxo de Zenão**: um sistema em que, num intervalo de tempo finito, possui um número infinito de transições de estado.



Para corrigir este paradoxo pode-se seguir várias estratégias. Por exemplo pode-se impor um valor mínimo no momento p para que se efectue a transição do modo F para o modo B. Para isso o jump deve ser modificado para algo da forma

$$\mathrm{switch}_{(\mathrm{F,B})} \equiv (p' = -a\,p) \wedge (p' \geq \lambda)$$

sendo $\lambda > 0$ um valor mínimo para um impulso que conduza a bola a uma trajetória ascendente.

Quando o valor do momento p' descer abaixo de λ, então $\mathrm{switch}_{(\mathrm{F,B})}$ não é válido e o sistema fica bloqueado no estado F. Neste modelo o número de transições de estado é sempre finito.

Em alternativa pode-se impor um tempo mínimo para efectuar a transição do modo F para o modo B. Para isso modifica-se o respetivo jump para

$$\mathrm{switch}_{(\mathrm{F,B})} \equiv (p' = -a\,p) \wedge (t' = t + \tau)$$

sendo $\tau > 0$ o tempo constante que demora a transição.

Neste modelo, como τ é não-nulo, um número infinito de mudanças de estado requer sempre um intervalo de tempo infinito.

Os limites definidos nestas duas alternativas não são impostos arbitrariamente mas têm um significado físico. Nomeadamente

1. O valor mínimo do momento relaciona-se com o atrito estático: em qualquer movimento existe sempre um momento mínimo necessário para vencer o atrito associado a uma mudança na orientação.
2. O valor mínimo no tempo de transição está relacionado com os limites físicos impostos à velocidade com que a informação viaja. A ocorrência da transição é um *efeito* derivado de uma *causa:* neste caso, a mudança de estado. Qualquer relação *causa* $\longrightarrow$ *efeito* implica uma comunicação de informação, e qualquer comunicação tem *tempos de latência* mínimos.

Composição de Autómatos Híbridos.

Vimos anteriormente que um sistema híbrido $\mathrm{H} \equiv \{\mathrm{A}_1, \cdots, \mathrm{A}_\ell\}$ que partilham o mesmo conjunto de eventos E. A **composição** de autómatos é uma forma particular de sistema híbrido formada apenas por dois autómatos.

Tem-se

$$\mathrm{H} \equiv \mathrm{A}_0 \otimes \mathrm{A}_1$$

em que

$$\mathrm{A}_i \equiv \langle \mathrm{X}_i, \Sigma_i, F_i, J_i, E \rangle \qquad i \in \{0, 1\}$$

Portanto os dois autómatos partilham o conjunto de eventos E.

Para efeitos do eventual sincronismo entre estes dois autómatos vamos recordar alguma terminologia:

- Vamos representar por $X_i \equiv (m_i, t_i, S_i)$ o estado das transições do autómato A_i. Nesse estado X_i incluímos explicitamente o modo m_i, o tempo próprio t_i e o valor S_i do vetor X_i excluído da componente do tempo.

- Qualquer transição contínua ("timed") no autómato A_i é marcada

$$X_i \xrightarrow{\tau_i} X_i'$$

identificando a duração do evento $\tau_i \equiv t_i' - t_i$. Aqui verifica-se sempre $m_i' = m_i$.

- Qualquer transição discreta ("untimed") nesse autómato é marcada

$$X_i \xrightarrow{e,\tau_i} X_i'$$

identificando não só a duração $\tau_i \equiv t_i' - t_i$ como também o evento que lhe está associado.

As **regras de sincronismo** são

1. O estado genérico da composição $\mathrm{H} \equiv \mathrm{A}_0 \otimes \mathrm{A}_1$ tem a forma (X_0, X_1) em que X_i é estado de A_i.
2. Uma transição do autómato A_0 só sincroniza com uma transição do autómato A_1 quando ambas têm a mesma duração.
3. Adicionalmente, quando ambas as transições são discretas, elas só sincronizam quando estão associadas ao mesmo evento.

Destas regras resultam as seguintes possibilidades de sincronismo cada uma das quais determina uma transição no sistema H:

> *Ocorre a transição* $(X_0, X_1) \rightarrow (X_0', X_1')$ *quando ocorre uma das seguintes circunstâncias*
>
> - *Ocorrem transições discretas*
>
> $$X_0 \xrightarrow{e_0, \tau_0} X_0' \qquad e \qquad X_1 \xrightarrow{e_1, \tau_1} X_1'$$
>
> *com* $e_0 = e_1$ *e* $\tau_0 = \tau_1$ *.*
>
> - *Ocorrem transições contínuas*
>
> $$X_0 \xrightarrow{\tau_0} X_0' \qquad e \qquad X_1 \xrightarrow{\tau_1} X_1'$$
>
> *com* $\tau_0 = \tau_1$ *.*
>
> - *Ocorre uma transição discreta e uma transição contínua*
>
> $$X_0 \xrightarrow{-, \tau_0} X_0' \qquad e \qquad X_1 \xrightarrow{\tau_1} X_1'$$
>
> *com* $\tau_0 = \tau_1$ *, ou vice-versa.*

Descrição FOTS do sistema híbrido $\mathrm{H} \equiv \mathrm{A}_0 \otimes \mathrm{A}_1$.

