Санкт-Петербургский государственный университет
информационных технологий, механики и оптики

Факультет информационных технологий и программирования
Кафедра компьютерных технологий

А. В. Смаль

Автоматическое доказательство в системе Секущие Плоскости

Научный руководитель: Э. А. Гирш, к. ф.-м. н., доцент,
старший научный сотрудник
лаборатории математической логики
ПОМИ РАН.

Санкт-Петербург
2008

Содержание

Введение

Система доказательств — это некоторый набор правил для формального описания доказательства некоторого факта. Если у факта есть доказательство, то он является тавтологией (если это не так, то будет существовать контрпример). Как по некоторой тавтологии определить какой длины будет её доказательство в некоторой системе доказательств? Сложность этой задачи показана в [7].

Одно из свойств языков из $\mathcal{NP}$ — это короткое (полиномиальной длины) доказательство принадлежности. Для доказательства $\mathcal{P} \neq \mathcal{NP}$ достаточно показать, что $co\mathcal{NP}$ не обладает этим свойством. К примеру, для доказательства *выполнимости* некоторой булевой формулы достаточно привести выполняющий набор. Для того, чтобы проверить такое доказательство, достаточно вычислить формулу на выполняющем наборе, что можно сделать за полиномиальное время, т. е. SAT $\in \mathcal{NP}$. Что можно сказать про доказательство *невыполнимости*? Можно привести таблицу истинности или показать, что резолюция [20] приводит к пустому дизъюнкту. Всегда ли такое доказательство будет коротким? Если это так, то $co\mathcal{NP} = \mathcal{NP}$. Для таблиц истинности это не так, т. к. таблица истинности должна содержать все возможные значения переменных, а значит её размер ограничен снизу 2^n, где n — количество переменных. Для резолюции доказана экспоненциальная нижняя оценка для некоторых видов формул [3, 4, 16].

Пропозициональные системы доказательств, предназначенные для доказательства тавтологий на языке пропозициональной логики, являются важным классом систем доказательств. S. Cook и R. Reckhow показали [8], что полиномиально ограниченная (т. е. длина доказательства любой тавтологии ограничена полиномом от длины тавтологии) пропозициональная система доказательств, существует тогда и только тогда, когда $co\mathcal{NP} = \mathcal{NP}$.

Помимо своей теоретической важности системы доказательств применимы для решения некоторых практических задач. Одно из таких применений — *автоматическое доказательства теорем*. Необходимость в автоматическом доказательстве теорем возникает во множестве областей: системы искусственного

интеллекта, верификация программ, верификация вычислительных схем, проверка моделей, проверка и поиск доказательств математических теорем.

К сожалению, автоматическое доказательство некоторой теоремы может оказаться очень сложной задачей. Рассмотрим неформально следующую задачу: по данной системе доказательств П и теореме $\mathcal{T}$ найти доказательство $\mathcal{T}$ в системе П. Какова сложность такой задачи? Интуитивно понятно, что сложность этой задачи не меньше, чем сложность самого доказательства, т. к. в результате поиска мы должны как минимум привести доказательство. Другими словами, если доказательство длинное, то и искать его придется долго.

Существует несколько алгоритмов для поиска доказательства в различных пропозициональных системах доказательств. Цель данной работы — предложить алгоритм для поиска доказательства в системе Секущие Плоскости.

Постановка задачи

Цель работы — разработать алгоритм для автоматического поиска доказательства в системе Секущие Плоскости.

Для этого необходимо решить следующие задачи:

1. рассмотреть существующие системы доказательств и подходы к построению автоматических систем доказательств,
2. исследовать выбранную систему доказательств для выявления возможных путей улучшения алгоритма,
3. на основе существующих разработок в этой области предложить алгоритм для поиска доказательств в системе Секущие Плоскости.

Требования к алгоритму

1. *Полнота.* Алгоритм в конечном счете должен гарантированно находить доказательство для любой тавтологии.
2. *Эффективность.* Поиск доказательства должен быть эффективным.
3. *Мощь.* Алгоритм должен быстро находить короткие решения для тех сложных тавтологий, которые имеют короткое решение.

Глава 1.

Системы доказательств

1.1. Основные определения

Определение. *Система доказательств* [8] для языка L — это полиномиально вычислимая функция из множества слов (доказательств) в L (чьи элементы рассматриваются как теоремы).

Определение. *Пропозициональная система доказательств* — это система доказательств для фиксированного $co\mathcal{NP}$-полного языка булевых тавтологий (например, тавтологии в ДНФ).

Если у нас есть две системы доказательств Π_1 и Π_2 для одного и того же языка L, мы можем сравнить их.

Определение. Будем говорить, что Π_1 *полиномиально симулирует* Π_2, если существует функция g сопоставляющая доказательствам для Π_2 доказательства для Π_1 так, что для каждой гипотезы π для Π_2 верно $\Pi_1(g(\pi)) = \Pi_2(\pi)$ и $g(\pi)$ не более чем в полиномиальное количество раз длиннее π.

Определение. Система доказательств Π_1 *экспоненциально отделена* от Π_2, если существует бесконечная последовательность слов $t_1, t_2, \ldots \in L$ такая, что длина самого короткого доказательства для t_i в системе Π_1 полиномиальна от длины t_i, а в системе Π_2 — экспоненциальна от длины t_i.

Определение. Система доказательств Π_1 *экспоненциально сильнее*, чем Π_2, если Π_1 полиномально симулирует Π_2 и экспоненциально отделена от неё.

1.2. Резолюционная система доказательств

Резолюционная система доказательств — это система для доказательства общезначимости формул пропозициональной логики, основанная на методе резолюции [20, 17]:

$$\frac{\vee A;\ \vee B}{\vee(A \cup B) \setminus \{p, \neg p\}}, \tag{1.1}$$

где A и B — множества литералов, $p \in A$ и $\neg p \in B$. Переменная p называется *контрарной* для A и B. Доказательством в данной системе является вывод пустого дизъюнкта. Если рассматривать конъюнкцию множества литералов как клоз, то полученная система применима для доказательства невыполнимости формул в КНФ. В [20, стр. 87–91] доказана полнота метода резолюции, т. е. для любого несовместного множества клозов метод резолюции приведет к получению пустого дизъюнкта.

Сложностью доказательства является количество дизъюнкций в выводе пустого дизъюнкта. Есть также версия резолюционной системы доказательств, в которой доказательством считается дерево вывода, а сложностью — количество узлов в этом дереве. Известна экспоненциальная нижняя оценка для обычной резолюционной системы доказательств [3, 16].

1.3. Полуалгебраические системы доказательств

Главная идея полуалгебраических систем доказательств заключается в том, чтобы преобразовать булеву формулу в КНФ в систему алгебраических уравнений или неравенств. Это позволяет использовать алгебраические факты для доказательства тавтологий.

1.3.1. Системы доказательств на основе уравнений

Существует множество систем доказательств для языков неразрешимых систем полиномиальных уравнений [15]. Для преобразования такой системы доказательств в пропозициональную систему доказательств необходимо преобразовать булеву тавтологию в систему полиномиальных уравнений.

Для того, чтобы преобразовать формулу F в ДНФ, возьмем отрицание $\neg F$ в КНФ и преобразуем каждый клоз в полиномиальное уравнение. Клоз содержащий переменные $x_{j_1}, \ldots, x_{j_t}$ $(t \leq k)$ преобразуется в

$$(1 - l_1) \cdot \ldots \cdot (1 - l_t) = 0, \tag{1.2}$$

где $l_i = x_{j_i}$, если переменная x_{j_i} входит в клоз без отрицания и $l_i = (1 - x_{j_i})$ в противном случае. Для каждой переменной x_i в систему также добавляется уравнение $x_i^2 - x_i = 0$. Эти добавочные уравнения гарантируют, что значение всех переменных $x_i \in \{0, 1\}$.

Заметим, что F является тавтологией тогда и только тогда, когда полученная система уравнений $S = \{f_1 = 0,\ f_2 = 0, \ldots, f_m = 0\}$ не имеет решения. Таким образом, для доказательства F достаточно доказать, что S не имеет решения.

Рассмотрим наиболее известные системы доказательств, основанные на полиномиальных уравнениях [13].

- **Nullstellensatz (NS).** Доказательство в этой системе — набор полиномов $g_1, \ldots, g_m$ таких, что
$$\sum_i f_i g_i = 1.$$
- **Polynomial Calculus (PC).** В этой системе есть два правила вывода
$$\frac{p_1 = 0;\ p_2 = 0}{p_1 + p_2 = 0} \quad \text{и} \quad \frac{p = 0}{p \cdot q = 0}.$$
Доказательством является вывод $1 = 0$ из S при помощи этих правил.
- **Positivstellensatz.** Для этой системы доказательством являются полиномы $g_1, \ldots, g_m$ и $h_1, \ldots, h_l$ такие, что
$$\sum_i f_i g_i = 1 + \sum_j h_j^2.$$
- **Positivstellensatz Calculus.** Доказательство — полиномы $h_1, \ldots, h_l$ и вывод
$$1 + \sum_j h_j^2 = 0$$
из S используя правила для **PC**.

