Математические методы верификации схем и программ

Лекторы:

Захаров Владимир Анатольевич

Подымов Владислав Васильевич

e-mail рассказчика:

valdus@yandex.ru

Осень 2018

Лекция 9

Системы реального времени

Временны́е автоматы

Неправдоподобные вычисления временны́х автоматов

Timed CTL

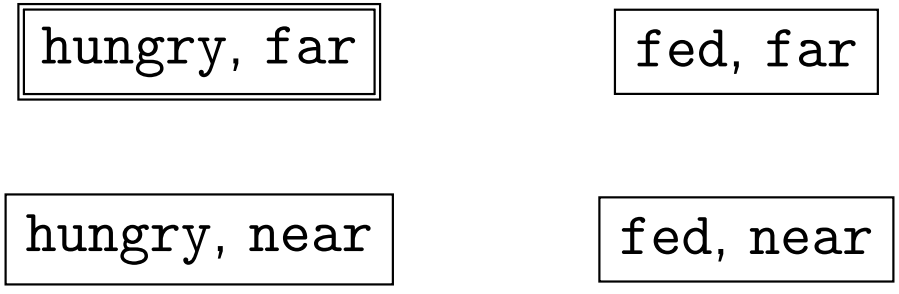
Задача model checking для Timed CTL

Системы реального времени

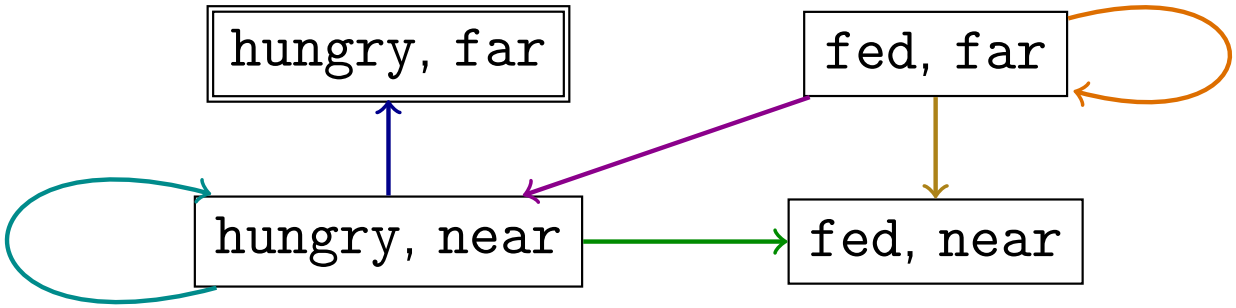
Начнём с примера:

- птица летает по полю и охотится на рой комаров
- птица бывает сытой (`fed`) и голодной (`hungry`) и летает возле роя (`near`) или далеко от него (`far`)
- птица рождается голодной далеко от роя
- если птица долго не ест, то начинает голодать
- голодная птица летит к рою и пытается схватить комара
- прилетев к рою, птица старается не улетать от него
- рой комаров, заметив птицу, пытается улететь

При попытке записать эту систему как модель Крипке "*в лоб*" возникнут 4 состояния:



Системы реального времени



При соединении состояний переходами возникает много нетривиальных вопросов, например:

- Всегда ли комары могут улететь от птицы?
- Всегда ли птица возле роя может перекусить комарами?
- Может ли птица сколь угодно долго летать возле роя и не кормиться?
- Может ли птица одновременно подлететь к рою и проголодаться (... и схватить комара [... и улететь])?

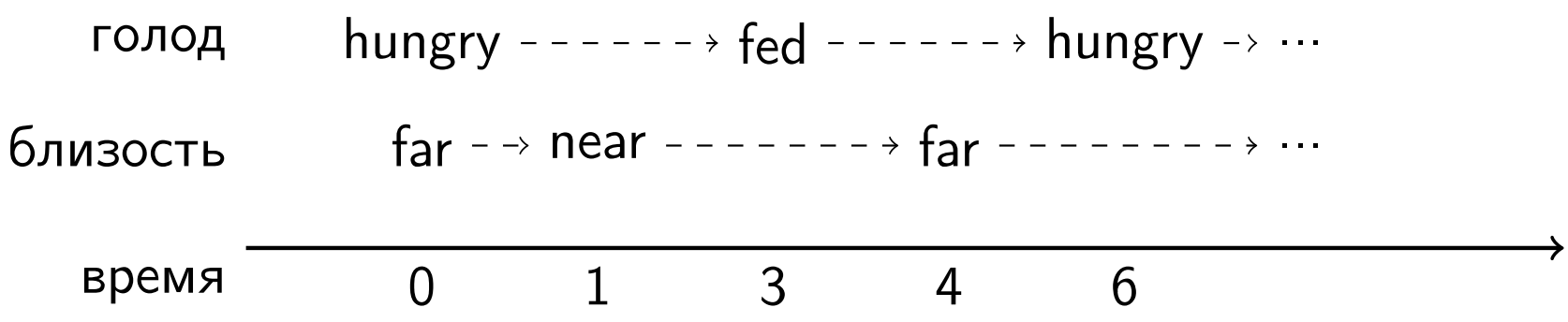
Ответы на эти вопросы для **каждой конкретной** птицы и **каждого конкретного** роя зависят от того, сколько времени требуется на каждое действие и ответную реакцию

Системы реального времени

Уточним систему из птицы и роя,
добавив временны́е характеристики:

- птица переваривает комара ровно 3 минуты
- птица, летящая к рою издалека,
  долетает до него не более чем за 1 минуту
- голодная птица, летающая возле роя,
  ловит комара не более чем за 2 минуты
- рой замечает летающую рядом птицу
  не менее чем за 3 минуты и мгновенно улетает

Уточнённая система может работать, например, так:

