



## Реализация элиминации кванторов для арифметики Пресбургера, обогащённой функцией $2^x$

**Автор:** Суханова Анжела Кирилловна, 371 группа (18.Б11-мм)

**Научный руководитель:** ассистент кафедры ИАС К. К. Смирнов

Санкт-Петербургский государственный университет  
Кафедра системного программирования

18 декабря 2020г.

- Проверка и доказательство корректности разрабатываемой программы очень важны, ведь они необходимы для контроля соответствия поведения программы ожидаемому и обеспечения её безопасности
- Одним из методов формальной верификации является решение задачи выполнимости формул в теориях (SMT)
- Так как в основе архитектуры компьютера лежат операции с битовыми векторами, то необходимо уметь решать SMT в теории битовых векторов
- Операции над последними можно свести к вычислениям в арифметике Пресбургера, обогащённой функцией  $2^x$ :  
 $\langle 0, 1, +, \leq, 2^x \rangle$

# Элиминация кванторов

- Легче определить, выполнимы ли формулы без кванторов
- Элиминация кванторов — это процесс преобразования формулы, содержащей кванторы, в эквивалентную бескванторную формулу
- Пример  
Пусть есть формула  $\exists x : 3 \leq x \leq z$ . Такой  $x$  найдётся, если  $3 \leq z$  (например,  $x = 3$ )

**Целью** данной работы является реализация элиминации кванторов для арифметики Пресбургера, расширенной функцией двоичной экспоненты

**Задачи:**

- Изучить алгоритм элиминации кванторов для расширенной арифметики Пресбургера и реализовать его
- Реализовать сведение формул над булевыми векторами к формулам в расширенной арифметике Пресбургера
- Внедрить реализации в SMT-решатель Boolector

# Выбор SMT-решателя и формата ввода

- В настоящее время существует несколько поддерживаемых, конкурентоспособных SMT-решателей, работающих с двоичными векторами: Boolector, Z3, CVC4 и другие.  
В рамках этой курсовой будет осуществляться работа с Boolector, так как он специализируется на теории битовых векторов, а также в течение многих лет побеждал в ежегодном соревновании между SMT-солверами — The SMT Competition
- Рассмотрены различные форматы ввода формул над битовыми векторами (Btor, Btor2, SMT-LIB, SMT-LIB v.2), и, как следствие, выбран один из них, а именно стандарт SMT-LIB v.2

# Текущие результаты

- Изучен алгоритм элиминации кванторов для расширенной арифметики Пресбургера
- Изучен исходный код Boolector-a
- Выбран формат ввода SMT-LIB v.2
- Начата реализация алгоритма для тривиального случая  $(\exists x : x \leq y)$ , на котором основываются остальные