Аннотация

Комбинаторная задача CSP позволяет выразить в единых терминах широкий спектр задач из различных областей математики, информатики и искусственного интеллекта. Общая задача CSP является NP-полной, однако, многие ограниченные версии этой задачи могут быть решены за полиномиальное время. Известно, что вычислительная сложность ограниченных задач CSP зависит лишь от множества полиморфизмов отношений, которые разрешено использовать в задаче. В статье показано, что если множество разрешенных отношений инвариантно относительно некоторой мальцевской операции, то соответствующая задача CSP может быть решена за полиномиальное время.

УДК 512.579

Полиномиальность мальцевских задач CSP

А. А. Булатов

1 Введение

Задача CSP[1)] является универсальным формализмом для широкого спектра задач из различных областей информатики, дискретной математики и искусственного интеллекта. Эта задача может быть определена несколькими способами. Наиболее краткой формой является следующая: дана конечная модель $\mathbb{A}$ и (не обязательно конечная) модель $\mathbb{B}$; определить, существует ли гомоморфизм из $\mathbb{A}$ в $\mathbb{B}$.

Общая задача CSP является NP-полной [13]. Однако, ограничивая класс моделей, которые участвуют в задаче, можно получить задачу, решаемую за полиномиальное время. Таким образом, поиск полиномиальных подзадач задачи CSP является важным направлением исследований. Продвижения в этом направлении позволяют совершенствовать эвристические алгоритмы, решающие задачу CSP. С теоретической точки зрения эти исследования помогают уточнить границу между полиномиальностью и NP-полнотой в широком круге комбинаторных задач.

Один из наиболее естественных способов ограничить задачу CSP — ограничить класс допустимых моделей-образов. Первый результат в этом направлении был получен Шефером [14] в случае булевой CSP, т.е. когда модель-образ двухэлементна. Шефер доказал, что существует шесть классов двухэлементных моделей таких, что булева задача CSP применительно к одному из этих классов является разрешимой за полиномиальное время и является NP-полной в остальных случаях. Этот результат известен как теорема Шефера о дихотомии. Позже Федер и Варди [8] нашли два больших класса конечных моделей (содержащих все шеферовские классы), для

1) От английского “Constraint Satisfaction Problem”; в немногочисленных русскоязычных работах по этой проблематике встречается также термин “Обобщенная выполнимость”.

которых задача CSP полиномиально разрешима. Первый из них состоит из задач ограниченной ширины, определяемой с помощью программ на языке Даталог. Каждая задача этого типа может быть решена с помощью несложного алгоритма, определяющего локальную совместность задачи. Второй класс был определен с помощью свойства моделей, которое Федер и Варди назвали способностью к подсчету.

Джевонс и его соавторы [12, 11, 6, 2] предложили для изучения задачи CSP использовать полиморфизмы отношений, входящих в модель. В указанных работах было найдено несколько типов операций таких, что если одна из операций этих типов сохраняет отношения модели, то соответствующая задача CSP полиномиально разрешима. Было также показано [7, 8], что модели, имеющие полиморфизм вида $xy^{-1}z$ для операций некоторой конечной группы, обладают способностью к подсчету, а потому соответствующие задачи могут быть решены за полиномиальное время. Любопытно, что указанные задачи составляют единственный известный случай, когда задача CSP может быть решена за полиномиальное время, но не имеет ограниченной ширины. Данный подход позволяет дать еще одно, чисто алгебраическое определение задачи CSP, как задачи о существовании непустой подалгебры прямого произведения семейства алгебр, некоторые (заданные) проекции которой являются подмножествами заданных подпрямых произведений соответствующих сомножителей.

В настоящей статье мы обобщаем результаты из [7, 8] на значительно более широкий класс операций — мальцевских операций. Напомним, что *мальцевской* называется тернарная операция d, удовлетворяющая тождествам $d(x, y, y) = d(y, y, x) = x$. Примером мальцевской операции служит операция $xy^{-1}z$ в группе. Основной результат данной статьи состоит в доказательстве того, что любая задача CSP, сооответствующая классу моделей, все отношения которых инвариантны относительно некоторой (фиксированной) мальцевской операции, может быть решена за полиномиальное время. Более того, мы представим алгоритм, который для каждой задачи этого типа за полиномиальное время находит базис множества решений такой, что каждое решение задачи может быть выражено через элементы базиса.

Статья организована следующим образом. Раздел 2 содержит определения, касающиеся задачи CSP и ее подзадач, ограниченных с помощью полиморфизмов моделей, а также формулировки основных результатов статьи. В разделе 3 мы формулируем и доказываем несколько свойств алгебр с мальцевской операцией, используемых при построении алгоритмов. В разделе 4 мы приводим алгоритм, решающий задачи CSP для моделей, обладающих мальцевским полиморфизмом, и определяем особый вид базиса множества решений такой задачи. Наконец, доказательство корректности, детальное описание процедур алгоритма и оценка его сложности содержатся в разделе 5.

2 Основные определения

2.1 Задача CSP

Пусть $\mathcal{A} = \{A_i \mid i \in I\}$ — семейство множеств. Подмножество ϱ множества $A_{i_1} \times \ldots \times A_{i_k}$ вместе с кортежем $(i_1, \ldots, i_k)$ называется k-местным *отношением* над $\mathcal{A}$ с *сигнатурой* $(i_1, \ldots, i_k)$. Множество $\{1, \ldots, n\}$ мы будем обозначать через $\underline{n}$, а компоненты k-местного кортежа $\mathbf{a}$ — через $\mathbf{a}[1], \ldots, \mathbf{a}[k]$.

Мы будем использовать более общую формулировку задачи CSP по сравнению со стандартной (см., напр., [11, 12]), введенную в [4].

Определение 2.1. Пусть Γ — множество отношений над семейством $\mathcal{A} = \{A_i \colon i \in I\}$. Задача CSP($\Gamma$) — это комбинаторная задача распознавания, условием которой является четверка $(V; \mathcal{A}; \sigma; \mathcal{C})$, где V — множество *переменных*, $\mathcal{A}$ — семейство *множеств значений* для переменных из V, $\sigma \colon V \to I$ — *сортовая функция*, $\mathcal{C}$ — множество *ограничений* $\{C_1, \ldots, C_q\}$. Каждое ограничение $C_i \in \mathcal{C}$ — это пара $\langle \mathbf{s}_i, \varrho_i \rangle$, где $\mathbf{s}_i = (v_1, \ldots, v_{m_i})$ — кортеж переменных длины m_i, называемый *областью ограничения*, а $\varrho_i \in \Gamma$ — m_i-местное отношение $\varrho_i \subseteq A_{\sigma(v_1)} \times \ldots \times A_{\sigma(v_{m_i})}$ на $\mathcal{A}$, называемое *отношением ограничения*. В задаче CSP спрашивается, существует ли *решение*, т.е. отображение f из V в $\bigcup_{i \in I} A_i$ такое, что для каждой переменной

$v \in V$ выполняется $f(v) \in A_{\sigma(v)}$ и для каждого ограничения $\langle \mathbf{s}_i, \varrho_i \rangle \in \mathcal{C}$, $\mathbf{s}_i = (v_1, \ldots, v_{m_i})$, кортеж $(f(v_1), \ldots, f(v_{m_i}))$ принадлежит ϱ_i.

