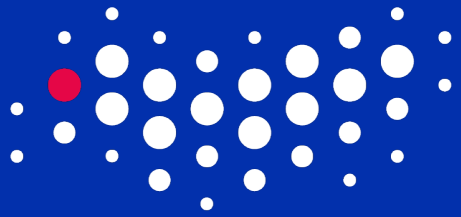


УНИВЕРСИТЕТ ИТМО

Разработка эффективных методов учета примеров поведения при синтезе автоматных моделей по темпоральным формулам

Давлетшин Р. О.
Научный руководитель: Ульянцев В. И.

13.06.2018

Задача синтеза автоматных систем

- Синтез автоматных моделей минимального размера — это довольно распространенная задача. Области её применения варьируется от проверки программного обеспечения и синтеза управляющих систем до задач биоинформатики

- Распространённым способом решения данной задачи является сведение к задаче о выполнимости булевой формулы

- Обычно спецификация для целевой реактивной системы задается в виде формул линейной темпоральной логики.

Bounded synthesis

- Новый перспективный подход к синтезу автоматных моделей по LTL спецификации
- На протяжении последних двух лет является лидером на соревнованиях по синтезу автоматных моделей SYNTCOMP в категориях скорости нахождения автоматных систем и качества синтезируемых моделей

Bounded synthesis

1. Построение автомата ко-Бюхи по заданным LTL формулам
2. Построение системы ограничений в виде булевой формулы для данного автомата ко-Бюхи и заданного ограничения на размер целевой системы
3. Решение полученной формулы
4. В случае успеха построение автоматной системы, иначе повторение алгоритма со 2-го пункта с увеличенным ограничением на размер системы

Примеры поведений

- Зачастую есть необходимость наряду со спецификацией в виде темпоральных формул дополнительно указать примеры поведения искомой системы или даже построить систему только по примерам поведения.

- В настоящий момент подход bounded synthesis поддерживает представление примеров поведения только в виде темпоральных формул

Примеры поведений

- В рамках данной работы будем называть сценариями последовательности пар векторов $\boldsymbol{i} \in 2^{|I|}$ и $\boldsymbol{o} \in 2^{|O|}$, задающие состояние переменных, контролируемых средой, и переменных, контролируемых системой.

- Считается, что реактивная система реализует примеры поведения, если в ней можно воспроизвести каждый сценарий из данного набора.

- Пример:

$$I = \{e_{11}, e_{12}, e_2, e_3, e_4\}, O = \{z_1, z_2, z_3\}$$

$$(e_{11}|z_1) \rightarrow (e_2|\,) \rightarrow (e_{12}|z_2) \rightarrow (e_2|\,)$$
$$(e_{11}|z_1) \rightarrow (e_4|z_3)$$

Методы представления примеров поведения

Представление примеров поведения в виде LTL формул

- Каждый элемент сценария $(\boldsymbol{i}_k|\boldsymbol{o}_k)$ последовательно заменяется на конструкцию
  $\boldsymbol{i}_k \rightarrow \boldsymbol{o}_k \wedge \mathrm{X}(\boldsymbol{i}_{k+1} \rightarrow \boldsymbol{o}_{k+1} \wedge \cdots)$

Представление примеров поведения в виде LTL формул

- Допустим, что $I = \{e_{11}, e_{12}, e_2, e_3, e_4\}$, $O = \{z_1, z_2, z_3\}$ и имеются сценарии:

$$(e_{11}|z_1) \rightarrow (e_2|\,) \rightarrow (e_{12}|z_2) \rightarrow (e_2|\,)$$
$$(e_{11}|z_1) \rightarrow (e_4|z_3)$$

