Сравнение инструментов анализа динамически формируемых строковых выражений

Автор: Александрия Георгий Гуливерович
Научный руководитель: магистр информационных технологий, ст. преп. С.В. Григорьев

Санкт-Петербургский государственный университет
Математико-Механический факультет
Кафедра системного программирования
344 группа

25 мая, 2015г.

Область применения

- Статическая проверка строковых выражений
- Поддержка возможностей IDE для встроенных языков
  - Диагностика ошибок
  - Подсветка синтаксиса
- Реинжиниринг ПО, например, анализ строковых выражений, при наличии динамически генерируемых SQL запросов
- Анализ SQL-инъекций

Постановка задач

- Выбрать сравниваемые инструменты
- Определить критерии сравнения
- Составить краткое описание сравниваемого инструмента
  - Основные функции
  - Поддерживаемые языки
- Провести сравнение инструментов
- Сделать выводы из результатов

Выбор инструментов сравнения

- Alvor
  - плагин Eclipse для проверки встроенного в Java SQL
- Java String Analyzer (JSA)
  - аппроксимация выражения регулярной грамматикой
- PHP String Analyzer (PHPSA)
  - аппроксимация выражения контекстно-свободной грамматикой
- IntelliLang
  - плагин к средам разработки PHPStorm и IntelliJ IDEA

Реализация

Критерии сравнения:

- Обнаружение ошибок
- Позиционирование ошибок
- Расширяемость языков
- Подсветка синтаксиса
- Проверка "на лету"
- Поддержка ветвлений
- Поддержка циклов

Классификация тестов

- Простые

```
String sql = "select id, first_name from persons";
```

- Вложенные

```
String example = "Select address FROM person WHERE FullName
    IN (SELECT fullName FROM employee WHERE exp>6)";
```

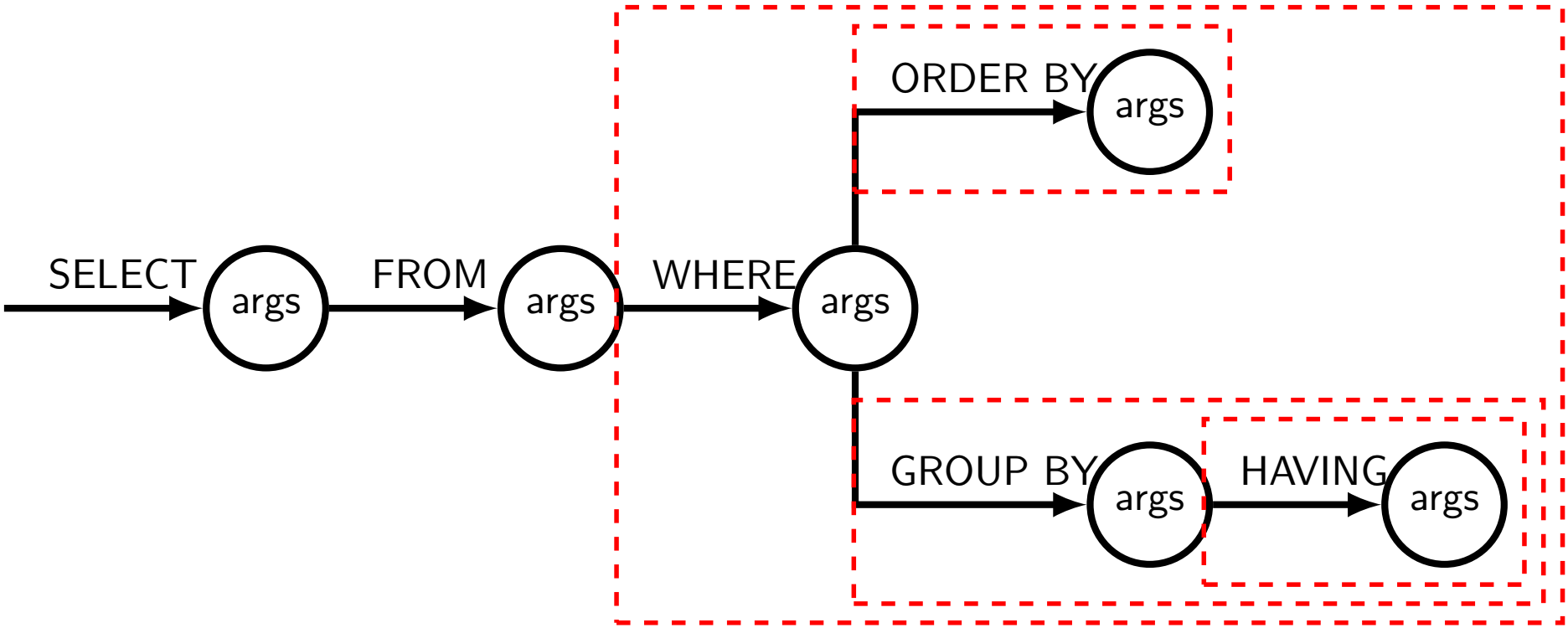
- С циклами

```
String abstract = "{\"SELECT \"}{(\"x FROM \")+, \"23\"}";
```

- С ветвлениями

```
String arg = "Select ref_num FROM TBC.PARTIES" + "{\"WHERE
   reg_num = 5", "WHERE social_id = 2\"}";
```

Генерация тестов



Итоги сравнения

Инструмент	Alvor	JSA	PHPSA	IntelliLang
Обнаружение ошибок	Да*	Да	Да˜	Да`
Позиционирование ошибок	Да*	Да	Нет	Да`
Расширяемость языков	Нет	Да	Нет	Да
Подсветка синтаксиса	Нет	Нет	Нет	Да
Инкрементальный анализ	Да	Нет	Нет	Да
Поддержка ветвлений	Да	Да	Да	Да
Поддержка циклов	Да´	Да	Да	Да

Да* – наличие данной особенности, но лишь для первого значения

Да˜ – для последнего

Да` – не во всех встроенных языках

Да´ – наличие возможности конструировать такие выражения, хотя плагин сообщает о не поддержке

Результаты

- Были выбраны сравниваемые инструменты
- Был составлен обзор данных инструментов
- Были сгенерированы тесты для сравнения
- Проведено сравнение инструментов
- Данная работа была представлена на конференции "Современные технологии в теории и практике программирования"
- Тезисы опубликованы в сборнике материалов конференции