Введение в моделирование и верификацию аппаратных и программных систем

Лекция 10: Разделенная нормальная форма для логики линейного времени LTL: условные обязательства и построение автомата.

Борис Юрьевич Конев

konev@liverpool.ac.uk

Liverpool University

Октябрь-Ноябрь 2007

Синтаксис LTL

Формулы строятся из

- Пропозициональных переменных *Prop*
- Пропозициональных связок **true**, **false**, $\neg$, $\vee$, $\wedge$, $\rightarrow$ и $\equiv$.
- Временных операторов, **X**, **F**, **G**, **U** и **W**.
- Множество формул (*WFF*)
  - Пропозициональные переменные
  - **true** и **false**
  - Если φ и ψ – формулы, то
    - $\neg\varphi$, $\varphi \wedge \psi$, $\varphi \vee \psi$, $\varphi \rightarrow \psi$, $\varphi \equiv \psi$
    - $\mathbf{X}\varphi$
    - $\mathbf{F}\varphi$
    - $\mathbf{G}\varphi$
    - $\varphi\mathbf{U}\psi$
    - $\varphi\mathbf{W}\psi$

  } формулы

Семантика

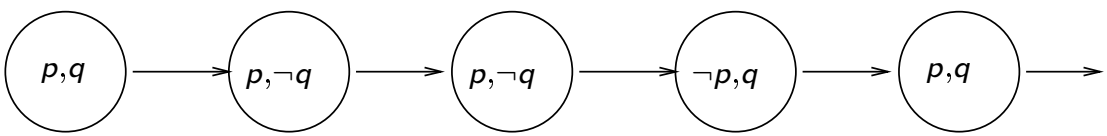
- LTL интерпретируется над дискретными линейными порядками, изоморфными множеству натуральных чисел $\mathbb{N}$.
- Интерпретация LTL, σ, это последовательность состояний

$$\sigma = s_0, s_1, s_2, s_3, \ldots$$

где каждое состояние s_i представляет собой множество пропозициональных переменных, истинных в i-й момент времени.

- Формулы интерпретируются в момент времени $i \in \mathbb{N}$.

$$(\sigma, i) \models A$$



Проверка LTL моделей

- Проверка моделей: по системе переходов S и LTL формуле φ определить, обладает ли S свойством φ, т.е., верно ли

$$S \models \varphi.$$

- Мы рассмотрели дедуктивный подход: построить формулу ψ_S т.ч. $S \models \varphi$ тогда и т.т., когда формула $\psi_S \rightarrow \varphi$ общезначима.
- Проблема: проверка общезначимости LTL формулы является PSPACE полной
- На самом деле, существуют алгоритмы, имеющие сложность

$$O(|S| \cdot 2^{|\varphi|}).$$

Автоматы и модели

Практически все реализации проверки LTL моделей (неформально говоря) используют следующий подход:

- Построить по формуле автомат
- Скомбинировать построенный автомат с системой переходов и либо
  - свести к проверке CTL моделей, либо
  - использовать автоматные техники

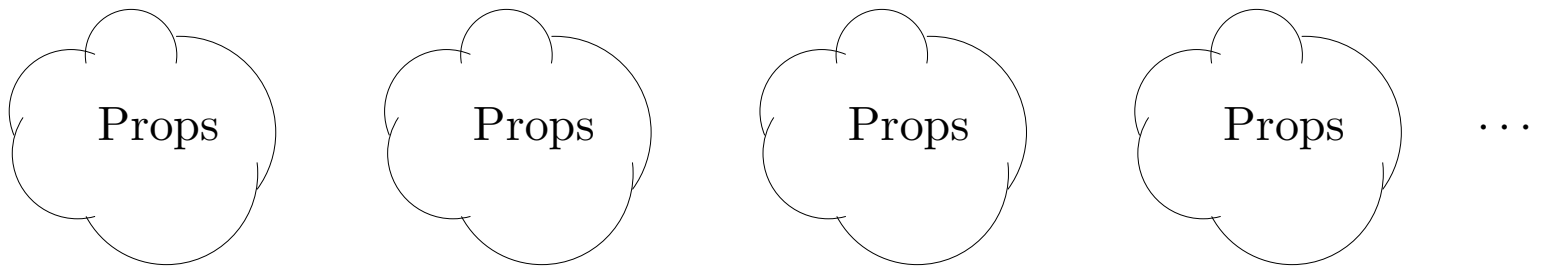
Разделенная нормальная форма DSNF для логики LTL

- Процесс построения автомата по произвольной LTL формуле довольно сложен.
- Во вводных курсах обычно принимается без доказательства.

- Мы пойдем другим путем: опишем фрагмент LTL
  - множество LTL формул в нормальной форме;
  - для него построение автомата существенно проще;
  - так как любая формула может быть приведена к нормальной форме, автомат для $DSNF(f)$ может быть использован и для f.