1.3.2. Системы доказательств на основе неравенств

Задача целочисленного линейного программирования определяется множеством неравенств с рациональными коэффициентами. Требуется найти набор целых чисел, который удовлетворяет всем неравенствам. Известно, что в такой постановке эта задача является $\mathcal{NP}$-полной. Если ограничиваться только 0-1 решением, то полученная задача также является $\mathcal{NP}$-полной. Системы доказательств на основе неравенств используют методы решения задач целочисленного линейного программирования для доказательства общезначимости пропозициональных формул.

Для определения пропозициональной системы доказательств основанной на неравенствах будем действовать аналогично. Для доказательства формулы F в ДНФ преобразуем $\neg F$ в систему линейных уравнений S такую, что F является тавтологией тогда и только тогда, когда S не имеет 0-1 решения. Для формулы в КНФ мы преобразуем каждый клоз содержащий переменные $x_{j_1}, \ldots, x_{j_t}$ $(t \leq k)$ в неравенство

$$l_1 + \cdots + l_t \geq 1, \tag{1.3}$$

где $l_i = x_{j_i}$, если переменная x_{j_i} входит в клоз без отрицания и $l_i = (1 - x_{j_i})$ в противном случае. Для каждой переменной x_i в систему S также добавляются неравенства

$$x_i \geq 0 \quad \text{и} \quad x_i \leq 1. \tag{1.4}$$

Рассмотрим наиболее известные системы, основанные на полиномиальных неравенствах [13].

- **Cutting Planes (CP)**. Исторически первая система доказательств на основе неравенств. Основана на алгоритме секущих плоскостей, предложенном R. Gomory [12] для решения задач целочисленного линейного программирования. В данной системе доказательств из системы неравенств S требуется вывести $0 \geq 1$ используя два правила вывода:

$$\frac{f_1 \geq 0; \ldots; \ f_t \geq 0}{\sum_{i=1}^{t} \lambda_i f_i \geq 0}, \tag{1.5}$$

  где $\lambda_i \geq 0$, и

$$\frac{\sum_i a_i x_i \geq c}{\sum_i a_i x_i \geq \lceil c \rceil}, \tag{1.6}$$

  где $a_i \in \mathbb{Z}$ и x_i — переменная. Все промежуточные неравенства должны иметь целые коэффициенты при переменных.

- **Lovász-Schrijver calculus (LS).** Данная система имеет большое количество вариаций [13]. В самом слабом случае системы доказательства **LS** противоречие должно быть получено при помощи (1.5) для линейных или квадратичных f_i и правил

$$\frac{f \geq 0}{fx \geq 0}, \quad \frac{f \geq 0}{f(1-x) \geq 0},$$

где f линейно, а x — переменная. В систему S также добавляются неравенства

$$x^2 - x \geq 0 \quad \text{и} \quad x - x^2 \geq 0$$

для каждой переменной x. В более сильных вариациях **LS** данная система расширяется за счет новых аксиом и правил вывода.

1.3.3. Динамические и статические системы доказательств

Системы доказательств делятся на два типа: *статические* и *динамические*. В динамических системах доказательством является некоторая последовательность шагов (применений правил вывода), которая приводит к противоречию. Напротив, в статических системах доказательство представляет собой некоторые множество математических объектов (к примеру, множество полиномов), которое удовлетворяют требуемому свойству, но ничего не говорится о способе получения этого множества. К динамическим системам относятся резолюция, **PC**, **Positivstellensatz Calculus**, **CP** и **LS**, а к статическим — **Nullstellensatz** и **Positivstellensatz**.

1.4. Почему именно Секущие Плоскости?

Зачем строить алгоритм для поиска доказательства именно в системе Секущие Плоскости? Для резолюции подробно описаны различные техники поиска доказательств [1, 2, 5]. В [11] описан алгоритм для поиска доказательства в одной из вариаций **LS**. Для **Nullstellensatz** и **Polynomial Calculus** в [14] и [6] соответственно предложены полиномиальные от длины доказательства алгоритмы для поиска доказательств. Система доказательств **CP** хороша тем, что это очень простая система доказательств с двумя правилами вывода. Несмотря на это она экспоненциально отделена от резолюционной системы доказательств (правда, есть и обратная оценка для tree-like **CP** [10]). Поэтому поиск доказательств в этой системе может оказаться менее сложным по сравнению с более сильными системами, но при этом более мощным, чем поиск резолюционных доказательств.

1.5. Сложные тавтологии

Рассмотрим несколько сложных тавтологий, которые позволяют оценить мощь **CP**. Первая тавтология, принцип Дирихле, экспоненциально отделяет **CP** от резолюционной системы доказательств, а вторая, раскраска клики, показывает пример проблемы, которая не имеет короткого решения в **CP**.

1.5.1. Принцип Дирихле

Вспомним принцип Дирихле:

> *Если в n клетках сидит m кроликов и $m > n$, то есть хотя бы одна клетка, в которой сидят два кролика.*

общепринятые сокращения: PHP (от *Pigeonhole Principle*) для принципа Дирихле и PHP_m^n для конкретной тавтологии.

Давайте запишем КНФ формулу для $\neg\mathrm{PHP}_m^n$. Для этого введем mn булевых переменных x_{ij}, $i \le m$, $j \le n$, имеющих смысл "i-й кролик сидит в j-й клетке". Для каждого кролика i запишем условие "кролик i сидит хотя бы в одной клетке":

$$x_{i1} \vee x_{i2} \vee \ldots \vee x_{in}.$$

Для каждой клетки k запишем условие "никакие два кролика не сидят в клетке k вместе":

$$\bigwedge_{i<k} (\neg x_{ik} \vee \neg x_{jk}).$$

Теперь сведем всё в единую формулу и получим

$$\bigwedge_i \bigvee_j x_{ij} \wedge \bigwedge_k \bigwedge_{i<j} (\neg x_{ik} \vee \neg x_{jk}). \tag{1.7}$$

Количество клозов в полученной формуле $m + nm(m-1)/2$.

В [3] доказана экспоненциальная $(2^{n/20})$ нижняя оценка на длину доказательства PHP_n^{n-1} методом резолюции. Для общего случая PHP_m^n экспоненциальная оценка была доказана позже [18, 19]. Полиномиальное доказательство для PHP_n^{n-1} в системе **CP** приведено в [9].

1.5.2. Раскраска клики

Рассмотрим раскраску графа G с n вершинами в $m-1$ цвет, если известно, что в графе есть клика размера m [16, 13]. Каждое ребро (i,j) задается 0-1 переменной p_{ij}. Переменные q_{ki} задают функцию (возможно многозначную) из множества целых чисел $\{1,\ldots,m\}$, обозначающих вершины m-клики, в множество вершин $\{1,\ldots,n\}$ графа G. Точнее, q_{ki} обозначает, что i-ая вершина графа G является k-ой вершиной m-клики. Переменные $r_{i\ell}$ задают (возможно многозначную) функцию окраски вершин в $m-1$ цвет. Переменная $r_{i\ell}$ обозначает, что вершина i окрашена в цвет ℓ.

Запишем все условия в виде пропозициональных формул в КНФ. Для каждого цвета ℓ верно, что не существует ребра (i,j), оба конца которого окрашены в этот цвет. Это можно записать следующим образом:

$$\bigwedge_{i<j}(\neg p_{ij} \vee \neg r_{i\ell} \vee \neg r_{j\ell}).$$

Каждая вершина i должна иметь цвет:

$$\bigwedge_{i}\bigvee_{\ell} r_{i\ell}.$$

Каждая вершина клики k сопоставлена хотя бы одной вершине графа:

$$\bigwedge_{k}\bigvee_{i} q_{ki}.$$

Каждая вершина графа i сопоставлена не более одной вершине клики:

$$\bigwedge_{i}\bigwedge_{k<k'}(\neg q_{ki} \vee \neg q_{k'i}).$$

Любые две вершины клики соединены ребром:

$$\bigwedge_{i<j}\bigwedge_{k\neq k'}(p_{ij} \vee \neg q_{ki} \vee \neg q_{k'j}).$$

Здесь во всех формулах $i,j \in \{1,\ldots,n\}$, $k,k' \in \{1,\ldots,m\}$, $\ell \in \{1,\ldots,m-1\}$.