- Сценарии в виде LTL формул:
- $(e_{11} \wedge \neg e_4 \wedge \neg e_{12} \wedge \neg e_3 \wedge \neg e_2) \rightarrow (z_1 \wedge \neg z_2 \wedge \neg z_3 \wedge X((e_2 \wedge \neg e_{11} \wedge \neg e_4 \wedge \neg e_{12} \wedge \neg e_3) \rightarrow (\neg z_1 \wedge \neg z_2 \wedge \neg z_3 \wedge X((e_{12} \wedge \neg e_{11} \wedge \neg e_4 \wedge \neg e_3 \wedge \neg e_2) \rightarrow (z_2 \wedge \neg z_1 \wedge \neg z_3 \wedge X((e_2 \wedge \neg e_{11} \wedge \neg e_4 \wedge \neg e_{12} \wedge \neg e_3) \rightarrow (\neg z_1 \wedge \neg z_2 \wedge \neg z3)))))))$
- $(e_{11} \wedge \neg e_4 \wedge \neg e_{12} \wedge \neg e_3 \wedge \neg e_2) \rightarrow (z_1 \wedge \neg z_2 \wedge \neg z_3 \wedge X((e_4 \wedge \neg e_{11} \wedge \neg e_{12} \wedge \neg e_3 \wedge \neg e_2) \rightarrow (z_3 \wedge \neg z_1 \wedge \neg z_2)))$

Дерево сценариев

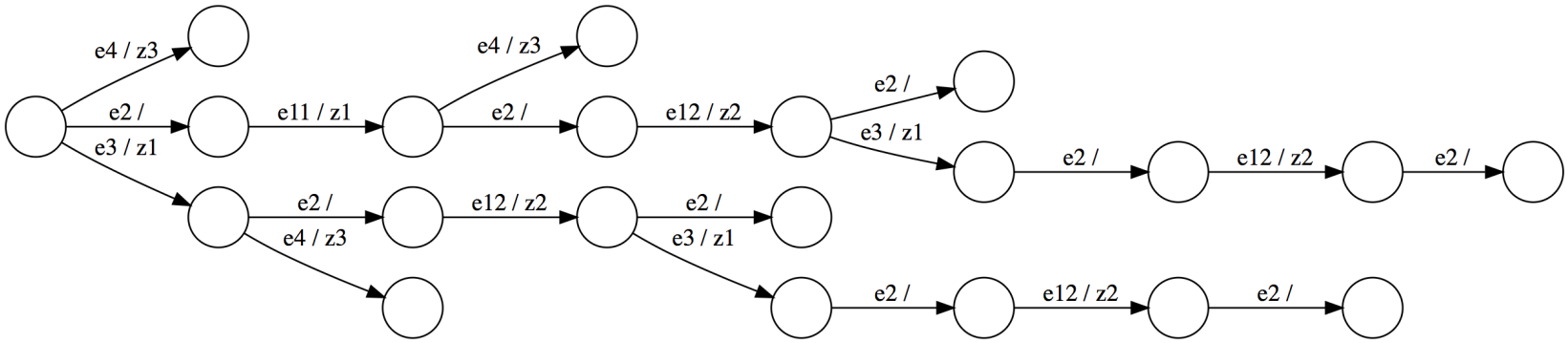
- Идея дерева сценариев стоит в объединении сценариев в дерево, где элементы сценариев представлены переходами между вершинами
- Дерево сценариев позволяет более эффективно представлять сценарии, так как одинаковые префиксы сценариев будут учтены только один раз

Дерево сценариев

- $(e_2|\,)$
  $(e_2|\,) \to (e_{11}|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_2|\,)$
  $(e_3|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_2|\,)$
  $(e_2|\,) \to (e_{11}|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_3|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_2|\,)$
  $(e_3|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_3|z_1) \to (e_2|\,) \to (e_{12}|z_2) \to (e_2|\,)$
  $(e_4|z_3)$
  $(e_2|\,) \to (e_{11}|z_1) \to (e_4|z_3)$
  $(e_3|z_1) \to (e_4|z_3)$

