# Математические методы верификации схем и программ

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

Блок 21

Логика деревьев вычислений (CTL)

Постановка задачи верификации моделей Крипке относительно CTL

Лектор:
**Подымов Владислав Васильевич**
E-mail:
**valdus@yandex.ru**

ВМК МГУ, 2023/2024, осенний семестр

# Вступление

LTL — это несложно устроенный язык формальной спецификации моделей Крипке

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

Естественно возникает желание уметь проверять, **существует** ли вычисление модели, удовлетворяющее свойству $\varphi$

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

$$M \models \forall\varphi \qquad\qquad M \models \exists\varphi$$

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 (Computation Tree Logic, CTL; она же логика ветвящегося времени),

- похожая на LTL, но
- содержащая такие кванторы, как выше, 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

Краткий синтаксис этих формул над множеством атомарных высказываний AP:

$$\begin{aligned} \Phi &::= \mathbb{t} \mid p \mid (\Phi \,\&\, \Phi) \mid (\neg\Phi) \mid (\mathbf{A}\varphi) \mid (\mathbf{E}\varphi), \\ \varphi &::= (\mathbf{X}\Phi) \mid (\Phi \mathbf{U} \Phi), \end{aligned}$$

где $\Phi$ — формула состояния (её же будем называть ctl-формулой), $\varphi$ — формула пути и $p \in \mathrm{AP}$

# Логика деревьев вычислений: синтаксис

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

- **A**$\varphi$: любой бесконечный путь, исходящий из текущего состояния, обладает свойством $\varphi$
- **E**$\varphi$: существует бесконечный путь, исходящий из текущего состояния и обладающий свойством $\varphi$

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

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

- **AG**$\Phi = \neg$**EF**$\neg\Phi$
- **EG**$\Phi = \neg$**AF**$\neg\Phi$

Приоритеты операций **A** и **E** одинаковы и такие же, как и $\neg$ и **X**, а в остальном — как в LTL

# Логика деревьев вычислений: примеры

**Примеры** ctl-формул и выражаемых ими свойств вычислительных систем:

- Цель может быть достигнута
$$\mathbf{EF}\mathit{goal}$$
- Как бы ни работал компьютер, есть возможность в дальнейшем его выключить
$$\mathbf{AGEF}\mathit{off}$$
- Тех, кто много грешит, неотвратимо настигнет кара
$$\mathbf{AG}(\mathit{too\_many\_sins} \rightarrow \mathbf{AF}\mathit{punishment})$$
- Если я захочу всё бросить, то смогу сделать это на следующий день
$$\mathbf{AG}(\mathit{want} \rightarrow \mathbf{EX}\mathit{quit})$$
- Если я провинюсь, то меня обязательно накажут на следующий день
$$\mathbf{AG}(\mathit{guilty} \rightarrow \mathbf{AX}\mathit{punisment})$$

# Логика деревьев вычислений: семантика

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

- Соотношение $M, s \models \mathbb{t}$ верно всегда
- $M, s \models p$, где $p \in \mathrm{AP} \Leftrightarrow p \in L(s)$
- $M, s \models \Phi_1 \,\&\, \Phi_2 \Leftrightarrow M, s \models \Phi_1$ 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 $\pi$ в $M$, исходящего из $s$, верно $M, \pi \models \varphi$
- $M, s \models \mathbf{E}\varphi \Leftrightarrow$ в $M$ существует бесконечный путь $\pi$, исходящий из $s$ и такой что $M, \pi \models \varphi$
- $M, \pi \models \mathbf{X}\Phi \Leftrightarrow M, \pi[2] \models \Phi$
- $M, \pi \models \Phi_1 \mathbf{U} \Phi_2 \Leftrightarrow$ 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.** **Для любых модели Крипке $M$, её бесконечного пути $\pi$ и ctl-формулы $\Phi$ верно:**
$M, \pi \models \mathbf{F}\Phi \Leftrightarrow$ **в $\pi$ содержится состояние $s$, для которого верно** $M, s \models \Phi$

