Синтез автомата Бюхи по формуле LTL

Занятие №8

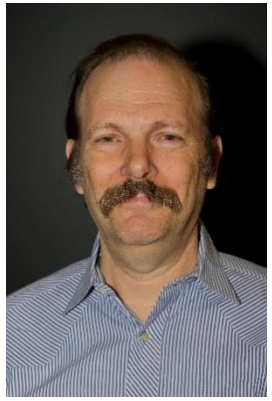
Ситуация, изучаемая нами в этой главе, напоминает диалог между «заказчиком», предъявляющим условия к поведению автомата, и «исполнителем», в задачу которого и входит построение подходящего автомата.

Б.А. Трахтенброт, Я.М. Барздинь.
Конечные автоматы (поведение и синтез)

Александр Сергеевич Камкин

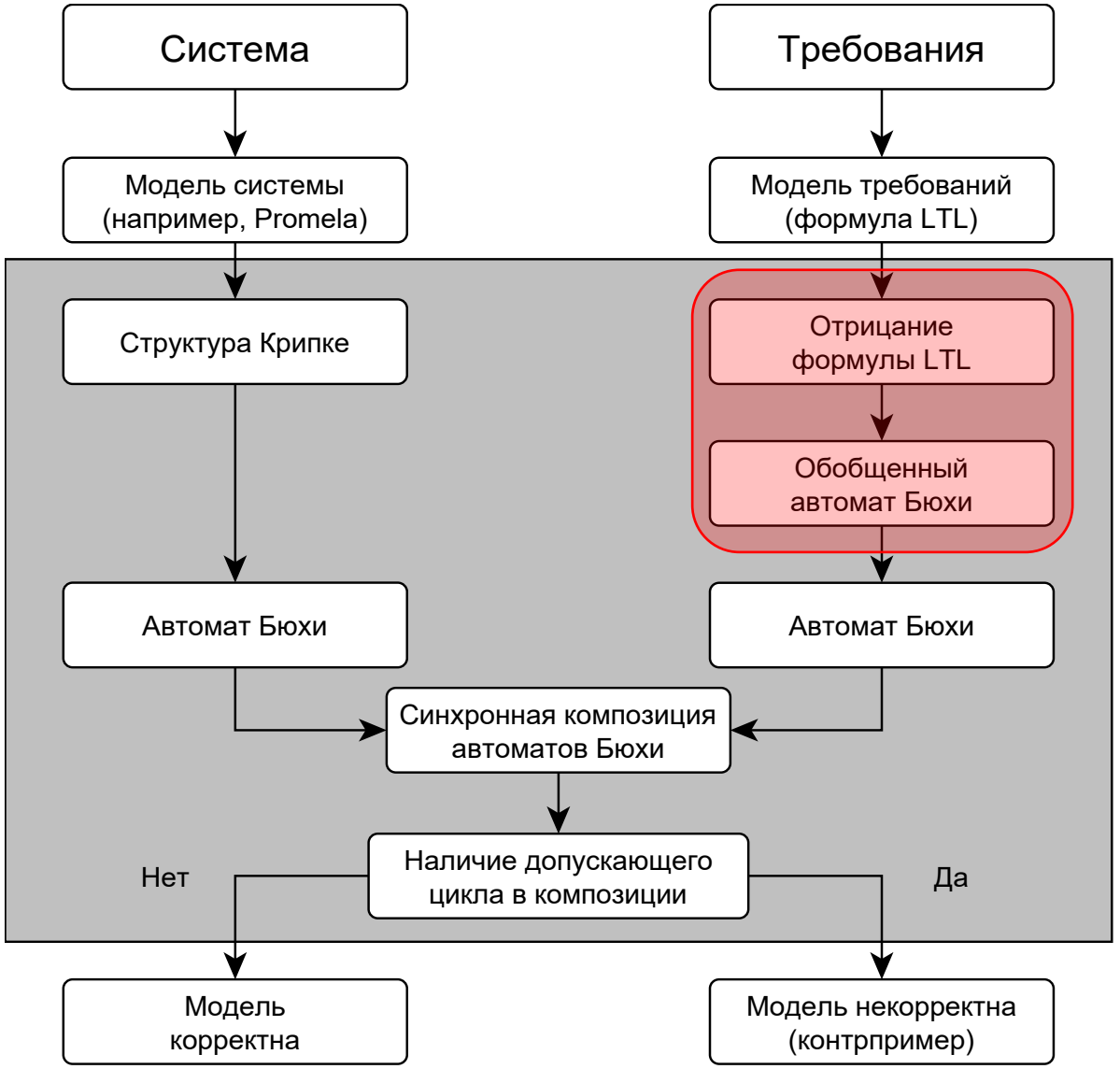
kamkin@ispras.ru

Общая схема теоретико-автоматного подхода



Moshe Y. Vardi
(1954)

Pierre Wolper
(1955)



Входные данные

Инструмент проверки моделей (например, Spin)

Преобразование обобщенного автомата Бюхи к обычному избыточно: проще искать несколько допускающих циклов

Результат

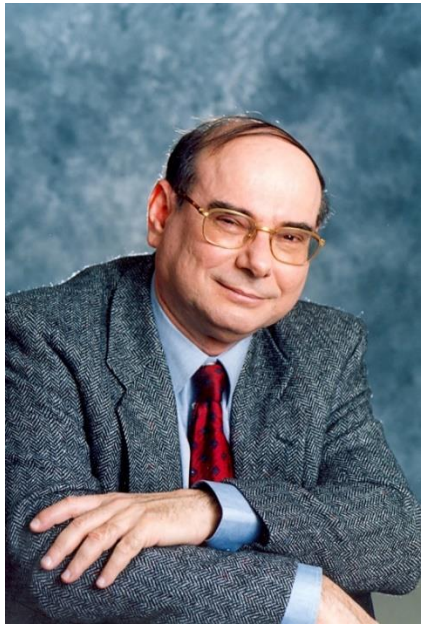
Постановка задачи синтеза

- **Вход**: формальная спецификация, описывающая поведение исполнителя
  - «Метаязык заказчика»
    - Регулярные выражения
