Система автоматического поиска доказательств теорем, основанная на специальном варианте обратного метода С.Ю. Маслова

Филипповский В. А.

Научный руководитель:
д. ф.-м. н., профессор Оревков В. П.

Рецензент:
ст. преп., Петухова Н. Д.

Санкт-Петербургский государственный университет
Математико-механический факультет
Кафедра информатики

Санкт-Петербург, 11 июня 2015

Общая характеристика исследования

- **Предмет исследования:** обратный метод (ОМ) поиска доказательств теорем
- **Цель исследования:** построить программную реализацию одного из вариантов ОМ и сравнить по эффективности ОМ с методом резолюций

Актуальность: возрождение интереса к ОМ

- 2001: В.В. Бурлуцким построена реализация ОМ для модальной логики КТ
- 2004: В.П. Оревковым при помощи ОМ была доказана рарешимость нового хорновского фрагмента исчисления предикатов
- 2005: Д.С. Ларионовым разработана конкретизация ОМ для автоэпистемической логики, которая применялась при построении экспертных систем
- 2010: Г.Е. Минцем при помощи ОМ была доказана рарешимость класса E
- 2012-2015: Т.М. Косовская и Н.Д. Петухова применили ОМ к решению задач логико-предметного распознавания образов

Актуальность

- автору неизвестны реализации ОМ на высокоуровневом языке (в открытом доступе программных реализаций нет)
- утверждение С.Ю. Маслова: обратный метод не уступает по эффективности методу резолюции (это предположение не исследовалось достаточно тщательно)

Задачи исследования

1. реконструировать общую схему ОМ
2. сравнить разные конкретные варианты ОМ
3. выбрать один вариант ОМ для программной реализации
4. выбрать класс доказуемых формул
5. построить программную реализацию выбранного варианта ОМ
6. сравнить по эффективности работу алгоритма ОМ с работой метода резолюций для выбранного класса формул

Задача 1: основная идея ОМ

Обратный метод позволяет построить специальное исчисление $\mathbf{G}^*$ *благоприятных* Σ*-наборов*:

- секвенция Σ в некотором логическом языке $\mathcal{L}$
- секвенциальное исчисление $\mathbf{G}$:
  - свойство подформульности
  - без правила сечения

Задача 1: теоремы о корректности и полноте

Теорема 1. (теорема о корректности.) *Если в исчислении* G^* *благоприятных* Σ*-наборов выводим пустой набор* $\square$, *то секвенция* Σ *выводима в исходном исчислении* G_0:

$$G^* \vdash \square \;\Rightarrow\; G_0 \vdash \Sigma.$$

Теорема 2. (теорема о полноте.) *Если секвенция* Σ *выводима в исходном исчислении* G_0, *то в соответствующем ей исчислении* G^* *благоприятных* Σ*-наборов выводим пустой набор* $\square$:

$$G_0 \vdash \Sigma \;\Rightarrow\; G^* \vdash \square.$$

Задача 2: конкретизации ОМ

Существует большое количество разных конкретизаций ОМ:

- для классической логики / для неклассической (конструктивная, эпистемическая, модальная)
- для логики предикатов без функциональных знаков / с функциональными знаками
- для логики без знака равенства / с равенством
- ОМ с разными дополнительными тактиками поиска вывода

Задача 3: специальный вариант ОМ

Требования к конкретизации ОМ:

1. для классической логики предикатов
2. язык не включает функциоанльных знаков и равенства
3. без дополнительных тактик поиска вывода
4. удобная для программной реализации

Задача 3: исходные язык, исчисление, вид секвенций

- язык $\mathcal{L}_0$
  - без функциональных знаков (кроме нульместных, констант)
  - без равенства
  - $\&$, $\vee$, $\neg$, $\exists$
- секвенциальное исчисление $\boldsymbol{G}_0$
  - свойство подформульности
  - без правила сечения
  - безантецедентное
- секвенция Σ

$$\to \exists x_1, \ldots, x_n \bigwedge_{i=1}^{\delta} A_i,$$

где A_i – дизъюнкции атомарных формул и их отрицаний

Задача 3: алгоритм построения разбивки

Определение. *Разбивкой* секвенции Σ будем называть список всех блоков A_i, выписанных в порядке их появления в секвенции:

$$A_1, A_2, \ldots, A_\delta.$$

Пример: Для секвенции

$$\to \exists x{,}y((R(a{,}x) \vee \neg R(x{,}b)) \;\&\; (Q(a{,}y) \vee \neg Q(y{,}b)))$$

