

Математические методы верификации схем и программ

mk.cs.msu.ru → Лекционные курсы
→ Математические методы верификации схем и программ

Блок 16

Логика деревьев вычислений (CTL)

Постановка задачи верификации
моделей Крипке относительно CTL

Лектор:

Подымов Владислав Васильевич

E-mail:

valdus@yandex.ru

Вступление

LTL — это несложно устроенный язык формальной спецификации моделей Крипке

Запись $M \models \varphi$ для модели Крипке M и ltl-формулы φ читается так:
Каждое вычисление модели удовлетворяет свойству формулы φ

Естественно возникает желание уметь проверять, **существует** ли вычисление модели, удовлетворяющее свойству φ

Это можно попробовать явно отразить в формуле и условно изобразить так (*и это уже не LTL*):

- ▶ Каждое вычисление ...: $M \models \forall \varphi$
- ▶ Существует вычисление ...: $M \models \exists \varphi$

Вступление

$$M \models \forall \varphi$$

$$M \models \exists \varphi$$

Желание поставить квантор относительно вычислений может возникнуть и «внутри» формулы — например:

Для любого начала вычисления **существует** способ его продолжить до **правильного**

Далее рассматривается **логика деревьев вычислений** (CTL),

- ▶ похожая на LTL, но
- ▶ содержащая такие кванторы и
- ▶ «двойственная» к LTL в том смысле, что
 - ▶ формулами LTL задаются свойства вычислений моделей Крипке,
 - ▶ а формулами CTL — свойства состояний

Логика деревьев вычислений: синтаксис

Формулы логики деревьев вычислений делятся на две категории:

- ▶ **Формулы состояния**: их истинностное значение задаётся **состоянием** модели Крипке
- ▶ **Формулы пути**: их истинностное значение задаётся **бесконечным путём** в модели Крипке

«Укороченный» синтаксис этих формул состояния и пути над множеством атомарных высказываний AP :

$$\Phi ::= \top \mid p \mid (\Phi \& \Phi) \mid (\neg \Phi) \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi),$$

$$\varphi ::= (\mathbf{X}\Phi) \mid (\Phi \mathbf{U}\Phi),$$

где Φ — **формула состояния** (её же будем называть **ctl-формулой**), φ — **формула пути** и $p \in AP$

Логика деревьев вычислений: синтаксис

По сравнению с LTL в языке появились две новых буквы (кванторы пути):

- ▶ **A** φ : любой бесконечный путь, исходящий из текущего состояния, обладает свойством φ
- ▶ **E** φ : существует бесконечный путь, исходящий из текущего состояния и обладающий свойством φ

Остальные операции имеют тот же содержательный смысл, что и в LTL

В «расширенный» синтаксис включим те же операции, что и для LTL (\vee , \rightarrow , **F**, **G**) с тем же содержательным смыслом и способом введения, кроме способа введения **G** (из-за ограничений синтаксиса):

- ▶ **AG** $\phi = \neg \mathbf{EF} \neg \phi$
- ▶ **EG** $\phi = \neg \mathbf{AF} \neg \phi$

Приоритеты операций **A** и **E** одинаковы и такие же, как и \neg и **X**, а в остальном приоритеты операций те же, что и в LTL

Логика деревьев вычислений: примеры

Примеры ctl-формул и выражаемых ими свойств вычислительных систем:

- ▶ Цель может быть достигнута

EF*goal*

- ▶ Как бы ни работал компьютер, есть возможность в дальнейшем его выключить

AGEF*off*

- ▶ Тех, кто много грешит, неотвратно настигнет кара

AG(*too _ many _ sins* → **AF***punishment*)

- ▶ Если я захочу всё бросить, то смогу сделать это на следующий день

AG(*want* → **EX***quit*)

- ▶ Если я провинюсь, то меня обязательно накажут на следующий день

AG(*guilty* → **AX***punished*)

Логика деревьев вычислений: семантика

Отношение выполнимости ctl-формулы Φ в состоянии s модели Крипке $M = (S, S_0, \rightarrow, L)$ ($M, s \models \Phi$) и формулы пути φ на бесконечном пути π модели M ($M, \pi \models \varphi$) определяются так:

- ▶ Соотношение $M, s \models \mathbf{t}$ верно всегда
- ▶ $M, s \models p$, где $p \in AP \Leftrightarrow p \in L(s)$
- ▶ $M, s \models \Phi_1 \& \Phi_2 \Leftrightarrow M, s \models \Phi_1$ и $M, s \models \Phi_2$
- ▶ $M, s \models \neg\Phi \Leftrightarrow M, s \not\models \Phi$
- ▶ $M, s \models \mathbf{A}\varphi \Leftrightarrow$ для любого бесконечного пути π в M , исходящего из s , верно $M, \pi \models \varphi$
- ▶ $M, s \models \mathbf{E}\varphi \Leftrightarrow$ в M существует бесконечный путь π , исходящий из s и такой что $M, \pi \models \varphi$
- ▶ $M, \pi \models \mathbf{X}\Phi \Leftrightarrow M, \pi[1] \models \Phi$
- ▶ $M, \pi \models \Phi_1 \mathbf{U}\Phi_2 \Leftrightarrow$ существует момент времени k , такой что
 - ▶ $M, \pi[k] \models \Phi_2$ и
 - ▶ для любого момента времени i , такого что $i < k$, верно $M, \pi[i] \models \Phi_1$