Часто множества значений всех переменных совпадают. Чтобы отличать этот важный частный случай, мы называем задачу CSP в общем случае *многосортной*, а задачу с единственным множеством значений — *односортной*. Условие односортной задачи может быть представлено в виде тройки $(V, A, \mathcal{C})$, где A — общее множество значений.

В данной статье все множества значений предполагаются конечными. *Размером* задачи считается длина представления всех кортежей из всех отношений ограничения. Множество Γ называется *полиномиальным*, если для каждого конечного подмножества $\Gamma' \subseteq \Gamma$ существует полиномиальный алгоритм, решающий задачу CSP(Γ'); множество Γ называется *NP-полным*, если CSP(Γ') NP-полна для некоторого конечного $\Gamma' \subseteq \Gamma$. Если существует единый полиномиальный алгоритм, решающий задачу CSP(Γ), то Γ называется *глобально полиномиальным*.

Пример 2.1. Система линейных уравнений над конечным полем F может быть представлена как задача CSP вида $(V, F, \mathcal{C})$, где V — множество переменных системы и каждое ограничение $\langle \mathbf{s}, \varrho \rangle$ из $\mathcal{C}$ соответствует одному уравнению. Тогда $\mathbf{s}$ — множество переменных, участвующих в уравнении, а ϱ — множество решений уравнения, т.е. гиперплоскость. Задача о решении систем линейных уравнений эквивалентна задаче CSP($\mathcal{F}$), где $\mathcal{F}$ — это модель, универсом которой является F, а отношениями — всевозможные гиперплоскости конечномерных векторных пространств над F.

Дальнейшие примеры задач CSP, включая существенно многосортные задачи, можно найти в [2, 3, 6, 11, 12].

2.2 Преобразования задач CSP

Для кортежа $\mathbf{a} = (\mathbf{a}[1], \ldots, \mathbf{a}[n])$ и множества $I = \{i_1, \ldots, i_k\} \subseteq \underline{n}$ мы обозначаем через $\mathbf{a}|_I$ *проекцию* $(\mathbf{a}[i_1], \ldots, \mathbf{a}[i_k])$ кортежа $\mathbf{a}$ на I. Далее, для n-местного отношения ϱ через $\varrho|_I$ обозначается отношение $\{\mathbf{a}|_I : \mathbf{a} \in \varrho\}$. Часто мы будем индексировать компоненты кортежей не натуральными числами, как обычно, а элементами другого множества, например, переменными из условия задачи CSP (индексное множество при этом предполагается упорядоченным некоторым фиксированным образом). В этом случае мы используем обозначение $(\mathbf{a}[i])_{i\in I}$, где I — индексное множество.

Возьмем задачу CSP $\mathcal{P} = (V; \mathcal{A} = \{A_i \mid i \in I\}; \sigma; \mathcal{C})$, где $\mathcal{C} = \{C_1, \ldots, C_q\}$ и $C_i = \langle \mathbf{s}_i, \varrho_i \rangle$, а также множество $V' \subseteq V$. *Частичным решением* $\mathcal{P}$ на V' называется отображение $\varphi\colon V' \to \bigcup_{v\in V'} A_{\sigma(v)}$ такое, что для любого $i \le q$ выполнено $\varphi(\mathbf{s}_i \cap V') \in \varrho_i\big|_{\mathbf{s}_i\cap V'}$. Заметим, что частичные решения можно рассматривать как решения *усеченной задачи* $\mathcal{P}_{V'} = (V'; \mathcal{A}; \sigma\big|_{V'}; \mathcal{C}_{V'})$, где $\sigma\big|_{V'}$ — ограничение σ на V', и $\mathcal{C}_{V'} = \{C'_1, \ldots, C'_q\}$, $C'_i = \langle \mathbf{s}_i \cap V', \varrho_i\big|_{\mathbf{s}_i\cap V'} \rangle$. Множество всех частичных решений на V' обозначается через $\mathcal{S}_{V'}$.

Задача $\mathcal{P}$ называется *k-согласованной*, если для любого не более чем k-элементного множества $V' \subseteq V$ равенство $\varrho_l\big|_{V'\cap\mathbf{s}_l} = \mathcal{S}_{V'}\big|_{V'\cap\mathbf{s}_l}$ справедливо для каждого $l \in \underline{q}$ и найдется $t \in \underline{q}$ такое, что $V' \subseteq \mathbf{s}_t$. Каждая задача $\mathcal{P}$ может быть преобразована к эквивалентной (т.е. имеющей то же множество решений) k-согласованной задаче $\mathcal{P}'$. Для этого мы добавляем все ограничения вида $\langle V', \mathcal{S}_{V'} \rangle$ для k-элементных подмножеств $V' \subseteq V$, а затем повторяем следующую процедуру до тех пор, пока она изменяет задачу: для каждого k-элементного множества $V' \subseteq V$ вычислить отношение $\mathcal{S}_{V'}$ и удалить из всех отношений ограничения те кортежи, соответствующие проекции которых не содержатся в $\mathcal{S}_{V'}$. Нетрудно видеть, что $\mathcal{P}'$ является k-согласованной и что указанная процедура может выполнена за полиномиальное время. Легко также видеть, что обе задачи имеют одно и то же множество решений. Мы будем называть полученную задачу *ассоциированной* с $\mathcal{P}$. В результате описанного преобразования множество значений, которые может принимать переменная $v \in V$ может измениться и стать отличным от $A_{\sigma(v)}$. Если $\mathcal{S}_{\{v\}} \in \mathcal{A}$, то мы можем переопределить $\sigma(v)$ так, чтобы $A_{\sigma(v)} = \mathcal{S}_{\{v\}}$. Поскольку во всех случаях, которые встретятся в дальнейшем, $\mathcal{S}_{\{v\}} \in \mathcal{A}$ справедливо для всех $v \in V$, сортовая функция в задаче $\mathcal{P}'$ будет предполагаться переопределенной указанным образом.

