Санкт-Петербургский государственный университет
Кафедра системного программирования

Фаззинг решателя Spacer

Автор: Суханова Анжела Кирилловна, группа 18.Б11-мм

Научный руководитель: доцент кафедры информатики СПбГУ, к.ф.-м.н. С. В. Григорьев

Консультанты: ассистент кафедры ИАС К. К. Смирнов, программист ООО «Интеллиджей Лабс» В. О. Соболь

Рецензент: программист-исследователь АНО ДПО «Научно-Исследовательский и Образовательный Центр «ДжетБрейнс» Ю. О. Костюков

Санкт-Петербург
20 мая 2022 г.

Введение

- В основе безопасности и корректной работы ПО лежит его тщательное тестирование и анализ
- В статическом анализе широко используются решатели систем дизъюнктов Хорна с ограничениями[1]. Spacer — один из самых эффективных Хорн-решателей, часть проекта Z3
- Важно тестировать анализаторы программ
- Фаззинг — это методика тестирования ПО, заключающаяся в анализе реакции программы на случайные входные данные
- **В настоящий момент не существует фаззеров Хорн-решателей**

[1] Constrained Horn Clauses (CHC)

Постановка задачи

Целью данной работы является разработка фаззера для тестирования решателя Spacer
Задачи:

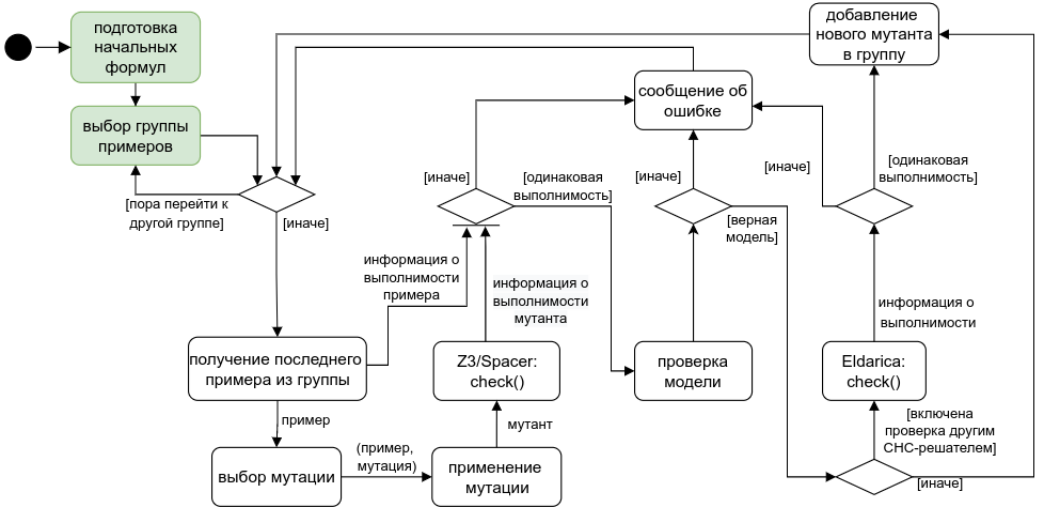
- Предложить способ фаззинга Хорн-решателей
- Спроектировать и создать фаззер, реализующий представленный способ
- Испытать разработанный фаззер на задаче фаззинга Хорн-решателя Spacer
- Реализовать инструмент, упрощающий примеры, на которых возникают ошибки