Как показано в [16] данная тавтология не имеет короткого (полиномиальной длины) доказательства в **CP**. В [13] предложено короткое доказательство для раскраски клики в некоторых вариациях **LS**.

Глава 2.

Анализ системы доказательств Секущие Плоскости

2.1. Небулевы клозы

Секущие Плоскости позволяют получать неравенства, которым не соответствует никакой клоз. Такие неравенства могут быть сильнее, нежели неравенства соответствующие булевым клозам. К примеру (W. Cook, C. Coullard и G. Turán, 1987 [9]):

$$\begin{array}{rl} & x_1 + x_2 \geq 1 \\ + & x_1 + x_3 \geq 1 \\ + & x_2 + x_3 \geq 1 \\ \hline & 2x_1 + 2x_2 + 2x_3 \geq 3 \end{array} \quad \Rightarrow \quad x_1 + x_2 + x_3 \geq \lceil 3/2 \rceil = 2. \tag{2.1}$$

Полученное неравенство сильнее, чем клоз $x_1 \vee x_2 \vee x_3$. Будем называть такие неравенства *небулевыми клозами*. Рассмотрим возможные способы получения небулевых клозов. Далее под словом “клоз” понимается неравенство, соответствующее этому клозу.

Будем искать вывод небулевых клозов для следующей системы уравнений.

1. Множество $X = \{x_1, \ldots, x_n\}$ — множество переменных.
2. В системе изначально есть только булевы клозы.
3. Нет клозов длины 1.
4. Все переменные входят в клозы положительно (т. е. без отрицания).

Такие ограничения позволяют не думать о том, что может случиться, если клозы содержат контрарные переменные. В дальнейшем для применения полученных результатов на практике для некоторой системы неравенств S над множеством переменных X, необходимо выделить некоторое множество переменных

$\tilde{X} \subset X$ и множество неравенств $\tilde{S} \subset S$ над $\tilde{X}$, не содержащие контрарные переменные. Тогда систему неравенств $\tilde{S}$ над множеством переменных $\tilde{X}$ можно рассматривать как самостоятельную.

Замечание. В качестве переменных x_i могут выступать произвольные суммы переменных, не имеющие общие слагаемые. К примеру, неравенства

$$x_1 + x_2 + x_3 + x_4 \geq 1, \quad x_1 + x_2 + x_5 + x_5 \geq 1, \quad x_3 + x_4 + x_5 + x_5 \geq 1,$$

можно записать в форме

$$x'_1 + x'_2 \geq 1, \quad x'_1 + x'_2 \geq 1, \quad x'_1 + x'_2 \geq 1,$$

положив

$$x'_1 = x_1 + x_2, \quad x'_2 = x_3 + x_4, \quad x'_3 = x_5 + x_6.$$

Это замечание справедливо для всех последующих теорем.

Введем обозначения:

- $\mathcal{I}_n = \{1, 2, \ldots, n\}$ — множество индексов от 1 до n,
- c_{ij} — 2-клоз $x_i + x_j \geq 1$.

2.2. Получение небулевых клозов с единичными коэффициентами

Начнём с самого простого случая. Этот случай часто ассоциируется с треугольником: если считать переменные вершинами графа, а 2-клозы — ребрами, то для этого случая граф имеет форму треугольника (рис. 1).

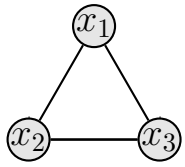

Рис. 1. Графическое изображение всех 2-клозов для трех переменных.

Теорема 1 ($n = 3$)**.** *Для получения небулевого клоза* $x_1+x_2+x_3 \geq 2$ *необходимо и достаточно трех клозов*

$$x_1 + x_2 \geq 1, \quad x_1 + x_3 \geq 1, \quad x_2 + x_3 \geq 1.$$

Доказательство. *Необходимость.* Предположим, что в системе есть все возможные клозы кроме одного 2-клоза. Не умаляя общности, можно считать, что в исходной системе отсутствует клоз $x_1 + x_2 \geq 1$. Тогда система включает следующие три клоза:

$$x_1 + x_2 + x_3 \geq 1, \quad x_1 + x_3 \geq 1, \quad x_2 + x_3 \geq 1.$$

Положим, $x_1 = x_2 = 0$, и $x_3 = 1$. В этом случае все клозы выполняются, но

$$x_1 + x_2 + x_3 = 1 < 2.$$

Достаточность. См. (2.1). □

Обобщим этот случай на произвольный n. Отметим, что если предыдущий случай ассоциировался с треугольником, то этот случай должен ассоциироваться с полным графом (рис. 2).

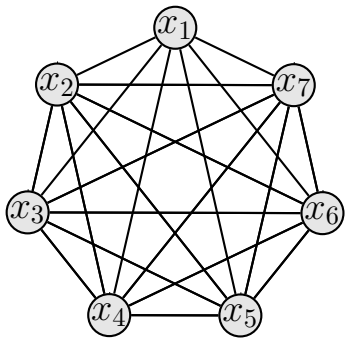

Рис. 2. Графическое изображение всех 2-клозов для 7 переменных.

Теорема 2 ($n \geq 3$)**.** *Для получения небулевого клоза*

$$\sum_{i=1}^{n} x_i \geq n - 1 \tag{2.2}$$

необходимо и достаточно наличие всех 2-клозов.

Доказательство. *Необходимость.* Предположим, что в системе есть все возможные клозы длины меньше n, кроме $x_p + x_q \geq 1$. Тогда положим,

$$x_i = \begin{cases} 0, & i \in \{p, q\}, \\ 1, & i \notin \{p, q\}. \end{cases}$$

Заметим, что такая интерпретация выполняет все возможные клозы. Но при этом

$$\sum_{i=1}^{n} x_i = n - 2 < n - 1.$$

Достаточность. (W. Cook, C. Coullard и G. Turán, 1987 [9]) Будем получать клозы рекурсивно по следующему алгоритму. Для получения

$$\sum_{i=a}^{b} x_i \geq b - a$$

получим

$$\sum_{i=a}^{b-1} x_i \geq b - a - 1 \quad \text{и} \quad \sum_{i=a+1}^{b} x_i \geq b - a - 1.$$

Используя клоз $x_a + x_b \geq 1$, получаем

$$\sum_{i=a}^{b-1} x_i + \sum_{i=a+1}^{b} x_i + (x_a + x_b) \geq 2(a - b - 1) + 1 \quad \Rightarrow \quad \sum_{i=a}^{b} x_i \geq b - a.$$

При $a = 1$ и $b = n$ получаем (2.2). □

Замечание. Полученная теорема может быть использована для получения длинных неравенств для доказательства PHP, т. к. там есть подмножества переменных, для которых существуют все 2-клозы.

Теорема 3 (Общая теорема для неравенств с единичными коэффициентами)**.** *Для получения небулевого клоза*

$$\sum_{i=1}^{n} x_i \geq n - m \tag{2.3}$$

необходимо и достаточно, чтобы для каждого множества индексов переменных $I \subset \mathcal{I}_n : |I| = m + 1$ существовало неравенство

$$\sum_{i \in J} x_i \geq 1, \quad \text{где } J \subseteq I.$$

Доказательство. *Необходимость.* Предположим, что в системе для некоторого множества $P \in \mathcal{I}_n : |P| = m+1$ и его подмножеств в системе нет ни одного клоза. Тогда рассмотрим следующую интерпретацию

$$x_i = \begin{cases} 0, & i \in P \\ 1, & i \notin P. \end{cases}$$

Заметим, что такая интерпретация выполняет все клозы (т. к. нет ни одного клоза, у которого все переменные имеют индекс из P). Но при этом

$$\sum_{i=1}^{n} x_i = n - m - 1 < n - m.$$

Достаточность. Для начала получим всех клозы вида

$$\sum_{i \in I} x_i \geq 1$$

используя более сильные клозы. Это можно сделать, т. к.

$$\sum_{i \in J \subset I} x_i \geq 1 \ \vee \ \forall i (x_i \geq 0) \quad \Rightarrow \quad \sum_{i \in I} x_i \geq 1.$$

Далее будем получать клозы рекурсивно по следующему алгоритму. Пусть

$$Q \subset \mathcal{I}_n \quad \text{и} \quad |Q| = m + 1 + r,$$

где $1 \leq r \leq n - m - 1$. Для получения

$$\sum_{i \in Q} x_i \geq r + 1$$

выделим из Q два дизъюнктных подмножества Q_1 и Q_2, причем $|Q_1| = m + 1$, $Q_2 = Q \setminus Q_1$ (т. е. $|Q_2| = r$).

$$\sum_{i \in Q_1} x_i + \sum_{j \in Q_1} \Big(\sum_{i \in Q_2} x_i + \sum_{\substack{i \in Q_1 \\ i \neq j}} x_i \Big) \geq 1 + (m+1)r.$$