**Утверждение.** **Для любых модели Крипке $M$, её бесконечного пути $\pi$ и ctl-формулы $\Phi$ верно:**
$M, \pi \models \mathbf{G}\Phi \Leftrightarrow$
**для любого состояния $s$ пути $\pi$ верно** $M, s \models \Phi$

Эти два утверждения обосновывать не будем ввиду их простоты

**Утверждение**
**Для любых модели Крипке $M$, состояния $s$ и ctl-формулы $\Phi$ верно:**
$M, s \models \mathbf{AGAF}\Phi \Leftrightarrow$ **для любого бесконечного пути $\pi$ 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 $M = (S, S_0, \to, L)$ относительно состояния $\mathfrak{s}$ называется бесконечное ориентированное дерево следующего вида

Дерево разбито на ярусы, пронумерованные моментами времени, и дуги из $i$-го яруса ведут только в $(i+1)$-й

Каждая вершина дерева помечена состоянием модели

0-й ярус состоит из одной вершины — корня, помеченного состоянием $\mathfrak{s}$

Если вершина $v$ $i$-го яруса помечена состоянием $s$ и $s \to s'$, то в развёртке из $v$ исходит дуга в вершину, помеченную $s'$

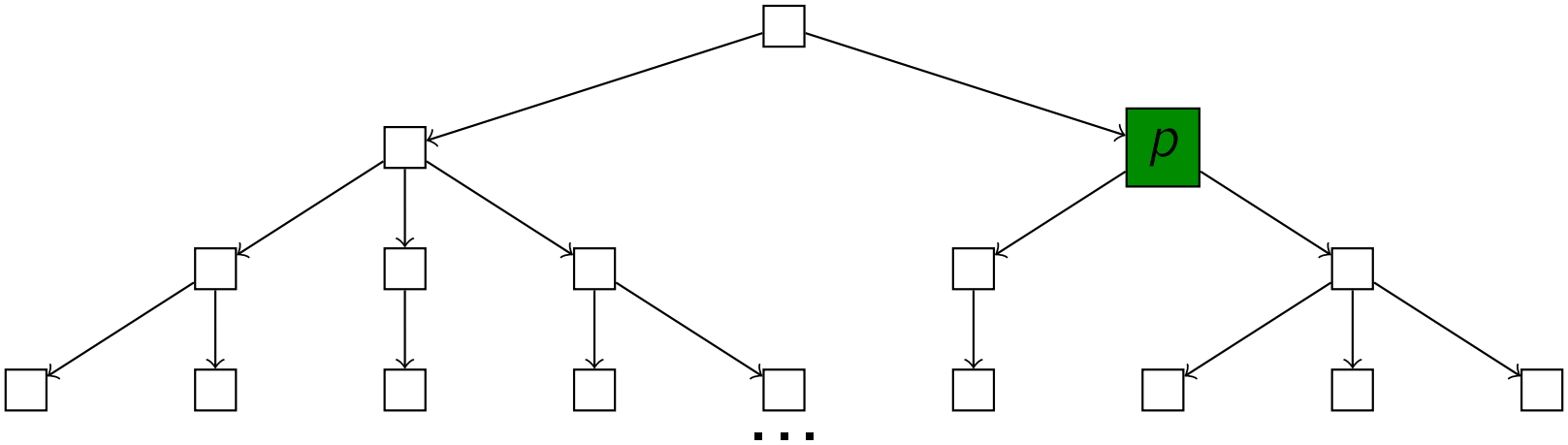
---

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

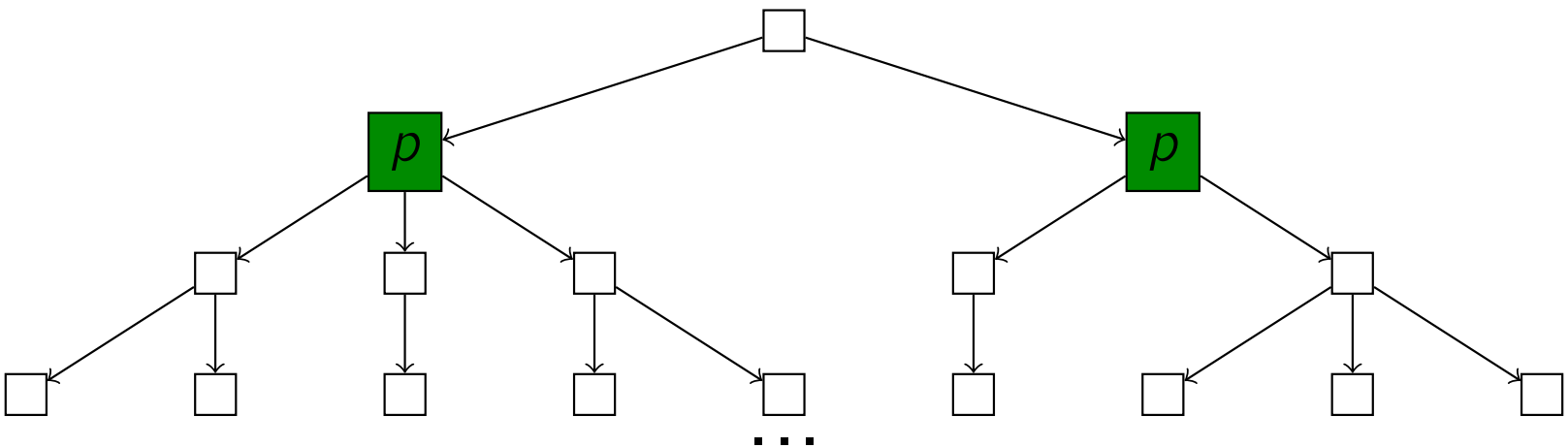
Можно проиллюстрировать эти сочетания на развёртке следующим образом