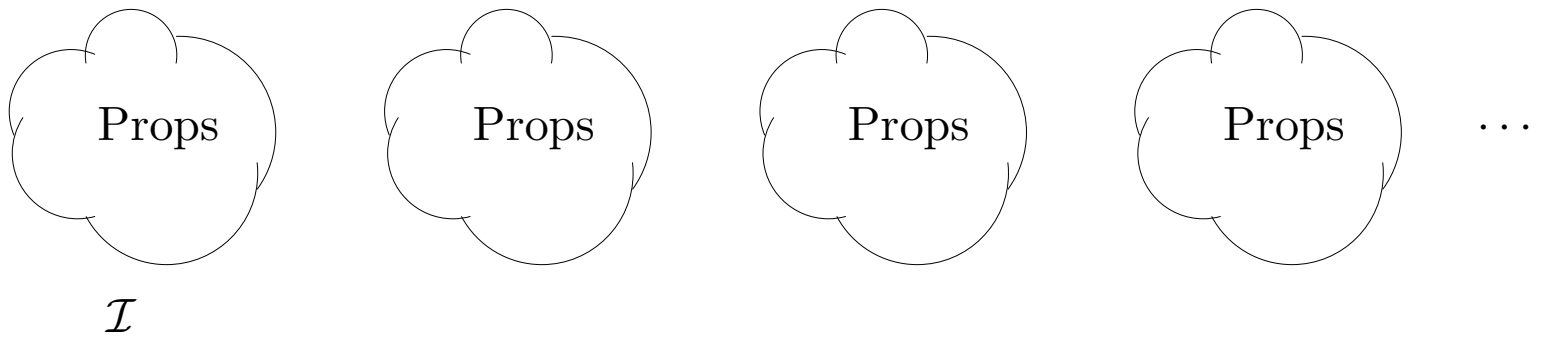
Очень неформально

$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



Очень неформально

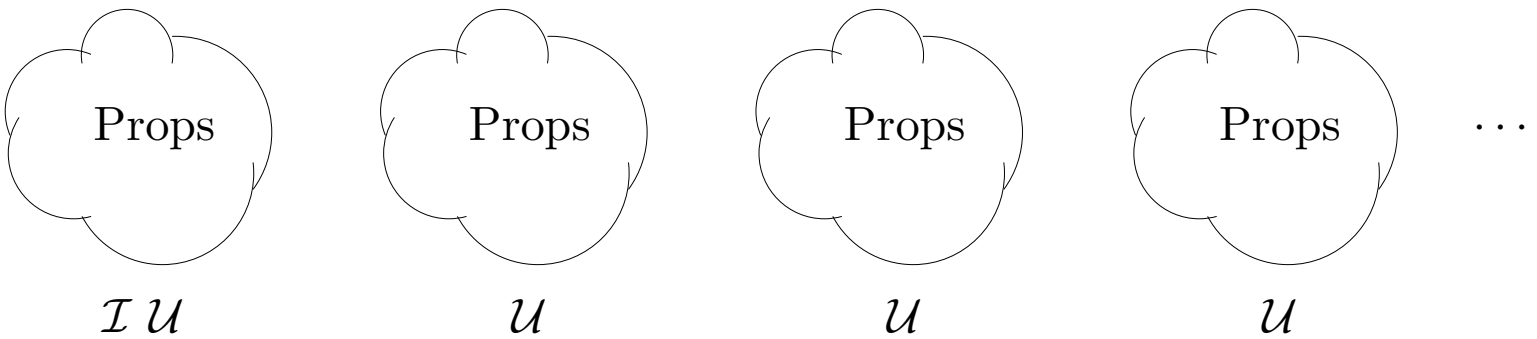
$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



- Часть формулы “действует” только в момент 0

Очень неформально

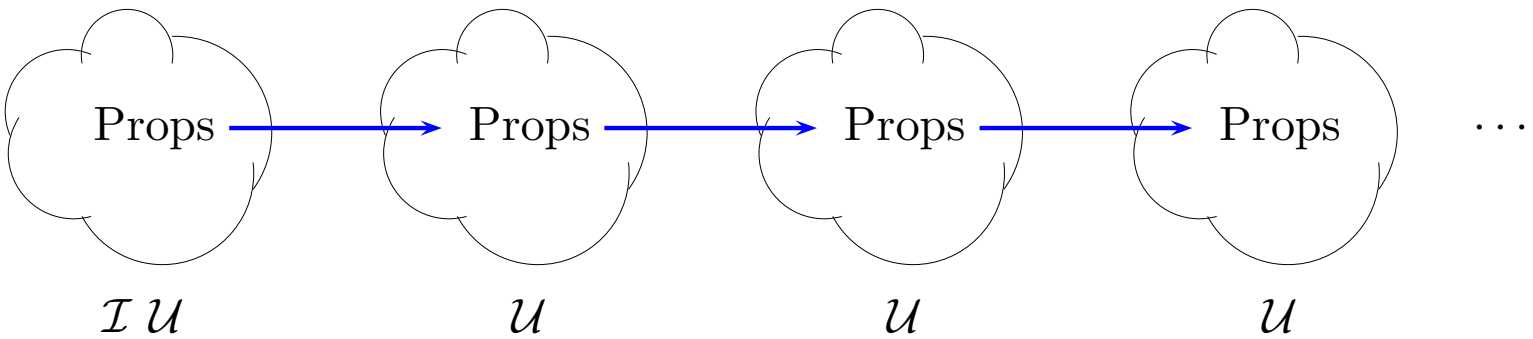
$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