Раскрываем скобки и приводим подобные слагаемые

$$\begin{aligned}
&\sum_{i \in Q_1} x_i + \sum_{j \in Q_1} \Big(\sum_{i \in Q_2} x_i + \sum_{\substack{i \in Q_1 \\ i \neq j}} x_i \Big) = \\
&\qquad = \sum_{i \in Q_1} x_i + \sum_{j \in Q_1} \sum_{i \in Q_2} x_i + \sum_{j \in Q_1} \Big(\sum_{i \in Q_1} x_i - x_j \Big) = \\
&\qquad = \sum_{i \in Q_1} x_i + (m+1) \sum_{i \in Q_2} x_i + (m+1) \sum_{i \in Q_1} x_i - \sum_{i \in Q_1} x_i = \\
&\qquad = (m+1) \sum_{i \in Q_1} x_i + (m+1) \sum_{i \in Q_2} x_i = \\
&\qquad\qquad = (m+1) \sum_{i \in Q} x_i \ \geq \ 1 + (m+1)r.
\end{aligned}$$

Применяя правило округления

$$\sum_{i \in Q} x_i \geq \lceil 1/(m+1) \rceil + r = r + 1.$$

При $r = n - m - 1$ получаем (2.3). □

Следствие 1. *Если из некоторой системы клозов C не следует неравенство*

$$\sum_{i=1}^{n} x_i \geq t,$$

то существует интерпретация, удовлетворяющая C такая, что

$$\sum_{i=1}^{n} x_i < t.$$

Доказательство. Пусть такой интерпретации не существует. Тогда C удовлетворяет достаточное условие теоремы, а значит удовлетворяет и необходимое. □

Применим полученную теорему к случаю 2-клозов.

Теорема 4. *Если в системе C есть только 2-клозы, то для получения неравенства*

$$\sum_{i=1}^{n} x_i \geq n - m$$

необходимо и достаточно, чтобы для каждого множества $I \in \mathcal{I}_n : |I| = m+1$ был клоз $x_p + x_q \geq 1 : p, q \in I$.

Доказательство. Применяем теорему 3, считая что $|J| = 2$. □

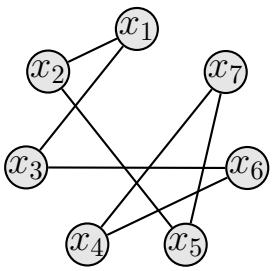

Рис. 3. Цикл нечётной длины на графе 2-клозов.

Один из интересных примеров применения теоремы 4 — это поиск цикла нечетной длины в графе 2-клозов (рис. 3. По данной теореме цикл 2-клозов позволяет вывести неравенство

$$\sum_{i=1}^{n} x_i \geq \lceil n/2 \rceil.$$

Если n — нечётное, то полученное неравенство будет небулевым клозом.

2.3. Получение небулевых клозов с произвольными коэффициентами

Будем рассматривать случаи, когда в результате вывода получено неравенство вида

$$\sum_{i=1}^{n} k_i x_i \geq t, \text{ где } \forall i \; k_i \in \mathbb{N}.$$

Лемма 1. *Если $k_j > t$, то*

$$\sum_{i=1}^{n} k_i x_i \geq t \quad \Leftrightarrow \quad t x_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i x_i \geq t.$$

Доказательство. $\boxed{\Rightarrow}$ Рассмотрим два случая.

1. Если $x_j = 1$, то верны оба неравенства.
2. Если $x_j = 0$, то из первого неравенства получаем

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} k_i x_i \geq t,$$

а следовательно, верно и второе неравенство.

$\boxed{\Leftarrow}$ Очевидно, т. к. $x_j \geq 0$. □

Следствие 2. *Можно рассматривать только клозы с коэффициентами не превосходящими t.*

Лемма 2. *Если $\sum\limits_{i=1}^{n} k_i < t$, то неравенство $\sum\limits_{i=1}^{n} k_i x_i \geq t$ невыполнимо.*

Доказательство.

$$\forall i(x_i \le 1) \quad \Rightarrow \quad \sum_{i=1}^{n} k_i x_i \le \sum_{i=1}^{n} k_i < t.$$

□

Следствие 3. *Если для полученного неравенства выполняются условия леммы, то исходная система противоречива.*

Будем рассматривать получение небулевых клозов с нетривиальными коэффициентами из системы 2-клозов. Более общая постановка представляется значительно более сложной. Для начала рассмотрим самый простой случай, когда один из коэффициентов равен 2, а все остальные единичные.

Теорема 5 ($k_j = 2$)**.** *Для получения небулевого клоза*

$$x_j + \sum_{i=1}^{n} x_i \ge n - 1$$

необходимо и достаточно наличие всех 2-клозов кроме некоторого клоза

$$x_p + x_q \ge 1, \quad p, q \ne j.$$

Доказательство. *Необходимость.* Рассмотрим два случая.

1. Пусть в системе есть все возможные клозы кроме $x_j + x_p$. Тогда интерпретация

$$x_i = \begin{cases} 0, & i \in \{j, p\}, \\ 1, & i \notin \{j, p\} \end{cases}$$

выполняет все клозы системы, но при этом

$$x_j + \sum_{i=1}^{n} x_i = n - 2 < n - 1.$$

2. Пусть в системе есть все возможные клозы кроме $x_{p_1} + x_{q_1}$ и $x_{p_2} + x_{q_2}$, где $p_1 \ne p_2$ и $p_1, p_2, q_1, q_2 \ne j$. Тогда интерпретация

$$x_i = \begin{cases} 0, & i \in \{p_1, p_2, q_1\}, \\ 1, & i \notin \{p_1, p_2, q_1\} \end{cases}$$

выполняет все клозы системы, но

$$x_j + \sum_{i=1}^{n} x_i = n - 2 < n - 1.$$

Достаточность. По теореме 2 можно вывести

$$\sum_{\substack{i=1 \\ i \neq p}}^{n} x_i \geq n - 2, \quad \text{и} \quad \sum_{\substack{i=1 \\ i \neq q}}^{n} x_i \geq n - 2.$$

Тогда

$$\sum_{\substack{i=1 \\ i \neq p}}^{n} x_i + \sum_{\substack{i=1 \\ i \neq q}}^{n} x_i + (x_j + x_p) + (x_j + x_q) \geq 2n - 2 \quad \Leftrightarrow \quad x_j + \sum_{i=1}^{n} x_i \geq n - 1.$$

□

Для доказательства следующей теоремы нам потребуется лемма.

Лемма 3. *Ни из какого множества клозов C нельзя получить*

$$\sum_{i=1}^{n} x_i \geq n.$$

Доказательство. Рассмотрим интерпретацию σ :

$$x_i = \begin{cases} 0, & i = 1, \\ 1, & i > 1. \end{cases}$$

В этой интерпретации $\sum\limits_{i=1}^{n} x_i = n - 1 < n$ и при этом выполняются все клозы. □

Теперь докажем более сложный случай: один из коэффициентов равен k, а остальные коэффициенты единичные.

Теорема 6 ($k_j = k$)**.** *Для получения небулевого клоза*

$$kx_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n - 1 \tag{2.4}$$

необходимо и достаточно наличие всех 2-клозов из некоторого множества C, для которого выполняются два условия:

$$C \setminus C_j \Leftrightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n - k - 1, \tag{2.5}$$

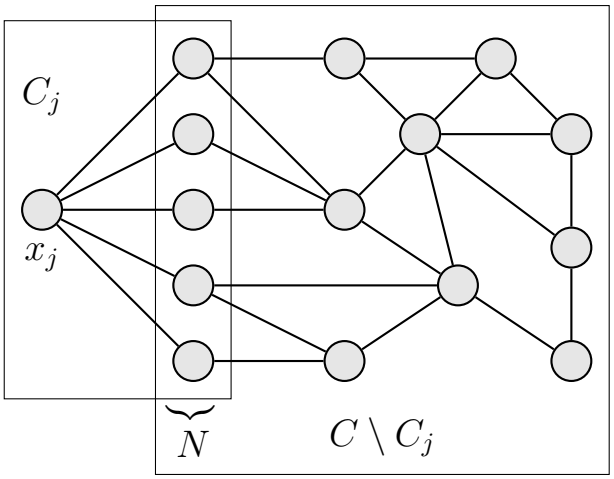

Рис. 4. Множества клозов C_j и $C \setminus C_j$.

где $C_j = \{c_{jq} \mid c_{jq} \in C\}$ *(все клозы содержащие* x_j*), и*

$$c_{ij} \in C \quad \forall i \neq j. \tag{2.6}$$

Доказательство. *Необходимость.* Докажем оба условия.