Фаззинг Хорн-решателей

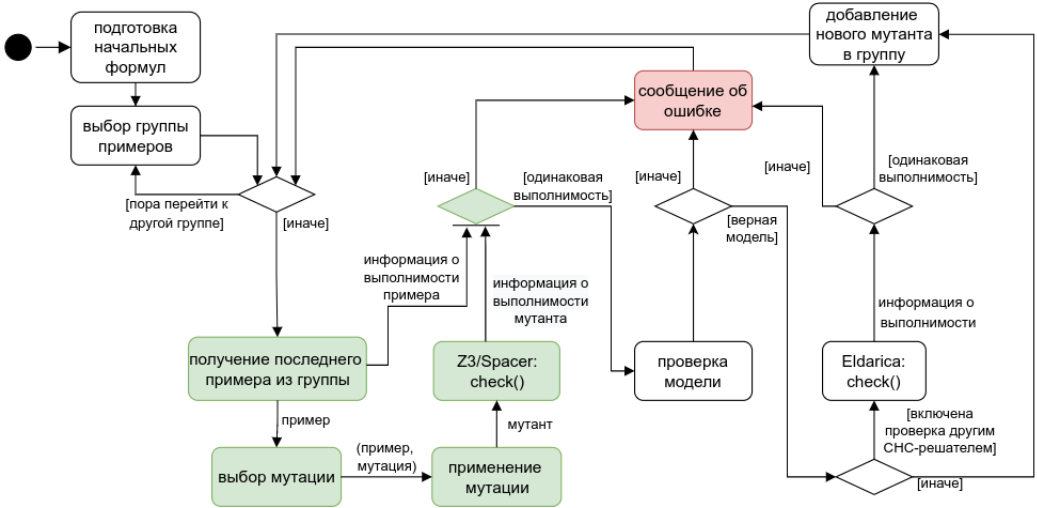
- Фаззеры SMT-решателей (STORM, BanditFuzz, FuzzSMT, Falcon и другие) малоэффективны в тестировании Хорн-решателей

- Для фаззинга Хорн-решателей больше подходит мутационный фаззинг
- Предлагается использовать только те мутации, которые сохраняют результат решения формулы

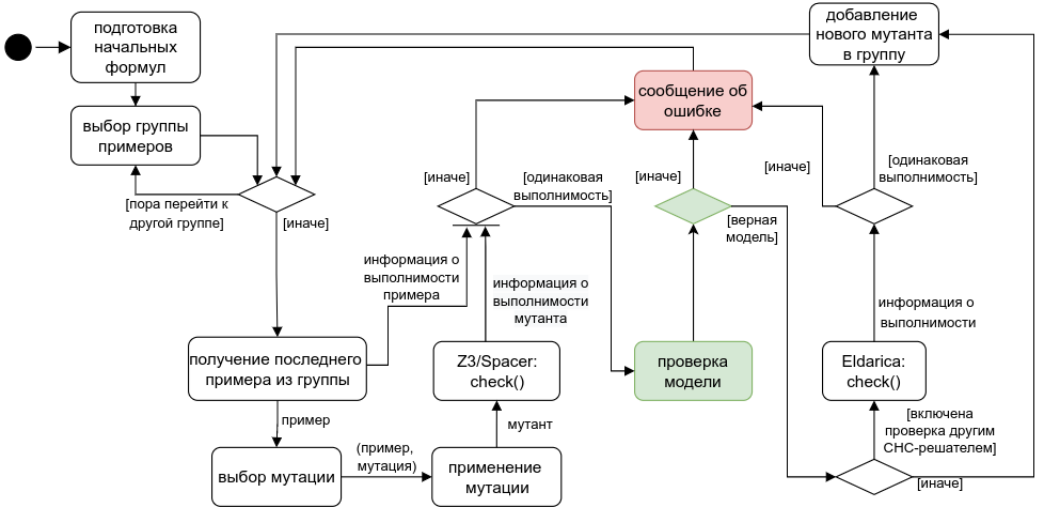
Реализация


подготовка начальных формул
выбор группы примеров
[пора перейти к другой группе]
[иначе]
получение последнего примера из группы
пример
выбор мутации
(пример, мутация)
применение мутации
мутант
Z3/Spacer: check()
информация о выполнимости мутанта
[иначе]
[одинаковая выполнимость]
информация о выполнимости примера
проверка модели
[иначе]
[верная модель]
сообщение об ошибке
[иначе]
[одинаковая выполнимость]
Eldarica: check()
информация о выполнимости
[включена проверка другим CHC-решателем]
[иначе]
добавление нового мутанта в группу