- Часть формулы “действует” только в момент 0
- Часть — везде

Очень неформально

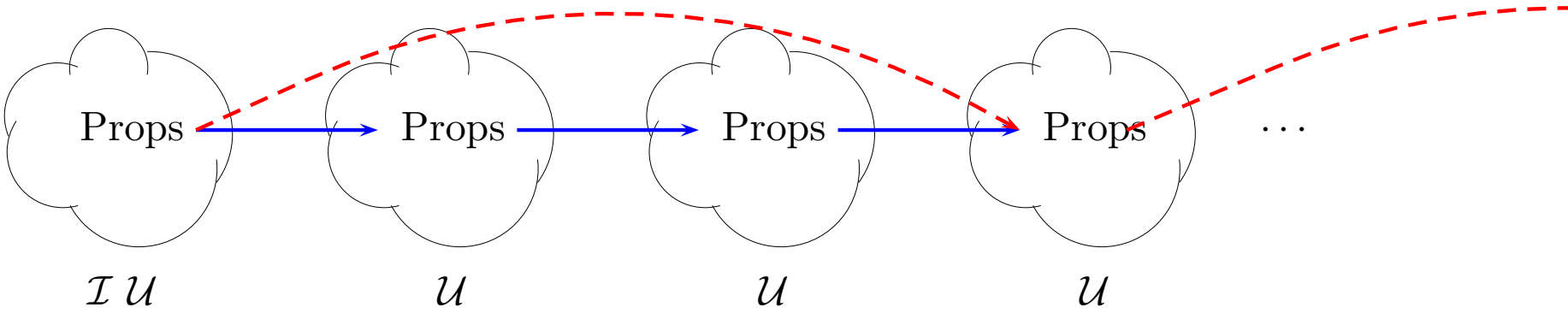
$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



- Часть формулы “действует” только в момент 0
- Часть — везде
- Часть передает информацию в следующий момент

Очень неформально

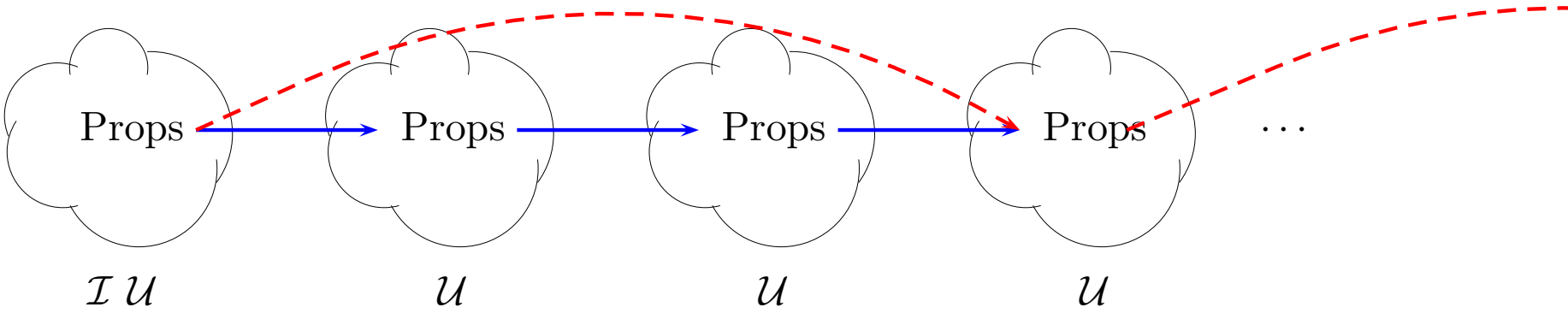
$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



- Часть формулы “действует” только в момент 0
- Часть — везде
- Часть передает информацию в следующий момент
- Часть передает информацию в будущее

Очень неформально

$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



- Часть формулы “действует” только в момент 0
- Часть — везде
- Часть передает информацию в следующий момент
- Часть передает информацию в будущее

Но это все может быть запутано струкрурой формулы

Divided Separated Normal Form (DSNF)

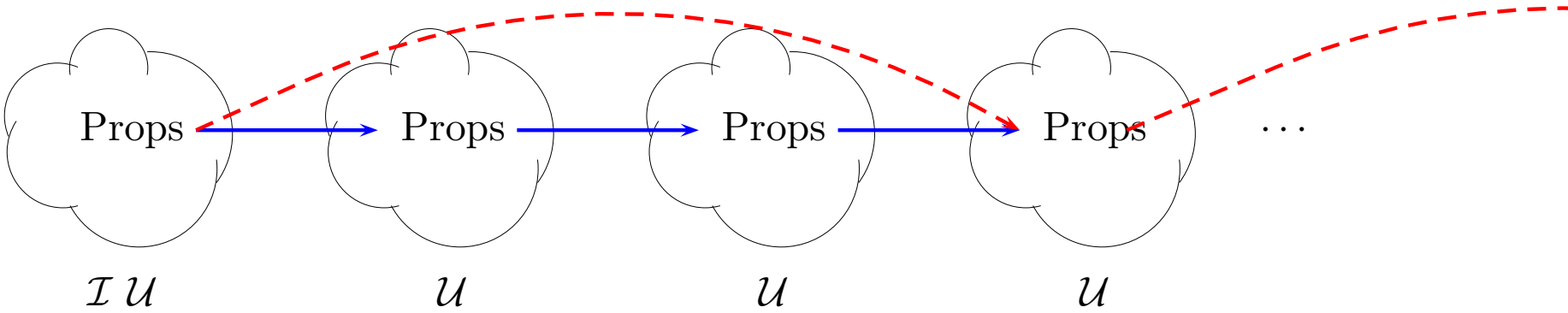
Четыре множества формул

1. Универсальная часть $\mathcal{U}$: множество пропозициональных формул;
2. Начальная часть $\mathcal{I}$: множество пропозициональных формул
3. Шаги $\mathcal{S}$: множество формул вида
$$\varphi \rightarrow \mathbf{X}\psi$$
4. Обязательства $\mathcal{E}$: множество формул вида
$$\mathbf{F}l,$$
где l — пропозициональный литерал

