Применение теории алгебр Клини и ее расширений для автоматизации доказательств в системе Coq

Головин Павел Андреевич, группа M3439
Научный руководитель: Чивилихин Даниил, к. т. н.
Научный консультант: Моисеенко Евгений
Рецензент: Трунов Антон

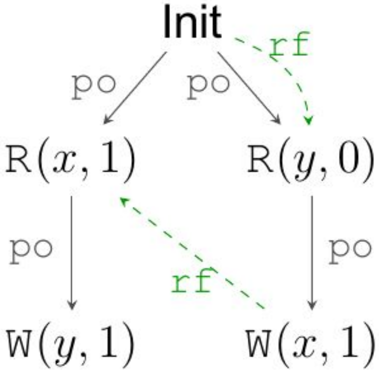
Введение: системы интерактивных доказательств

Agda

HOL
Interactive Theorem Prover

Введение: модели памяти

$$
\begin{array}{c|c}
a := [x] & b := [y] \\
[y] := 1 & [x] := 1
\end{array}
$$



Введение: Алгебры Клини (KA)

$$KA \triangleq \langle \cup, \cdot, \_^{*}, \emptyset, 1 \rangle$$

Полнота и корректность теории
относительно бинарных отношений:

$$KA \vdash r_1 \leq r_2 \Leftrightarrow \models r_1 \subseteq r_2$$

Цель работы

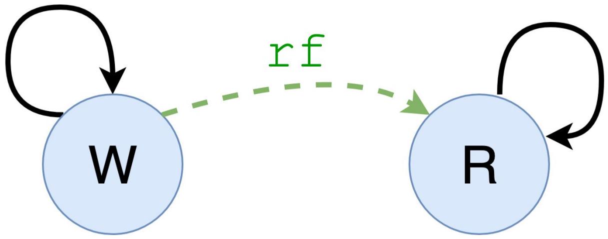
Исследовать возможность применения теории Клини для упрощения доказательств в системе Coq, которые связаны с моделями памяти.

Клини алгебра с тестами (KAT)

$$KAT \triangleq KA + [\cdot] \qquad [p] \triangleq \{(a, a) : p(a)\}$$

Пример:

$$\mathtt{rf} \subseteq [\mathtt{W}] \cdot \mathtt{rf} \cdot [\mathtt{R}]$$



Клини алгебра с тестами (KAT)

- Поддержка гипотез вида $r \leq 0 \vdash \ldots$

- Есть есть реализация в Coq (relation-algebra, Pous Damien)

УНИВЕРСИТЕТ ИТМО

Hahn (V. Vafeiadis)

- Содержит базовый формализм для моделей памяти
- Содержит доказательства различных свойств бинарных отношений
- Используется во многих моделях:
(JS MM, IMM, weakestmo)

Задачи работы

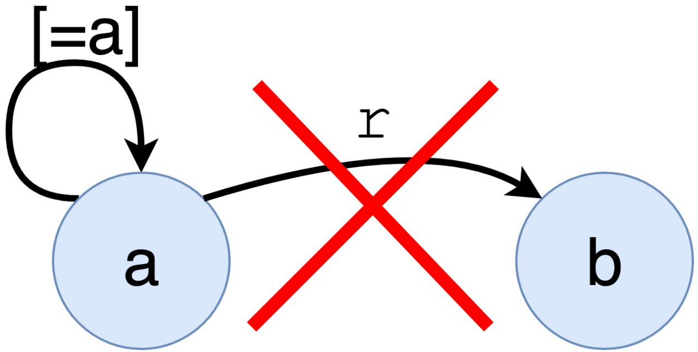
- Интегрировать средства автоматического вывода неравенств из relation-algebra в hahn
- Упростить доказательства в hahn
- Оценить упрощение доказательства

Решение

- Сопоставить сигнатуру KAT с определениями в hahn
- Доказать выполнение аксиом KAT
- По возможности переформулировать определения в hahn через сигнатуру KAT

Пример переформулирования: max_elt r a

Старое определение: $\forall (\mathtt{b} : \mathtt{A}), \neg(\mathtt{r}\ \mathtt{a}\ \mathtt{b})$



