Реализация синхронизирующего решателя дизъюнктов Хорна

Черниговская Лидия Александровна

научный руководитель: ст.преп.каф.СП Я.А.Кириленко
консультант: программист JetBrains Д.А.Мордвинов

рецензент: кандидат наук, постдокторант, Принстонский университет

Г.Г.Федюкович

Санкт-Петербург, 2018

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Вычисление длины списка

$$xs = nil \wedge l = 0 \Rightarrow len(xs, l)$$
$$xs = cons(x, xs') \wedge l = l' + 1 \wedge len(xs', l') \Rightarrow len(xs, l)$$
$$xs = ys \wedge l_1 \neq l_2 \wedge len(xs, l_1) \wedge len(ys, l_2) \Rightarrow \bot$$

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Вычисление длины списка

$$xs = nil \wedge l = 0 \Rightarrow len(xs, l)$$
$$xs = cons(x, xs') \wedge l = l' + 1 \wedge len(xs', l') \Rightarrow len(xs, l)$$
$$xs = ys \wedge l_1 \neq l_2 \wedge len(xs, l_1) \wedge len(ys, l_2) \Rightarrow \bot$$

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Вычисление длины списка

$$xs = nil \wedge l = 0 \Rightarrow len(xs, l)$$
$$xs = cons(x, xs') \wedge l = l' + 1 \wedge \mathbf{len}(xs', l') \Rightarrow len(xs, l)$$
$$xs = ys \wedge l_1 \neq l_2 \wedge \mathbf{len}(xs, l_1) \wedge \mathbf{len}(ys, l_2) \Rightarrow \bot$$

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Вычисление длины списка

$$xs = nil \wedge l = 0 \Rightarrow \mathbf{len}(xs, l)$$
$$xs = cons(x, xs') \wedge l = l' + 1 \wedge len(xs', l') \Rightarrow \mathbf{len}(xs, l)$$
$$xs = ys \wedge l_1 \neq l_2 \wedge len(xs, l_1) \wedge len(ys, l_2) \Rightarrow \bot$$

Введение

- Большинство задач из области автоматических рассуждений сводится к решению логики первого порядка
- Система ограниченных дизъюнктов Хорна

Вычисление длины списка

$$xs = nil \wedge l = 0 \Rightarrow len(xs, l)$$
$$xs = cons(x, xs') \wedge l = l' + 1 \wedge len(xs', l') \Rightarrow len(xs, l)$$
$$xs = ys \wedge l_1 \neq l_2 \wedge len(xs, l_1) \wedge len(ys, l_2) \Rightarrow \bot$$

Введение

- Хорн-решатели
  - SPACER/Z3 (Университет Торонто, Microsoft Research)
  - Eldarica
  - CVC4
  - ...
- Решение
  - Контрпример
  - Безопасный индуктивный инвариант
- Поиск инварианта — неразрешимая задача

Пример операции синхронного произведения

- ***Synchronizing Constrained Horn Clauses***, *Dmitry Mordvinov, Grigory Fedyukovich, 2017*

Исходная система

$$\varphi' \wedge f(x'') \Rightarrow f(x')$$
$$\psi' \wedge g(y'') \Rightarrow g(y')$$
$$\varphi \Rightarrow f(x)$$
$$\psi \Rightarrow g(y)$$
$$e \wedge \mathbf{f}(a) \wedge \mathbf{g}(b) \Rightarrow \bot$$

Трансформированная система

Пример операции синхронного произведения

- ***Synchronizing Constrained Horn Clauses***, *Dmitry Mordvinov, Grigory Fedyukovich, 2017*

Исходная система

$$\varphi' \wedge \mathbf{f}(x'') \Rightarrow \mathbf{f}(x')$$
$$\psi' \wedge \mathbf{g}(y'') \Rightarrow \mathbf{g}(y')$$
$$\varphi \Rightarrow \mathbf{f}(x)$$
$$\psi \Rightarrow \mathbf{g}(y)$$
$$e \wedge \mathbf{f}(a) \wedge \mathbf{g}(b) \Rightarrow \bot$$

Трансформированная система

$$e \wedge \mathbf{fg}(a, b) \Rightarrow \bot$$

Пример операции синхронного произведения

- ***Synchronizing Constrained Horn Clauses***, *Dmitry Mordvinov, Grigory Fedyukovich, 2017*

Исходная система

$$\varphi' \wedge \mathbf{f}(x'') \Rightarrow \mathbf{f}(x')$$
$$\psi' \wedge \mathbf{g}(y'') \Rightarrow \mathbf{g}(y')$$
$$\varphi \Rightarrow \mathbf{f}(x)$$
$$\psi \Rightarrow \mathbf{g}(y)$$
$$e \wedge \mathbf{f}(a) \wedge \mathbf{g}(b) \Rightarrow \bot$$