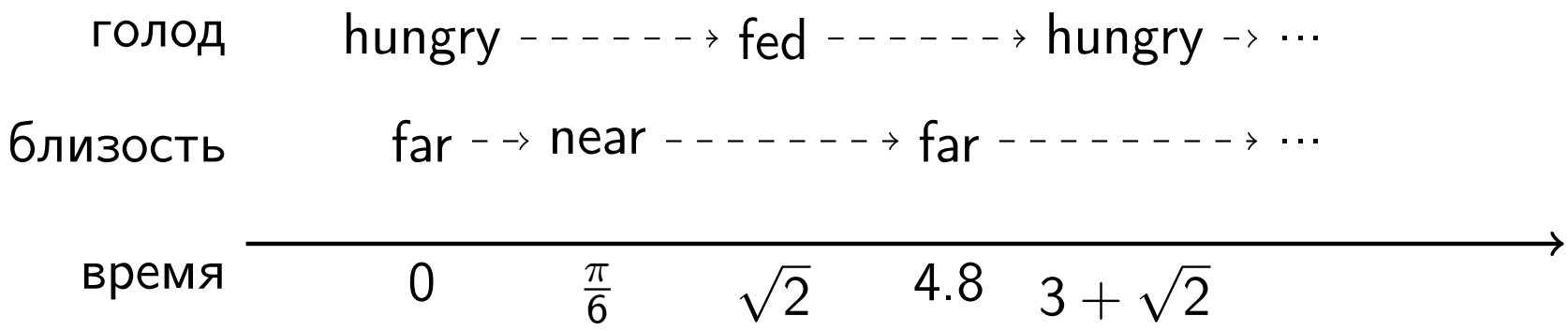


Системы реального времени

Уточним систему из птицы и роя,
добавив временны́е характеристики:

- птица переваривает комара ровно 3 минуты
- птица, летящая к рою издалека,
  долетает до него не более чем за 1 минуту
- голодная птица, летающая возле роя,
  ловит комара не более чем за 2 минуты
- рой замечает летающую рядом птицу
  не менее чем за 3 минуты и мгновенно улетает

Уточнённая система может работать, например, так:

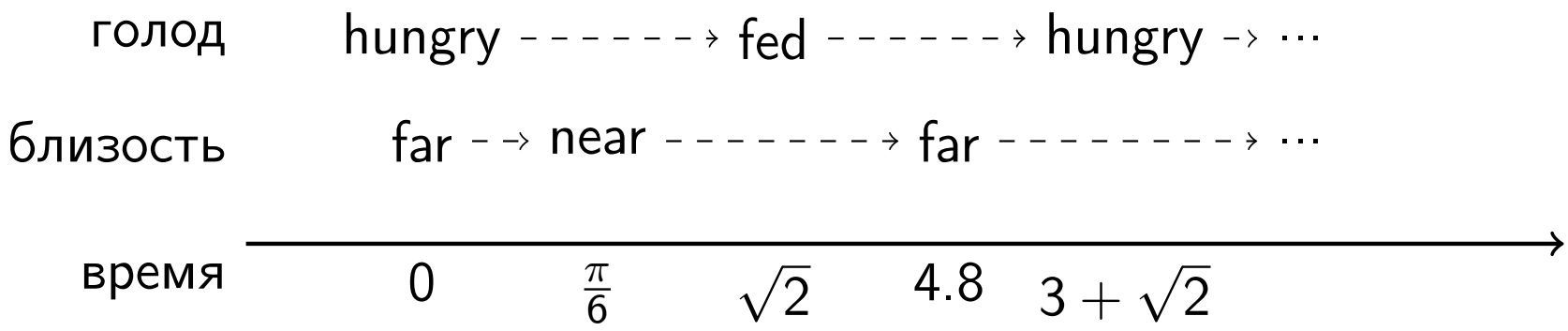


Системы реального времени

Уточним систему из птицы и роя,
добавив временны́е характеристики:

- птица переваривает комара ровно 3 минуты
- птица, летящая к рою издалека,
  долетает до него не более чем за 1 минуту
- голодная птица, летающая возле роя,
  ловит комара не более чем за 2 минуты
- рой замечает летающую рядом птицу
  не менее чем за 1 минуту и мгновенно улетает

Уточнённая система может работать, например, так:

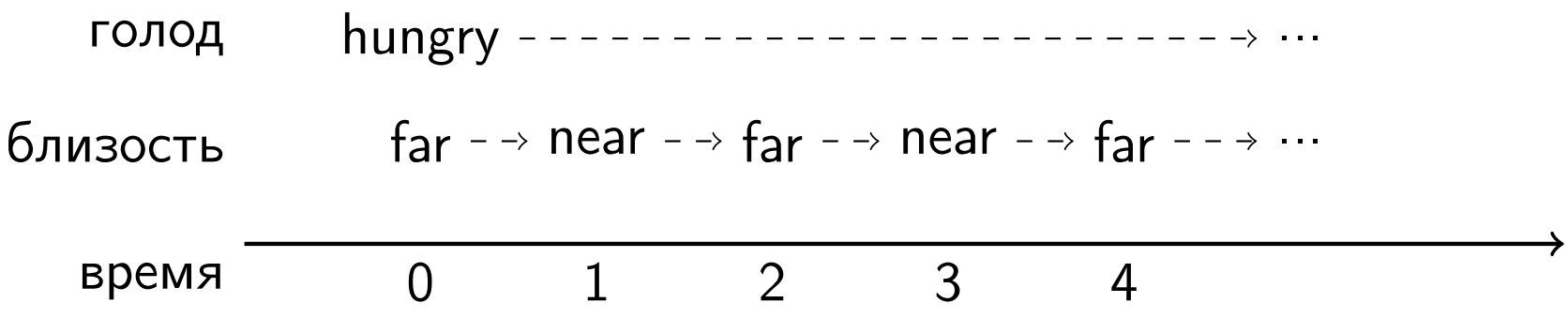


Системы реального времени

Уточним систему из птицы и роя,
добавив временны́е характеристики:

- птица переваривает комара ровно 3 минуты
- птица, летящая к рою издалека,
  долетает до него не более чем за 1 минуту
- голодная птица, летающая возле роя,
  ловит комара не более чем за 2 минуты
- рой замечает летающую рядом птицу
  не менее чем за 1 минуту и мгновенно улетает