Логика деревьев вычислений: основные свойства

Утверждение. $M, s \models \mathbf{AGAF}\Phi \Leftrightarrow$ для любого бесконечного пути π в M , начинающегося в s , существует бесконечно много попарно различных моментов времени i , таких что $M, \pi[i] \models \Phi$

Доказательство. Аналогично утверждению про $\mathbf{GF}\varphi$ для LTL

Логика деревьев вычислений: основные свойства

Развёрткой модели Крипке $M = (S, S_0, \rightarrow, L)$ относительно состояния s называется бесконечное ориентированное дерево, которое можно представить как строящееся поярусно так:

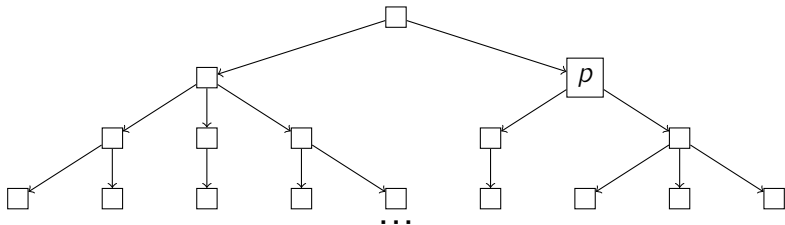
- ▶ Корень (0-й ярус) помечен состоянием s
- ▶ Для каждой вершины, помеченной некоторым состоянием s' , в следующий ярус добавляется по одному ребёнку для каждого перехода $s' \rightarrow s''$, и этот ребёнок помечен состоянием s''

В расширенном синтаксисе ctl-формул содержится 8 сочетаний QO квантора пути Q и темпорального оператора O : **AX, EX, AF, EF, AG, EG, AU** и **EU**

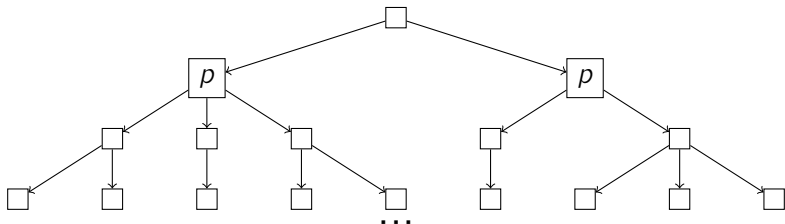
Можно проиллюстрировать эти сочетания на развёртке следующим образом