    - LTL, S1S (монадическая логика предикатов 2-ого порядка)
    - Пре- и постусловия
- **Выход**: автомат (программа), реализующая формальную спецификацию
  - «Метаязык исполнителя»
    - Конечный автомат (диаграмма состояний или таблица переходов)
    - Автомат Бюхи (автомат Мюллера или автомат Рабина)
    - Программа

Темпоральная логика линейного времени (LTL)

$$\varphi ::= p \mid \neg\varphi \mid \varphi \vee \varphi \mid \mathbf{X}\varphi \mid \varphi \, \mathbf{U} \, \varphi$$

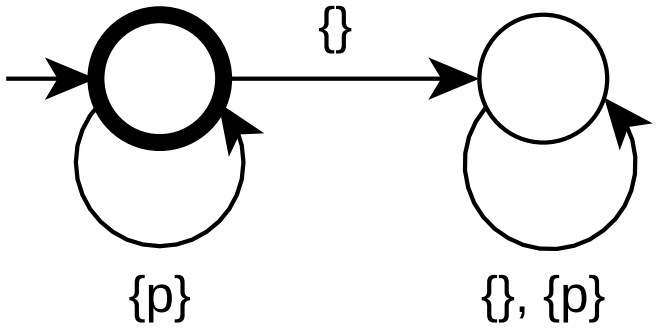
- $\mathbf{X}\varphi$ — формула φ истинна в следующий момент времени
- $\varphi \, \mathbf{U} \, \psi$ — формула ψ истинна *сейчас* или станет истинной *в будущем*, но до этого момента (не включительно) должна быть истинна формула φ
- *Производные логические связки* ($\wedge$, $\rightarrow$) *и темпоральные операторы* ($\mathbf{F}$, $\mathbf{G}$) *для простоты не рассматриваем*