Уточнённая система может работать, например, так:



Системы реального времени

Система реального времени (СРВ) — это система, поведение которой существенно зависит не только от того, в каком порядке изменяются состояния компонентов системы, но и от того, **за какое время** происходит изменение состояний

В некоторых СРВ для выполняемых задач формулируются директивные сроки, несоблюдение которых считается фатальным сбоем с бессмысленностью продолжения работы:

- птица не поела вовремя — умерла
- парашют не раскрылся в срок — тоже не очень хорошо
- команда в процессоре не выполнилась
  за нужное число тактов —
  весь процессор на свалку, и ставить новый исправный

СРВ с такими директивными сроками
принято называть жёсткими

Системы реального времени

Система реального времени (СРВ) — это система, поведение которой существенно зависит не только от того, в каком порядке изменяются состояния компонентов системы, но и от того, **за какое время** происходит изменение состояний

В некоторых СРВ срыв директивных сроков, хотя и приводит к нежелательным последствиям, но в целом допускается:

- поспал на два часа меньше —
  будешь вялым, но день продержишься
- почта задержалась на год — печально, но жить можно
- процесс освободил память на полминуты позже плана —
  операционная система “подвиснет”,
  но позже восстановит темп работы

СРВ с такими директивными сроками
принято называть мягкими

Далее рассматриваются только **жёсткие** СРВ

Системы реального времени

В *состоянии* СРВ должно явно или неявно содержаться реальное время:

$$\boxed{\text{hungry,near,2'53''}} \rightarrow ?$$

Аппарат моделей Крипке и темпоральных логик, введённый *в предыдущих лекциях*, невозможно *напрямую* применить для верификации систем с такими состояниями:

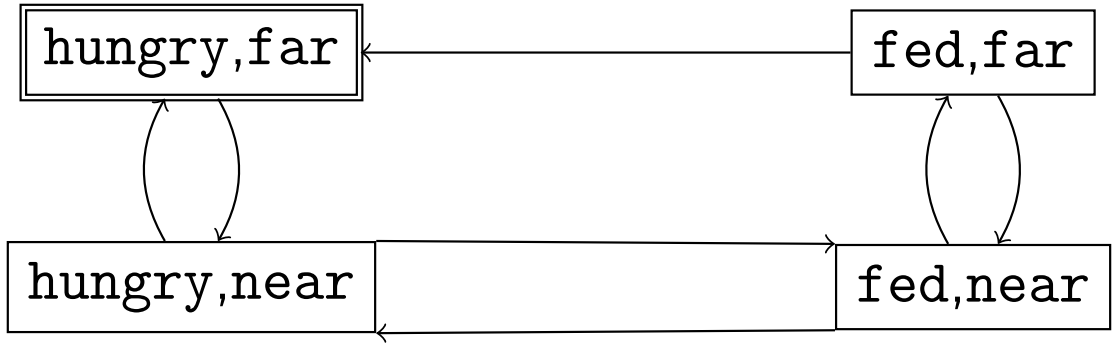
модель Крипке конечна, трасса её выполнения счётна,
а число состояний и трасса выполнения СРВ континуальны

Чтобы преодолеть эти трудности, достаточно:

1. Предложить способы конечного описания СРВ и дискретного описания трасс выполнения СРВ
2. Адаптировать понятия, введённые для темпоральных логик, к реальному времени
3. Свести верификацию СРВ относительно логик реального времени к верификации моделей Крипке относительно дискретных логик (*в следующей лекции*)

Временны́е автоматы на примере

Обратно к голодным птицам:



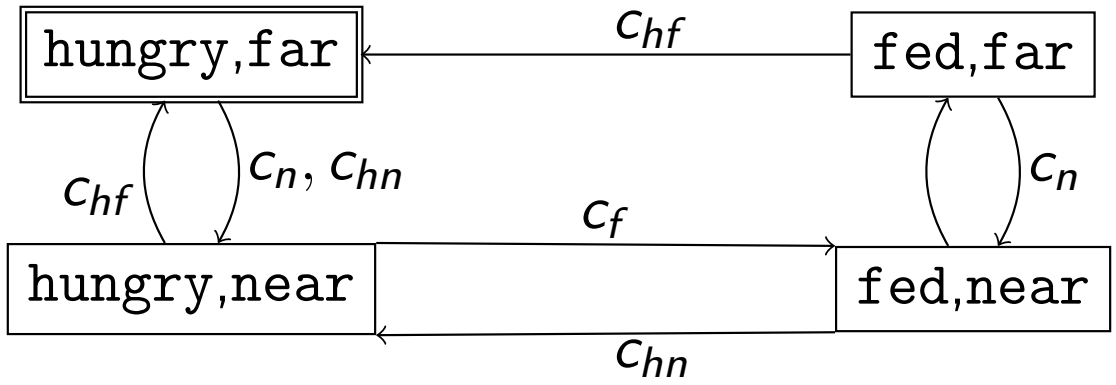
Попробуем уточнить эту модель временны́ми характеристиками **конкретной** птицы и **конкретного** роя

Добавим в модель часы-секундомеры:

- каждые часы показывают,
  сколько времени прошло после их последнего сброса
  (если не сбрасывались, то с момента рождения птицы)
- сбрасывать часы будем по желанию
  при выполнении переходов

Временны́е автоматы на примере

Обратно к голодным птицам:

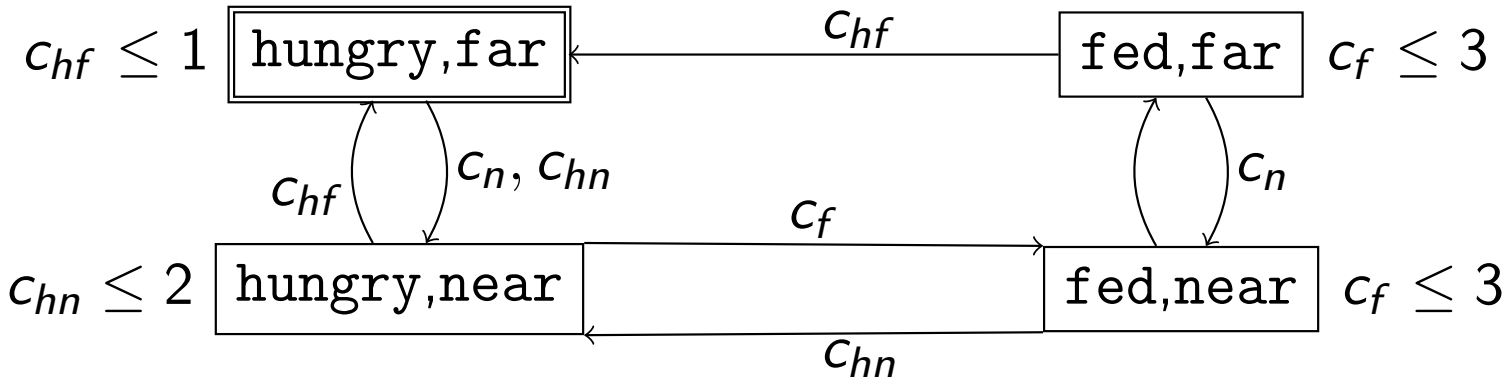


Часы ...	**сбрасываются каждый раз, когда ...**
c_f	птица хватает комара
c_n	птица подлетает к рою
c_{hf}	птица обнаруживает себя голодной далеко от роя
c_{hn}	птица обнаруживает себя голодной возле роя

Пометим каждый переход часами,
сбрасываемыми при его выполнении

Временны́е автоматы на примере

Обратно к голодным птицам:



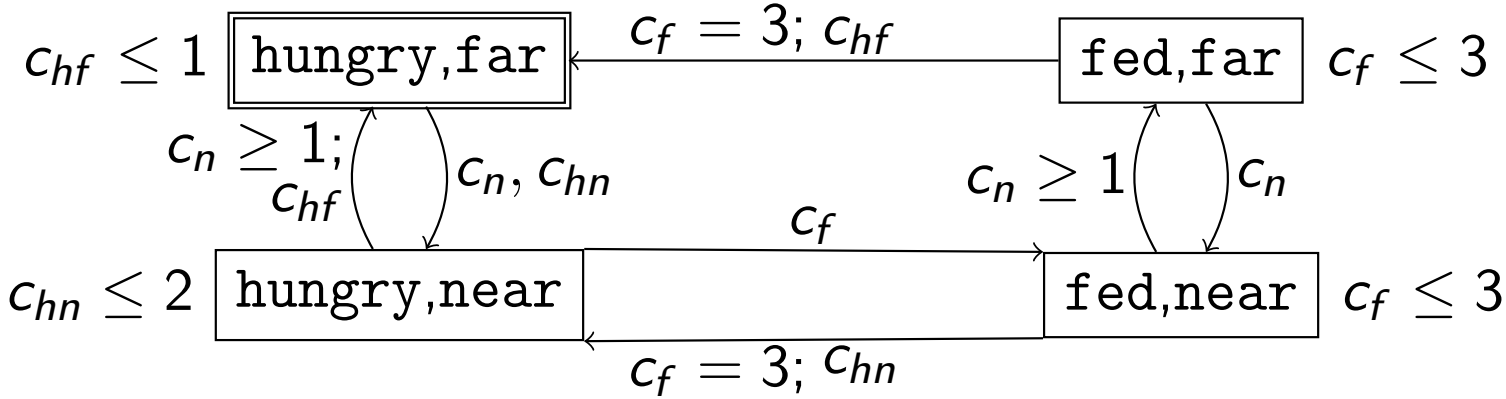
Согласно характеристикам птицы и роя, в некоторых состояниях невозможно находиться сколь угодно долго:

- птица не может быть сытой дольше 3 минут
- птица не может голодать далеко от роя дольше 1 минуты
- птица не может голодать возле роя дольше 2 минут

Разметим состояния
соответствующими ограничениями на часы (инвариантами)

Временны́е автоматы на примере

Обратно к голодным птицам:



Согласно характеристикам птицы и роя,
некоторые переходы могут выполняться не всегда:

- птица становится голодной
  ровно через 3 минуты после обеда
- рой не может улететь от птицы,
  пока она не налетает 1 минуту возле роя

Разметим переходы
соответствующими ограничениями на часы (предусловиями)

В результате получился временной автомат,
описывающий поведение птицы и роя комаров

Временны́е автоматы

$\mathbb{N}_0$ — множество всех целых неотрицательных чисел

Элементарными временны́ми ограничениями
над множеством часов $\mathcal{C}$ называются выражения вида
true, $x < k$, $x \leq k$, $x - y < k$ и $x - y \leq k$, где $x, y \in \mathcal{C}$ и $k \in \mathbb{N}_0$

$ETC(\mathcal{C})$ — множество всех
элементарных временны́х ограничений над $\mathcal{C}$

Синтаксис временны́х ограничений над $\mathcal{C}$
задаётся формой Бэкуса-Наура

$$g \ ::= \ (etc) \ \mid \ (g \,\&\, g) \ \mid \ (\neg g),$$

где g — временно́е ограничение и $etc \in ETC(\mathcal{C})$

Скобки в записи временны́х ограничений могут опускаться
по обычным соглашениям о приоритете операций

$TC(\mathcal{C})$ — множество всех временны́х ограничений над $\mathcal{C}$

Временны́е автоматы

$\mathbb{R}_{\geq 0}$ — множество всех неотрицательных действительных чисел
$\mathbb{R}_{>0}$ — множество всех положительных действительных чисел

Оценкой часов множества $\mathcal{C}$ называется отображение вида

$$\nu : \mathcal{C} \to \mathbb{R}_{\geq 0}$$

Выполнимость временно́го ограничения tc на оценке часов ν ($\nu \models tc$) определяется естественным образом:

- $\nu \models \mathbf{true}$
- $\nu \models x \bowtie k \quad \Leftrightarrow \quad \nu(x) \bowtie k$
- $\nu \models x - y \bowtie k \quad \Leftrightarrow \quad \nu(x) - \nu(y) \bowtie k$
- $\nu \models tc_1 \,\&\, tc_2 \quad \Leftrightarrow \quad \nu \models tc_1$ и $\nu \models tc_2$
- $\nu \models \neg tc_1 \quad \Leftrightarrow \quad \nu \not\models tc_1$

Временно́е ограничение инвариантно, если в нём **не содержатся** подвыражения $x - y < k$, $x - y \leq k$ и связка $\neg$

$IC(\mathcal{C})$ — множество всех инвариантных временны́х ограничений над $\mathcal{C}$

Временны́е автоматы

Другие отношения и связки, которые могут использоваться в (**неинвариантных**) временны́х ограничениях:

$$
\begin{aligned}
\textbf{false} &\equiv \neg\textbf{true} \\
g_1 \vee g_2 &\equiv \neg(g_1 \,\&\, g_2) \\
g_1 \rightarrow g_2 &\equiv \neg g_1 \vee g_2 \\
x \geq k &\equiv \neg(x < k) \\
x - y \geq k &\equiv \neg(x - y < k) \\
x > k &\equiv \neg(x \leq k) \\
x - y > k &\equiv \neg(x - y \leq k) \\
x = k &\equiv (x \leq k) \,\&\, (x \geq k) \\
x - y = k &\equiv (x - y \leq k) \,\&\, (x - y \geq k) \\
x \neq k &\equiv \neg(x = k) \\
x - y \neq k &\equiv \neg(x - y = k)
\end{aligned}
$$

Временны́е автоматы

Временной автомат над множеством атомарных высказываний AP — это система $(L, \ell_0, \xi, \mathcal{C}, I, T)$, где

- L — конечное множество состояний
- ℓ_0 — начальное состояние, $\ell_0 \in L$
- $\xi : L \to 2^{AP}$ — разметка состояний событиями
- $\mathcal{C}$ — конечное множество часов
- $I : L \to IC(\mathcal{C})$ — разметка состояниий инвариантами
- $T \subseteq L \times TC(\mathcal{C}) \times 2^{\mathcal{C}} \times L$ — отношение переходов
  - (l_1, g, X, l_2) — переход из состояния l_1 в состояние l_2 с предусловием g и множеством сбрасываемых часов X
  - наглядная запись перехода: $l_1 \xrightarrow{g,X} l_2$

Временны́е автоматы

В элементарных временны́х ограничениях значения часов сравниваются только с числами из $\mathbb{N}_0$

В частности, выражения "$x < \sqrt{2}$" и "$x < \frac{2}{3}$" **не являются** элементарными временны́ми ограничениями

Принято полагать, что элементарные ограничения с нецелыми числами в правой части излишни:

- любое действительное число может быть приближено рациональным с любой точностью
- любой конечный набор рациональных чисел можно привести к общему знаменателю
- рациональные числа, используемые в записи автомата и предъявляемых к нему требований, можно домножить на общий знаменатель с сохранением смысла требований ("замедлить" модельное время относительно реального)

Временны́е автоматы

Вычислительная конфигурация временно́го автомата $A = (L, \ell_0, \xi, \mathcal{C}, I, T)$ имеет вид (ℓ, ν), где $\ell \in L$ и $\nu : \mathcal{C} \to \mathbb{R}_{\geq 0}$

Для технической простоты иногда будем полагать, что часы автомата упорядочены: $\mathcal{C} = (x_1, \ldots, x_m)$ — и записывать конфигурацию (ℓ, ν) в виде $(\ell, \nu(x_1), \ldots, \nu(x_m))$

Начальная конфигурация автомата A имеет вид $(\ell_0, 0, 0, \ldots, 0)$

В определении вычисления автомата понадобятся следующие способы преобразования произвольной оценки часов ν:

- $\nu + d$ — оценка часов, такая что $(d \in \mathbb{R}_{\geq 0})$
  $(\nu + d)(x) = \nu(x) + d$ для любых часов x
- $\nu[X]$ — оценка часов, такая что: $(X \subseteq \mathcal{C})$
  - $\nu[X](x) = 0$, если $x \in X$
  - $\nu[X](x) = \nu(x)$, если $x \notin X$

Временны́е автоматы

В определении вычисления автомата понадобятся следующие способы преобразования конфигурации $\sigma = (\ell, \nu)$:

- $\sigma + d = (\ell, \nu + d)$ $\qquad (d \in \mathbb{R}_{\geq 0})$
- $\sigma[X] = (\ell, \nu[X])$ $\qquad (X \subseteq C)$
- $\sigma[\ell/\ell'] = (\ell', \nu)$ $\qquad (\ell'$ — состояние автомата$)$

Конфигурации (*дискретно*) преобразуются автоматом A в процессе вычисления двумя способами (*описанными далее*):

1. Продвижение времени ($\sigma \mapsto \sigma'$)
2. Выполнение перехода ($\sigma \hookrightarrow \sigma'$)

Отношение шага вычисления $\to$ автомата A — это объединение отношений $\mapsto$ и $\hookrightarrow$

Временны́е автоматы

Рассмотрим временной автомат $A = (L, \ell_0, \xi, \mathcal{C}, I, T)$
и конфигурацию $c = (\ell, \nu)$

Продвижение времени

$\sigma \overset{d}{\mapsto} \sigma'$, если: $\quad (d \in \mathbb{R}_{>0})$

- $\sigma' = \sigma + d$
- $\nu + d \models I(\ell)$

$\sigma \mapsto \sigma'$, если существует число d, $d \in \mathbb{R}_{>0}$, такое что $\sigma \overset{d}{\mapsto} \sigma'$

Выполнение перехода

$\sigma \overset{\ell \xrightarrow{g,X} \ell'}{\hookrightarrow} \sigma'$, если: $\quad (\ell \xrightarrow{g,X} \ell' \in T)$

- $\sigma' = \sigma[X][\ell/\ell']$
- $\nu \models g$
- $\nu[X] \models I(\ell')$