1. Пусть условие (2.5) не выполняется:

$$C \setminus C_j \not\Rightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n - k - 1,$$

т. е. существует такая интерпретация σ_j для которой

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} x_i < n - k - 1.$$

Дополним σ_j значением $x_j = 1$ и заметим, что получившаяся интерпретация не выполняет (2.4).

2. Пусть условие (2.6) не выполняется. Рассмотрим множество соседей $N = \{q \mid c_{jq} \in C\}$ (рис. 4). Для любой интерпретации σ, в которой x_j принимает значение 0, все переменные x_q, $q \in N$ принимают значение 1. Рассмотрим такую интерпретацию. Подставляя в (2.4) значения для x_j и ее соседей, получаем

$$\sum_{\substack{i \notin N \\ i \neq j}} x_i \geq n - |N| - 1. \tag{2.7}$$

Посчитаем, сколько переменных стоит в левой части: $n - |N| - 1$. По лемме 3 такое неравенство 2.7 нельзя получить из множества клозов. Таким образом, $|N| = n - 1$.

Достаточность. По теореме 4 условие (2.5) эквивалентно тому, что для каждого множества $J \subset \mathcal{I}_n \setminus \{j\}$ такого, что $|J| = k + 1$, в $C \setminus C_j$ существует клоз $c_{pq} : p, q \in J$. Заметим, что это же свойство будет выполняться и для C, т. е.

$$\forall J \subset \mathcal{I}_n : |J| = k + 1 \quad \exists c_{pq} \in C : p, q \in J.$$

Докажем это, рассмотрев два случая.

1. $j \in J$. По условию (2.6) $\forall i \in J : i \neq j \; c_{ij} \in C$.
2. $j \notin J$. Тогда верно следствие для $C \setminus C_j$.

По теореме 4 из множества клозов C выводимо неравенство

$$\sum_{i=1}^{n} x_i \geq n - k.$$

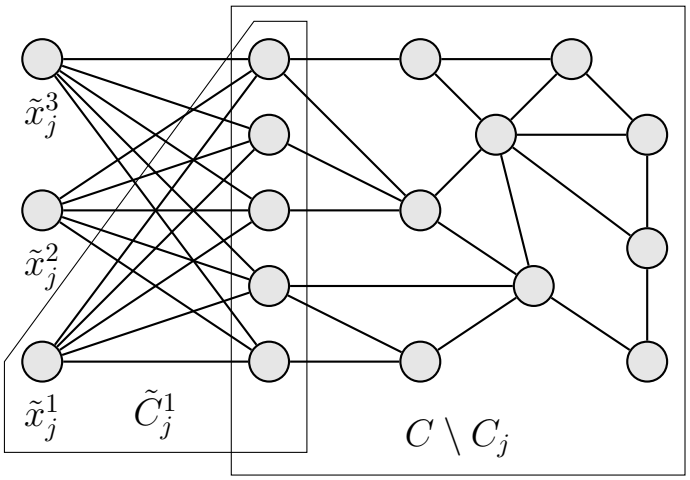

Рис. 5. Замена x_j на “виртуальные” переменные $\tilde{x}_j^i$.

Будем вместо множества C рассмотрим множество

$$\tilde{C} = (C \setminus C_j) \cup \bigcup_{i=1}^{k} \tilde{C}_j^i,$$

где $\tilde{C}_j^i$ это “аналог” множества C_j, где вместо x_j используется некоторая “виртуальная” переменная $\tilde{x}_j^i$ (рис. 5). Заметим, что для полученного множества

также выполняется свойство

$$\forall J \subset \mathcal{I}_n : |J| = k+1 \quad \exists c_{pq} \in \tilde{C} : p, q \in J.$$

В любом множестве размера $k+1$ либо все переменные из $\mathcal{I}_n \setminus \{j\}$ (тогда есть клоз по теореме 4 для множества клозов C), либо есть не более k "виртуальных" (тогда есть клоз для виртуальной и невиртуальной переменной).

Таким образом, из $\tilde{C}$ выводится неравенство

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} x_i + \sum_{i=1}^{n} \tilde{x}_j^i \geq n-1.$$

Теперь склеим все "виртуальные" переменные, т. е. положим $\forall i \ \tilde{x}_j^i = x_j$. Заметим, что это не нарушает никакие условия. Мы просто будем рассматривать только те интерпретации, в которых все $\tilde{x}_j^i$ равны друг другу. Можно также посмотреть на это с другой стороны: представим, что в процессе вывода мы не всегда приводили подобные слагаемые для x_j.

В общем, получаем

$$\sum_{i=1}^{n} x_i \geq n-1.$$

□

Лемма 4. *Пусть A и B — два множества клозов, причем $B \subseteq A$. Тогда, если*

$$A \Leftrightarrow \sum x_i \geq a \quad \textit{и} \quad B \Leftrightarrow \sum x_i \geq b,$$

то $a \geq b$.

Доказательство. По теореме 3 добавление новых клозов может только увеличить правую часть полученного неравенства. □

Обобщим предыдущую теорему на случай произвольной правой части.

Теорема 7 ($k_j = k, \geq n-m$)**.** *Для получения небулевого клоза*

$$kx_j + \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n-m \tag{2.8}$$

необходимо и достаточно наличие всех 2-клозов из некоторого множества C, для которого выполняются два условия:

$$C \setminus C_j \Leftrightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n - m - k, \tag{2.9}$$

где $C_j = \{c_{jq} \mid c_{jq} \in C\}$ (все клозы содержащие x_j),

$$C \setminus C_N \Leftrightarrow \sum_{\substack{i \notin N \\ i \neq j}} x_i \geq n - m - |N|, \tag{2.10}$$

где $N = \{q \mid c_{jq} \in C\}$ (множество соседей j) и $C_N = \{c_{pq} \mid p \in N\}$ (рис. 6).

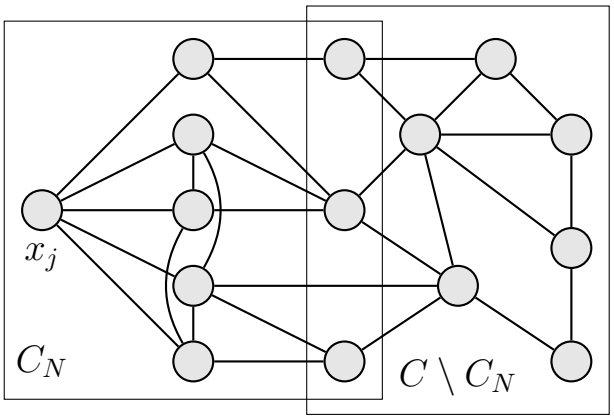

Рис. 6. Множества клозов C_N и $C \setminus C_N$.

Доказательство. *Необходимость.*

1. Пусть условие (2.9) не выполняется:

$$C \setminus C_j \not\Leftrightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} x_i \geq n - m - k,$$

т. е. существует такая интерпретация σ_j, для которой

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} x_i < n - m - k.$$

Дополним σ_j значением $x_j = 1$ и заметим, что получившаяся интерпретация не выполняет (2.8).

2. Пусть условие (2.10) не выполняется:

$$C \setminus C_N \not\Rightarrow \sum_{\substack{i \notin N \\ i \neq j}} x_i \geq n - m - |N|,$$

т. е. существует такая интерпретация σ_N, для которой

$$\sum_{\substack{i \notin N \\ i \neq j}} x_i < n - m - |N|.$$

Дополним σ_N значениями

$$x_i = \begin{cases} 0, & i = j, \\ 1, & i \in N. \end{cases}$$

Заметим, что получившаяся интерпретация не выполняет (2.8).

Достаточность. Заметим, что $C_j \subseteq C_N$, а значит

$$C \setminus C_N \subseteq C \setminus C_j.$$

Отсюда по лемме 4 следует, что $|N| \geq k$.

По теореме 4 условие (2.9) эквивалентно тому, что для каждого множества $J \subset \mathcal{I}_n \setminus \{j\}$ размера $k+m$ в $C \setminus C_j$ существует клоз $c_{pq} : p, q \in J$. Аналогично, условие (2.10) эквивалентно тому, что для каждого множества $J \subset \mathcal{I}_n \setminus (N \cup \{j\})$ такого, что $|J| = m$, в $C \setminus C_N$ существует клоз $c_{pq} : p, q \in J$.

Докажем, что подобное свойство

$$\forall J \subset \mathcal{I}_n : |J| = k + m \quad \exists c_{pq} \in C : p, q \in J.$$

будет выполняться и для C. Рассмотрим три случая.

1. $j \notin J$. В этом случае верно следствие для $C \setminus C_j$.
2. $j \in J$ и $J \cap N \neq \emptyset$. По определению множества N $\exists c_{ij} : i \in J \cap N$.
3. $j \in J$ и $J \cap N = \emptyset$. Т. к. $|J \setminus \{j\}| = k + m - 1 \geq m$, то над множеством J существует клоз из $C \setminus C_N$.