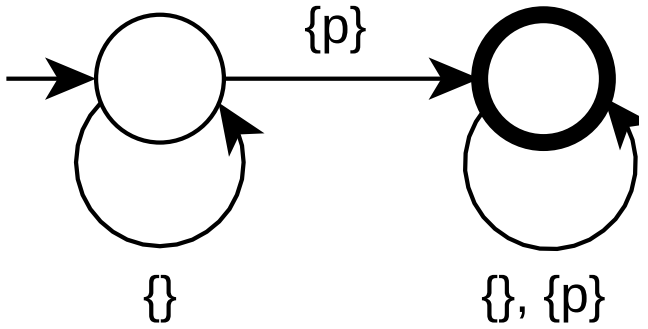
Amir Pnueli
(1941 – 2009)

Примеры автоматов Бюхи для формул LTL

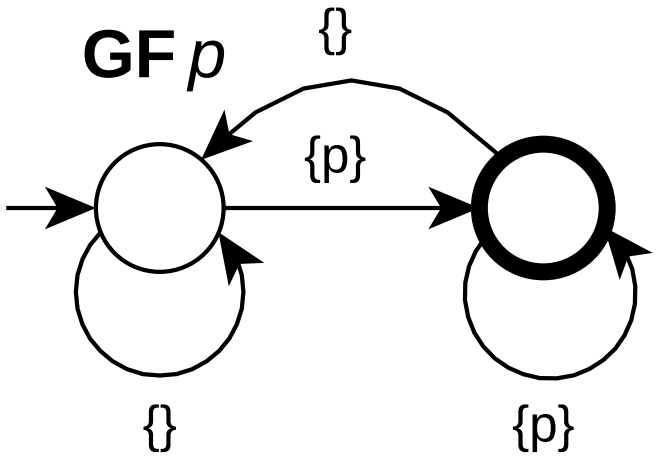
G *p*



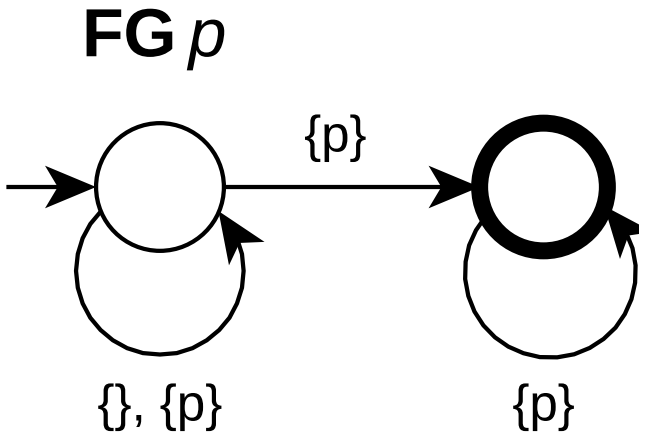
F *p*



GF *p*



FG *p*



Метафора реализации обязательств

- Темпоральная формула имеет «обязательства»
  - $\mathbf{F}\psi$ обязуется *когда-нибудь* удовлетворить свойство ψ
  - $\mathbf{G}\psi$ обязуется удовлетворять свойство ψ *всегда*
- Обязательства сложной формулы есть
  - обязательства ее подформул
- Реализация обязательств сложной формулы есть
  - *согласованная* реализация обязательств ее подформул

Замыкание формулы (closure)

- c$losure(\varphi)$ – множество всех подформул формулы φ, включая φ, вместе с их отрицаниями
- **Пример**: c$losure\big((p \vee q)\ \mathbf{U}\ (p \wedge q)\big)$
  - p
  - q
  - $(p \vee q)$
  - $(p \wedge q)$
  - $(p \vee q)\ \mathbf{U}\ (p \wedge q)$

  Подформулы без отрицаний
  - $\neg p$
  - $\neg q$
  - $\neg(p \vee q)$
  - $\neg(p \wedge q)$
  - $\neg\big((p \vee q)\ \mathbf{U}\ (p \wedge q)\big)$

  Подформулы с отрицаниями (будем для краткости опускать)

Пример: $(\{p\}\,\{q\}\,\{p,q\}\,\{q\}\,\emptyset)^{\omega} \vDash (p \vee q)\ \mathbf{U}\ (p \wedge q)$?