Смысл: $\mathcal{I} \wedge \mathbf{G}\mathcal{U} \wedge \mathbf{G}\mathcal{S} \wedge \mathbf{G}\mathcal{E}$

Пример

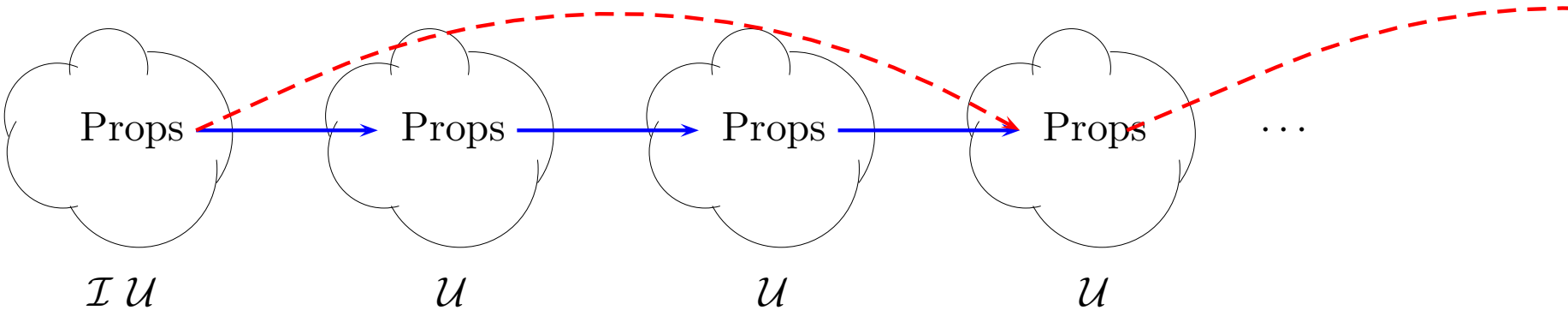
$$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$$



- $\mathcal{I} = \{(q \vee q)\}$
- $\mathcal{U} = \{r\}$
- $\mathcal{S} = \{p \rightarrow \mathbf{X}q\}$
- $\mathcal{E} = \{\mathbf{F}p\}$

Пример

$(p \vee q) \wedge \mathbf{G}r \wedge \mathbf{G}(p \rightarrow \mathbf{X}q) \wedge \mathbf{GF}p$



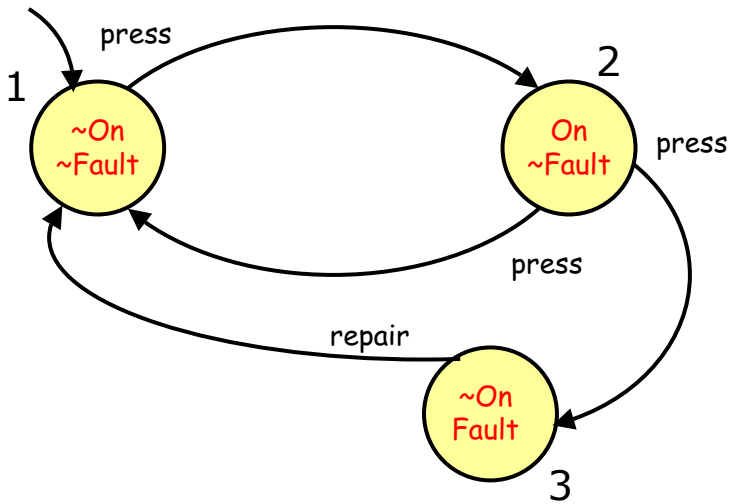
- $\mathcal{I} = \{(q \vee q)\}$
- $\mathcal{U} = \{r\}$
- $\mathcal{S} = \{p \rightarrow \mathbf{X}q\}$
- $\mathcal{E} = \{\mathbf{F}p\}$

G подразумевается неявно

Модель выключателя

$$\mathcal{I} = \{p_1\}$$

$$\mathcal{U} = \left\{ \begin{array}{l} (p_1 \rightarrow \neg On, \neg Fault), \\ (p_2 \rightarrow On, \neg Fault), \\ (p_3 \rightarrow \neg On, Fault), \\ (p_1 \rightarrow \neg p_2, \neg p_3), \\ (p_2 \rightarrow \neg p_1, \neg p_3), \\ (p_3 \rightarrow \neg p_1, \neg p_2) \end{array} \right\}$$



$$\mathcal{S} = \left\{ \begin{array}{l} (p_1 \rightarrow \mathbf{X} p_2), \\ (p_2 \rightarrow \mathbf{X}(p_1 \vee Next p_3)), \\ (p_3 \rightarrow \mathbf{X} p_1) \end{array} \right\}$$

Условие “справедливости”

$$\mathcal{E} = \{\mathbf{F} Fault\}$$

План действий

- Сведение к DSNF
- Связь моделей φ и $DSNF(\varphi)$
- Автомат, принимающий модели $DSNF(\varphi)$

План действий

- Сведение к DSNF
  - Сведение к NNF
  - Переименованние подформул и характеризация с неподвижной точкой
  - Условные обязательсства
  - Безусловные обязательсства
- Связь моделей φ и $DSNF(\varphi)$
- Автомат, принимающий модели $DSNF(\varphi)$