Трансформированная система

$$\varphi' \wedge \psi' \wedge \mathbf{fg}(x'', y'') \Rightarrow \mathbf{fg}(x', y')$$
$$\varphi' \wedge \psi \wedge \mathbf{fg}(x'', y) \Rightarrow \mathbf{fg}(x', y)$$
$$\varphi \wedge \psi' \wedge \mathbf{fg}(x, y'') \Rightarrow \mathbf{fg}(x, y')$$
$$\varphi \wedge \psi \Rightarrow \mathbf{fg}(x, y)$$
$$e \wedge \mathbf{fg}(a, b) \Rightarrow \bot$$

Синхронное произведение

Исходная система

$$\varphi' \wedge f(x'') \Rightarrow f(x')$$
$$\psi' \wedge g(y'') \Rightarrow g(y')$$
$$\varphi \Rightarrow f(x)$$
$$\psi \Rightarrow g(y)$$
$$e \wedge f(a) \wedge g(b) \Rightarrow \bot$$

Трансформированная система

$$\varphi' \wedge \psi' \wedge fg(x'', y'') \Rightarrow fg(x', y')$$
$$\varphi' \wedge \psi \wedge fg(x'', y) \Rightarrow fg(x', y)$$
$$\varphi \wedge \psi' \wedge fg(x, y'') \Rightarrow fg(x, y')$$
$$\varphi \wedge \psi \Rightarrow fg(x, y)$$
$$e \wedge fg(a, b) \Rightarrow \bot$$

- Затратная операция
- Может ухудшить ситуацию

Синхронизационные леммы

- Логические соотношения между аргументами синхронизируемых дизъюнктов
- Выполняются на протяжении всего рекурсивного вычисления

Постановка задачи

1. Изучить и реализовать алгоритм синхронного произведения дизъюнктов Хорна на базе SPACER/Z3
2. Предложить алгоритм поиска синхронизационных лемм и реализовать его
3. Провести эксперименты

Поиск синхронизационных лемм: I подход

Идея

- Синхронизационная лемма — ограничение вызывающего синхронизацию правила
  - для примера с длиной списка
    $\rho(xs, l_1, ys, l_2) = xs = ys \wedge l_1 \neq l_2$
- Индуктивность проверяется с помощью запросов к решателю
- Итеративно отбрасываются конъюнкты

Поиск синхронизационных лемм: I подход

Идея

- Синхронизационная лемма — ограничение вызывающего синхронизацию правила
  - для примера с длиной списка
    $\rho(xs, l_1, ys, l_2) = xs = ys \wedge l_1 \neq l_2$
- Индуктивность проверяется с помощью запросов к решателю
- Итеративно отбрасываются конъюнкты

Недостатки

- Синхронизационная лемма состоит только из конъюнктов ограничения

Поиск синхронизационных лемм: II подход

Идея

- Делегировать поиск синхронизационных лемм Хорн-решателю

Поиск синхронизационных лемм: II подход

Идея

- Делегировать поиск синхронизационных лемм Хорн-решателю

Исходная система

$$\varphi \Rightarrow f(x)$$
$$\varphi'(x, x') \wedge f(x) \Rightarrow f(x')$$
$$\psi \Rightarrow g(y)$$
$$\psi'(y, y') \wedge g(y) \Rightarrow g(y')$$
$$e(a, b) \wedge f(a) \wedge g(b) \Rightarrow \bot$$

Система для синхронизационной леммы ρ

$$e(a, b) \Rightarrow \rho(a, b)$$
$$\varphi' \wedge \psi' \wedge \rho(x', y') \Rightarrow \rho(x, y)$$
$$? \Rightarrow \bot$$