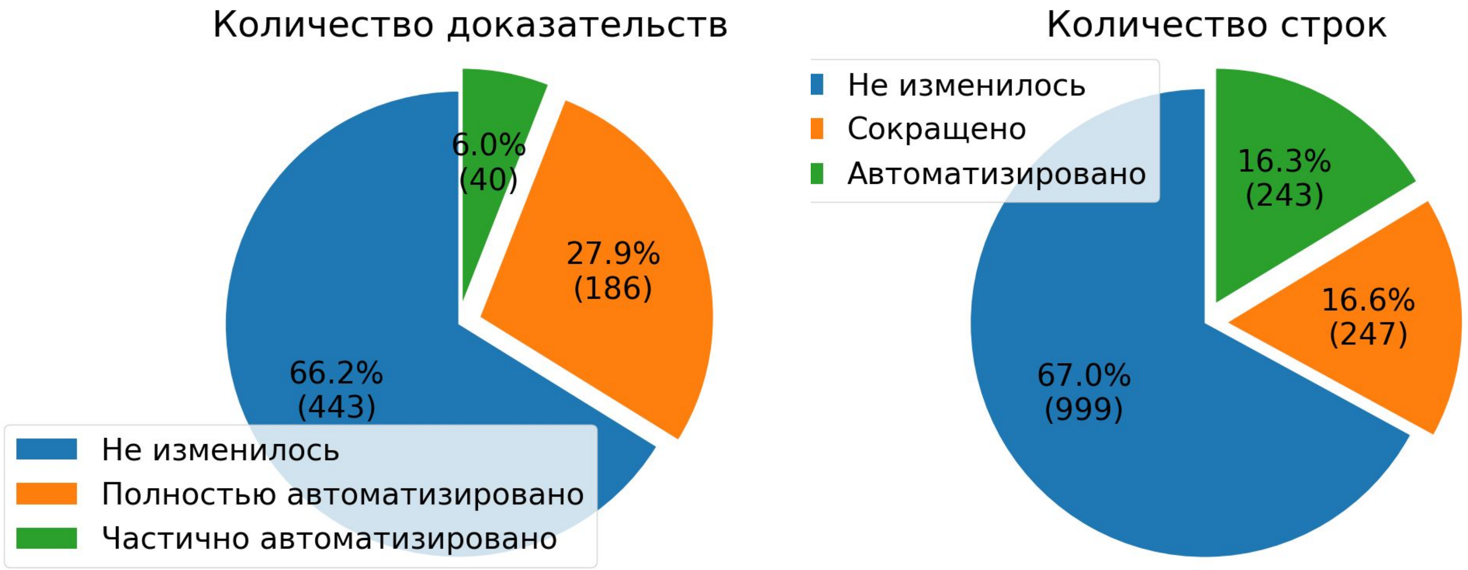
В сигнатуре КАТ: $[=\mathtt{a}] \cdot \mathtt{r} \leq \emptyset$

Пример переформулирования: max_elt r a

```
Lemma max_elt_iff_kat: ∀ (a: A) (r: relation A),
    max_elt r a ↔ [=a] · r ≤ ∅.

Lemma max_elt_t: ∀ (a: A) (r: relation A)
  max_elt r a → max_elt (r^+) a.
Proof.
  hahn_hkat.
Qed.
  hkat.
Qed.
```

Статистика упрощения



- Размер кода: 315 строк
  - 157 - тактики и сигнатура КАТ
  - 158 - переформулировки определений

Результаты работы:

- В hahn добавлены новые команды hahn_(h)kat для автоматизации свойств бинарных отношений
- С их помощью автоматизировано около 500 строк доказательств
- Упростилось 30% лемм о свойствах бинарных отношений

Бланк

Запасной слайд: Проблемы использования (h)kat

- Проблема с выводом типов-параметров
  - (h)kat скопирован и параметры прописаны явно
- Большое время агрегации гипотез (до 1 минуты)
  - Все переформулирования были даны сразу в форме $r < 0$ (ускорение в разы)
  - Переупорядочивание порядка перебора гипотез (ускорение на 10-20 %)
- Отсутствие поддержки гипотезы вида $r < [p]r[q]$
  - Добавлена лемма, которая разбивает ее на два $r < [p]r$ и $r < r[q]$

Запасной слайд: Сравнение расширений теории Клини

Название	Пример доказываемого свойства бинарных отношений	Сложность	Реализация в Coq
KA	Рефлексивность, Транзитивность	PSpace	relation-algebra, atbr
KAT	Предикаты на доменах	PSpace	relation-algebra
KAC	Функциональные отношения	PSpace	—
KL	Ацикличность, Разность	EXPSpace	—
KAl_{Lang}	—	EXPSpace	—