По теореме 4 из множества клозов C выводимо неравенство

$$\sum_{i=1}^{n} x_i \geq n - m - k.$$

Будем действовать подобно предыдущей теореме, т. е. вместо множества C рассмотрим множество

$$\tilde{C} = (C \setminus C_j) \cup \bigcup_{i=1}^{k} \tilde{C}_j^i,$$

где $\tilde{C}_j^i$ это "аналог" множества C_j, где вместо x_j используется некоторая "виртуальная" переменная $\tilde{x}_j^i$ (рис. 5). Заметим, что для полученного множества также выполняется свойство

$$\forall J \subset \mathcal{I}_n : |J| = k + m \quad \exists c_{pq} \in \tilde{C} : p, q \in J.$$

В каждом множестве размера $k + m$ есть либо m, вершин не принадлежащих N, либо $k + m$ невиртуальных вершин, либо виртуальная вершина и её сосед. Во всех трех случаях для такого множества существует 2-клоз.

Таким образом, из $\tilde{C}$ выводится неравенство

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} x_i + \sum_{i=1}^{n} \tilde{x}_j^i \geq n - m.$$

Положим $\forall i \ \tilde{x}_j^i = x_j$. Аргументы в пользу этого шага такие же как в доказательстве достаточности для теоремы 6: просто будем рассматривать только те интерпретации, в которых все $\tilde{x}_j^i$ равны друг другу.

В результате получаем

$$\sum_{i=1}^{n} x_i \geq n - m.$$

□

Сформулируем общую теорему. К сожалению, на данный момент найдено только доказательство необходимости.

Теорема 8 (Обобщенная)**.** *Для получения небулевого клоза*

$$\sum_{i=1}^{n} k_i x_i \geq n - m \tag{2.11}$$

из 2-клозов необходимо, чтобы множество 2-клозов C удовлетворяло следующие два условия для каждого $j \in \mathcal{I}_n$:

$$C \setminus C_j \Leftrightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i x_i \geq n - m - k_j, \tag{2.12}$$

$$C \setminus C_N \Leftrightarrow \sum_{\substack{i \notin N \\ i \neq j}} k_i x_i \geq n - m - \sum_{i \in N} k_i, \tag{2.13}$$

где C_j, C_N и N определяются аналогично теореме 7.

Доказательство. Докажем оба условия.

1. Пусть условие (2.12) не выполняется:

$$C \setminus C_j \not\Rightarrow \sum_{\substack{i=1 \\ i \neq j}}^{n} k_i x_i \geq n - m - k,$$

т. е. существует такая интерпретация X_j, для которой

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} k_i x_i < n - m - k_j.$$

Дополним σ_j значением $x_j = 1$ и заметим, что получившаяся интерпретация не выполняет (2.11).

2. Пусть условие (2.13) не выполняется:

$$C \setminus C_N \not\Rightarrow \sum_{\substack{i \notin N \\ i \neq j}} k_i x_i \geq n - m - \sum_{\substack{i \notin J \\ i \neq j}} k_i,$$

т. е. существует такая интерпретация σ_N, для которой

$$\sum_{\substack{i \notin N \\ i \neq j}} k_i x_i < n - m - \sum_{\substack{i \notin J \\ i \neq j}} k_i.$$

Дополним σ_N значениями

$$x_i = \begin{cases} 0, & i = j, \\ 1, & i \in N. \end{cases}$$

Заметим, что получившаяся интерпретация не выполняет (2.11). □

Можно показать, что данное условие действительно является необходимым и достаточным для существования решения системы C, но не понятно как вывести (2.11) из (2.12) и (2.13) используя правила вывода **CP**.

Глава 3.

Построение алгоритма для Секущих Плоскостей

Для того, чтобы получить алгоритм для поиска доказательств в системе Секущие Плоскости обратимся к идеям изложенным в [11].

3.1. Моделирование упорядоченной резолюции

Рассмотрим модификацию резолюционной системы доказательств — *упорядоченную резолюцию* [1, 2]. Основная идея этой системы заключается в том, чтобы сократить количество выводимых клозов за счёт ограничения правил вывода. Для этого на множестве переменных вводится порядок и каждый клоз может участвовать в резолюции только для своей старшей переменной.

Рассмотрим каркас алгоритма для поиска доказательства в системе упорядоченной резолюции.

Алгоритм Ordered-Resolution

1: ввести порядок на множестве переменных
2: **while** не получен пустой дизъюнкт **do**
3: выбрать пару клозов c_i и c_j, контрарных по старшей переменной
4: построить резольвенту c' для c_i и c_j
5: **if** c' — единичный дизъюнкт **then**
6: подставить соответствующее значение во все клозы
7: **else if** клоз c' не тавтология и не слабее какого-то другого клоза **then**
8: добавим клоз c' в систему
9: **end if**
10: **end while**

Ordered-Resolution не содержит указания как именно выбирать пару клозов (c_i, c_j) для резолюции. В зависимости от того, какую стратегию поиска пар клозов для резолюции использовать, могут получаться различные алгоритмы. Одна из таких стратегий — стратегия *насыщения уровня* [20]. Проиллюстрируем данную стратегию: пусть изначально есть некоторое множество

клозов S_0. Перебирая все возможные пары клозов, для которых можно провести резолюцию в соответствии с заданным порядком, из системы S_0 выводится множество клозов S_1. После того, как все пары из S_0 рассмотрены, перебираются пары клозов $(c_1, c_2) : c_1 \in S_0 \cup S_1,\ c_2 \in S_1$, и, таким образом, получается множество S_2. И так далее, на k-м этапе выводится множество клозов S_k на основе пар клозов

$$(c_1, c_2) : c_1 \in S_0 \cup S_1 \cup \ldots \cup S_{k-1},\ c_2 \in S_{k-1}.$$

Аналогично упорядоченной резолюции определим систему доказательств *упорядоченные Секущие Плоскости*: два неравенства могут складываться тогда и только тогда, когда они имеют общую старшую переменную. Докажем, что упорядоченные Секущие Плоскости могут моделировать упорядоченную резолюцию.

Теорема 9. *Система доказательств упорядоченные Секущие Плоскости может моделировать доказательство в системе упорядоченной резолюции.*

Доказательство. Пусть $\{x_1, \ldots, x_n\}$ — множество переменных. По (1.3) в **CP** каждому клозу соответствует неравенство. Пусть x_k — контрарная переменная для двух клозов, тогда

$$\frac{x_k \vee \bigvee A;\ \neg x_k \vee \bigvee B}{\bigvee(A \cup B)}.$$

В **CP** это будет выглядеть так

$$\frac{x_k + \sum A \geq 1;\ (1 - x_k) + \sum B \geq 1}{\sum A + \sum B \geq 1}.$$

В случае, если $A \cap B = \emptyset$, то полученное неравенство соответствует клозу, полученному при резолюции. Если же $A \cap B \neq \emptyset$, то полученное неравенство будет иметь вид

$$\sum(A \triangle B) + 2\sum(A \cap B) \geq 1. \tag{3.1}$$

Воспользуемся неравенствами 1.4

$$(x_i \geq 0) \wedge (x_i \leq 1) \quad \Rightarrow \quad l_i \geq 0.$$

Отсюда

$$\sum(A \triangle B) \geq 0. \tag{3.2}$$

Складывая (3.1) и (3.2), получаем

$$2\sum(A\triangle B) + 2\sum(A\cap B) \geq 1 \quad \Rightarrow \quad 2\sum(A\cup B) \geq 1.$$

Умножаем полученное неравенство на $1/2$ и округляем

$$\sum(A\cup B) \geq \lceil 1/2 \rceil = 1.$$

Таким образом, полученное неравенство соответствует клозу, полученному при резолюции. □

Аналогично Ordered-Resolution можно построить каркас алгоритма для системы упорядоченных Секущих Плоскостей.

Алгоритм Ordered-CP

1: ввести порядок на множестве переменных
2: **while** не получено неравенство $0 \geq 1$ **do**
3: выбрать пару клозов c_i и c_j, контрарных по старшей переменной
4: промоделировать резолюцию и получить клоз c'
5: **if** в клозе c' есть двойки **then**
6: избавиться от них в соответствии с теоремой 9
7: **end if**
8: **if** c' — единичный клоз **then**
9: подставить соответствующее значение во все клозы
10: **else if** клоз c' не тавтология и не слабее какого-то другого клоза **then**
11: добавить клоз c' в систему
12: **end if**
13: **end while**

Применяя стратегию насыщения уровня для поиска пар клозов, получаем простейший алгоритм для поиска доказательства в упорядоченных Секущих Плоскостях. Обозначим такой алгоритм Ordered-CP-Saturate.