Логика деревьев вычислений: основные свойства

EXp

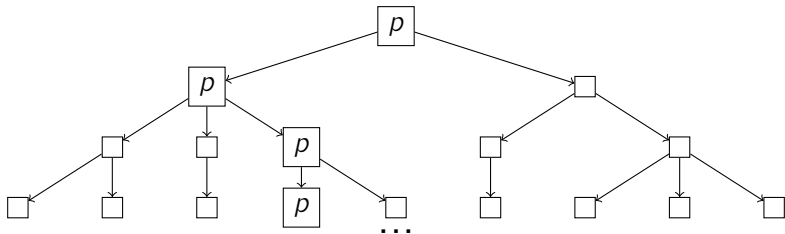


AXp

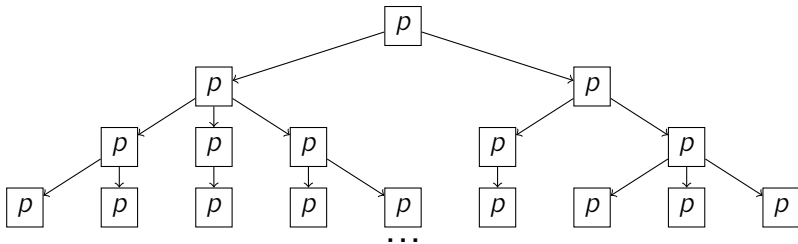


Логика деревьев вычислений: основные свойства

EGp

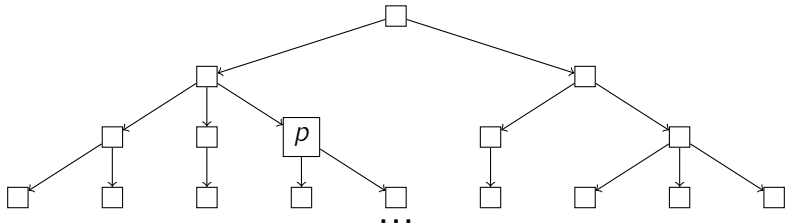


AGp

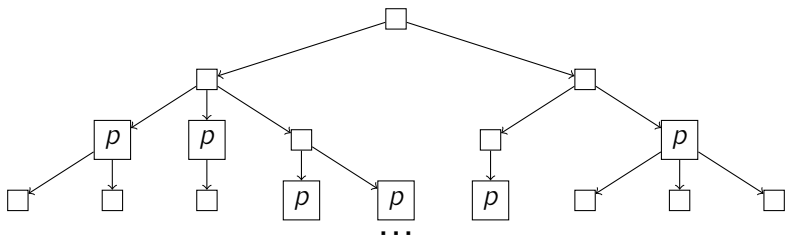


Логика деревьев вычислений: основные свойства

EFp

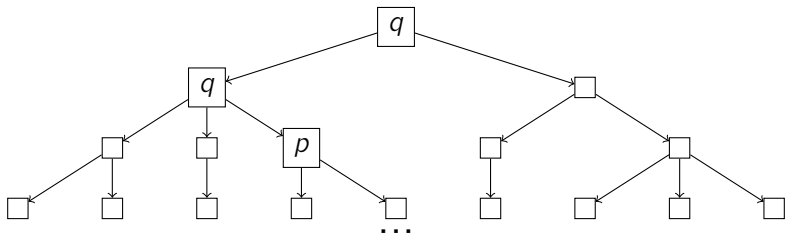


AFp

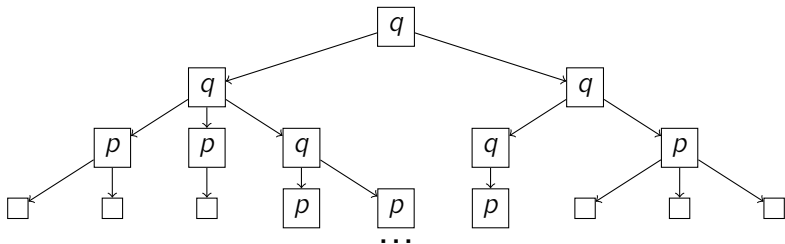


Логика деревьев вычислений: основные свойства

$E(qUp)$



$A(qUp)$



Логика деревьев вычислений: основные свойства

Будем говорить, что ctl-формулы φ и ψ **равносильны** ($\varphi \sim \psi$), если для любой модели Крипке M и любого состояния s справедлива равносильность

$$M, s \models \varphi \Leftrightarrow M, s \models \psi$$

Согласно укороченному и расширенному синтаксисам, 8 комбинаций квантора пути и темпорального оператора (**AX**, **EX**, **AF**, **EF**, **AG**, **EG**, **AU** и **EU**) *выражаются* через 4, обозначенные в укороченном синтаксисе:

- ▶ **AF** $\varphi \sim \mathbf{A}(\uparrow\mathbf{U}\varphi)$
- ▶ **EF** $\varphi \sim \mathbf{E}(\uparrow\mathbf{U}\varphi)$
- ▶ **AG** $\varphi \sim \neg\mathbf{EF}\neg\varphi$
- ▶ **EG** $\varphi \sim \neg\mathbf{AF}\neg\varphi$

Логика деревьев вычислений: основные свойства

Несложно убедиться в такой равносильности:

Утверждение. $\mathbf{AX}\varphi \sim \neg\mathbf{EX}\neg\varphi$

Значит, достаточно иметь только три комбинации: **EX**, **AU** и **EU**

Такой набор комбинаций: достаточно маленький (*в идеале — минимальный*), через который выражаются остальные комбинации, — принято называть темпоральным **базисом** CTL

Утверждение. $\mathbf{A}(\varphi\mathbf{U}\psi) \sim \neg\mathbf{E}(\neg\psi\mathbf{U}(\neg\varphi \& \neg\psi)) \& \neg\mathbf{EG}\neg\psi$

Доказательство. Можете попробовать самостоятельно

Это значит, что базисом CTL является и такой набор: **EX**, **EG** и **EU**

В теоретическом анализе CTL (доказательствах), как правило, будет использоваться один из двух упомянутых базисов

Задача model checking относительно CTL

Для модели Крипке M и ctl-формулы φ записью $Sat(M, \varphi)$ будем обозначать множество всех состояний s этой модели, для которых верно $M, s \models \varphi$

Ctl-формула φ **выполняется на модели** $M = (S, S_0, \rightarrow, L)$ ($M \models \varphi$), если справедливо включение $S_0 \subseteq Sat(M, \varphi)$

Небольшое пояснение:

- ▶ Ctl-формула делит все состояния модели на **хорошие** (в которых формула выполняется) и **плохие** (в которых формула не выполняется)
- ▶ Соотношение $M \models \varphi$ означает, что состояние, в котором система начинает выполняться, обязательно **хорошее**

Задача model checking для CTL (MC-CTL) формулируется так:

Для заданной модели Крипке M и заданной ctl-формулы φ проверить справедливость соотношения

$$M \models \varphi$$