- 31 элемент

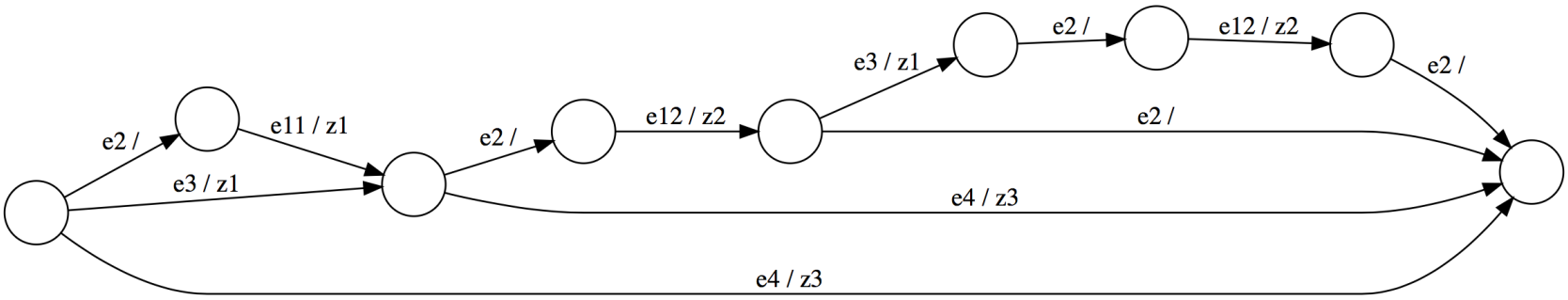
Дерево сценариев



- 21 вершина

Граф сценариев

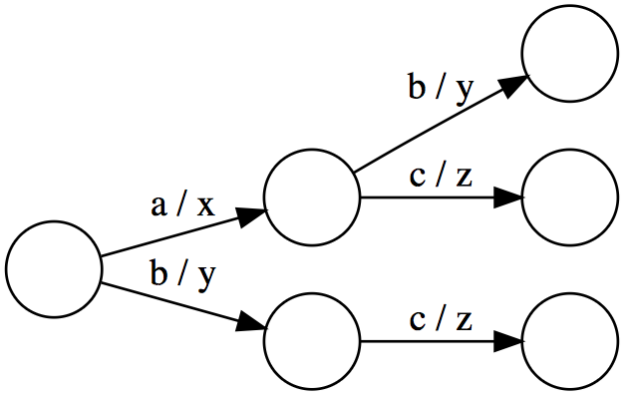
- Граф сценариев позволяет еще более эффективно представлять сценарии

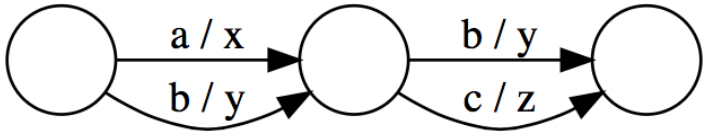


- 9 вершин

Граф сценариев

- Случай, при котором порождается новые сценарии





- Появился сценарий $(b|y) \rightarrow (b|y)$, которого не было в исходном наборе

Сведение к задаче SAT

- Введем новый тип переменных $s_{t,j}$
- $s_{t,j} = True$ тогда и только тогда, когда состояние t системы переходов соответствует вершине j графа сценариев

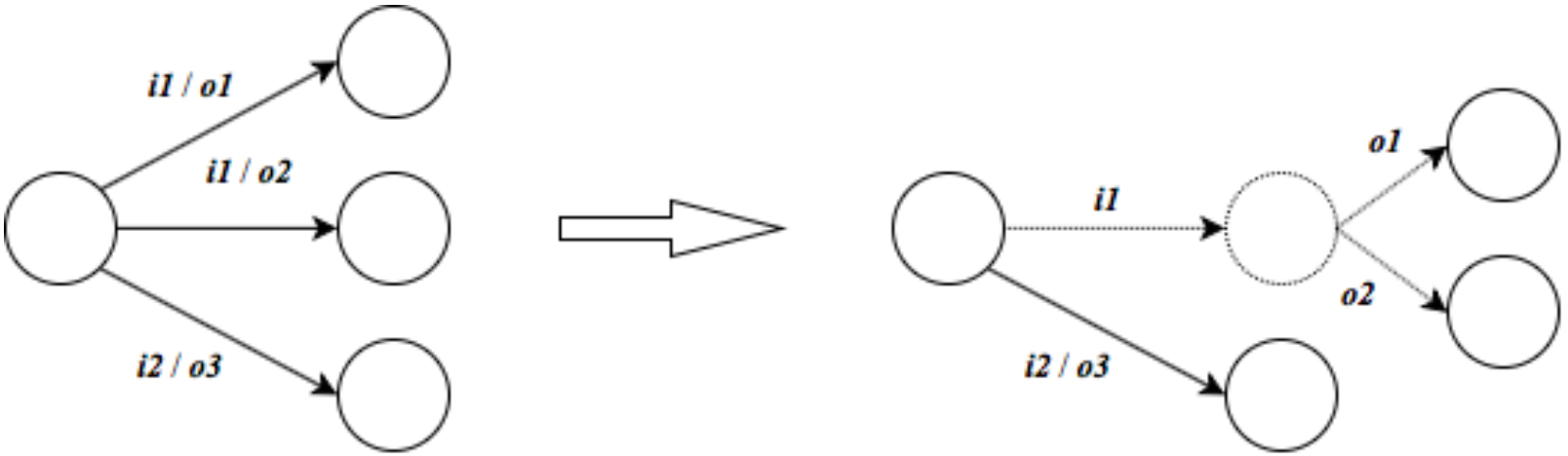
Сведение к задаче SAT (Версия 1)