Еще одно преобразование часто позволяет сократить количество переменных в задаче. Пусть $\mathcal{P}$ — 3-согласованная задача CSP. Для каждого отношения ограничения ϱ_i определим ориентированный граф $G(\varrho_i)$ следующим образом: вершинами графа являются компоненты кортежа $\mathbf{s}_i$, и вершины v, w соединены дугой тогда и только тогда, когда существует отображение $\pi\colon A_{\sigma(v)} \to A_{\sigma(w)}$ такое, что $\varrho\big|_{\{v,w\}}$ является подмножеством *графика* π, т.е. отношения $\{(a, \pi(a))\colon a \in A_{\sigma(v)}\}$. Через $G(\mathcal{P})$ мы обозначаем транзитивное замыкание объединения $G(\varrho_1)\cup\ldots\cup G(\varrho_q)$. Как нетрудно понять, 3-согласованность влечет, что для любой дуги (u, v) этого графа и любых ограничений $\langle \mathbf{s}, \varrho\rangle$, $\langle \mathbf{s}', \varrho'\rangle$ таких, что $u, v \in \mathbf{s}\cap\mathbf{s}'$, если $\varrho\big|_{\{u,v\}}$ — график отображения $\pi\colon A_{\sigma(u)} \to A_{\sigma(u)}$, то $\varrho'\big|_{\{u,v\}}$ — график того же отображения. Кроме того, для любых дуг $(u, v), (v, w)$ графа $G(\mathcal{P})$, если $\mathcal{S}_{\{u,v\}}$ и $\mathcal{S}_{\{v,w\}}$ являются графиками отображений $\pi_1\colon A_{\sigma(u)} \to A_{\sigma(v)}$ и $\pi_2\colon A_{\sigma(v)} \to A_{\sigma(w)}$ соответственно, то $\mathcal{S}_{\{u,w\}}$ является графиком $\pi\colon A_{\sigma(u)} \to A_{\sigma(w)}$, где $\pi = \pi_1 \circ \pi_2$.

Значения переменных из одной и той же сильно связной компоненты графа связаны взаимно однозначными соответствиями. Формально это свойство может быть записано следующим образом. Выберем представителя из каждой сильно связной компоненты и обозначим множество выбранных представителей через V'. Для каждой $v \in V$ найдется $v' \in V'$ и взаимно-однозначное отображение $\pi_v\colon A_{\sigma(v')} \to A_{\sigma(v)}$ такие, что $\mathcal{S}_{\{v',v\}}$ — график π_v. Тогда $\mathcal{P}$ может быть преобразована в задачу $\mathcal{P}' = (V'; \mathcal{A}; \sigma'; \mathcal{C}')$, где $\sigma' = \sigma\big|_{V'}$ и в каждом ограничении $C_i = \langle \mathbf{s}_i, \varrho_i\rangle \in \mathcal{C}$ каждая переменная $v \in \mathbf{s}_i = (v_1, \ldots, v_m)$ заменяется на v', а отношение ϱ_i — на отношение $\{(\pi_{v_1}^{-1}(\mathbf{a}[v_1]), \ldots, \pi_{v_m}^{-1}(\mathbf{a}[v_m]))\colon \mathbf{a} \in \varrho_i\}$. Затем мы удаляем повторяющиеся элементы из области ограничения и соответствующие им компоненты отношения ограничения. Очевидно, что каждое решение $\mathcal{P}$ является продолжением некоторого решения $\mathcal{P}'$ и, обратно, каждое решение $\mathcal{P}'$ является ограничением решения $\mathcal{P}$. Каждая сильно связная компонента графа $G(\mathcal{P}')$ одноэлементна. Такую задачу мы будем называть *приведенной*. Тогда $\mathcal{P}'$ — приведенная задача, *ассоциированная* с $\mathcal{P}$. Отметим еще, что если каждая сильно связная компонента графа $G(\varrho)$ для отношения ϱ одноэлементна, то ϱ мы также будем называть приведенным.

2.3 Алгебраические свойства задачи CSP

Алгебраический подход к изучению сложности задач CSP(Γ) в случае односортных отношений был предложен в [5, 11, 12]. Приведем необходимые определения и результаты.

Говорят, что m-местное отношение ϱ *инвариантно* относительно n-местной операции f [говорят также, что f *сохраняет* ϱ], если для любых $\mathbf{a}^1, \ldots, \mathbf{a}^n \in \varrho$, выполнено $(f(\mathbf{a}^1[1], \mathbf{a}^2[1], \ldots, \mathbf{a}^n[1]), \ldots, f(\mathbf{a}^1[m], \mathbf{a}^2[m], \ldots, \mathbf{a}^n[m]) \in \varrho$. Для множества отношений Γ через $\mathsf{Pol}\ \Gamma$ обозначается множество всех операций, сохраняющих все отношения из Γ. Аналогично, если C — множество операций, то $\mathsf{Inv}\ C$ обозначает множество всех отношений, инвариантных относительно всех операций из C.

Теорема 2.1 ([11]). *Пусть* Γ — *множество отношений над конечным множеством и* $\Gamma' \subseteq \mathsf{Inv\ Pol}\ \Gamma$ *конечно. Тогда задача* CSP(Γ') *сводится к* CSP(Γ) *за полиномиальное время.*

Следствие 2.1. *Множество отношений* Γ *полиномиально тогда и только тогда, когда* $\mathsf{InvPol}\ \Gamma$ *полиномиально.*

Каждому множеству отношений Γ над множеством A и, соответственно, задаче CSP(Γ) можно сопоставить алгебру $(A; \mathsf{Pol}\ \Gamma)$; обратно, каждой конечной алгебре $\mathbb{A} = (A; F)$ соответствует задача CSP($\mathsf{Inv}\ F$). По теореме 2.1 если Γ_1, Γ_2 соответствуют термально эквивалентным алгебрам, то они полиномиальны [NP-полны] одновременно. Алгебра $\mathbb{A}$ называется *(глобально) полиномиальной* [*NP-полной*] если $\mathsf{Inv}\ F$ (глобально) полиномиально [NP-полно].