Сведение к NNF

NNF-формула:

- Из пропозициональных связок допускаются только $\wedge$, $\vee$, $\neg$
- Отрицания применяются только к пропозициональным переменным

$$
\begin{aligned}
\neg\mathbf{X}\varphi &\equiv \mathbf{X}\neg\varphi;\\
\neg\mathbf{G}\varphi &\equiv \mathbf{F}\neg\varphi;\\
\neg\mathbf{F}\varphi &\equiv \mathbf{G}\neg\varphi;\\
\neg(\varphi\mathbf{U}\psi) &\equiv \neg\psi\mathbf{W}(\neg\varphi\wedge\neg\psi));\\
\neg(\varphi\mathbf{W}\psi) &\equiv \neg\psi\mathbf{U}(\neg\varphi\wedge\neg\psi).
\end{aligned}
$$

Для любой формулы φ и интерпретации σ:

$$\sigma \models \varphi \Longleftrightarrow \sigma \models \mathit{NNF}(\varphi)$$

Пример

Переименовывание подформул

Рекурсивно переименуем временные подформулы, начиная с самых вложенных:

φ — формула, ψ — её подформула вида $\mathbf{F}\psi_1$, $\mathbf{G}\psi_1$, $\psi_1\mathbf{U}\psi_2$ или $\psi_1\mathbf{W}\psi_2$

- Заменить все вхождения ψ на новую пропозициональную переменную p
- Добавить новый конъюнкт $\mathbf{G}(p \rightarrow \psi)$

Пример

Переименование и интерпретации

Интерпретация σ^* рассширяет интерпретацию σ, если

- $(\sigma, i) \models p \to (\sigma^*, i) \models p$
- $(\sigma, i) \models \neg p \to (\sigma^*, i) \models \neg p$

При этом, σ^* может придавать значение пропозициональным переменным, которым σ не придает никакого значения.

Например, $\{a, \neg b, x, y\}$ рассширяет $\{a, \neg b\}$;
$\{\neg a, \neg b, x, y\}$ не является рассширением $\{a, \neg b\}$.

Упражнение

Пусть формула φ^* получена переименованием подформул φ.

- *Любая $\sigma : \sigma \models \varphi$ может быть рассширена до σ^*: $\sigma^* \models \varphi^*$;*
- *Для любой $\sigma^* : \sigma^* \models \varphi^*$ имеет место $\sigma^* \models \varphi$.*

Представление неподвижной точкой

Переименование вводит импликации вида

$$\begin{array}{llll} \mathbf{G}(p & \rightarrow & \mathbf{G}\psi_1); & \qquad \mathbf{G}(p \rightarrow \mathbf{X}\psi_1); \\ \mathbf{G}(p & \rightarrow & \psi_1 \mathbf{U} \psi_2); & \qquad \mathbf{G}(p \rightarrow \mathbf{F}\psi_1); \\ \mathbf{G}(p & \rightarrow & \psi_1 \mathbf{W} \psi_2); & \end{array}$$

Заметим что

$$\mathbf{G}\psi_1 \equiv \psi_1 \wedge \mathbf{X}\mathbf{G}\psi_1$$

- Мы уже использовали подобные эквивалентности (для CTL), чтобы представить временные операторы в виде неподвижной точки.
- Теперь мы введем новые переменные.

$\mathbf{G}(p \to \mathbf{G}\psi_1)$

Пусть $\psi = \mathbf{G}(p \to \mathbf{G}\psi_1)$. Рассмотрим

$$\psi^* = \mathbf{G}(p \to r) \wedge \mathbf{G}(r \to \mathbf{X}r) \wedge \mathbf{G}(r \to \psi_1),$$

где r — новая переменная.

Теорема

- *Любая* $\sigma : \sigma \models \mathbf{G}(p \to \mathbf{G}\psi_1)$ *может быть рассширена до* σ^*: $\sigma^* \models \psi^*$;
- *Для любой* $\sigma^* : \sigma^* \models \psi^*$ *имеет место* $\sigma^* \models \mathbf{G}(p \to \psi_1)$.

Доказательство ($\Longrightarrow$):

Определим $(\sigma^*, i) \models r \iff (\sigma, i) \models \mathbf{G}\psi_1$

($\Longleftarrow$):

Заметим, что $(\sigma^*, i) \models r$ влечет $(\sigma^*, i) \models \mathbf{G}\psi_1$

$\mathbf{G}(p \to \psi_1 \mathbf{U} \psi_2)$

Пусть $\psi = \mathbf{G}(p \to \psi_1 \mathbf{U} \psi_2)$. Рассмотрим

$$\begin{aligned}\psi^* = & \mathbf{G}(p \to \mathbf{F}\psi_2) \\ & \wedge \mathbf{G}(p \to (\psi_1 \wedge s) \vee \psi_2) \\ & \wedge \mathbf{G}(s \to \mathbf{X}((\psi_1 \wedge s) \vee \psi_2))\end{aligned}$$

где s — новая переменная.

Теорема

- *Любая* $\sigma : \sigma \models \mathbf{G}(p \to \psi_1 \mathbf{U} \psi_2)$ *может быть рассширена до* σ^*: $\sigma^* \models \psi^*$;
- *Для любой* $\sigma^* : \sigma^* \models \psi^*$ *имеет место* $\sigma^* \models \mathbf{G}(p \to \psi_1 \mathbf{U} \psi_2)$.