разбивкой является список формул:

$$\underset{1}{R(a{,}x) \vee \neg R(x{,}b)} \quad \underset{2}{Q(a{,}y) \vee \neg Q(y{,}b)}$$

Задача 3: язык для выражения систем зависимостей

Определение. *Системой уравнений S в переменных и константах с неизвестными $y_1, \ldots, y_m$ (связкой)* будем называть систему равенств вида:

$$S \rightleftharpoons \begin{cases} \alpha_1 = \beta_1 \\ \alpha_2 = \beta_2 \\ \ldots \\ \alpha_n = \beta_n \end{cases}$$

- $y_1, \ldots, y_m$ – переменные языка $\mathcal{L}_0$
- $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ — константы языка $\mathcal{L}_0$ или выражения вида y_i^k, где y_i – переменная c_k-той формулы разбивки $(1 \leqslant i \leqslant m)$

Задача 3: правила образования одночленных наборов

- формула F:

$$\exists x_1, \ldots, x_n \left(A_1 \wedge \ldots \wedge A_{i-1} \wedge \boxed{A_i} \wedge A_{i+1} \wedge \ldots \wedge A_\delta \right)$$

- блок A_i:

$$\left(\ldots \vee \boxed{R(\alpha_1, \ldots, \alpha_n)} \vee \ldots \vee \boxed{\neg R(\beta_1, \ldots, \beta_n)} \vee \ldots \right)$$

- система уравнений S:

$$\begin{cases} \alpha_1 = \beta_1 \\ \alpha_2 = \beta_2 \\ \ldots \\ \alpha_n = \beta_n \end{cases}$$

- выражение $\{i; S\}$ – одночленный замкнутый набор

Задача 3: правила образования двучленных наборов

- формула F:

$$\exists x_1, \ldots, x_n \left(A_1 \wedge \ldots \wedge \boxed{A_i} \wedge \ldots \wedge \boxed{A_j} \wedge \ldots \wedge A_\delta\right)$$

- блок A_i: $\left(\ldots \vee \boxed{R(\alpha_1, \ldots, \alpha_n)} \vee \ldots\right)$ блок A_j: $\left(\ldots \vee \boxed{\neg R(\beta_1, \ldots, \beta_n)} \vee \ldots\right)$
- система уравнений S:

$$\begin{cases} \alpha_1 = \beta_1 \\ \alpha_2 = \beta_2 \\ \ldots \\ \alpha_n = \beta_n \end{cases}$$

- выражение $\{i, j; S\}$ – двучленный замкнутый набор

Задача 3: правила вывода исчисления благоприятных наборов

- правило A

$$\frac{\text{Набор } \mathbf{H} \quad - \quad \text{допустимый замкнутый набор}}{\text{Набор } \mathbf{H} \quad - \quad \text{благоприятный набор}}$$

Задача 3: правила вывода исчисления благоприятных наборов

- правило Б

$$
\frac{\left.\begin{array}{c}\{\alpha_1, \cancel{\boxed{1}}\ ; S_1\},\\ \ldots,\\ \{\alpha_\delta, \cancel{\boxed{\delta}}\ ; S_\delta\}.\end{array}\right\} \quad - \quad \text{благоприятные наборы} \\ \text{Связка } S^* = [S^\circ \cup S_1 \cup \ldots \cup S_\delta] \setminus \{x_i^{k_j+1}\}_{i=1}^{n}{}_{j=1}^{\delta} \text{ допустима}}{\{\alpha_1, \ldots, \alpha_\delta; S^*\} \quad - \quad \text{благоприятный набор}}
$$

Задача 3: правила вывода исчисления благоприятных наборов

- правило склейки

$$\frac{\{i_1, \ldots, \boxed{i_g}, \ldots, i_{h-1}, \boxed{\cancel{i_h}}, i_{h+1}, \ldots, i_l; S\} \quad \text{– благоприятный набор} \qquad i_g = i_h \ (1 \leqslant g, h \leqslant l) \qquad \text{Связка } S^* = [S \cup S^\square] \backslash \{x_i^h\}_{i=1}^n \text{ допустима}}{\{i_1, \ldots, i_g, \ldots, i_{h-1}, i_{h+1}, \ldots, i_l; S^*\} \quad \text{– благоприятный набор}}$$