В случае многосортных отношений аналогичные определения вводятся следующим образом. Пусть $\mathcal{A}$ — класс однотипных алгебр и t — (n-местный) терм класса $\mathcal{A}$. Терм t сохраняет (m-местное) многосортное отношение ϱ над классом носителей алгебр из $\mathcal{A}$ с сигнатурой $(i_1, \ldots, i_m)$ если для любых $\mathbf{a}^1, \ldots, \mathbf{a}^n \in \varrho$ справедливо $t((\mathbf{a}^1[1], \ldots, \mathbf{a}^1[m]), \ldots, (\mathbf{a}^n[1], \ldots, \mathbf{a}^n[m])) = (t^{\mathbb{A}_{i_1}}(\mathbf{a}^1[1], \ldots, \mathbf{a}^n[1]), \ldots, t^{\mathbb{A}_{i_m}}(\mathbf{a}^1[m], \ldots, \mathbf{a}^n[m])) \in \varrho$.

Для класса $\mathcal{A}$ однотипных алгебр $\mathsf{Inv}\ \mathcal{A}$ обозначает класс всех многосортных отношений над классом носителей алгебр из $\mathcal{A}$, инвариантных относительно термов класса $\mathcal{A}$. Иными словами, $\mathsf{Inv}\ \mathcal{A}$ является классом носителей подалгебр прямых произведений алгебр из $\mathcal{A}$. Нам будет удобно рассматривать элементы $\mathsf{Inv}\ \mathcal{A}$ и как отношения, игнорируя их алгебраическую структуру, и как алгебры однотипные с алгебрами из $\mathcal{A}$. Классу $\mathcal{A}$ мы также ставим в соответствие многосортную задачу CSP, полагая $\mathrm{CSP}(\mathcal{A}) = \mathrm{CSP}(\mathsf{Inv}\ \mathcal{A})$. Класс $\mathcal{A}$ называется (*глобально*) *полиномиальным*, если множество $\mathsf{Inv}\ \mathcal{A}$ (глобально) полиномиально. Класс $\mathcal{A}$ называется *NP-полным*, если $\mathsf{Inv}\ \mathcal{A}$ NP-полное.

Отметим, что алгебраические свойства задачи CSP позволяют сформулировать ее следующим образом. Даны алгебры $\mathbb{A}_1, \ldots, \mathbb{A}_n$, подмножества $I_1, \ldots, I_m \subseteq \{1, \ldots, n\}$ и подалгебры $\mathbb{C}_1, \ldots, \mathbb{C}_m$ такие, что $\mathbb{C}_j$ является подалгеброй прямого произведения $\prod_{i \in I_j} \mathbb{A}_i$; определить, существует ли алгебра $\mathbb{B}$ произведения $\prod_{i=1}^n \mathbb{A}_i$, для которой проекция на каждое из множеств I_j есть подмножество из $\mathbb{C}_j$.

Мы можем теперь сформулировать главный результат данной статьи.

Теорема 2.2. *Конечный класс конечных однотипных алгебр с мальцевской термальной операцией глобально полиномиален.*

Кроме того, алгоритм, решающий задачу CSP, соответствующую конечному классу конечных однотипных алгебр $\mathcal{A}$ с указанным свойством, позволяет найти базис множества решений задач этого вида. Мы называем множество решений B *базисом*, если его мощность полиномиальна относительно размера задачи и каждое решение может быть представлено в виде $\mathbf{d}(\mathbf{d}(\ldots \mathbf{d}(\mathbf{d}(\ldots \mathbf{d}(\mathbf{a}_k, \mathbf{a}_{k-1}, \mathbf{b}_{k-1}), \ldots), \mathbf{a}_l, \mathbf{b}_l), \ldots), \mathbf{a}_1, \mathbf{b}_1)$, в котором $\mathbf{d}$ обозначает мальцевский терм класса $\mathcal{A}$, $\mathbf{a}_1, \ldots, \mathbf{a}_k, \mathbf{b}_1, \ldots, \mathbf{b}_{k-1} \in B$, и $k \leq l \cdot n$, где l — максимальная длина цепи в решетках конгруэнций алгебр из $\mathcal{A}$, а n — количество переменных в задаче.

Существование такого базиса для любой подалгебры прямого произведения алгебр с мальцевской операцией тривиально. Основным результатом, таким образом, является возможность найти базис за полиномиальное время, если алгебра представлена в виде пересечения алгебр, базисы которых известны (как легко понять, алгебраическая формулировка задачи

CSP является частным случаем этой подстановки). Нетрудно видеть, что теорема 2.2 может быть сформулирована следующим образом.

Теорема 2.3. *Пусть базисы подалгебр $\mathbb{C}_1, \ldots, \mathbb{C}_m$ прямого произведения $\mathbb{A}_1 \times \ldots \mathbb{A}_n$ известны. Тогда базис алгебры $\bigcup_{i=1}^m \mathbb{C}_i$ может быть найден за полиномиальное время.*

3 Свойства алгебр с мальцевской операцией

В этом разделе мы сформулируем и докажем несколько свойств мальцевских алгебр, которые будут постоянно использоваться в статье. Для кортежей $\mathbf{a} = (\mathbf{a}[1], \ldots, \mathbf{a}[n])$ и $\mathbf{b} = (\mathbf{b}[1], \ldots, \mathbf{b}[m])$, через $(\mathbf{a}, \mathbf{b})$ обозначается кортеж $(\mathbf{a}[1], \ldots, \mathbf{a}[n], \mathbf{b}[1], \ldots, \mathbf{b}[m])$, а через $\langle \mathbf{a}, \mathbf{b} \rangle$ — пара кортежей. Следующее предложение содержит три простых наблюдения.

Предложение 3.1. *Пусть $\mathbb{D}$ — подпрямое произведение алгебр $\mathbb{D}_1, \ldots, \mathbb{D}_n$ с мальцевской операцией и пусть $I \subseteq \underline{n}$.*
1. *$\mathbb{D}$ прямоугольно, т.е. если $\mathbf{a}, \mathbf{b} \in \mathbb{D}\big|_I, \mathbf{c}, \mathbf{d} \in \mathbb{D}\big|_{\underline{n}-I}$ и $(\mathbf{a}, \mathbf{c}), (\mathbf{a}, \mathbf{d}), (\mathbf{b}, \mathbf{c}) \in \mathbb{D}$, то $(\mathbf{b}, \mathbf{d}) \in \mathbb{D}$.*
2. *Отношение $\theta_I = \{\langle \mathbf{a}, \mathbf{b} \rangle \in (\mathbb{D}\big|_I)^2 \mid$ существует $\mathbf{c} \in \mathbb{D}\big|_{\underline{n}-I}$ такой, что $(\mathbf{a}, \mathbf{c}), (\mathbf{b}, \mathbf{c}) \in \mathbb{D}\}$ является конгруэнцией алгебры $\mathbb{D}_I$.*
3. *$\mathbb{D}$ является дизъюнктным объединением множеств вида $B \times C$, где B — это θ_I-класс, а C — это $\theta_{\underline{n}-I}$-класс.*

Поскольку чем меньше основных операций содержит алгебра, тем сложнее соответствующая ей задача CSP, для доказательства того, что рассматриваемый класс алгебр полиномиален, достаточно изучить случай, когда он имеет лишь одну основную операцию — мальцевскую.