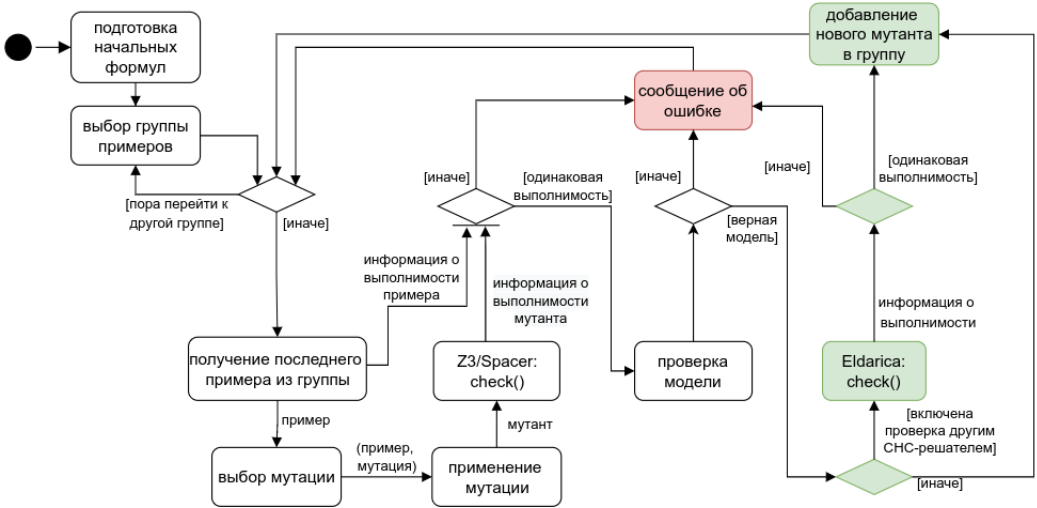
Реализация


подготовка начальных формул
выбор группы примеров
[пора перейти к другой группе]
[иначе]
получение последнего примера из группы
пример
выбор мутации
(пример, мутация)
применение мутации
мутант
Z3/Spacer: check()
информация о выполнимости мутанта
информация о выполнимости примера
[иначе]
[одинаковая выполнимость]
проверка модели
[иначе]
[верная модель]
сообщение об ошибке
[иначе]
[одинаковая выполнимость]
Eldarica: check()
информация о выполнимости
[включена проверка другим CHC-решателем]
[иначе]
добавление нового мутанта в группу

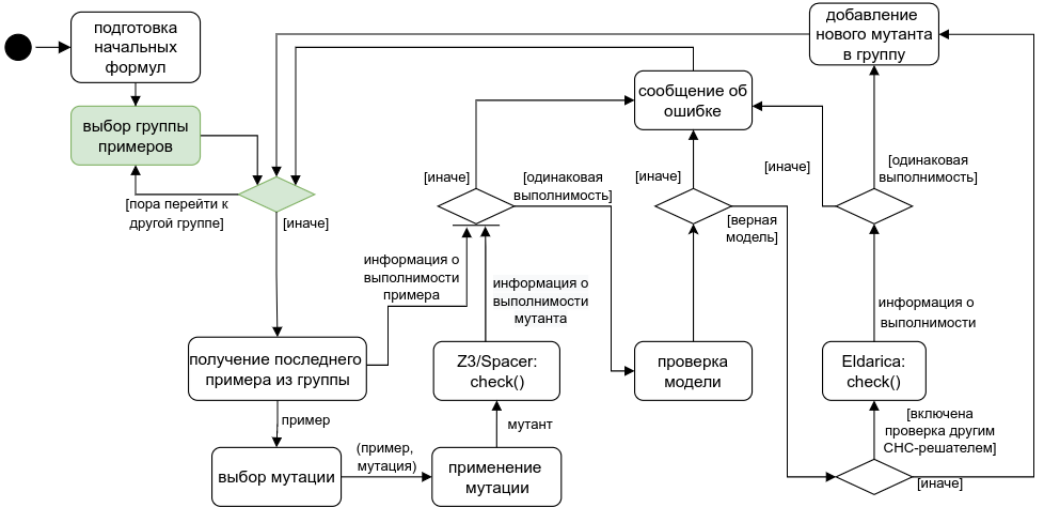
Реализация


подготовка начальных формул
выбор группы примеров
[пора перейти к другой группе]
[иначе]
получение последнего примера из группы
пример
выбор мутации
(пример, мутация)
применение мутации
мутант
Z3/Spacer: check()
информация о выполнимости мутанта
[иначе]
[одинаковая выполнимость]
информация о выполнимости примера
сообщение об ошибке
[иначе]
проверка модели
[верная модель]
[иначе]
[одинаковая выполнимость]
добавление нового мутанта в группу
информация о выполнимости
Eldarica: check()
[включена проверка другим CHC-решателем]
[иначе]