Задача 3: новая нотация для ОМ

- нотация ОМ достаточно сложна
- если упростить нотацию ОМ, то будет проще запрограммировать ОМ
- специальный вариант ОМ тоже не решает вопрос удобства нотации
- проблему решает новый способ записи
- новая нотация проще воспринимается и её легче запрограммировать

Задача 3: алгоритм преобразования традиционной нотации в новую

- Выражения типа
$$x_n^i = a,$$
где a – некоторая константа, преобразуются в $x_n = a$ и записываются в квадратных скобках у i-того компонента набора:
$$i[x_n = a]$$

Задача 3: алгоритм преобразования традиционной нотации в новую (продолжение)

- Выражения типа
$$x_n^i = y_m^j,$$
где y_m^j – переменная, преобразуются в два выражения:
  - $x_n = z$
  - $y_m = z$

  для некоторой новой переменной z и записываются в квадратных скобках:
  - у i-того компонента набора:
$$i[x_n = z]$$
  - у j-того компонента набора:
$$j[y_m = z]$$

Задача 3: пример вывода ОМ

Рассмотрим секвенцию Σ:

$$\rightarrow \exists x,y((R(a,x) \vee \neg R(x,b)) \ \wedge \ (Q(a,y) \vee \neg Q(y,b)))$$

Замкнутыми наборами для рассматриваемой секвенции будут:

$$[1,\ 1;\ x^1 = b,\ x^2 = a]\ [1,\ 1;\ x^1 = a,\ x^2 = b]$$
$$[2,\ 2;\ y^1 = b,\ y^2 = a]\ [2,\ 2;\ y^1 = a,\ y^2 = b]$$

или в другой нотации:

$$\{1[x = b],\ 1[x = a]\}\ \{1[x = a],\ 1[x = b]\}$$
$$\{2[y = b],\ 2[y = a]\}\ \{2[y = a],\ 2[y = b]\}$$

Задача 3: пример вывода ОМ

Вывод пустого набора для секвенции Σ в исчислении $\mathbf{G}^*$:

В старой нотации:			В новой нотации:		
1.	$\{1, 1; x^1 = b, x^2 = a\}$	A	1.	$\{1[x = b], 1[x = a]\}$	A
2.	$\{1, 1; x^1 = a, x^2 = b\}$	A	2.	$\{1[x = a], 1[x = b]\}$	A
3.	$\{2, 2; y^1 = b, y^2 = a\}$	A	3.	$\{2[y = b], 2[y = a]\}$	A
4.	$\{2, 2; y^1 = a, y^2 = b\}$	A	4.	$\{2[y = a], 2[y = b]\}$	A

Задача 3: пример вывода ОМ

В старой нотации:

$$5.\quad \frac{\{1,\ 1;\ x^1{=}b, x^2{=}a\} \qquad \{2,\ 2;\ y^1{=}b, y^2{=}a\}}{\begin{array}{c}\{1,\ 2, \frac{1}{2}; x^1{=}b, \cancelto{x^3}{x^2}{=}a, \cancelto{y^2}{y^1}{=}b, \cancelto{y^3}{y^2}{=}a\} \\ \{1,\ 2, \cancel{\tfrac{1}{2}}; x^1 = b, \cancel{x^3 = a}, y^2 = b, \cancel{y^3 = a}\} \\ \{1,\ 2;\ x^1 = b, y^2 = b\}\end{array}} \qquad \text{Б, 1, 3}$$

В новой нотации:

$$5.\quad \frac{\{1[x{=}b],\ \cancel{1[x{=}a]}\} \qquad \{2[y{=}b],\ \cancel{2[y{=}a]}\}}{\{1[x{=}b], 2[y{=}b]\}} \qquad \text{Б, 1, 3}$$

Задача 3: пример вывода ОМ

6. $\dfrac{\{1[x=a],\ \cancel{1[x=b]}\}\qquad\{2[y=a],\ \cancel{2[y=b]}\}}{\{1[x=a],2[y=a]\}}$ Б, 2, 4