$c \hookrightarrow c'$, если в A существует переход t, такой что $c \overset{t}{\hookrightarrow} c'$

Временны́е автоматы

Трассой автомата, исходящей из конфигурации σ
(или, коротко, σ-трассой),
называется последовательность конфигураций вида

$$\sigma \to \sigma_1 \to \sigma_2 \to \ldots,$$

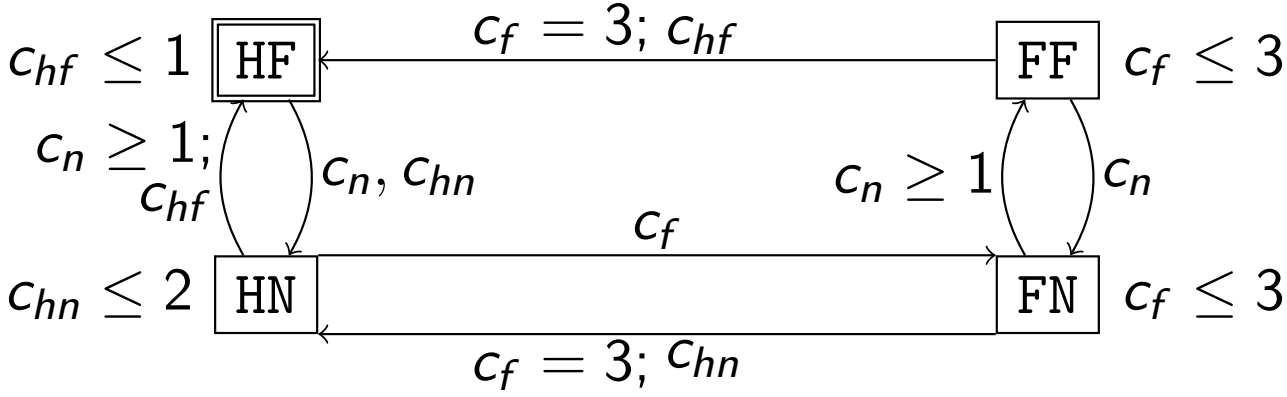
Частичным вычислением автомата называется трасса,
исходящая из начальной конфигурации

Конфигурация σ называется тупиковой, если
не существует конфигурации σ', такой что $\sigma \to \sigma'$

Трасса называется полной, если она бесконечна или
оканчивается тупиковой конфигурацией

Вычислением автомата называется полная трасса,
исходящая из начальной конфигурации

Временны́е автоматы



Пример частичного вычисления этого автомата:

(*порядок часов:* c_f, c_n, c_{hf}, c_{hn})

$$
\begin{aligned}
&(HF,\ 0,\ 0,\ 0,\ 0) \mapsto (HF,\ \tfrac{\pi}{6},\ \tfrac{\pi}{6},\ \tfrac{\pi}{6},\ \tfrac{\pi}{6}) \\
\hookrightarrow &(HN,\ \tfrac{\pi}{6},\ 0,\ \tfrac{\pi}{6},\ 0) \mapsto (HN,\ \tfrac{\pi+6}{6},\ 1,\ \tfrac{\pi+6}{6},\ 1) \\
\mapsto &(HN,\ \tfrac{\pi+12}{6},\ 2,\ \tfrac{\pi+12}{6},\ 2) \hookrightarrow (HF,\ \tfrac{\pi+12}{6},\ 2,\ 0,\ 2) \\
\hookrightarrow &(HN,\ \tfrac{\pi+12}{6},\ 0,\ 0,\ 0) \hookrightarrow (FN,\ 0,\ 0,\ 0,\ 0) \\
\mapsto &(FN,\ \sqrt{2},\ \sqrt{2},\ \sqrt{2},\ \sqrt{2}) \hookrightarrow (FF,\ \sqrt{2},\ \sqrt{2},\ \sqrt{2},\ \sqrt{2}) \\
\hookrightarrow &(FN,\ \sqrt{2},\ 0,\ \sqrt{2},\ \sqrt{2}) \mapsto (FN,\ 3,\ 3-\sqrt{2},\ 3,\ 3) \\
\hookrightarrow &(HN,\ 3,\ 3-\sqrt{2},\ 3,\ 0) \hookrightarrow (HF,\ 3,\ 3-\sqrt{2},\ 0,\ 0)
\end{aligned}
$$

Неправдоподобные вычисления автоматов

Длительностью $delay(\sigma \to \sigma')$ шага вычисления $\sigma \to \sigma'$ называется число

- d, если $\sigma \overset{d}{\mapsto} \sigma'$
- 0, если $\sigma \hookrightarrow \sigma'$

Длительностью трассы $\sigma_1 \to \sigma_2 \to \sigma_3 \to \ldots$ называется

- сумма $\sum_{i=1}^{k} delay(\sigma_i \to \sigma_{i+1})$, если трасса конечна и содержит $(k+1)$ конфигурацию
- предел ряда $\sum_{i=1}^{\infty} delay(\sigma_i \to \sigma_{i+1})$, если трасса бесконечна (длительность бесконечна, если ряд расходится)

Неправдоподобные вычисления автоматов

Полная трасса конвергентна, если её длительность конечна, и дивергентна, если её длительность бесконечна

Вычислением Зенона (или зеноновским вычислением) называется конвергентное вычисление, в котором выполнение перехода ($\hookrightarrow$) встречается бесконечно часто

Примеры вычислений

Дивергентные вычисления:

$(\ell, 0) \mapsto (\ell, 1) \mapsto (\ell, 2) \mapsto \ldots \mapsto (\ell, n) \mapsto \ldots$

$(\ell_1, 0) \mapsto (\ell_1, 1) \hookrightarrow (\ell_2, 0) \mapsto (\ell_2, 1) \hookrightarrow \ldots \mapsto (\ell_n, 1) \hookrightarrow (\ell_n, 0) \mapsto \ldots$

Конвергентные незеноновские вычисления:

$(\ell_1, 0) \mapsto (\ell_1, 1) \hookrightarrow (\ell_2, 0) \mapsto (\ell_2, 2)$ — тупиковая конфигурация

$(\ell, 0) \mapsto (\ell, \frac{1}{2}) \mapsto (\ell, \frac{2}{3}) \mapsto \ldots \mapsto (\ell, \frac{n-1}{n}) \mapsto \ldots$

Вычисление Зенона:

$(\ell_1, 0) \mapsto (\ell_1, \frac{1}{2}) \hookrightarrow (\ell_2, 0) \mapsto (\ell_2, \frac{1}{4}) \hookrightarrow \ldots \hookrightarrow (\ell_n, 0) \mapsto (\ell_n, \frac{1}{2^n}) \hookrightarrow \ldots$

Неправдоподобные вычисления автоматов

"Реальная" СРВ выполняется в условиях неограниченно возрастающего времени, и как следствие, **конвергентные** вычисления временны́х автоматов принято считать неправдоподобными: не соответствующими никаким "реалистичным" выполнениям моделируемой СРВ

При этом **каждым** временны́м автоматом порождается хотя бы одно конвергентное вычисление, а каждым нетривиальным автоматом — бесконечно много таких вычислений

Некоторые конвергентные вычисления исключаются из рассмотрения при формулировке верифицируемых свойств, а некоторые — **до** и **независимо от** формулировки свойств

Временной автомат A корректен, если выполнены два условия:

- ни одно его вычисление не является зеноновским
- любое его частичное вычисление может быть продолжено до дивергентного вычисления

Timed CTL

Логика ветвящегося реального времени (Timed CTL; TCTL) — аналог CTL, адаптированный к особенностям поведения СРВ

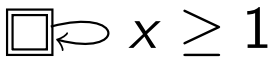
Минимальный синтаксис TCTL-формул над множеством атомарных высказываний AP и множеством часов $\mathcal{C}$ задаётся формой Бэкуса-Наура
$\varphi ::= a \mid (etc) \mid (\varphi \,\&\, \varphi) \mid (\neg\varphi) \mid (\mathbf{E}(\varphi \mathbf{U} \varphi)) \mid (\mathbf{A}(\varphi \mathbf{U} \varphi))$,
где φ — TCTL-формула, $a \in AP$ и $etc \in ETC(\mathcal{C})$

Содержательная трактовка кванторов **E**, **A** и оператора **U** схожа с их трактовкой в CTL,
но адаптирована к особенностям выполнения СРВ:

- **E**Φ: существует **дивергентное** выполнение СРВ, для которого верно Φ
- **A**Φ: для любого **дивергентного** выполнения СРВ верно Φ
- φ**U**ψ: в **реальном** будущем станет верным ψ, а до тех пор будет верно φ

Timed CTL: неявные конфигурации трасс

Рассмотрим такие *корректный* временной автомат A
с часами x, y и TCTL-формулу φ:



$$\mathbf{A}(\mathbf{true}\mathbf{U}(y = 1))$$

Согласно содержательной трактовке,
φ выполняется для CPB, моделируемой автоматом A:
длительность любого дивергентного выполнения CPB рано или поздно становится равной 1

Под свойство φ должны подходить, в числе прочих,
вычисления A вида

$$(\ell, 0, 0) \mapsto (\ell, 2, 2) \to \dots$$

В таких вычислениях *подразумевается*, что
значение 1 достигается часами y между значениями 0 и 2,
но соответствующая конфигурация **в явном виде отсутствует**

В семантике TCTL-формул должны быть учтены все такие
неявно подразумевающиеся конфигурации

Timed CTL: неявные конфигурации трасс

Рассмотрим произвольную трассу τ произвольного автомата:

$$\sigma_0 \to \sigma_1 \to \sigma_2 \to \dots$$

Конфигурация σ порождается на i-м шаге трассы τ, где $i \geq 1$, если

- $\sigma = \sigma_i$ или
- $\sigma_{i-1} \overset{d}{\mapsto} \sigma_i$, $\sigma_{i-1} \overset{d'}{\longmapsto} \sigma$ и $d' < d$

Конфигурация σ порождается трассой τ, если она совпадает с σ_0 или порождается на каком-либо шаге трассы

Timed CTL

Рассмотрим временной автомат $A = (L, \ell_0, \xi, \mathcal{C}, I, T)$ над AP, его конфигурацию $\sigma = (\ell, \nu)$ и TCTL-формулу φ над $\mathcal{C}$ и AP

Формула φ выполняется в конфигурации σ автомата A ($A, \sigma \models \varphi$) в следующих случаях:

- $A, \sigma \models a$, где $a \in AP \quad \Leftrightarrow \quad a \in \xi(\ell)$
- $A, \sigma \models etc$, где $etc \in ETC(\mathcal{C}) \quad \Leftrightarrow \quad \nu \models etc$
- $A, \sigma \models \psi \,\&\, \chi \quad \Leftrightarrow \quad A, \sigma \models \psi$ и $A, \sigma \models \chi$
- $A, \sigma \models \neg\psi \quad \Leftrightarrow \quad A, \sigma \not\models \psi$
- $A, \sigma \models \mathbf{E}\Phi \quad \Leftrightarrow \quad$ существует дивергентная σ-трасса τ автомата A, такая что $A, \tau \models \Phi$
- $A, \sigma \models \mathbf{A}\Phi \quad \Leftrightarrow \quad$ для любой дивергентной σ-трассы τ автомата A верно $A, \tau \models \Phi$

Timed CTL

Рассмотрим временной автомат $A = (L, \ell_0, \xi, \mathcal{C}, I, T)$ над AP, его конфигурацию $\sigma = (\ell, \nu)$ и TCTL-формулу φ над $\mathcal{C}$ и AP

Формула φ выполняется в конфигурации σ автомата A ($A, \sigma \models \varphi$) в следующих случаях:

- $A, \tau \models \psi \mathbf{U} \chi$,
  где $\tau = (\sigma_0 \to \sigma_1 \to \dots)$ — дивергентная трасса $\Leftrightarrow$
  - $A, \sigma_0 \models \chi$ или
  - существуют номер k, $k \geq 1$, и конфигурация σ, порождаемая на k-м шаге трассы τ, такие что
    - $A, \sigma \models \chi$ и
    - для всех конфигураций δ, порождаемых трассой $\sigma_0 \to \sigma_1 \to \dots \to \sigma_k \to \sigma$, верно $A, \delta \models \psi \vee \chi$

TCTL-формула φ выполняется на автомате A ($A \models \varphi$), если она выполняется в начальной конфигурации этого автомата

Timed CTL: “до тех пор, пока”

$A, \sigma \models \mathbf{E}(\psi \mathbf{U} \chi) \Leftrightarrow$ ... для любой конфигурации δ, порождаемой трассой τ, справедливо соотношение $A, \delta \models \psi \vee \chi$

Рассмотрим такие автомат A над часами x, y и формулу φ:

$$\mathbf{A}((y \leq 1)\mathbf{U}(y > 1))$$

Верно соотношение $A, (\ell, 0, 0) \models \varphi$,
и это адекватно содержательной трактовке формулы φ:
существует дивергентное выполнение СРВ,
длительность которого когда-нибудь превозойдёт 1**,**
а до тех пор не будет превосходить 1

Нетривиальное отличие определений семантики **U** в TCTL и CTL* — формула $\psi \vee \chi$ в конце определения: в аналогичном месте определения для CTL* располагается формула ψ

Такое отличие

- несущественно: $\psi \mathbf{U} \chi \equiv (\psi \vee \chi)\mathbf{U}\chi$ в CTL*
- необходимо: если заменить $\psi \vee \chi$ на ψ,
  то соотношение $A, (\ell, 0, 0) \models \varphi$ станет **неверным**

Timed CTL

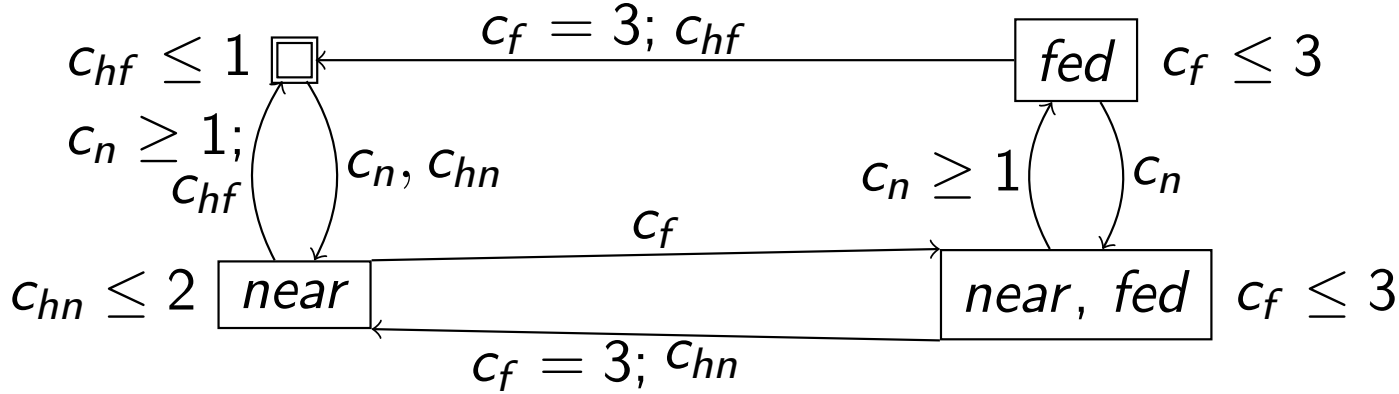
В TCTL-формулах могут встречаться и другие *привычные* булевы связки и темпоральные операторы:

$$\varphi \vee \psi \equiv \neg(\neg\varphi \,\&\, \neg\psi) \qquad \varphi \to \psi \equiv \neg\varphi \vee \psi$$
$$\mathbf{E}(\varphi \mathbf{R} \psi) \equiv \neg\mathbf{E}(\neg\varphi \mathbf{U} \neg\psi) \qquad \mathbf{A}(\varphi \mathbf{R} \psi) \equiv \neg\mathbf{A}(\neg\varphi \mathbf{U} \neg\psi)$$
$$\mathbf{EF}\varphi \equiv \mathbf{E}(\mathbf{true}\mathbf{U}\varphi) \qquad \mathbf{AF}\varphi \equiv \mathbf{A}(\mathbf{true}\mathbf{U}\varphi)$$
$$\mathbf{AG}\varphi \equiv \neg\mathbf{EF}\neg\varphi \qquad \mathbf{EG}\varphi \equiv \neg\mathbf{AF}\neg\varphi$$

Содержательная трактовка операторов **F**, **G**, **R** настолько же естественна, как и трактовка оператора **U**:

- $\mathbf{F}\varphi$: в **реальном** будущем станет верным φ
- $\mathbf{G}\varphi$: в **реальном** будущем всегда верно φ
- $\varphi\mathbf{R}\psi$: пока в **реальном** будущем не станет верным φ, будет верно ψ (при этом φ может никогда не стать верным)

Timed CTL



Ещё несколько примеров свойств, задаваемых TCTL-формулами

- Голодная птица всегда имеет возможность накормиться

$$\mathbf{AG}(\neg fed \to \mathbf{EF}\, fed)$$

- Птица не может летать голодной вдалеке от роя дольше минуты

$$\neg\mathbf{EF}(\neg fed \,\&\, \neg near \,\&\, c_{hf} > 1)$$

- За две минуты с того момента, как птица обнаруживает себя голодной возле роя, обязательно решится, оказалась ли удачной охота на комаров

$$\mathbf{AG}(c_{hn} = 0 \to \mathbf{AF}(c_{hn} \le 2 \,\&\, (far \vee fed)))$$

Задача model checking для TCTL

Для заданного корректного временно́го автомата A и заданной TCTL-формулы φ проверить справедливость соотношения

$$A \models \varphi$$