Состояние s	Пометка $L(s)$	Разметка подформулами φ
s_0	$\{p\}$	$\{p, (p \vee q), \varphi\}$
s_1	$\{q\}$	$\{q, (p \vee q), \varphi\}$
s_2	$\{p, q\}$	$\{p, q, (p \vee q), (p \wedge q), \varphi\}$
s_3	$\{q\}$	$\{q, (p \vee q)\}$
s_4	$\emptyset$	$\emptyset$

Состояния B_φ: атомы $closure(\varphi)$

$s \subseteq closure(\varphi)$ – *элементарное множество* (*атом*), если

- для всех $\chi \in closure(\varphi)$
  - $\chi \in s \Leftrightarrow \neg\chi \notin s$
- для всех $(\chi \vee \psi) \in closure(\varphi)$
  - $(\chi \vee \psi) \in s \Leftrightarrow \chi \in s$ или $\psi \in s$
- для всех $(\chi \mathbf{U} \psi) \in closure(\varphi)$
  - $(\chi \mathbf{U} \psi) \in s$ и $\psi \notin s \Rightarrow \chi \in s$
  - $\psi \in s \Rightarrow (\chi \mathbf{U} \psi) \in s$

Условия локальной согласованности

Построение элементарных множеств

- Выписать $p \in AP$ и подформулы вида $\mathbf{X}\psi$, предварительно их упростив

$$\mathbf{X}\neg\psi \equiv \neg\mathbf{X}\psi \quad \text{и} \quad \mathbf{X}(\chi \vee \psi) \equiv \mathbf{X}\chi \vee \mathbf{X}\psi$$

- Перебрать все комбинации значений истинности этих условий
  - для каждой построить множество истинных подформул, полученных из этих условий применением классических логических связок
- Для каждой подформулы вида $\chi\ \mathbf{U}\ \psi$ (в порядке от простых к сложным) и каждого множества s, построенного на предыдущем шаге
  - если $\psi \in s$, добавить подформулу $\chi\ \mathbf{U}\ \psi$ в множество s
  - если $\psi \notin s$ и $\chi \in s$, построить копию s с добавленной подформулой $\chi\ \mathbf{U}\ \psi$
  - в противном случае оставить s без изменений

Пример: атомы $(p \vee q)\ \mathbf{U}\ (p \wedge q)$

p	q	**Насыщение (классические связки)**	**Насыщение (темпоральные операторы)**
$false$	$false$	$\emptyset$	$s_1 = \emptyset$
$true$	$false$	$\{p, (p \vee q)\}$	$s_2 = \{p, (p \vee q)\}$
			$s_3 = \{p, (p \vee q), \varphi\}$
$false$	$true$	$\{q, (p \vee q)\}$	$s_4 = \{q, (p \vee q)\}$
			$s_5 = \{q, (p \vee q), \varphi\}$
$true$	$true$	$\{p, q, (p \vee q), (p \wedge q)\}$	$s_6 = \{p, q, (p \vee q), (p \wedge q), \varphi\}$

Переходы $B_\varphi: s \to s'$

Условия реализации обязательств:

- для всех $\mathbf{X}\psi \in closure(\varphi)$
  - $\mathbf{X}\psi \in s \Leftrightarrow \psi \in s'$
- для всех $\chi\ \mathbf{U}\ \psi \in closure(\varphi)$
  - $\chi\ \mathbf{U}\ \psi \in s \Leftrightarrow \psi \in s$ или же $\chi \in s$ и $\chi\ \mathbf{U}\ \psi \in s'$