Напомним, что пара конгруэнций (α, β) алгебры $\mathbb{A}$ образует *простой интервал*, если β покрывает α в решетке конгруэнций алгебры $\mathbb{A}$. Теория ручных конгруэнций (см. [10]) позволяет присвоить каждому простому интервалу один из типов $\mathbf{1}, \ldots, \mathbf{5}$. Типы простых интервалов оказывают сильное влияние на сложность задачи CSP, соответствующей алгебре. Например, в [3] показано, что если в решетке конгруэнций алгебры найдется интервал типа $\mathbf{1}$, то алгебра NP-полна.

Нам не потребуется общее определение типов простых интервалов, мы рассмотрим лишь случай алгебр, имеющих мальцевскую операцию. Пусть $\mathbb{A} = (A; \mathbf{d})$ — конечная алгебра указанного вида, $\mathbf{d}$ — ее мальцевская операция и (α, β) —простой интервал. Пусть также $\beta/_{\alpha}$ обозначает конгруэнцию алгебры $\mathbb{A}/_{\alpha}$, индуцированную конгруэнцией β. Простые интервалы в решетке конгруэнций такой алгебры могут иметь лишь типы **2** и **3**. При этом (α, β) имеет тип **2** тогда и только тогда, когда для любого $\beta/_{\alpha}$-класса B алгебры $\mathbb{A}/_{\alpha}$ и любого $a \in B$ алгебра $(B; \mathbf{d}^{\theta}(x, a, y), \mathbf{d}^{\theta}(a, x, a), a)$ является абелевой группой. В противном случае (α, β) имеет тип **3**. Напомним, что наименьшая нетривиальная конгруэнция подпрямо неразложимой алгебры называется *монолитом.* Следующее свойство хорошо известно.

Предложение 3.2. *Пусть $\mathbb{A}$ — подпрямо неразложимая алгебра с мальцевской операцией, μ — ее монолит и $a \neq b$. Тогда для любых $c, d \in \mathbb{A}$ таких, что $(c, d) \in \mu$, найдется термальная операция $f(x, y_1, \ldots, y_n)$ и $e_1, \ldots, e_n \in \mathbb{A}$ такие, что $f(a, e_1, \ldots, e_n) = c$, $f(b, e_1, \ldots, e_n) = d$.*

Пусть $\mathbb{D}$ — приведенное подпрямое произведение подпрямо неразложимых алгебр $\mathbb{D}_1, \ldots, \mathbb{D}_n$, имеющих мальцевскую операцию, конгруэнция μ_i является монолитом алгебры $\mathbb{D}_i$ и $\underline{0}_i$ обозначает отношение равенства на $\mathbb{D}_i$, $i \in \underline{n}$. Пусть также $I \subseteq \underline{n}$ и δ — некоторая конгруэнция $\mathbb{D}\big|_I$. Алгебра $\mathbb{D}$ называется *I-прямоугольной* по модулю δ если $\delta \subseteq \theta_I$.

Предложение 3.3. *Если $\mathbb{D}$ — приведенная (если рассматривать ее как отношение) алгебра и $i \in \underline{n}$ таково, что $(\underline{0}_i, \mu_i)$ имеет тип* **3**, *и i — вершина степени захода 0 в графе $G(\mathbb{D})$, то $\mathbb{D}$ является $\{i\}$-прямоугольной по модулю μ_i.*

Доказательство данного предложения требует большего числа сведений из теории ручных конгруэнций, чем мы можем привести в статье. Все необходимые определения и факты могут быть найдены в книге [10].

Доказательство. Без ограничения общности мы можем полагать $i = 1$. Допустим, что алгебра $\mathbb{D}$ не $\{1\}$-прямоугольна по модулю μ_1. Тогда $\mu_1 \not\subseteq \theta_{\{1\}}$ и, следовательно, $\theta_{\{1\}} = \underline{0}_1$. Пусть $J \subseteq \underline{n}$ — минимальное подмножество, удовлетворяющее условиям: $1 \in J$ и $\mathbb{D}\big|_J$ не $\{1\}$-прямоугольна. Так как алгебра $\mathbb{D}$ приведенная, любая бинарная проекция $\mathbb{D}\big|_{\{1,i\}}$ отношения $\mathbb{D}$ является $\{1\}$-прямоугольной по модулю μ_1. Следовательно, J по крайней мере трехэлементно. Не ограничивая общности, положим $J = \underline{n}$.

Если $\mathbf{f}$ — термальная операция алгебры $\mathbb{D}$, то f_i обозначает соответствующую термальную операцию алгебры $\mathbb{D}_i$. Поскольку $(\underline{0}_1, \mu_1)$ имеет тип **3**, из результатов [1] следует, что для любого нетривиального μ_1-класса B найдутся 2-элементное множество $N \subseteq B$ (мы полагаем $N = \{0,1\}$), термальная операция $\mathbf{g}(x, y, z_1, \ldots, z_k)$ алгебры $\mathbb{D}$ и $\mathbf{a}_1, \ldots, \mathbf{a}_k \in \mathbb{D}$ такие, что операция $\mathbf{f}(x, y) = \mathbf{g}(x, y, \mathbf{a}_1, \ldots, \mathbf{a}_k)$ удовлетворяет следующим условиям: $f_1(\mathbb{D}_1, \mathbb{D}_1) \subseteq N$, f_1 является полурешеточной операцией на N, т.е. $f_1(0,1) = f_1(1,0) = f_1(1,1) = 1$, $f_1(0,0) = 0$, для любого $i \neq 1$ и любых $a, b, c, d \in \mathbb{D}_i$ таких, что $(a,c), (b,d) \in \mu_i$, справедливо равенство $f_i(a,b) = f_i(c,d)$, наконец, операция $\mathbf{f}(x,x)$ удовлетворяет тождеству $\mathbf{f}(\mathbf{f}(x,x), \mathbf{f}(x,x)) = \mathbf{f}(x,x)$. Рассмотрим кортеж $\mathbf{a} = (\mathbf{a}[3], \ldots, \mathbf{a}[n]) \in \mathbb{D}\big|_{\underline{n}-\{1,2\}}$ такой, что $(0, \mathbf{a}), (1, \mathbf{a}) \in \mathbb{D}\big|_{\underline{n}-\{2\}}$, и обозначим через A [соответственно B] множество всех $c \in \mathbb{A}_2$ со свойством $(0, c, \mathbf{a}) \in \mathbb{D}$ [соответственно $(1, c, \mathbf{a}) \in \mathbb{D}$]. Заметим, что A, B являются $\theta_{\{2\}}$-классами, а по предположению $\theta_{\{1\}} = \underline{0}_1$ имеем $A \cap B = \emptyset$. Заменяя $\mathbf{a}$ элементом $f(\mathbf{a}, \mathbf{a})$, мы можем предположить, что $\mathbf{f}(\mathbf{a}, \mathbf{a}) = \mathbf{a}$, а значит $f_2(A, A) \subseteq A$, $f_2(B, B), f_2(A, B), f_2(B, A) \subseteq B$.