Доказательство ($\Longrightarrow$):

Определим $(\sigma^*, i) \models s \iff (\sigma, i) \models (\neg\psi_2 \wedge \psi_1 \mathbf{U} \psi_2)$

($\Longleftarrow$):

Заметим, что $(\sigma^*, i) \models (s \wedge \mathbf{F}\psi_2)$ влечет $(\sigma^*, i) \models \psi_1 \mathbf{U} \psi_2$

$\mathbf{G}(p \to \psi_1 \mathbf{W} \psi_2)$

Пусть $\psi = \mathbf{G}(p \to \psi_1 \mathbf{W} \psi_2)$. Рассмотрим

$$\begin{aligned} \psi^* = & \mathbf{G}(p \to (\psi_1 \wedge s) \vee \psi_2) \\ & \wedge \mathbf{G}(s \to \mathbf{X}((\psi_1 \wedge s) \vee \psi_2)) \end{aligned}$$

где s — новая переменная.

Теорема

- *Любая* $\sigma : \sigma \models \mathbf{G}(p \to \psi_1 \mathbf{W} \psi_2)$ *может быть рассширена до* σ^*: $\sigma^* \models \psi^*$;
- *Для любой* $\sigma^* : \sigma^* \models \psi^*$ *имеет место* $\sigma^* \models \mathbf{G}(p \to \psi_1 \mathbf{W} \psi_2)$.

Условные обязательства

Осталось разобраться с формулами вида

$$\psi = \mathbf{G}(p \to \mathbf{F}\psi_1)$$

Их называют условными обязательствами.

Рассмотрим

$$\begin{aligned}\psi^* = &\mathbf{G}((p \wedge \neg\psi_1) \to w) \wedge \\ &\mathbf{G}((w \wedge \mathbf{X}\neg\psi_1) \to \mathbf{X}w) \wedge \\ &\mathbf{GF}\neg w\end{aligned}$$

где w — новая переменная.

Теорема

- *Любая* $\sigma : \sigma \models \mathbf{G}(p \to \mathbf{F}\psi_1)$ *может быть рассширена до* σ^*: $\sigma^* \models \psi^*$;
- *Для любой* $\sigma^* : \sigma^* \models \psi^*$ *имеет место* $\sigma^* \models \mathbf{G}(p \to \mathbf{F}\psi_1)$.

Условные обязательства

Осталось разобраться с формулами вида

$$\psi = \mathbf{G}(p \to \mathbf{F}\psi_1)$$

Их называют условными обязательствами.

Рассмотрим

$$\begin{aligned}\psi^* = &\mathbf{G}((p \wedge \neg\psi_1) \to w) \wedge \\ &\mathbf{G}(w \to \mathbf{X}(\psi_1 \vee w)) \wedge \\ &\mathbf{GF}\neg w\end{aligned}$$

где w — новая переменная.

Теорема

- *Любая* $\sigma : \sigma \models \mathbf{G}(p \to \mathbf{F}\psi_1)$ *может быть рассширена до* σ^*: $\sigma^* \models \psi^*$;
- *Для любой* $\sigma^* : \sigma^* \models \psi^*$ *имеет место* $\sigma^* \models \mathbf{G}(p \to \mathbf{F}\psi_1)$.

Доказательство ($\Longrightarrow$)

$\psi = \mathbf{G}(p \to \mathbf{F}\psi_1)$;
$\psi^* = \mathbf{G}((p \wedge \neg\psi_1) \to w) \wedge \mathbf{G}((w \wedge \mathbf{X}\neg\psi_1) \to \mathbf{X}w) \wedge \mathbf{GF}\neg w$

Пусть $\sigma \models \{\mathbf{G}(p \to \mathbf{F}\psi_1)\}$. Рассмотрим два случая

1. $\sigma \models \mathbf{GF}p$.
   Значит, $\sigma \models \mathbf{GF}\psi_1$.
   Определим $(\sigma^*, i) \models \neg w \Leftrightarrow (\sigma, i) \models \psi$
2. $\sigma \models \mathbf{FG}\neg p$. Рассмотрим два подслучая
   - $\sigma \models \mathbf{G}\neg p$.
     Определим $(\sigma^*, i) \models \neg w$ для всех $i \in \mathbb{N}$.
   - Существует $j \in \mathbb{N}$ т.ч. $(\sigma, j) \models p$ и для всех $i > j$, $(\sigma, i) \models \neg p$. Тогда найдется $k \geqslant j$ т.ч. $(\sigma, k) \models \psi_1$.

     Определим

$$\begin{array}{lll} (\sigma^*, i) \models \neg w \Leftrightarrow (\sigma^*, i) \models \psi_1 & \text{если} & i < k, \\ (\sigma^*, i) \models \neg w & \text{если} & i \geqslant k. \end{array}$$

Доказательство ($\Longleftarrow$)

$\psi = \mathbf{G}(p \to \mathbf{F}\psi_1)$;
$\psi^* = \mathbf{G}((p \wedge \neg\psi_1) \to w) \wedge \mathbf{G}((w \wedge \mathbf{X}\neg\psi_1) \to \mathbf{X}w) \wedge \mathbf{GF}\neg w$

Пусть $\sigma^* \models \psi^*$. Предположим, $\sigma^* \not\models \mathbf{G}(p \to \mathbf{F}\psi_1)$, то есть, $\sigma^* \models \mathbf{F}(p \wedge \mathbf{G}\neg\psi_1)$.
Значит, найдется $m \in \mathbb{N}$ такое что $(\sigma^*, m) \models p$ и для всех $n \geqslant m$, $(\sigma^*, n) \models \neg\psi_1)$. Тогда для всех $n \geqslant m$ $(\sigma^*, n) \models w$.
Противоречие.