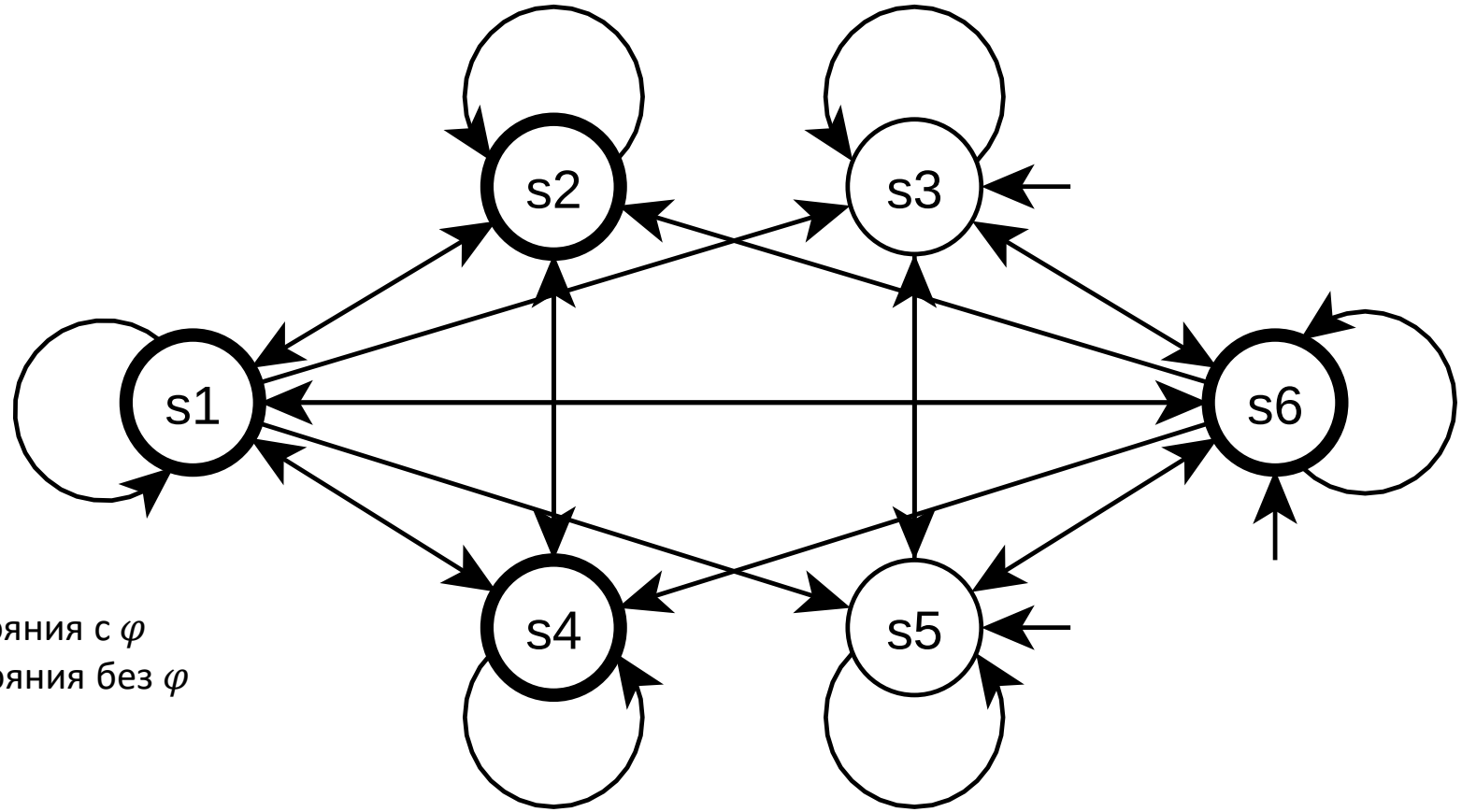
$$\delta(s, x) = \begin{cases} \{\, s' \mid s \to s' \,\}, & \text{если } x = (s \cap AP) \\ \emptyset, & \text{иначе} \end{cases}$$

Начальные и допускающие состояния B_φ

- Начальные состояния B_φ
  - $S_0 = \{s \in atoms(\varphi) \mid \varphi \in s\}$
- Допускающие состояния B_φ
  - $\boldsymbol{\mathcal{F}} = \left\{\mathcal{F}_{\chi \,\mathbf{U}\, \psi}\right\}_{\chi \,\mathbf{U}\, \psi \in closure(\varphi)}$, где
  - $\mathcal{F}_{\chi \,\mathbf{U}\, \psi} = \{s \in atoms(\varphi) \mid (\chi \,\mathbf{U}\, \psi) \notin s \vee \psi \in s\}$