- Поиск соответствия между вершинами графа сценариев и состояниями системы переходов
- $\bigwedge_{t \in T} \bigwedge_{j \in ST} s_{t,j} \rightarrow \bigwedge_{(j', \boldsymbol{i}, \boldsymbol{o}) \in out(j)} \bigvee_{t' \in T} (\tau_{t, \boldsymbol{i}, t'} \wedge \boldsymbol{o}_{t, \boldsymbol{i}} \wedge s_{t', j'})$
- Ассимптотика: $\mathcal{O}(n^2 \cdot |SG|^2 \cdot |O|)$
- $n = |T|$ — размер системы переходов, $|SG|$ — размер графа сценариев, $|I|$ и $|O|$ размеры множеств переменных

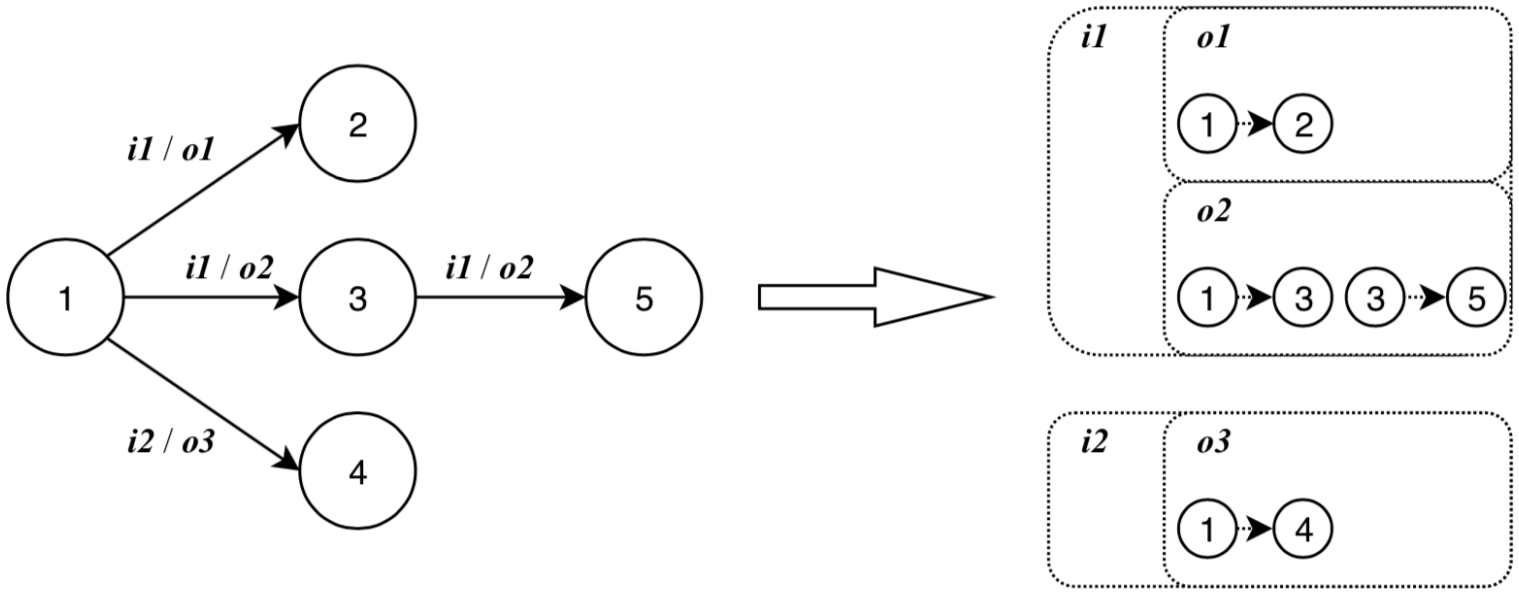
Сведение к задаче SAT (Версия 2)