Пример

Поведенческий граф

Пусть $DSNF =< \mathcal{U}, \mathcal{I}, \mathcal{S}, \mathcal{E} >$. Пусть $sig(DSNF) = Prop$.

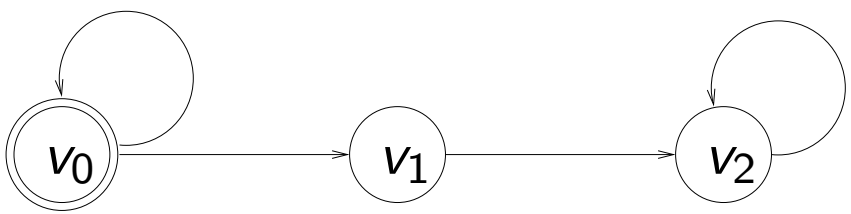
- Вершины графа G — интрепретации переменных $Prop$ такие что $L(v) \models \mathcal{U}$.
- Вершины v и v' соединены дугой если
  - для каждого $(P \rightarrow \mathbf{X}Q) \in \mathcal{S}$, если $L(v) \models P$ то $L(v') \models Q$.
- Вершина v называется начальной в G если $L(v) \models \mathcal{I} \cup \mathcal{U}$.

Поведенческий граф H для $DSNF$ это максимальный подграф G, определяемый множеством вершин, достижимых из начальных.

Пример

$$\mathcal{I} = \{\ a \wedge \neg l\ \}$$
$$\mathcal{U} = \emptyset$$
$$\mathcal{E} = \{\ \mathbf{F}l\ \}$$

$$\mathcal{S} = \left\{ \begin{array}{l} a \wedge \neg l \rightarrow \mathbf{X}((a \wedge \neg l) \vee (a \wedge l)) \\ a \wedge l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \\ \neg a \wedge \neg l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \end{array} \right\}$$



$L(v_0) = \{a, \neg l\}; \quad L(v_1) = \{a, l\}; \quad L(v_2) = \{\neg a, \neg l\}.$

Редуцированный поведенческий граф

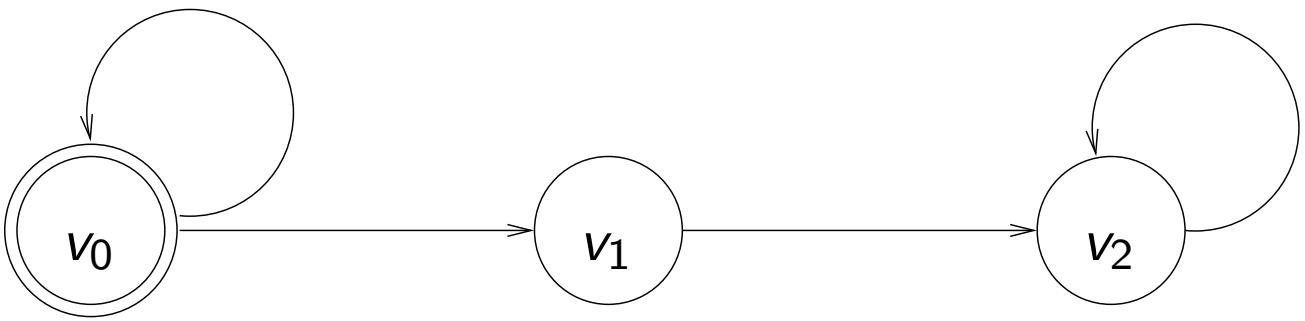
Редуцированный поведенческий граф H_R это граф, полученный из H рекурсивным удалением всех вершин v таких, что

- v не имеет потомка
- для какой-то $\mathbf{F}l \in \mathcal{E}$, не существует пути из v в вершину v' такую, что $L(v') \models l$.

Пример

$$\mathcal{I} = \{\ a \wedge \neg l\ \}$$
$$\mathcal{U} = \emptyset$$
$$\mathcal{E} = \{\ \mathbf{F}l\ \}$$

$$\mathcal{S} = \left\{ \begin{array}{l} a \wedge \neg l \rightarrow \mathbf{X}((a \wedge \neg l) \vee (a \wedge l)) \\ a \wedge l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \\ \neg a \wedge \neg l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \end{array} \right\}$$

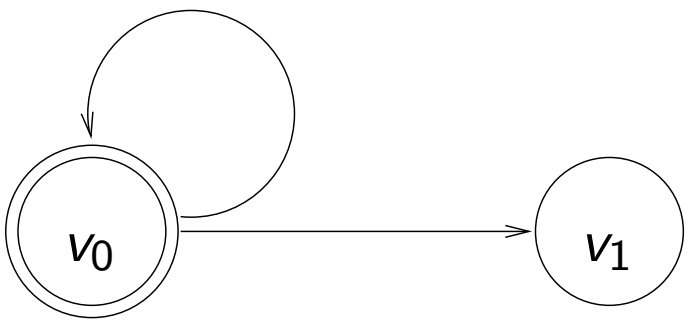


$L(v_0) = \{a, \neg l\}; \quad L(v_1) = \{a, l\}; \quad L(v_2) = \{\neg a, \neg l\}.$