Пример: B_φ для $\varphi \equiv (p \vee q)\ \mathbf{U}\ (p \wedge q)$

$s_1 = \emptyset$
$s_2 = \{p, (p \vee q)\}$
$s_3 = \{p, (p \vee q), \varphi\}$
$s_4 = \{q, (p \vee q)\}$
$s_5 = \{q, (p \vee q), \varphi\}$
$s_6 = \{p, q, (p \vee q), (p \wedge q), \varphi\}$



$\delta(s_1) = \{s_1, \dots, s_6\}$ — все состояния
$\delta(s_2) = \{s_1, s_2, s_4\}$ — нет переходов в состояния с φ
$\delta(s_3) = \{s_3, s_5, s_6\}$ — нет переходов в состояния без φ
$\delta(s_4) = \{s_1, s_2, s_4\}$
$\delta(s_5) = \{s_3, s_5, s_6\}$
$\delta(s_6) = \{s_1, \dots, s_6\}$

Задача: B_φ для $\varphi \equiv \mathbf{G}\{p \to \mathbf{X}q\}$

- $\varphi \equiv \mathbf{G}\{p \to \mathbf{X}q\} \equiv \neg\big(true\ \mathbf{U}\ (p \wedge \neg\mathbf{X}q)\big)$
- $\Sigma = 2^{\{p,q\}} = \{\emptyset, \{p\}, \{q\}, \{p,q\}\}$
- $closure(\varphi) = \{true, p, q, \mathbf{X}q, (p \wedge \neg\mathbf{X}q), \big(true\ \mathbf{U}\ (p \wedge \neg\mathbf{X}q)\big), \dots\}$
- $S = atoms(\varphi) = ?$
- $S_0 = ?$
- $\mathcal{F} = ?$
- $\delta = ?$

Задача: $atoms\left(\neg\left(true\ \mathbf{U}\ (p \wedge \neg\mathbf{X}q)\right)\right)$

p	q	$\mathbf{X}q$	Насыщение (классические связки)	Насыщение (темпоральные операторы)
$false$	$false$	$false$	$\{true\}$	?
$true$	$false$	$false$	$\{true, p, (p \wedge \neg\mathbf{X}q)\}$	?
$false$	$true$	$false$	$\{true, q\}$	?
$false$	$false$	$true$	$\{true, \mathbf{X}q\}$	?
$true$	$true$	$false$	$\{true, p, q, (p \wedge \neg\mathbf{X}q)\}$	?
$true$	$false$	$true$	$\{true, p, \mathbf{X}q\}$	?
$false$	$true$	$true$	$\{true, q, \mathbf{X}q\}$	?
$true$	$true$	$true$	$\{true, p, q, \mathbf{X}q\}$	?

Задача: $atoms\left(\neg\left(true\ \mathbf{U}\ (p \wedge \neg\mathbf{X}q)\right)\right)$

p	q	$\mathbf{X}q$	Насыщение (классические связки)	Насыщение (темпоральные операторы)
$false$	$false$	$false$	$\{true\}$	$s_1 = \{true\}$
				$s_2 = \{true, \neg\varphi\}$
$true$	$false$	$false$	$\{true, p, (p \wedge \neg\mathbf{X}q)\}$	$s_3 = \{true, p, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$
$false$	$true$	$false$	$\{true, q\}$	$s_4 = \{true, q\}$
				$s_5 = \{true, q, \neg\varphi\}$
$false$	$false$	$true$	$\{true, \mathbf{X}q\}$	$s_6 = \{true, \mathbf{X}q\}$
				$s_7 = \{true, \mathbf{X}q, \neg\varphi\}$
$true$	$true$	$false$	$\{true, p, q, (p \wedge \neg\mathbf{X}q)\}$	$s_8 = \{true, p, q, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$
$true$	$false$	$true$	$\{true, p, \mathbf{X}q\}$	$s_9 = \{true, p, \mathbf{X}q\}$
				$s_{10} = \{true, p, \mathbf{X}q, \neg\varphi\}$
$false$	$true$	$true$	$\{true, q, \mathbf{X}q\}$	$s_{11} = \{true, q, \mathbf{X}q\}$
				$s_{12} = \{true, q, \mathbf{X}q, \neg\varphi\}$
$true$	$true$	$true$	$\{true, p, q, \mathbf{X}q\}$	$s_{13} = \{true, p, q, \mathbf{X}q\}$
				$s_{14} = \{true, p, q, \mathbf{X}q, \neg\varphi\}$