Далее, поскольку $\mathbb{D}\big|_{\{1,2\}}$ $\{1\}$-прямоугольна по модулю μ_1, для любых $a \in A, b \in B$ имеем $(0, b), (1, a) \in \mathbb{D}\big|_{\{1,2\}}$. Возьмем $\mathbf{b} \in \mathbb{D}_{\underline{n}-\{1,2\}}$ такой, что $(0, b, \mathbf{b}) \in \mathbb{D}$. Таким образом, $\mathbf{d}\left((0, a, \mathbf{a}), (1, b, \mathbf{a}), (0, b, \mathbf{b})\right) = (e, a, \mathbf{b}) \in \mathbb{D}$, где $e = \mathbf{d}(0, 1, 0)$. Тогда $\mathbf{f}\left((e, a, \mathbf{b}), (e, a, \mathbf{b})\right) = (e', a', \mathbf{b}') \in \mathbb{D}$, где $e' \in \{0, 1\}$. Положим $f_2(b, b) = b'$ и заметим, что $a' \in A$, $b' \in B$. Если $e' = 0$, то $(0, b', \mathbf{b}') = \mathbf{f}\left((0, b, \mathbf{b}), (0, b, \mathbf{b})\right) \in \mathbb{D}$ и $(0, a', \mathbf{b}') \in \mathbb{D}$, следовательно, $a' \overset{\theta_{\{2\}}}{\equiv} b'$, что противоречит предположению $A \cap B = \emptyset$. Значит, $e' = 1$, и мы получаем $(0, b', \mathbf{b}'), (1, a', \mathbf{b}') \in \mathbb{D}$. Тогда $\mathbf{f}\left((0, b', \mathbf{b}'), (1, a', \mathbf{b}')\right) = (1, b'', \mathbf{b}') \in \mathbb{D}$, где $b'' \in B$. С другой стороны, $\mathbf{f}\left((1, a', \mathbf{b}'), (1, a', \mathbf{b}')\right) = (1, a'', \mathbf{b}') \in \mathbb{D}$, где $a'' \in A$. Наконец, поскольку $(1, b'', \mathbf{a}), (1, b'', \mathbf{b}'), (1, a'', \mathbf{b}') \in \mathbb{D}$, прямоугольность отношения $\mathbb{D}$ влечет $(1, a'', \mathbf{a}) \in \mathbb{D}$, а потому $a'' \in B$. Мы вновь получаем противоречие с предположением $A \cap B = \emptyset$.

4 Алгоритм

В следующих двух разделах мы опишем полиномиальный алгоритм, решающий задачу CSP($\mathcal{A}$) для конечного класса $\mathcal{A}$ однотипных конечных алгебр с мальцевской операцией, замкнутого относительно взятия подалгебр и гомоморфных образов. Зафиксируем некоторый мальцевский терм класса $\mathcal{A}$ и обозначим его через $\mathbf{d}$. Можно считать, что $\mathbf{d}$ —единственная основная операция алгебр из $\mathcal{A}$. В силу конечности $\mathcal{A}$ все параметры и объекты, с ним связанные, можно считать известными. В частности, мы будем предполагать известными все свойства "небольших" прямых произведений алгебр из $\mathcal{A}$, мощность которых не превосходит мощности наибольшей алгебры из $\mathcal{A}$.

4.1 Планирование

Наш алгоритм работает в две стадии. На первой стадии он упрощает исходную задачу, раскладывая в подпрямое произведение те области значений, которые могут быть разложены, и факторизуя по модулю монолита подпрямо неразложимые области значений. Эту первую стадию мы называем *планированием*. После того как задача станет тривиальной (все области значений одноэлементны), алгоритм начинает вторую стадию — построение базиса множества решений. В данном разделе мы опишем стадию планирования.

Возьмем частную задачу $\mathcal{P} = (V; \mathcal{A}; \sigma; \{C_1, \dots, C_q\})$ из CSP($\mathcal{A}$). Для краткости мы обозначаем алгебру $\mathbb{A}_{\sigma(v)}$ через $\mathbb{A}_v$, опуская сортовую функцию. Мы можем предположить, что $\mathcal{P}$ 3-согласованная, приведенная и что все алгебры $\mathbb{A}_v$ подпрямо неразложимы. Первые два требования могут быть достигнуты с помощью процедур, описанных в разделе 2.2, последнее условие может быть удовлетворено повторением для каждой переменной $v \in V$ следующей процедуры, которую мы будем называть *разложением*. Через $\underline{0}_v$ и μ_v мы обозначаем отношение равенства и монолит алгебры $\mathbb{A}$ соответственно (последнее обозначение имеет смысл только если $\mathbb{A}$ подпрямо неразложима).

Пусть $\eta_{v,1},\dots,\eta_{v,m}$ — неразложимые в пересечение конгруэнции алгебры $\mathbb{A}_v$ такие, что $\eta_{v,1}\wedge\ldots\wedge\eta_{v,m}=\underline{0}_v$. Введем следующие обозначения $\Delta=\{\eta_{v,1},\dots,\eta_{v,m}\}$, $\mathbb{A}'_{(v,1)}=\mathbb{A}_v/_{\eta_{v,1}},\dots,\mathbb{A}'_{(v,m)}=\mathbb{A}_v/_{\eta_{v,m}}$ и $t_v=m$. Тогда $\mathbb{A}_v$ является подпрямым произведением алгебр $\mathbb{A}'_{(v,1)},\dots,\mathbb{A}'_{(v,l)}$. Далее, для каждой переменной $w\in V-\{v\}$ положим присвоить $t_w=1$, $\eta_{w,1}=\underline{0}_w$, $\Delta_w=\{\eta_{w,1}\}$ и $\mathbb{A}'_{(w,1)}=\mathbb{A}_w$. Теперь задача $\mathcal{P}':=(W;\{\mathbb{A}'_w\colon w\in W\};\sigma';\{C'_1,\dots,C'_q\})$ определена следующим образом: $W=\bigcup_{w\in V}\{(w,j)\colon 1\le j\le t_w\}$, $C'_t=\langle\mathbf{s}'_t,\varrho'_t\rangle$, для каждого $1\le t\le q$, где $\mathbf{s}'_t=\bigcup_{w\in\mathbf{s}_t}\{(w,j)\colon 1\le j\le t_w\}$, $\varrho'_t=\{(\mathbf{a}[w]^{\eta_{w,1}},\dots,\mathbf{a}[w]^{\eta_{w,t_w}})_{w\in\mathbf{s}_t}\colon(\mathbf{a}[w])_{w\in\mathbf{s}_t}\in\varrho_t\}$, наконец, σ' ставит в соответствие переменной $w\in W$ алгебру $\mathbb{A}'_w$.