- Вторая версия кодировки использует предикат полноты системы переходов
- $\bigwedge_{t \in T} \bigwedge_{\boldsymbol{i} \in 2^I} \bigvee_{t' \in T} \tau_{t,\boldsymbol{i},t'}$
- $\bigwedge_{t \in T} \bigwedge_{j \in ST} s_{t,j} \to \bigwedge_{(j',\boldsymbol{i},\boldsymbol{o}) \in out(j)} \bigwedge_{t' \in T} (\tau_{t,\boldsymbol{i},t'} \to (\boldsymbol{o}_{t,\boldsymbol{i}} \wedge s_{t',j'}))$
- Ассимптотика: $\mathcal{O}(n^2 \cdot |SG|^2 \cdot |O|)$

Кластеризованный граф сценариев
Вершинная кластеризация



Кластеризованный граф сценариев
Глобальная кластеризация



Сведение к задаче QSAT (Версия 1)

- Преемник первой версии кодировки при сведении к задаче SAT
- $\bigwedge_{t \in T} \bigwedge_{j \in SG} s_{t,j} \rightarrow \bigwedge_{(j', \boldsymbol{i}, \boldsymbol{o}) \in out(j)} \boldsymbol{i} \rightarrow \boldsymbol{o}_t \wedge \bigvee_{t' \in T} (\tau_{t,t'} \wedge s_{t',j'})$
- Ассимптотика: $\mathcal{O}(n \cdot |SG|^2 \cdot (|I| + |O| + n))$

Сведение к задаче QSAT (Версия 2)

- В данной версии кодировки используется подход глобальной кластеризации
- $\bigwedge_{\boldsymbol{i} \in IC} \boldsymbol{i} \to \bigwedge_{t \in T} \bigwedge_{j \in SG(\boldsymbol{i})} s_{t,j} \to \bigwedge_{(j', \boldsymbol{o}) \in out(j, \boldsymbol{i})} \boldsymbol{o}_t \wedge \bigvee_{t' \in T} (\tau_{t,t'} \wedge s_{t',j'})$
- Ассимптотика: $\mathcal{O}(|IC| \cdot (|I| + n \cdot |SG|^2 \cdot (|O| + n)))$
- $|IC|$ — количество глобальных кластеров