Замечание. Может показаться, что данный алгоритм выведет бóльшее число клозов, чем упорядоченная резолюция: если два клоза контрарны по и старшей переменной и по какой-то еще, то в результате резолюции будет получена тавтология, а в **CP** контрарные переменные просто сократятся. Но это неверно — неравенство полученное в **CP** также будет тавтологией.

$$\frac{x_1 \vee x_2 \vee x_3;\ \neg x_1 \vee \neg x_2 \vee x_4}{x_2 \vee \neg x_2 \vee x_3 \vee x_4}$$

$$\frac{x_1 + x_2 + x_3 \geq 1;\ (1 - x_1) + (1 - x_2) + x_4 \geq 1}{x_3 + x_4 \geq 0}$$

Таким образом данный алгоритм эквивалентен Ordered-Resolution с насыщением уровня, т. е. в процессе своей работы он выведет те же клозы.

3.2. Улучшение алгоритма

Давайте проанализируем Ordered-CP-Saturate.

1. Доказательство обязательно будет получено, т. к. моделируется упорядоченная резолюция. Другими словами, построенный алгоритм полон.

2. Короткое доказательство для сложных тавтологий вроде PHP_n^{n-1} не будет найдено. Это объясняется тем, что алгоритм не делает ничего, кроме моделирования упорядоченной резолюции.

3. В случае, если при сложении двух неравенств получилось неравенство с двойками, то впоследствии оно заменяется на версию с единичными коэффициентами, а исходное неравенство забывается. Т. е. все неравенства в системе имеют единичные коэффициенты. Если в коротком доказательстве для некоторой тавтологии участвует неравенство с нетривиальными коэффициентами, то такое неравенство не будет найдено.

Данный алгоритм можно улучшить несколькими способами.

1. Самое слабое улучшение — это добавить поиск “треугольников” из 2-клозов и получать новые неравенства в соответствии с теоремой 1.

2. Более мощное улучшение — это поиск обобщённых троек, который используется в доказательстве теоремы 2:

$$\sum_{i \in J \cup \{a\}} x_i \geq r_a, \qquad \sum_{i \in J \cup \{b\}} x_i \geq r_b, \quad x_a + x_b \geq 1,$$

где $a < j < b$ $(\forall j \in J)$. Складывая такие тройки клозов, будем получать

$$\sum_{i \in J \cup \{a,b\}} x_i \geq \lceil (r_a + r_b + 1)/2 \rceil.$$

3. Использование теоремы 4 позволит получать более сильные неравенства для циклов нечетной длины в графе 2-клозов.

4. Опираясь на теорему 3, можно распознавать некоторые классы хороших случаев и, таким образом, получать более сильные неравенства с единичными коэффициентами.

5. Применение теоремы 5 или её обобщений, теорем 6 и 7, позволяет получать более общие неравенства. Вероятно это можно как-то использовать для поиска доказательства с нетривиальными коэффициентами.

Не очень понятно, как использовать улучшение 5 на практике, т. к. время его работы может оказаться экспоненциальным. Поэтому эффективный поиск доказательств, в которых участвуют неравенства с нетривиальными коэффициентами, является открытым вопросом. Улучшение 3 применимо только для 2-клозов. Можно воспользоваться вариантом 2, что позволит алгоритму находить короткое доказательство для PHP. Мы же воспользуемся вариантом 4.

Надо отметить, что в общем случае время поиска множества клозов, удовлетворяющего теореме 4, экспоненциально. Поэтому мы искусственно ограничим размер искомого множества. Будем искать наборы из k неравенств, которые в сумме дают неравенство с коэффициентом $k-1$ при всех переменных и свободным членом, не делящимся на k:

$$\sum_{i\in J_1} x_i \geq r_1, \quad \sum_{i\in J_2} x_i \geq r_2, \quad \dots \quad \sum_{i\in J_k} x_i \geq r_k,$$

причем

$$\sum_{i\in J_1} x_i + \sum_{i\in J_2} x_i + \dots + \sum_{i\in J_k} x_i = (k-1)\sum_{i\in J} x_i,$$

где $r_1 + r_2 + \dots + r_k \bmod k \neq 0$, а $J = \bigcup_{i=1}^{k} J_i$. Складывая такие неравенства, получим

$$\sum_{i\in J} x_i \geq \lceil (r_1 + r_2 + \dots + r_k)/k \rceil.$$

Потребуем также, чтобы исходные неравенства не содержали контрарные переменные. Будем называть набор из k таких неравенств *k-срезом*. Заметим также, что неравенство полученное из k-среза, не является булевым клозом, но все его коэффициенты — единицы. Таким образом, в улучшенном алгоритме не будет неравенств с нетривиальными коэффициентами.

Покажем, что добавление в алгоритм поиска 3-срезов, позволяет алгоритму найти короткое доказательство для PHP.

Теорема 10. *Если расширить* Ordered-CP-Saturate*, поиском* 3*-срезов, то полученный алгоритм найдет короткое решение* PHP*.*

Доказательство. Перепишем PHP_m^n в виде неравенств, где переменная x_{ij} означает, что i-й кролик сидит в j-й клетке.

$$\sum_{j=1}^{n} x_{ij} \geq 1, \qquad \forall i : 1 \leq i \leq m, \tag{3.3}$$

$$-x_{ij} - x_{kj} \geq -1, \qquad \forall i, k, m : 1 \leq i < k \leq m,\ 1 \leq j \leq n. \tag{3.4}$$

По теореме 4 из неравенств (3.4) выводятся n неравенств

$$-\sum_{i=1}^{m} x_{ij} \geq -1. \tag{3.5}$$

В доказательстве этой теоремы используется поиск троек неравенств, удовлетворяющих определению 3-среза. Поэтому эти неравенства будут найдены алгоритмом.

После этого не более, чем через $m+n$ насыщений уровня, будет получена сумма всех неравенств (3.3) и (3.5) (каждая переменная входит в эту сумму дважды: положительно и отрицательно, а значит будет получена резольвента). Эта сумма приводит к противоречию: $0 \geq m - n > 0$, т. к. $m > n$. □

Приведем описание алгоритма, основанного на Ordered-CP-Saturate и дополненного поиском 3-срезов.

Алгоритм Ordered-CP-3-Cut

1: ввести порядок на множестве переменных
2: для каждого 3-среза вывести “сильное” неравенство
3: **while** не получено неравенство $0 \geq 1$ **do**
4: выбрать пару клозов c_i и c_j с одинаковой старшей переменной
5: **if** у c_i и c_j разные коэффициенты при старшей переменной **then**
6: промоделировать резолюцию и получить клоз c'
7: **if** в клозе c' есть двойки **then**
8: избавиться от них в соответствии с теоремой 9

end if
if c' — единичный клоз **then**
подставить соответствующее значение во все клозы
else if клоз c' не тавтология и не слабее какого-то другого клоза **then**
добавить клоз c' в систему
end if
else if у c_i и c_j одинаковые коэффициенты при старшей переменной **then**
if существует клоз c_k: (c_i, c_j, c_k) — 3-срез **then**
получить клоз c' из (c_i, c_j, c_k)
if клоз c' не тавтология и не слабее какого-то другого клоза **then**
добавить клоз c' в систему
end if
end if
end if
end while

Для поиска пар неравенств (c_i, c_j) как и раньше будем также применять стратегию насыщения уровня. При этом применим следующую эвристику: все неравенства, которые участвовали в некотором k-срезе, будем отмечать как "устаревшие". Если в паре (c_i, c_j) оба неравенства "устаревшие", то такую пару мы пропускаем (и откладываем на потом, чтобы сохранить полноту алгоритма). Такая эвристика позволяет резко снизить количество выводимых клозов.

3.3. Обобщенный принцип Дирихле

Рассмотрим обобщенный принцип Дирихле.

> *Если в n клетках сидит m кролик и $m > kn$, то есть хотя бы одна клетка в которой сидит $k+1$ кролик.*

Будем обозначать такую тавтологию $k\mathrm{PHP}_m^n$.

Запишем КНФ формулу для $\neg k\mathrm{PHP}_m^n$. Для этого введем mn булевых переменных x_{ij}, $i \le m$, $j \le n$, имеющих смысл "i-й кролик сидит в j-й клетке". Для каждого кролика i запишем условие "кролик i сидит хотя бы в одной клетке" (как и для обычного PHP):

$$x_{i1} \vee x_{i2} \vee \ldots \vee x_{in}.$$

Для каждой клетки k запишем условие "никакие $k+1$ кролик не сидят в клетке j вместе":

$$\bigvee_{i \in J} \neg x_{ij}, \quad \forall J \subset \mathcal{I}_n : |J| = k+1.$$

Количество клозов в полученной формуле $m + n\binom{m}{k+1}$. Преобразуем КНФ в неравенства.

$$x_{i1} + x_{i2} + \cdots + x_{in} \geq 1, \tag{3.6}$$

$$-\sum_{i \in J} x_{ij} \geq -k, \quad \forall J \subset \mathcal{I}_n : |J| = k+1. \tag{3.7}$$

Как нужно изменить Ordered-CP-3-Cut, чтобы он находил решение обобщенного принципа Дирихле? Рассмотрим $k\mathrm{PHP}^n_m$.