Дадим сначала неформальное описание стадии планирования. Прежде всего алгоритм выбирает вершину (переменную) графа $G(\mathcal{P})$ со степенью захода 0 и факторизует соответствующую область значений по ее монолиту. Затем с помощью процедуры разложения он находит подпрямое разложение получившейся алгебры, преобразует ограничения, в которые входит эта переменная. После этого полученная задача трансформируется к 3-согласованной и приведенной. Далее описанный процесс повторяется до тех пор, пока все области значений не станут одноэлементными. Поскольку процедура планирования может быть использована более одного раза, мы опишем ее как подпрограмму.

Вход. $\mathcal{P}^1=(V^1;\{\mathbb{A}^1_v:v\in V^1\};\sigma^1;\{C^1_1,\dots,C^1_q\})$, все $\mathbb{A}^1_v$ подпрямо неразложимы и $\mathcal{P}^1$ является 3-согласованной и приведенной.

Выход. Следующие последовательности:

$(\mathcal{P}'^2,\dots,\mathcal{P}'^k)$, где $\mathcal{P}'^l=(W^l;\{\mathbb{A}^l_v:v\in W^l\};\sigma'^l;\{C'^l_1,\dots,C'^l_q\})$, $C'^l_t=\langle\mathbf{s}^l_t,\varrho^l_t\rangle$ и $|\mathbb{A}^k_v|=1$ для всех $v\in W^k$;

$(G^2,\dots,G^{k-1})$, где $G^l=G(\mathcal{P}'^l)$, $(V^2,\dots,V^k)$, где $V^l\subseteq W^l$ состоит из представителей сильно связных компонент графа G^l, и $(v^1,\dots,v^{k-1})$, где $v^l\in V^l$ принадлежит сильно связной компоненте G^l степени захода 0;

$(\mathcal{P}^2,\dots,\mathcal{P}^k)$, где $\mathcal{P}^l=\mathcal{P}'^l\big|_{V^l}$;

$(\Delta^2,\dots,\Delta^{k-1})$, где Δ^l — множество неразложимых в пересечение конгруэнций алгебры $\mathbb{A}^l_{v^l}$ таких, что $\bigwedge_{\delta\in\Delta^l}\delta = \mu^l_{v^l}$.

АЛГОРИТМ

Повторять следующие шаги **пока** $|\mathbb{A}^l_v| \neq 1$ для какого-нибудь $v \in V^l$.

Шаг 1. **Выбрать** вершину $v^l \in V^l$ графа $G(\mathcal{P}^l)$ степени захода 0.

(*Если* $(\underline{0}^l_{v^l}, \mu^l_{v^l})$ *имеет тип* **3**, *то мы говорим, что* l*-ая итерация имеет тип* **3**, *в противном случае* l*-ая итерация имеет тип* **2**.)

Шаг 2. **Присвоить** $\mathcal{P}'' := (V^l; \{\mathbb{B}_v : v \in V^l\}; \sigma; \{C''_1, \dots, C''_q\})$, где $\mathbb{B}_v := \mathbb{A}^l_{v^l}/_{\mu^l_{v^l}}$ если $v = v^l$, в противном случае $\mathbb{B}_v := \mathbb{A}^l_v$. $C''_j = \langle \mathbf{s}^l_j, \varrho''^l_t\rangle$ и $\varrho''^l_t = \{(\mathbf{a}[v])_{v\in\mathbf{s}^l_t} :$ найдется $\mathbf{b} \in \varrho^l_t$ такой, что $\mathbf{a}[v^l] = \mathbf{b}[v^l]/_{\mu^l_v}$ и, если $v \neq v^l$, то $\mathbf{a}[v] = \mathbf{b}[v]\}$.

Шаг 3. **Применить** процедуру разложения к $\mathcal{P}''$ и переменной v^l. Полученную задачу обозначить через $\mathcal{P}'^{l+1} := (W^{l+1}; \{\mathbb{A}^{l+1}_v : v \in W^{l+1}\}; \sigma'^{l+1}; \{C'^{l+1}_1, \dots, C'^{l+1}_q\})$, а множество использованных неразложимых в пересечение конгруэнций алгебры $\mathbb{A}^l_{v^l}$, соответствующих использованным конгруэнциям $\mathbb{B}$ — через Δ^l.

Шаг 4. **Установить 3-согласованность**; **найти** орграф $G^{l+1} = G(\mathcal{P}'^{l+1})$, множество V^{l+1} представителей сильно связных компонент G^{l+1} и **присвоить** $\mathcal{P}^{l+1} := \mathcal{P}'^{l+1}\big|_{V^{l+1}}$.

4.2 Базис множества решений

Все объекты, участвующие в задаче — переменные, кортежи, области значений, отношения — меняются по ходу исполнения алгоритма. Нам будет удобно использовать специальные обозначения для этих изменяющихся объектов.

Рассмотрим задачу $\mathcal{P}^l$, полученную на l-ой итерации, и пусть $v \in V^l$. Тогда

$v{\uparrow}^{l+1}$ обозначает кортеж $((v,1)', \dots, (v,t_v)')$, где $(v,i)' \in V^{l+1}$ — представитель сильно связной компоненты графа G^{l+1}, содержащей (v,i) для $v \in V^l$ такого, что $t_v = |\Delta^l_v|$;

$a{\uparrow}^{l+1}$ обозначает $(a^{\eta_{v,1}}, \dots, a^{\eta_{v,t_v}})$, где $a \in \mathbb{A}^l_v$ и $\{\eta_{v,1}, \dots, \eta_{v,t_v}\} = \Delta^i_v$;

$\mathbf{a}{\uparrow}^{l+1} = (\mathbf{a}[w]{\uparrow}^{l+1})_{w\in W}$, где $\mathbf{a} = (\mathbf{a}[w])_{w\in W}$, $W \subseteq V^l$ (таким образом,

$\mathbf{a}{\upharpoonleft}^{l+1}$ — кортеж, компонентами которого являются компоненты кортежей $\mathbf{a}[w]{\upharpoonleft}^{l+1}$);

$\varrho{\upharpoonleft}^{l+1} = \{\mathbf{a}{\upharpoonleft}^{l+1} \colon \mathbf{a} \in \varrho\}$, где ϱ — отношение над $\{\mathbb{A}^l_w \colon w \in W\}$.