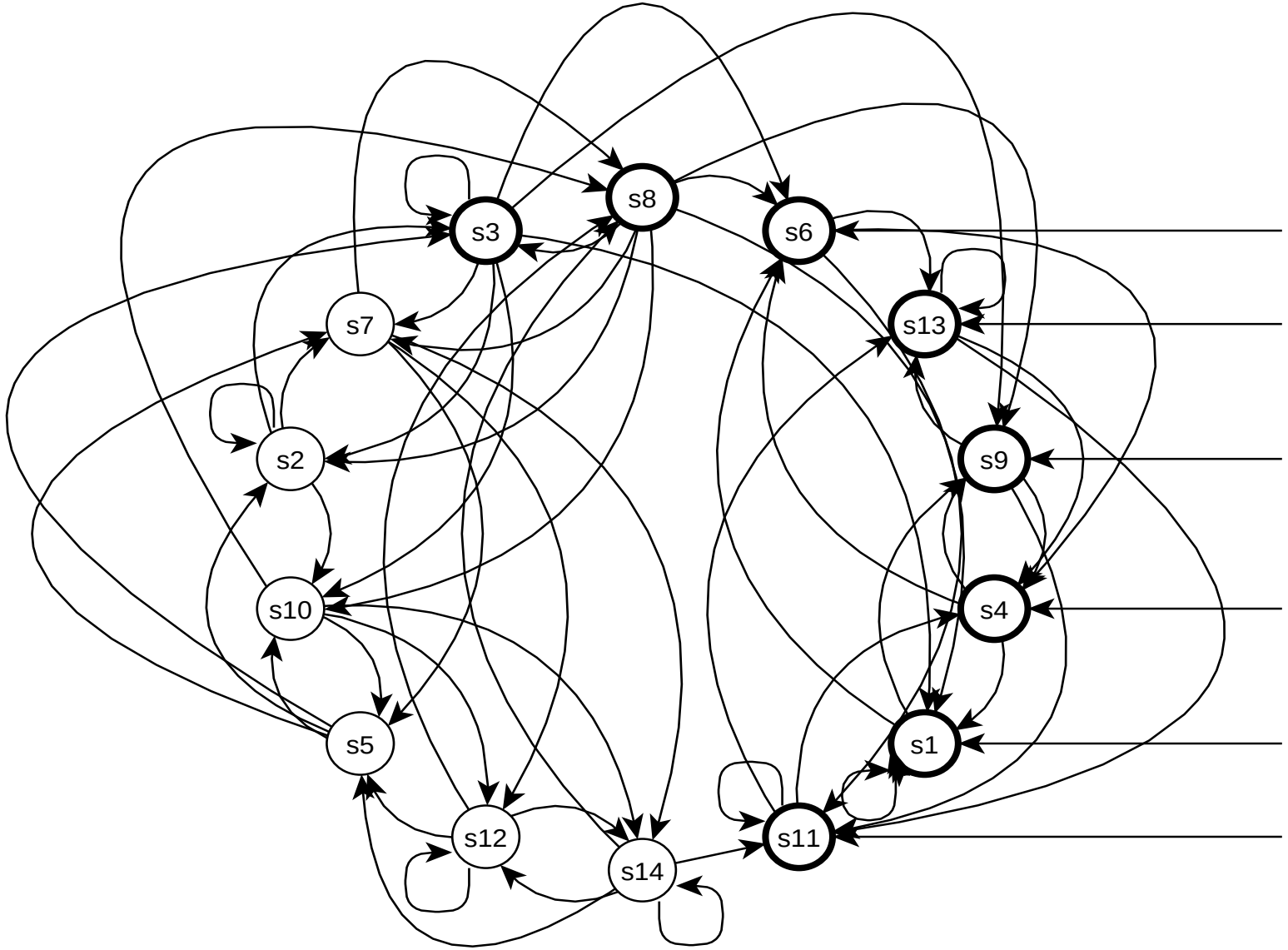
Задача: переходы B_φ

Начальное состояние перехода	Конечные состояния перехода
$s_1 = \{true\}$	?
$s_2 = \{true, \neg\varphi\}$	?
$s_3 = \{true, p, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$	?
$s_4 = \{true, q\}$	?
$s_5 = \{true, q, \neg\varphi\}$	?
$s_6 = \{true, \mathbf{X}q\}$	?
$s_7 = \{true, \mathbf{X}q, \neg\varphi\}$	?
$s_8 = \{true, p, q, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$	?
$s_9 = \{true, p, \mathbf{X}q\}$	?
$s_{10} = \{true, p, \mathbf{X}q, \neg\varphi\}$	?
$s_{11} = \{true, q, \mathbf{X}q\}$	?
$s_{12} = \{true, q, \mathbf{X}q, \neg\varphi\}$	?
$s_{13} = \{true, p, q, \mathbf{X}q\}$	?
$s_{14} = \{true, p, q, \mathbf{X}q, \neg\varphi\}$	?

Задача: переходы B_φ

Начальное состояние перехода: s	**Конечные состояния перехода:** $\delta(s)$
$s_1 = \{true\}$	$\{s_1, s_6, s_9\}$
$s_2 = \{true, \neg\varphi\}$	$\{s_2, s_3, s_7, s_{10}\}$
$s_3 = \{true, p, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$	$\{s_1, s_2, s_3, s_6, s_7, s_9, s_{10}\}$
$s_4 = \{true, q\}$	$\delta(s_1)$
$s_5 = \{true, q, \neg\varphi\}$	$\delta(s_2)$
$s_6 = \{true, \mathbf{X}q\}$	$\{s_4, s_{11}, s_{13}\}$