Пример

$$\mathcal{I} = \{\ a \wedge \neg l\ \}$$
$$\mathcal{U} = \emptyset$$
$$\mathcal{E} = \{\ \mathbf{F}l\ \}$$

$$\mathcal{S} = \left\{ \begin{array}{l} a \wedge \neg l \rightarrow \mathbf{X}((a \wedge \neg l) \vee (a \wedge l)) \\ a \wedge l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \\ \neg a \wedge \neg l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \end{array} \right\}$$

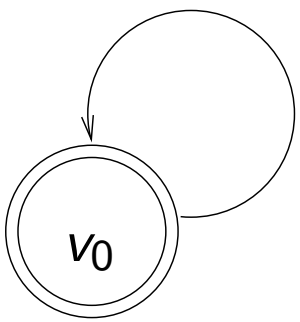


$L(v_0) = \{a, \neg l\}; \quad L(v_1) = \{a, l\}; \quad L(v_2) = \{\neg a, \neg l\}.$

Пример

$$\mathcal{I} = \{\ a \wedge \neg l\ \}$$
$$\mathcal{U} = \emptyset$$
$$\mathcal{E} = \{\ \mathbf{F}l\ \}$$

$$\mathcal{S} = \left\{ \begin{array}{l} a \wedge \neg l \rightarrow \mathbf{X}((a \wedge \neg l) \vee (a \wedge l)) \\ a \wedge l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \\ \neg a \wedge \neg l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \end{array} \right\}$$



$L(v_0) = \{a, \neg l\}; \quad L(v_1) = \{a, l\}; \quad L(v_2) = \{\neg a, \neg l\}.$

Пример

$$\mathcal{I} = \{\ a \wedge \neg l\ \}$$
$$\mathcal{U} = \emptyset$$
$$\mathcal{E} = \{\ \mathbf{F}l\ \}$$

$$\mathcal{S} = \left\{ \begin{array}{l} a \wedge \neg l \rightarrow \mathbf{X}((a \wedge \neg l) \vee (a \wedge l)) \\ a \wedge l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \\ \neg a \wedge \neg l \rightarrow \mathbf{X}(\neg a \wedge \neg l) \end{array} \right\}$$

$L(v_0) = \{a, \neg l\}; \quad L(v_1) = \{a, l\}; \quad L(v_2) = \{\neg a, \neg l\}.$

Графы и модели

Лемма

Если $\sigma \models DSNF(\varphi)$ то существует путь π в графе H_R такой что $\sigma(i) = \pi(i)$.

Лемма

Пусть π — путь в графе H_R такой, что каждая пропозициональная переменная l, где $\mathbf{F}l \in \mathcal{E}$, встречается в π бесконечно часто. Тогда $\pi \models DSNF(\varphi)$

Следствие: формула $DSNF(\varphi)$ выполнима тогда и только тогда, когда H_R не пуст.

Поведенческий граф как система переходов

- Пусть $S = (Q, T, q_0, L)$ — система переходов
- Пусть φ — LTL-формула; $DSNF(\varphi) = \langle \mathcal{U}, \mathcal{I}, \mathcal{S}, \mathcal{E} \rangle$;
- Заметим, что редуцированный поведенческий граф H_R есть “обобщенная” система переходов с условиями справедливости.

$$S_{DSNF(\varphi)} = (Q_{DSNF}, T_{DSNF}, Q_{DSNF_I}, L_{DSNF})$$

- $S \models \varphi \iff$ для любого пути σ через S найдется путь π через $S_{DSNF(\varphi)}$ такой, что π есть расширение σ и π удовлетворяет условиям справедливости.

Сведение к существованию пути в произведении

- Система переходов $S = (Q, T, q_0, L)$ и LTL формула φ.
- Рассмотрим отрицание формулы φ и построим $S_{DSNF(\neg\varphi)} = (Q_{DSNF}, T_{DSNF}, Q_{0DSNF}, L_{DSNF})$
- Построим декартово произведение $S^*(Q^*, T^*, Q_0^*, L^*) = S \times S_D$:

  $Q^* = \{(q, q_D) \mid L_D(q_D)$ расширяет $L(q)\}$,

  $T^* = \{(q, q_D) \to (q', q'_D) \mid (q \to q') \in T,\ (q_D \to q'_D) \in T_d\}$,

  $Q_0^* = \{(q_0, q_{0D}) \mid q_{0D} \in Q_{0D}\}$,

  $L^*(q, q_D) = L_D(q_D)$.

- Определим условия справедливости C (исходя из $\mathcal{E}$) для данной системы и
- Если в S^* существует бесконечный путь удовлетворяющий условиям справедливости, то в S существует путь удовлетворяющий $\neg\varphi$.

Сведение к существованию пути в произведении

"Если в S^* существует бесконечный путь удовлетворяющий условиям справедливости, то в S существует путь удовлетворяющий $\neg\varphi$"

- Сводится к проверке CTL формулы $\mathbf{EG}\mathrm{True}$ с условиями справедливости.
- Сложность: $O(|S| \cdot 2^{|\varphi|})$

Как это делает NuSMV?

- Введение одной переменной удваивает число вершин поведенческого графа.
- NuSMV не приводит LTL формулы к DSNF.
- В остальном — так же.