Para descrever o sistema híbrido H mum FOTS vamos considerar

Estado

Definido pelas variáveis Y formado pela união dos conjuntos de variáveis dos dois autómatos A_i.

$$\mathrm{Y} \equiv \{m_0, t_0, \mathrm{X}_0, m_1, t_1, \mathrm{X}_1\}$$

Predicado $\mathbf{init}(\mathrm{Y})$

$$\mathbf{init}(\mathrm{Y}) \equiv \mathbf{init}_0(m_0, t_0, \mathrm{X}_0) \wedge \mathbf{init}_1(m_1, t_1, \mathrm{X}_1)$$

Predicado $\mathbf{trans}(\mathrm{Y}, \mathrm{Y}')$

As transições em H são os sincronismos entre as transições de um autómato com as transições do outro. Temos 4 tipos de sincronismo: "untimed-untimed", "timed-timed", "untimed-timed" e "timed-untimed".

Como vimos, só existe sincronismo quando as durações coincidirem. Por isso em todas as transições que vão aparecer em $\mathbf{trans}(\mathrm{Y}, \mathrm{Y}')$ vais existir um predicado

$$\mathbf{eqd}(\mathrm{Y}, \mathrm{Y}') \equiv (t_0' - t_0 = t_1' - t_1)$$

Este termo vai estar implícito nos vários sincronismos e só é explicitamente colocado na definição da relação de transição global $\mathbf{trans}(\mathrm{Y}, \mathrm{Y}')$.

$$\mathbf{untimed} \equiv \bigvee_{e \in E} \mathbf{untimed}_{0,e} \wedge \mathbf{untimed}_{1,e}$$

$$\mathbf{timed} \equiv \bigvee_{m \in \Sigma_0} \bigvee_{n \in \Sigma_1} \mathbf{timed}_{0,m} \wedge \mathbf{timed}_{1,n}$$

$$\mathbf{mixed} \equiv \bigvee_{e \in E} \bigvee_{n \in \Sigma_1} \mathbf{untimed}_{0,e} \wedge \mathbf{timed}_{1,e} \vee \bigvee_{e \in E} \bigvee_{m \in \Sigma_0} \mathbf{timed}_{0,m} \wedge \mathbf{untimed}_{1,e}$$

Finalmente a relação global é

$$\mathbf{trans} \equiv \mathbf{eqd} \wedge (\mathbf{untimed} \vee \mathbf{timed} \vee \mathbf{mixed})$$

Este conjunto de sincronismos pode ser muito grande tornando a utilização deste modelo na verificação de propriedades temporais deste tipo de sistemas, muito complexa.

Mas é possível fazer uma simplificação se assumirmos algumas hipóteses sobre a duração das transições. Nomeadamente pode-se assumir que:

i. Todas as transições "untimed" têm duração 0; todas contêm um termo $(t' = t)$.
ii. Todas as transições "timed" têm duração não-nula; todas contêm um termo $(t' > t)$.

Nesse caso nenhuma transição "untimed" sincroniza com uma transição "timed", e a comparação das durações só é relevante para o sincronismo de duas transições "timed".

Com estas hipóteses tem-se

$$\mathbf{trans} \equiv \mathbf{untimed} \vee \mathbf{timed}$$

sendo

$$\mathbf{untimed} \equiv \bigvee_{e \in E} \mathbf{untimed}_{0,e} \wedge \mathbf{untimed}_{1,e}$$

$$\mathbf{timed} \equiv \bigvee_{m \in \Sigma_0} \bigvee_{n \in \Sigma_1} \mathbf{timed}_{0,m} \wedge \mathbf{timed}_{1,n} \wedge \mathbf{eqd}$$

Exemplo

Vamos construir o FOTS para representar o sistema híbrido que resulta da composição do termostato e do contador.

Variáveis.

As variáveis do FOTS são a união dos conjuntos de variáveis dos dois autómatos híbridos.

$$\mathrm{Y} \equiv \langle m, t, x, n, \tau, c \rangle$$

Estados iniciais

A conjunção dos dois estados iniciais dos HA's

$$\mathbf{init}(\mathrm{Y}) \equiv (m = \mathrm{INIT}) \wedge (n = \mathrm{INIT}) \wedge (t = 0) \wedge (\tau = 0) \wedge (x = 0) \wedge (c = 0)$$

Relação de transição $\mathbf{trans}(\mathrm{Y}, \mathrm{Y}')$

Como todas as transições "untimed" têm duração nula e todas as transições "time" têm duração positiva não-nula só existem dois tipos de sincronismos: entre duas transições "untimed" e entre duas transições "timed" distintas de INIT.
Vamos aqui apresentar um exemplo de cada um destes tipos; os restantes sincronismos processam-se de forma análoga a estes dois.

$\mathbf{untimed}_{\text{init}} \equiv$

$$\{ \begin{array}{l} (m = \text{INIT}) \wedge (n = \text{INIT}) \wedge (m' = \text{OFF}) \wedge (n = \text{INIT})) \wedge (n' = \text{OFF}) \quad \wedge \\ (x' = x) \wedge (c' = c) \wedge (t' = t) \wedge (\tau' = \tau) \\ \qquad\qquad\qquad\qquad \ldots \end{array}$$

$\mathbf{timed}_{\text{ON,OFF}} \equiv$

$$\left\{ \begin{array}{l} (m = \text{ON}) \wedge (n = \text{OFF}) \wedge (m' = \text{OFF}) \wedge (n = \text{OFF})) \wedge (n' = \text{ON}) \quad \wedge \\ (5(x' = x) \geq 3(t' - t)) \wedge (x \leq 22) \wedge (x' \leq 22) \wedge (t' > t) \quad \wedge \\ (c' = c) \wedge (\tau' - \tau = t' - t) \\ \qquad\qquad\qquad\qquad \ldots \end{array}$$