$s_7 = \{true, \mathbf{X}q, \neg\varphi\}$	$\{s_5, s_8, s_{12}, s_{15}\}$
$s_8 = \{true, p, q, (p \wedge \neg\mathbf{X}q), \neg\varphi\}$	$\delta(s_3)$
$s_9 = \{true, p, \mathbf{X}q\}$	$\delta(s_6)$
$s_{10} = \{true, p, \mathbf{X}q, \neg\varphi\}$	$\delta(s_7)$
$s_{11} = \{true, q, \mathbf{X}q\}$	$\delta(s_6)$
$s_{12} = \{true, q, \mathbf{X}q, \neg\varphi\}$	$\delta(s_7)$
$s_{13} = \{true, p, q, \mathbf{X}q\}$	$\delta(s_6)$
$s_{14} = \{true, p, q, \mathbf{X}q, \neg\varphi\}$	$\delta(s_7)$

Задача: B_φ для $\varphi \equiv \mathbf{G}\{p \rightarrow \mathbf{X}q\}$



Домашнее задание

- Выпишите атомы для следующих формул LTL:
  - $\mathbf{G}\{p \rightarrow \mathbf{F}q\}$
  - $p\ \mathbf{U}\ (\mathbf{X}q)$
  - $\mathbf{G}\{p \rightarrow (p\ \mathbf{U}\ q)\}$
  - $(\mathbf{FG}p) \rightarrow (\mathbf{GF}q)$
- Постройте автомат Бюхи для следующей формулы LTL:
  - $\mathbf{G}\{p \rightarrow (p\ \mathbf{U}\ q)\}$

Практикум №1

- Реализовать рассмотренный алгоритм построения автомата Бюхи по формуле LTL
  - Язык программирования C++
  - Используемые библиотеки
    - Представление формулы LTL: `ltl.h`
    - Представление автомата Бюхи: `fsm.h`