Запасной слайд: переформулирования

Название	Оригинальное определение (в логике первого порядка)	*KAT*
Переформулирование утверждений, которые можно использовать в качестве гипотез		
`upward_closed r p`	$\forall xy. r\ x\ y \Rightarrow p\ y \Rightarrow p\ x$	$r \cdot [p] \leqslant [p] \cdot r$
`doma r p`	$\forall xy. r\ x\ y \Rightarrow p\ x$	$r \leqslant [p] \cdot r$
`domb r p`	$\forall xy. r\ x\ y \Rightarrow p\ y$	$r \leqslant r \cdot [p]$
`max_elt a r`	$\forall y. \neg(r\ a\ y)$	$[eq\ a] \cdot r \leqslant 0$
`min_elt a r`	$\forall x. \neg(r\ x\ a)$	$r \cdot [eq\ a] \leqslant 0$
`wmax_elt a r`	$\forall y. r\ a\ y \Rightarrow a = y$	$[eq\ a] \cdot r \leqslant [eq\ a] \cdot r \cdot [eq\ a]$
`wmin_elt a r`	$\forall x. r\ x\ a \Rightarrow a = x$	$r \cdot [eq\ a] \leqslant [eq\ a] \cdot r \cdot [eq\ a]$
`DOM a r`	$\forall xy. r\ x\ y \Rightarrow x = a$	$r \leqslant [eq\ a] \cdot r$
`COD a r`	$\forall xy. r\ x\ y \Rightarrow y = a$	$r \leqslant r \cdot [eq\ a]$

Запасной слайд: переформулирования

Переформулированные утверждений, которые нельзя использовать в качестве гипотез		
`transitive r`	$\forall xyz. r\ x\ z \Rightarrow r\ z\ y \Rightarrow r\ x\ y$	$r \cdot r \leqslant r$
`reflexive r`	$\forall x. r\ x\ x$	$1 \leqslant r$
Переформулирование определений отношений		
`restr_rel p r`	$\forall xy. r\ x\ y \wedge p\ x \wedge p\ y$	$[p] \cdot r \cdot [p]$
`clos_refl r`	$\forall xy. x = y \vee r\ x\ y$	$1 \cup r$

где (`eq a : A` → **`Prop`**) - предикат равенства с `a`, (`r : relation A`) - отношение, (`a, x, y : A`) - события, (`p: A` → **`Prop`**) - предикаты на событиях, `A` - тип доменов отношений, событий

Запасной слайд: вне сигнатуры KAT

Таблица 3 – Переформулирование определений, которые не удалось выразить в KAT, но можно выразить в других расширениях алгебры Клини

Название	Оригинальное определение (в логике первого порядка)	Новое определение
`irreflexive r`	$\forall x. \neg (r\ x\ x)$	$1 \cap r \leqslant 0$
`acyclic r`	$irreflexive\ r^{+}$	$1 \cap r^{+} \leqslant 0$
`is_total r`	$\forall xy. r\ x\ y \vee r\ y\ x$	$\top \leqslant r \cup r^{\smile}$
`cross_rel p1 p2`	$\forall xy. p_1\ x \wedge p_2\ y$	$[p_1] \cdot \top \cdot [p_2]$
`singl_rel a b`	$\forall xy. x = a \wedge y = b$	$[eq\ a] \cdot \top \cdot [eq\ b]$

Пояснение: красным выделены не входящие в сигнатуру KAT связки, где $\top$ - универсальное отношение, ($\mathtt{p_1, p_2 : A \to}$ **Prop**) - предикаты на событиях

Запасной слайд: Виды гипотез используемых hkat

$$r \leq 0 \qquad a = b, a \leq b$$

$$[a] \cdot x = x \cdot [b], [a] \cdot x \leq x \cdot [b]$$

$$x \cdot [a] = [b] \cdot x, x \cdot [a] \leq [b] \cdot x$$

$$r \leq [a] \cdot r, r \leq r \cdot [a]$$

$$[a] \cdot r = [a], r \cdot [a] = [a]$$

Запасной слайд: примеры общезначимых (не)равенств

$$\vdash x \le x \cup y \qquad \vdash x \le x^*$$

$$\vdash (x^* \cdot y^*)^* = (x \cup y)^*$$

$$\vdash (x \cup y)^+ \le x^+ \cup (y^+ \cdot x^*) \cup (y^* \cdot (x^+ \cdot y^+)^+ \cdot x^*)$$

Запасной слайд: примеры доказательств из гипотез

$$x \leq 0 \vdash x^+ \leq 0$$

$$x \leq 0, y \leq 0 \vdash x \cup y \leq 0$$

$$[= a] \cdot r_1 \leq \emptyset, r_2 \leq r_2 \cdot [= a] \vdash r_1 \cdot r_2^* = r_1$$

Запасной слайд: примеры исполнения

$$
\begin{array}{l} a := [x] \\ [y] := 1 \end{array} \;\Big\|\; \begin{array}{l} b := [y] \\ [x] := 1 \end{array}
$$