# Логика деревьев вычислений: основные свойства

**EX**$p$

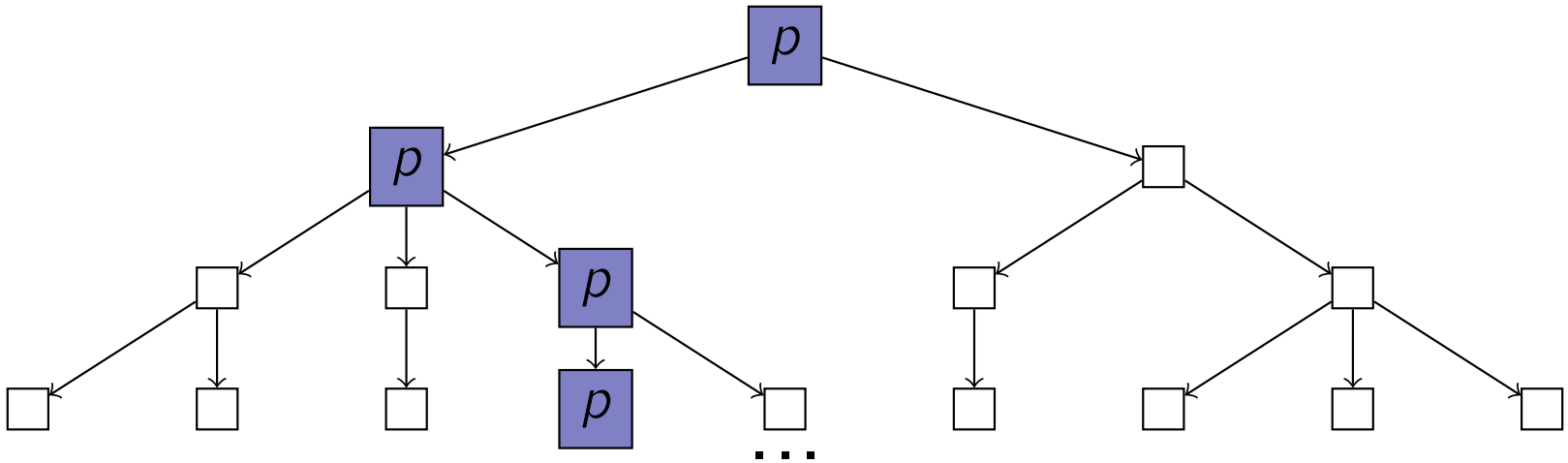



**AX**$p$

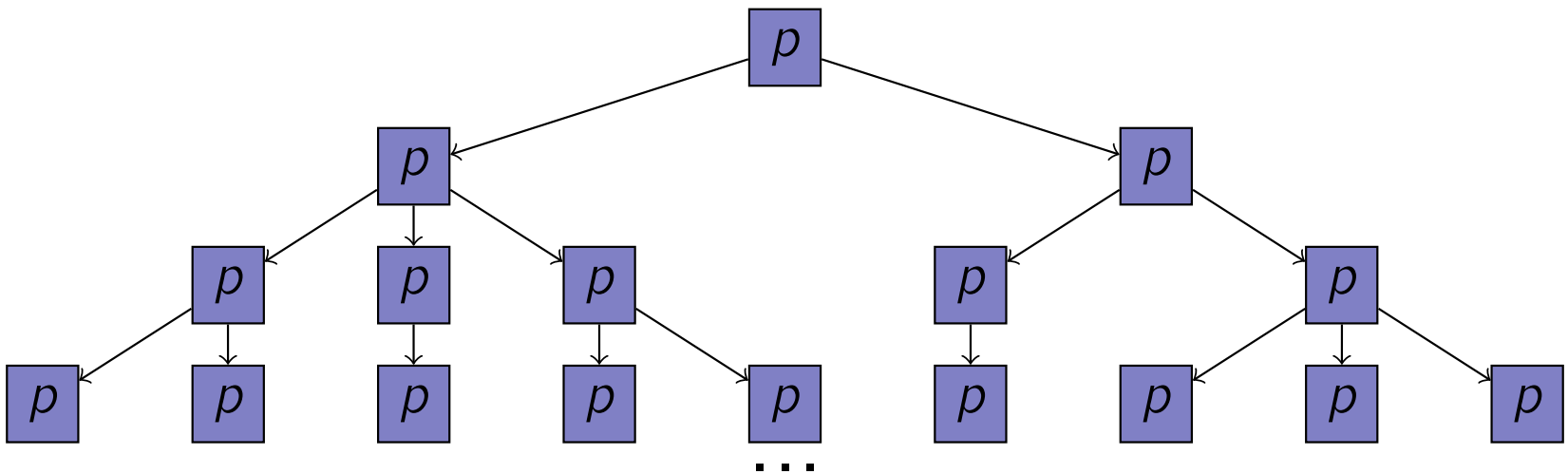


# Логика деревьев вычислений: основные свойства

**EG**$p$

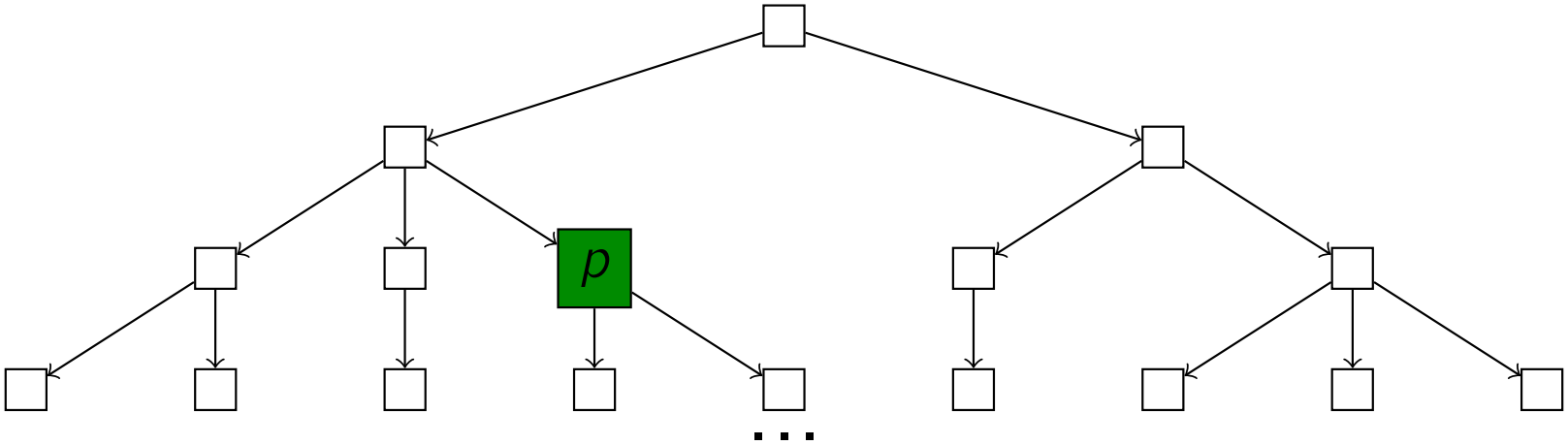



**AG**$p$

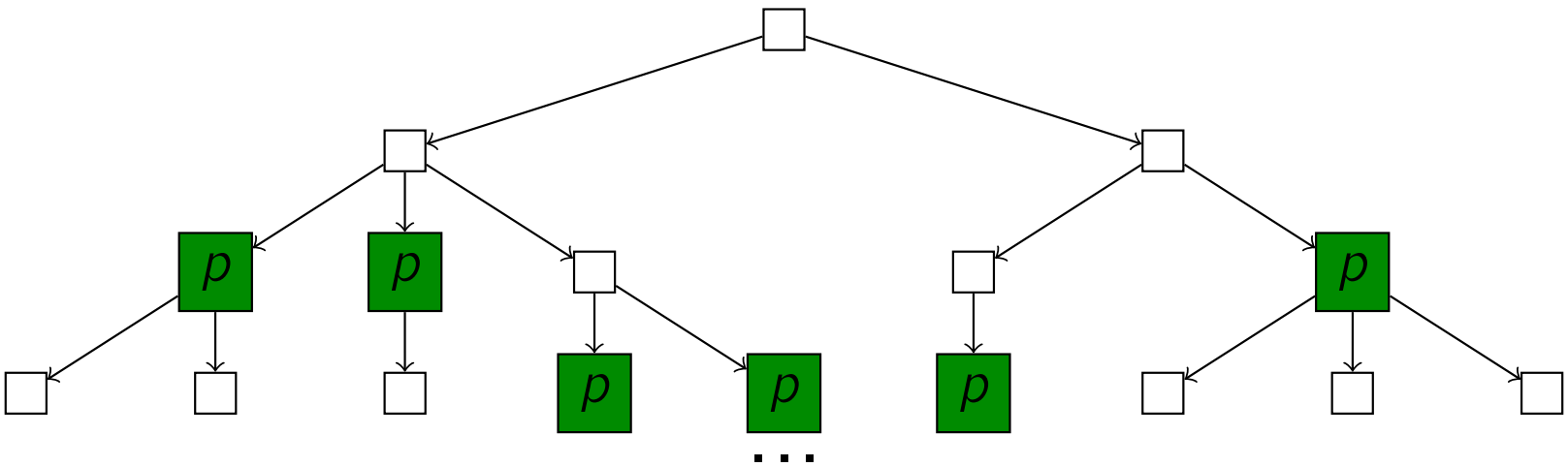


# Логика деревьев вычислений: основные свойства

**EF**$p$

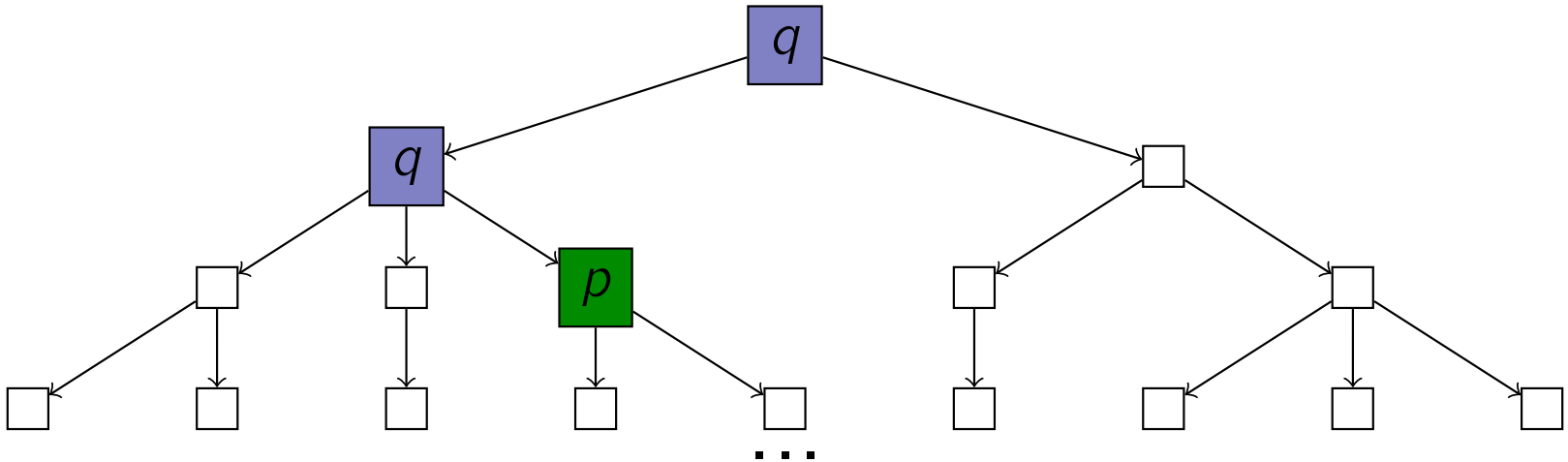



**AF**$p$

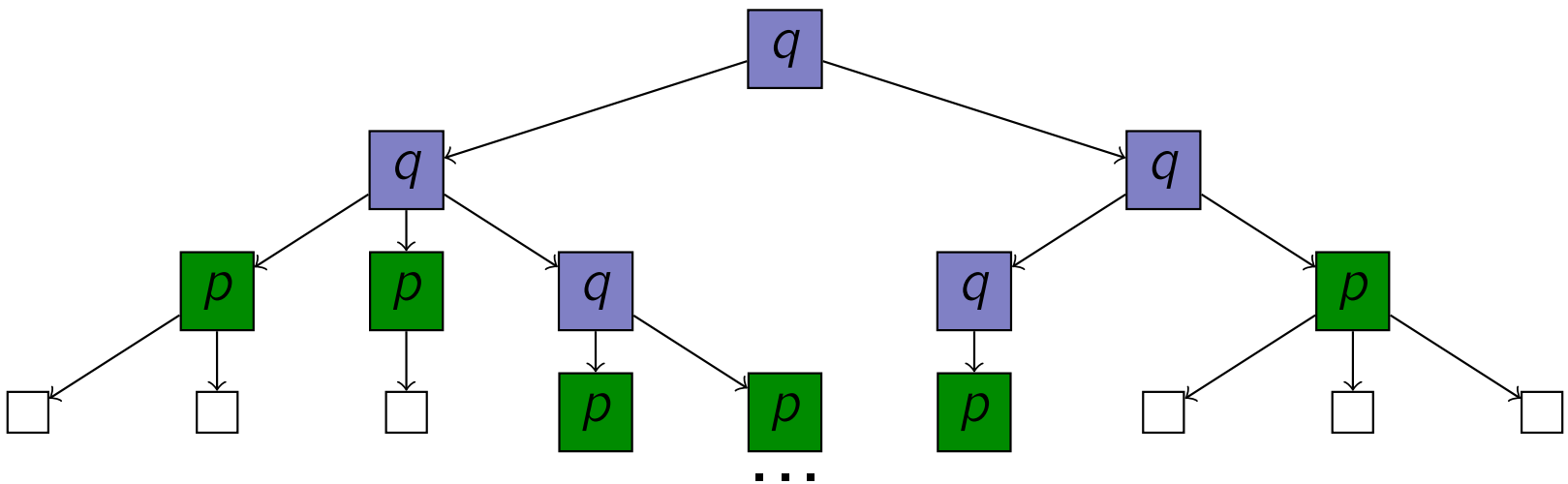


# Логика деревьев вычислений: основные свойства

$\mathbf{E}(q\mathbf{U}p)$




$\mathbf{A}(q\mathbf{U}p)$