7. $\dfrac{\{1[x=b],\ \cancel{2[y=b]}\}\qquad\{1[x=b],\ \cancel{1[x=a]}\}}{\{1[x=b],1[x=b]\}}$ Б, 5, 1

8. $\dfrac{\{1[x=b],\cancel{1[x=b]}\}}{\{1[x=b]\}}$ склейка, 7

9. $\dfrac{\{\cancel{1[x=a]},2[y=a]\}\qquad\{\cancel{2[y=b]},2[y=a]\}}{\{2[y=a],2[y=a]\}}$ Б, 6, 3

10. $\dfrac{\{2[y=a],\cancel{2[y=a]}\}}{\{2[y=a]\}}$ склейка, 9

11. $\dfrac{\{\cancel{1[x=b]}\}\qquad\{\cancel{2[y=a]}\}}{\square}$ Б, 8, 10

Задача 4: класс доказуемых формул

Выбран класс формул следующего вида:

$$\rightarrow \exists x_1, \ldots, x_n \bigwedge_{i=1}^{\delta} A_i,$$

где A_i – дизъюнкции атомарных формул и их отрицаний.

Примеры:

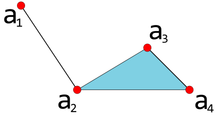
$$\rightarrow \exists x(R(a,x) \vee \neg R(x,b))$$

$$\rightarrow \exists x((P(x) \vee \neg P(a)) \ \wedge \ (P(x) \vee \neg P(b)))$$

$$\rightarrow \exists x,y((R(a,x) \vee \neg R(x,b)) \ \wedge \ (Q(a,y) \vee \neg Q(y,b)))$$

Задача 4: тестовое множество формул

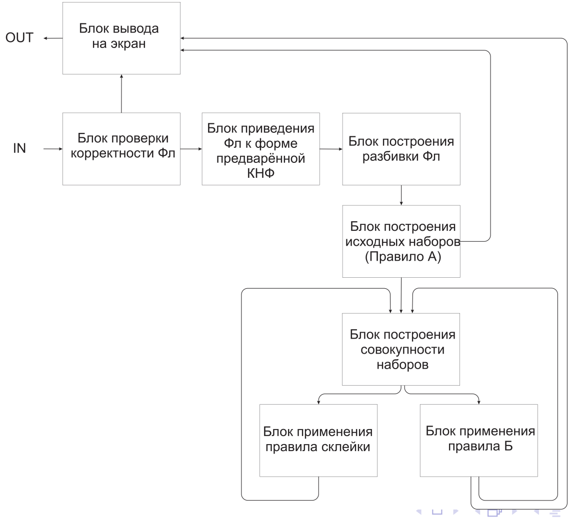
- задача распознавания клик в графе



- сведение этой задачи к проблеме выводимости секвенций вида:

$$\to \exists x_1, x_2, x_3 \begin{pmatrix} \neg R(a_1,a_2) \vee \neg R(a_2,a_3) \vee \neg R(a_2,a_4) \vee \neg R(a_3,a_4) \vee R(x_1,x_2) \\ \wedge \\ \neg R(a_1,a_2) \vee \neg R(a_2,a_3) \vee \neg R(a_2,a_4) \vee \neg R(a_3,a_4) \vee R(x_1,x_3) \\ \wedge \\ \neg R(a_1,a_2) \vee \neg R(a_2,a_3) \vee \neg R(a_2,a_4) \vee \neg R(a_3,a_4) \vee R(x_2,x_3) \end{pmatrix}$$

Задача 5: программная реализация специального варианта ОМ



Задача 6: сравнение ОМ с методом резолюций

Таблица: Результаты замера времени работы алгоритма обратного метода

Сложность формул (количество ЭФ)	**Среднее время вывода (сек.)**	**95%-доверительный интервал**
7	1.3	1.3 ± 0.1
15	28.3	28.3 ± 2.2
30	808.1	808.1 ± 32.4

Таблица: Результаты замера времени работы алгоритма метода резолюции

Сложность формул (количество ЭФ)	**Среднее время вывода (сек.)**	**95%-доверительный интервал**
7	6.2	6.2 ± 0.3
15	31.8	31.8 ± 3.8
30	963.7	963.7 ± 27.2

Результаты и выводы

1. предложена новая нотация для ОМ
2. написана программная реализация специального варианта ОМ
3. произведено сравнение алгоритмов ОМ и метода резолюций по времени