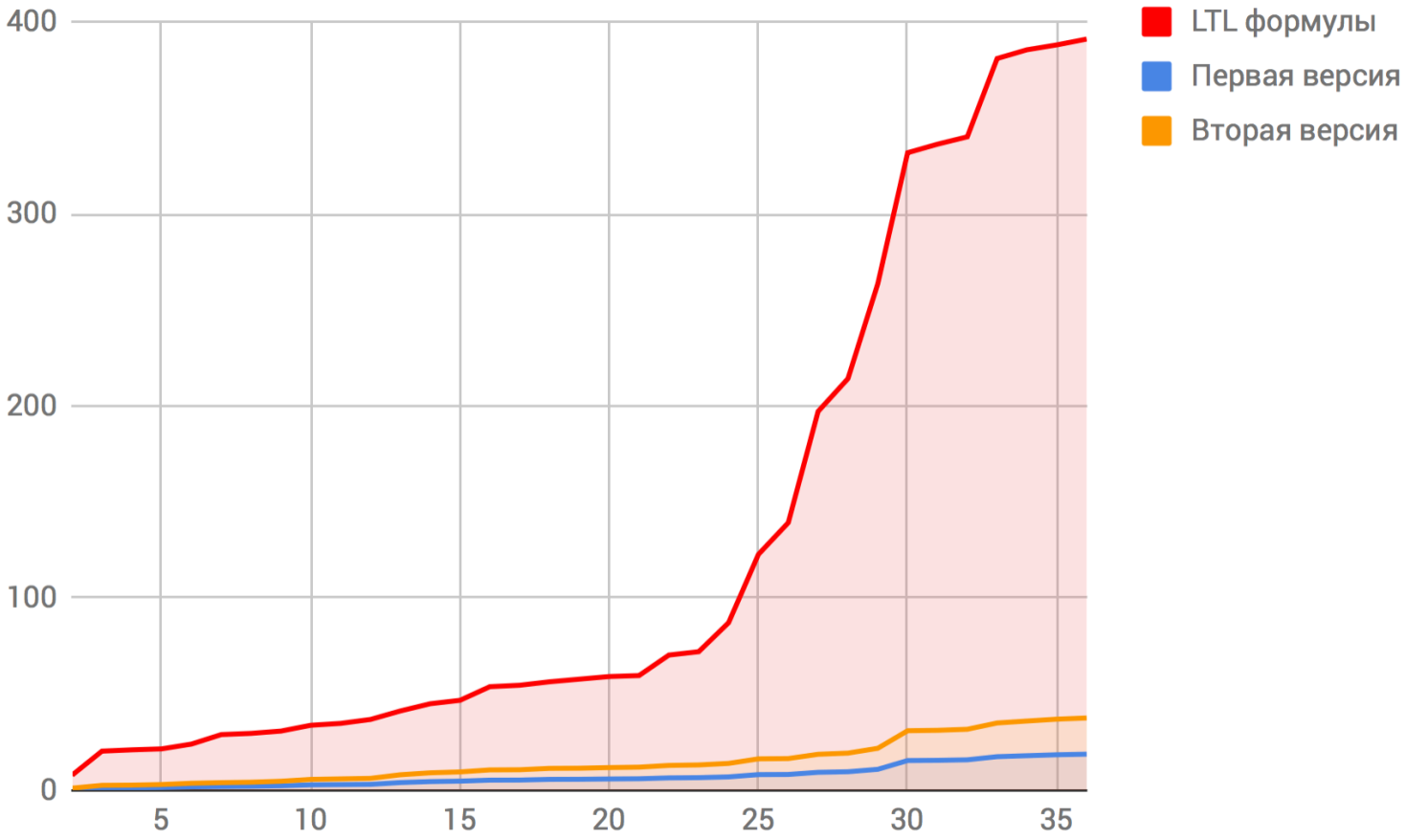
Сведение к задаче QSAT (Версия 3)

- В данной версии кодировки используется подход вершинной кластеризации, а также учитывается предикат полноты системы переходов
- $\bigwedge_{t \in T} \bigvee_{t' \in T} \tau_{t,t'}$
- $\bigwedge_{t \in T} \bigwedge_{j \in SG} s_{t,j} \to \bigwedge_{\boldsymbol{i} \in IC(j)} \boldsymbol{i} \to \bigwedge_{(j', \boldsymbol{o}) \in out(j, \boldsymbol{i})} \boldsymbol{o}_t \wedge \bigwedge_{t' \in T} (\tau_{t,t'} \to s_{t',j'})$
- Ассимптотика: $\mathcal{O}(n \cdot |SG|^2 \cdot (|O| + |I| + n))$