# Логика деревьев вычислений: основные свойства

Будем говорить, что ctl-формулы $\Phi$ и $\Psi$ равносильны ($\Phi \sim \Psi$), если для любой модели Крипке $M$ и любого состояния $s$ справедлива равносильность

$$M, s \models \Phi \Leftrightarrow M, s \models \Psi$$

Согласно краткому и полному синтаксисам, справедливы следующие равносильности, позволяющие *выразить* темпоральные комбинации **AF**, **EF**, **AG** и **EG** через комбинации краткого синтаксиса:

- $\mathbf{AF}\Phi \sim \mathbf{A}(\mathbb{t}\mathbf{U}\Phi)$
- $\mathbf{EF}\Phi \sim \mathbf{E}(\mathbb{t}\mathbf{U}\Phi)$
- $\mathbf{AG}\Phi \sim \neg\mathbf{EF}\neg\Phi$
- $\mathbf{EG}\Phi \sim \neg\mathbf{AF}\neg\Phi$

Кроме того, несложно убедиться в такой равносильности:

**Утверждение.** $\mathbf{AX}\Phi \sim \neg\mathbf{EX}\neg\Phi$

Значит, при составлении формул можно обойтись тремя комбинациями:

**EX**, **AU** и **EU**

# Логика деревьев вычислений: основные свойства

**EX**, **AU** и **EU**

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

**Утверждение.** $\mathbf{A}(\Phi\mathbf{U}\Psi) \sim \neg\mathbf{E}(\neg\Psi\mathbf{U}(\neg\Phi \,\&\, \neg\Psi)) \,\&\, \neg\mathbf{EG}\neg\Psi$

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 $\Phi$ записью $Sat(M, \Phi)$ будем обозначать множество всех состояний $s$ этой модели, для которых верно $M, s \models \Phi$

Ctl-формула $\Phi$ выполняется на модели $M = (S, S_0, \to, L)$ ($M \models \Phi$), если справедливо включение $S_0 \subseteq Sat(M, \Phi)$

*Небольшое пояснение*:

- Ctl-формула делит все состояния модели на хорошие (в которых формула выполняется) и плохие (в которых формула не выполняется
- Соотношение $M \models \Phi$ означает, что все состояния, в которых система может начать своё выполнение, хорошие

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

**Для заданной модели Крипке $M$ и заданной ctl-формулы $\Phi$ проверить справедливость соотношения**

$$M \models \Phi$$