Реализация


подготовка начальных формул
выбор группы примеров
[пора перейти к другой группе]
[иначе]
получение последнего примера из группы
пример
выбор мутации
(пример, мутация)
применение мутации
мутант
Z3/Spacer: check()
информация о выполнимости примера
[иначе]
[одинаковая выполнимость]
информация о выполнимости мутанта
проверка модели
[иначе]
[верная модель]
сообщение об ошибке
[иначе]
[одинаковая выполнимость]
информация о выполнимости
Eldarica: check()
[включена проверка другим CHC-решателем]
[иначе]
добавление нового мутанта в группу

Реализация


подготовка начальных формул
выбор группы примеров
[пора перейти к другой группе]
[иначе]
получение последнего примера из группы
пример
выбор мутации
(пример, мутация)
применение мутации
мутант
Z3/Spacer: check()
информация о выполнимости мутанта
информация о выполнимости примера
[иначе]
[одинаковая выполнимость]
проверка модели
[иначе]
[верная модель]
сообщение об ошибке
[иначе]
[одинаковая выполнимость]
Eldarica: check()
информация о выполнимости
[включена проверка другим CHC-решателем]
[иначе]
добавление нового мутанта в группу

Детали реализации

- Язык реализации — Python
- Начальные данные были взяты с соревнований CHC-COMP, SV-COMP и из наборов бенчмарков к статьям (всего 3404 формулы)
- Фаззер использует 79 мутаций

Упрощение условий возникновения ошибки

- Сокращение цепочки мутации по алгоритму дельта-отладки

- Сокращение примера посредством удаления частей его абстрактного синтаксического дерева

Обнаруженные ошибки

Исправленные разработчиками Z3:

- При удвоении одного элемента конъюнкции результат решения системы менялся с «выполнимо» на «невыполнимо»[2]
- При решении примера с параметром решателя fp.xform.array_blast результат менялся с «выполнимо» на «невыполнимо»[3]
- Строилась неверная модель[4]

В процессе исправления:

- Строится неверная модель[5]

[2] Проблема 5714
[3] Проблема 5833
[4] Проблемы 5858, 5862, 5863, 5865, 5866, 5869, 5874, 5882, 5903
[5] Проблема 5920

Результаты

- Предложен способ фаззинга Хорн-решателей
- Спроектирован и разработан фаззер[6] для тестирования решателя Spacer с разными эвристиками сортировки примеров, возможностью взвешенного выбора мутаций, а также использованием Хорн-решателя Eldarica
- С помощью спроектированного фаззера обнаружены ошибки в Хорн-решателе Spacer, о которых проинформированы разработчики Z3. Примеры, на которых возникали ошибки, были добавлены в систему регрессионного тестирования Z3[7]
- Реализовано сокращение проблемных примеров и цепочек мутаций

[6] https://github.com/AnzhelaSukhanova/HornFuzz
[7] https://github.com/Z3Prover/z3test/pull/46

Используемые мутации

- Эквивалентные переписывания, которые предлагает API Z3
- Изменение параметров решателя, влияющих на ход решения примера
- $\varphi \wedge \psi \to \psi \wedge \varphi$
- $\varphi \wedge \psi \to \varphi \wedge \psi \wedge \varphi$
- $\varphi \wedge \psi \wedge \tau \to \varphi \wedge (\psi \wedge \tau)$
- $\varphi \vee \psi \to \psi \vee \varphi$
- $\forall (x, y, z).\ \psi(x, y, z) \to \forall (y, z, x).\ \psi(x, y, z)$
- $x < c \to (x < c) \wedge (x < c + 1)$
- Добавление в CHC систему дизъюнктов, не меняющих выполнимость системы

Дизъюнкты Хорна с ограничениями

Формулы в логике первого порядка вида $\forall V(\varphi \wedge p_1(X_1) \wedge \cdots \wedge p_n(X_n)) \rightarrow h(X)$, где

- φ — формула в теории первого порядка, называемая ограничением;
- V — переменные;
- $X_1, \ldots X_n$ — термы над V;
- $p_1, \ldots, p_n$ — неинтерпретированные предикатные символы;
- h — неинтерпретированный предикатный символ или $\bot$.

Оценка эффективности фаззера