Теорема 11. *Если расширить* Ordered-CP-Saturate *поиском* $k+1$*-срезов, то полученный алгоритм найдет короткое решение* $k\mathrm{PHP}^n_m$.

Доказательство. Пусть есть система неравенств C над множеством переменных $X = \{x_1, \ldots, x_m\}$ и для любого $Z \subset X$: $|Z| = k$ в C есть неравенство

$$\sum_{x_i \in Z} x_i \geq 1.$$

Докажем, что находя $k+1$-срезы можно вывести неравенство

$$\sum_{i=1}^{m} x_i \geq n - k.$$

Будем получать неравенства рекурсивно. Для получения неравенства

$$\sum_{i \in J} x_i \geq r, \quad |J| = k + r,$$

выберем $L \subset J : |L| = k$. Далее рекурсивно получим k неравенства

$$\sum_{i \in J \setminus \{\ell\}} x_i \geq r - 1, \quad \forall \ell \in L.$$

Складывая их с неравенством $\sum_{i \in L} x_i \geq 1$, получаем

$$k \sum_{i \in J} x_i \geq k(r-1) + 1 \quad \Rightarrow \quad \sum_{i \in J} x_i \geq \lceil (k(r-1)+1)/k \rceil = r.$$

□

Замечание. В доказательстве теоремы 11 было получено альтернативное доказательство достаточного условия для теоремы 3.

Заключение

Результаты исследования

1. Приведен обзор существующих систем доказательств.
2. Проведен анализ системы доказательств Секущие Плоскости.
   (a) Полный анализ получения неравенств с единичными коэффициентами. Выведены условия получения произвольного неравенства с единичными коэффициентами.
   (b) Отдельный случай — получение неравенств из 2-клозов.
   (c) Общий анализ для неравенств с произвольными коэффициентами.
   (d) Анализ для неравенств с одним нетривиальным коэффициентом, полученных из 2-клозов.
3. На основе [11] предложен алгоритм для поиска доказательств в системе Секущие Плоскости.

Предложенный в главе 3 алгоритм (Ordered-CP-3-Cut + поиск 4-срезов) был реализован. Для сравнения был также реализован алгоритм алгоритм для упорядоченной резолюции с насыщением уровня. В таблицах 1 и 2 приведено сравнение предложенного алгоритма и алгоритма упорядоченной резолюции. Алгоритмы сравниваются по количеству клозов, которые были порождены в процессе поиска доказательства. В качестве значения берётся среднее для нескольких запусков алгоритма с разным (случайным) порядком, заданным на переменных. Приведенное сравнение показывает, что на некоторых классах задач приведённый алгоритм работает эффективнее алгоритма упорядоченной резолюции.

Тавтология	**Размер системы**	**Упорядоченная резолюция с насыщением уровня**	**Предложенный алгоритм**
PHP_4^3	22	73	48
PHP_5^4	45	308	108
PHP_6^5	81	3 110	223
PHP_7^6	133	—	395
PHP_8^7	204	—	710
PHP_9^8	297	—	1 082
PHP_{10}^9	415	—	1 752
PHP_8^3	92	910	305
PHP_6^4	66	1 010	183
PHP_7^4	91	2 805	279
PHP_8^4	120	5 950	401

Таблица 1. Сравнение количества клозов, полученных в процессе поиска доказательства, для упорядоченной резолюции с насыщением уровня и преложенного алгоритма на примере тавтологий вида PHP_m^n.

Тавтология	**Размер системы**	**Упорядоченная резолюция с насыщением уровня**	**Предложенный алгоритм**
$2\mathrm{PHP}_5^2$	25	86	71
$2\mathrm{PHP}_6^2$	46	263	158
$2\mathrm{PHP}_7^2$	77	484	272
$2\mathrm{PHP}_7^3$	112	2 205	540
$2\mathrm{PHP}_8^3$	176	—	1201

Таблица 2. Сравнение количества клозов, полученных в процессе поиска доказательства, для упорядоченной резолюции с насыщением уровня и преложенного алгоритма на примере тавтологий вида $2\mathrm{PHP}_m^n$.

Список литературы

1. *Bachmair Leo, Ganzinger Harald.* A Theory of Resolution: Tech. Rep. MPI–I–97–2–005: 1997.

2. *Bachmair Leo, Ganzinger Harald.* Resolution Theorem Proving // Handbook of Automated Reasoning. — 2001. — Pp. 19–99.

3. *Beame Paul, Pitassi Toniann.* Simplified and Improved Resolution Lower Bounds // IEEE Symposium on Foundations of Computer Science. — 1996. — Pp. 274–282.

4. *Ben-Sasson Eli, Wigderson Avi.* Short proofs are narrow — resolution made simple // *J. ACM.* — 2001. — Vol. 48, no. 2. — Pp. 149–169.

5. *Bonet Maria Luisa, Galesi Nicola.* A Study of Proof Search Algorithms for Resolution and Polynomial Calculus // Proc. of the 40th Annual IEEE Symposium on Foundations of Computer Science (FOCS'99). — New York, NY, USA: IEEE Press, 1999. — Pp. 422–432.

6. *Clegg Matthew, Edmonds Jeffery, Impagliazzo Russell.* Using the Groebner basis algorithm to find proofs of unsatisfiability. — 1996. — Pp. 174–183.

7. *Cook Stephen A.* The complexity of theorem-proving procedures // STOC '71: Proceedings of the third annual ACM symposium on Theory of computing. — New York, NY, USA: ACM, 1971. — Pp. 151–158.

8. *Cook Stephen A., Reckhow Robert A.* The Relative Efficiency of Propositional Proof Systems // *J. Symb. Log.* — 1979. — Vol. 44, no. 1. — Pp. 36–50.

9. *Cook W., Coullard C. R., Turán G.* On the complexity of cutting-plane proofs // *Discrete Appl. Math.* — 1987. — Vol. 18, no. 1. — Pp. 25–38.

10. Exponential Separations between Restricted Resolution and Cutting Planes Proof Systems / Maria Luisa Bonet, Juan Luis Esteban, Nicola Galesi, Jan Johannsen // IEEE Symposium on Foundations of Computer Science. — 1998. — Pp. 638–647.

11. First report on the semialgebraic prover / S. S. Fedin, A. Kojevnikov, B. Konev et al. — Steklov Institute of Mathematics at St.Petersburg Preprint.

12. *Gomory Ralph E.* An algorithm for integer solutions to linear programs // Recent Advances in Mathematical Programming. — New-York: McGraw-Hill, 1963. — Pp. 269–302.

13. *Grigoriev Dima, Hirsch Edward A., Pasechnik Dmitrii V.* Complexity of Semialgebraic Proofs // Symposium on Theoretical Aspects of Computer Science. — 2002. — Pp. 419–430.

14. *Beame P., Impagliazzo R., Krajíček J. et al.* Lower bounds on Hilbert's Nullstellensatz and propositional proofs. — 1996.

15. *Pitassi Toniann.* Unsolvable Systems of Equations and Proof Complexity // ICM: Proceedings of the International Congress of Mathematicians. — 1998.

16. *Pudlák Pavel.* Lower Bounds for Resolution and Cutting Plane Proofs and Monotone Computations // *The Journal of Symbolic Logic.* — 1997. — Vol. 62, no. 3. — Pp. 981–998.

17. *Pudlák Pavel.* On the complexity of propositional calculus // Sets and Proofs, Invited papers from Logic Colloquium'97. — Cambridge Univ. Press, 1999. — Pp. 197–218.

18. *Raz Ran.* Resolution Lower Bounds for the Weak Pigeonhole Principle // *Electronic Colloquium on Computational Complexity (ECCC).* — 2001. — Vol. 8, no. 21.

19. *Razborov Alexander A.* Improved Resolution Lower Bounds for the Weak Pigeonhole Principle // *Electronic Colloquium on Computational Complexity (ECCC).* — 2001. — Vol. 8, no. 55.

20. *Чень Ч., Ли Р.* Математическая логика и автоматическое доказательство теорем / Под ред. С. Ю. Маслова. — М.: Наука. Главная редакция физико-математической литературы, 1983. — 360 с.