Поиск синхронизационных лемм: II подход

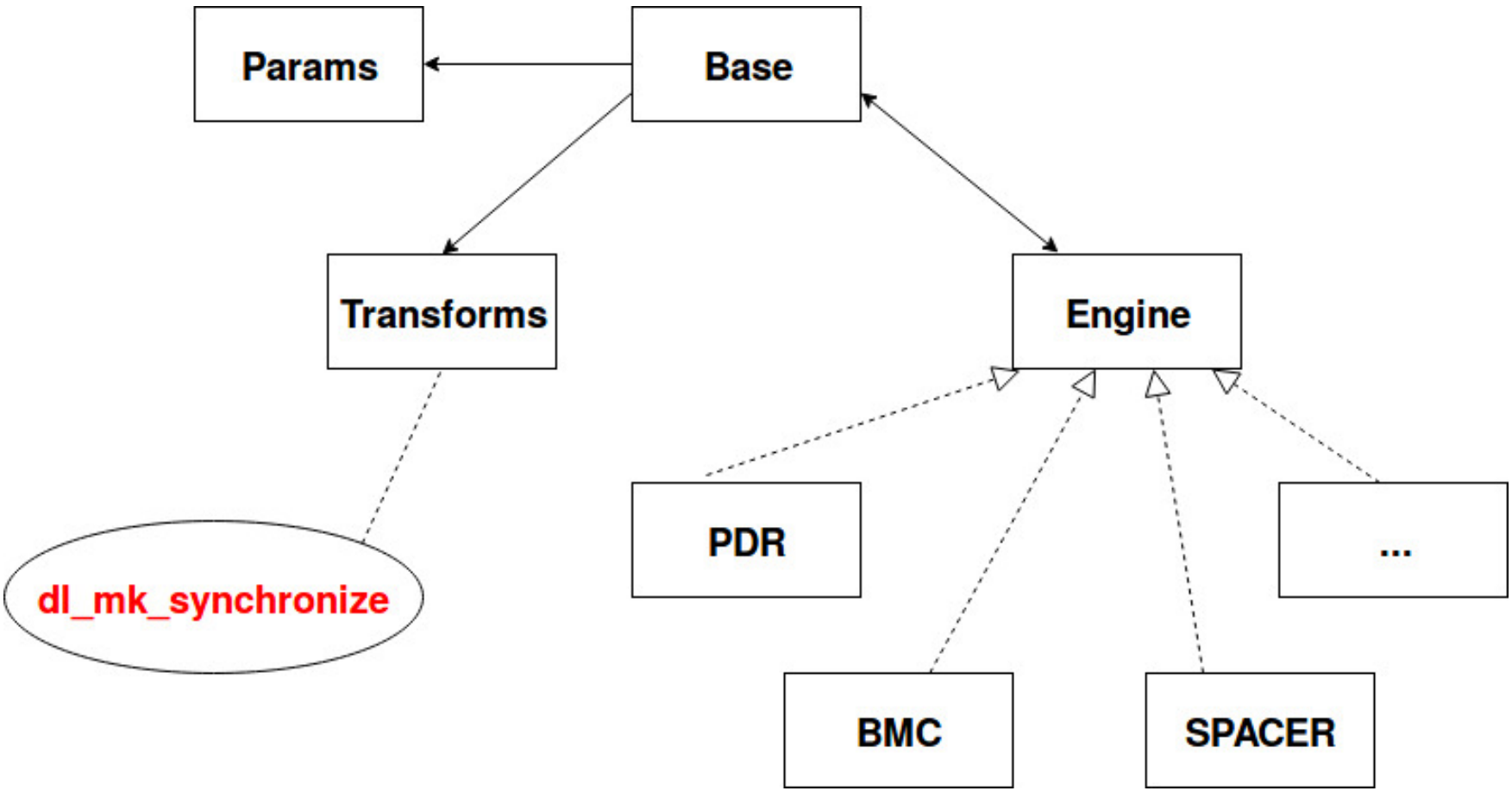
Исходная система

$$\varphi \Rightarrow f(x)$$
$$\varphi'(x, x') \wedge f(x) \Rightarrow f(x')$$
$$\psi \Rightarrow g(y)$$
$$\psi'(y, y') \wedge g(y) \Rightarrow g(y')$$
$$e(a, b) \wedge f(a) \wedge g(b) \Rightarrow \bot$$

Ситуация "рассинхронизации"

$$\varphi' \wedge \rho(x, y) \wedge \rho(x', y) \Rightarrow \bot$$
$$\psi' \wedge \rho(x, y) \wedge \rho(x, y') \Rightarrow \bot$$

Архитектура ядра Z3



Эксперименты

- CHC-Comp
- *Verifying Safety of Functional Programs with Rosette/Unbound, 2017*

прогр.	кол-во	SPACER/Z3	$Sync_1$	$Sync_2$
вып.	30	6	25	8
невып.	30	30	30	30

Результаты

- Изучен и реализован алгоритм синхронизации дизъюнктов Хорна на базе SPACER/Z3
- Предложен и реализован алгоритм поиска синхронизационных лемм, основанный на отбрасывании конъюнктов
- Предложен и реализован алгоритм поиска синхронизационных лемм, основанный на формировании нового запроса к Хорн-решателю
- Поставлены эксперименты