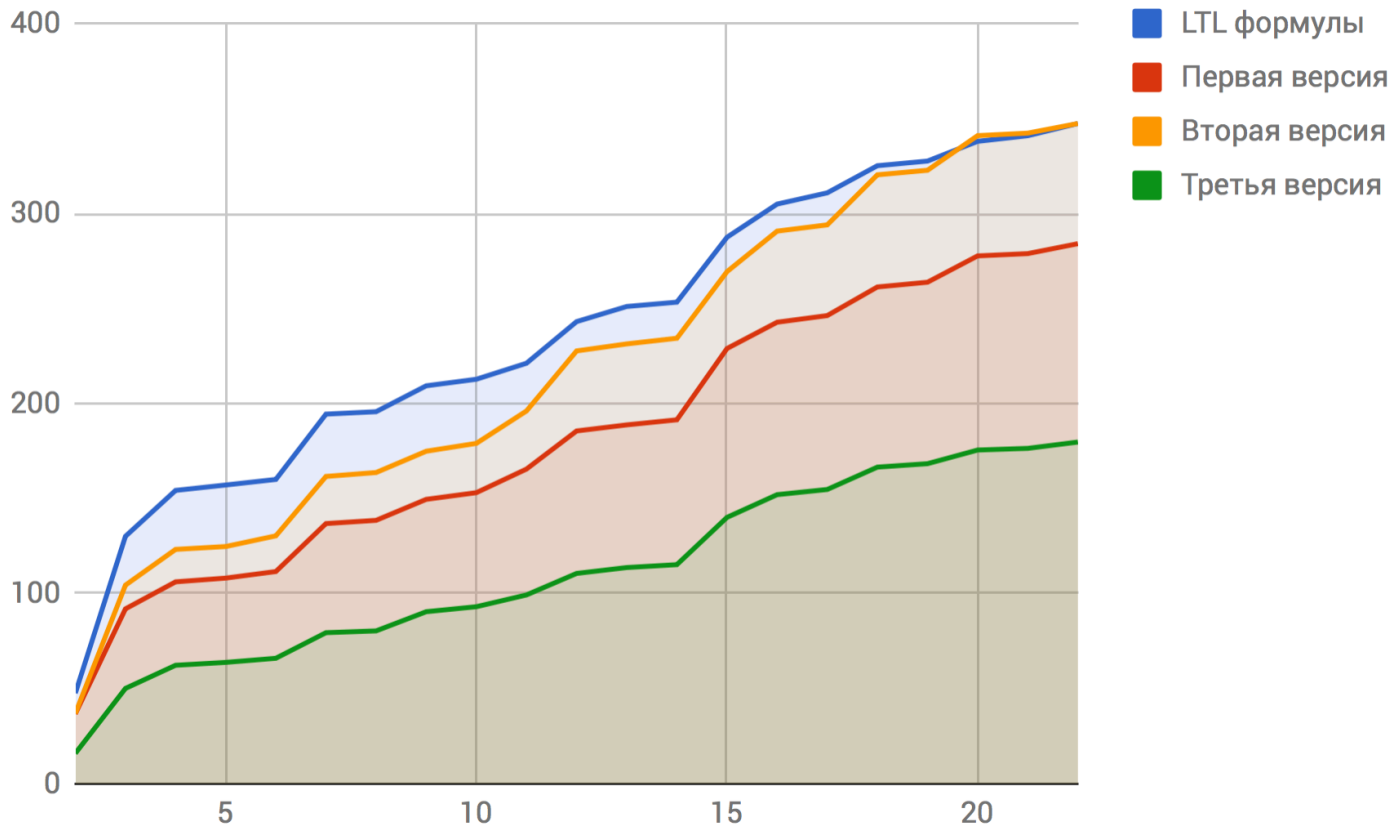
Анализ результатов

- Тестирование проводилось на наборе сущностей соревнования SYNTCOMP 2017
- Для тестирования для каждой автоматной системы были случайным образом сгенерированы примеры поведения
- Для каждых входных данных и каждого метода производилось 20 запусков, среди которых выбиралось среднее время на каждом этапе, также перед этим предварительно выполнялось по 5 запусков без замеров времени

Результаты для SAT



Результаты для QSAT



Анализ результатов SAT

Использованный метод / этап алгоритма	Первая версия	Вторая версия	LTL формулы
Время построения автомата ко-Бюхи, с	0.1	0.1	5.82
Время генерации формулы, с	0.9	0.86	2
Время решения формулы, с	2	2.6	11.7
Общее время, с	3	3.56	19.52

Анализ результатов QSAT

Использованный метод / этап алгоритма	Первая версия	Вторая версия	Третья версия	LTL формулы
Время построения автомата ко-Бюхи, с	0.014	0.018	0.015	3.24
Время генерации формулы, с	0.1	0.11	0.1	0.17
Время решения формулы, с	4.8	6.4	3.4	5
Общее время, с	4.914	6.528	3.515	8.41

Выводы

- Предложены новые варианты представления примеров поведения в виде кластеризованных графов сценариев
- Разработаны эффективные методы учета примеров поведения при синтезе автоматных моделей по темпоральным формулам на основе подхода синтеза автоматных моделей с ограничением на размер целевой системы
- Предложенные методы показали кратное превосходство относительно представления сценариев в виде темпоральных формул, как в случае со сведением к задаче SAT, так при сведении к задаче QSAT

Дальнейшая работа

- Продолжение исследований в данной области
- Написание статьи по результатам работы

УНИВЕРСИТЕТ ИТМО

Спасибо за внимание!