Заметим, что для каждого $\mathbf{a}$ нетрудно построить $\mathbf{a}'$ такой, что $\mathbf{a}'{\upharpoonleft}^{l+1} = \mathbf{a}$. Для этого выберем элемент a такой, что $a{\upharpoonleft}^{l+1} = \mathbf{a}|_{v^l{\upharpoonleft}^{l+1}}$, и положим $\mathbf{a}'[w] = \mathbf{a}[(w,1)]$ при $w \neq v^l$ и $(w,1) \in V^{l+1}$, $\mathbf{a}'[w] = a$ при $w = v^l$; в противном случае $\mathbf{a}'[w] = \varphi_{w',w}(\mathbf{a}'[w'])$, где $w' \in V^{l+1}$ — переменная принадлежащая той же сильно связной компоненте G^{l+1}, что и w.

Предположим, что $v{\upharpoonleft}^j$, $a{\upharpoonleft}^j$, $\mathbf{a}{\upharpoonleft}^j$, $\varrho{\upharpoonleft}^j$ уже определены. Тогда

$v{\upharpoonleft}^{j+1} = (v_1{\upharpoonleft}^{j+1}, \dots, v_t{\upharpoonleft}^{j+1})$, где $v{\upharpoonleft}^j = (v_1, \dots, v_t)$;

$a{\upharpoonleft}^{j+1} = (\mathbf{a}[w]{\upharpoonleft}^{j+1})_{w \in v{\upharpoonleft}^j}$, где $a \in \mathbb{A}^l_v$, $(\mathbf{a}[w])_{w \in v{\upharpoonleft}^j} = a{\upharpoonleft}^j$;

$\mathbf{a}{\upharpoonleft}^{j+1} = (\mathbf{a}[w]{\upharpoonleft}^{j+1})_{w \in W{\upharpoonleft}^j}$, где $\mathbf{a} = (\mathbf{a}[w])_{w \in W}$, $W \subseteq V^l$;

$\varrho{\upharpoonleft}^{j+1} = \{\mathbf{a}{\upharpoonleft}^{j+1} \colon \mathbf{a} \in \varrho\}$, где ϱ — отношение над $\{\mathbb{A}^l_w \colon w \in W \subseteq V^l\}$.

На каждой итерации алгоритма мы находим базис множества решений $\mathcal{S}^l$ задачи $\mathcal{P}^l$. Поскольку все отношения ограничений являются подалгебрами прямых произведений областей значений, множество $\mathcal{S}^l$ также является подалгеброй произведения $\mathbb{A}^l = \prod_{v \in V^l} \mathbb{A}^l_v$ и искомый базис B будет порождающим множеством для $\mathcal{S}^l$. Базис B будет иметь вид $B = B^k \cup \ldots \cup B^l$, где $B^k{\upharpoonleft}^i \cup \ldots \cup B^i{\upharpoonleft}^i$ — базис множества $\mathcal{S}^l{\upharpoonleft}^i$ (которое не обязательно совпадает с $\mathcal{S}^i$, однако включение $\mathcal{S}^l{\upharpoonleft}^i \subseteq \mathcal{S}^i$ справедливо всегда) для каждого $l < i \le k$. Так как алгебры $\mathbb{A}^k_v$ тривиальны, имеем $\mathcal{S}^k = B^k = \{\mathbf{a}\}$. Мы говорим, что кортеж $\mathbf{a}$ может быть *B-разложен*. Далее, обозначим $\mu^l_{v^l}$-классы через $H^l_1, \dots, H^l_s$. Тогда $B^l = B^l_1 \cup \ldots \cup B^l_s$, где для каждого $1 \le p \le s$ найдутся $H'^l_p \subseteq H^l_p$ такой, что $H'^l_p = H^l_p$ или $|H'^l_p| = 1$, и $(\mathbf{a}[w])_{w \in V^l - \{v^l\}} \in \prod_{w \in V^l - \{v^l\}} \mathbb{A}^l_w$ такой, что $B^l_p = \{\mathbf{a}_b : b \in H'^l_p\}$, $\mathbf{a}_b[w] = b$ если $w = v^l$, и $\mathbf{a}_b[w] = \mathbf{a}[w]$, если $w \neq v^l$.

Пусть $B - B^l = \{\mathbf{c}_1, \dots, \mathbf{c}_n\}$. Кортеж $\mathbf{b}$ может быть *B-разложен*, если $\mathbf{b} = \mathbf{d}(\mathbf{b}', \mathbf{a}_b, \mathbf{a}_c)$, где $b = \mathbf{b}'[v^l]$, $c = \mathbf{b}[v^l]$ и $\mathbf{b}'$ таков, что $\mathbf{b}'{\upharpoonleft}^{l+1}$ может быть $(B - B^l){\upharpoonleft}^{l+1}$-разложен и если $\mathbf{b}'{\upharpoonleft}^{l+1} = f(\mathbf{c}_1{\upharpoonleft}^{l+1}, \dots, \mathbf{c}_n{\upharpoonleft}^{l+1})$ есть $(B - B^l){\upharpoonleft}^{l+1}$-разложение, то $\mathbf{b}' = f(\mathbf{c}_1, \dots, \mathbf{c}_n)$.

Такое разложение кортежа $\mathbf{b}$ мы будем называть *стандартным B-разложением*. Множество B называется *стандартным базисом* множества

$\mathcal{S}^l$, если $B \subseteq \mathcal{S}^l$ и каждый кортеж $\mathbf{b} \in \mathcal{S}^l$ имеет стандартное B-разложение. Как нетрудно проверить, следующие леммы вытекает из предложения 3.3 и прямоугольности отношений, инвариантных относительно мальцевской операции.

Лемма 4.1. *Пусть B — стандартный базис отношения ϱ. Тогда ϱ — алгебра, порожденная множеством B.*

Лемма 4.2. *Пусть множество $\mathcal{S}^l$ — подпрямое произведение алгебр $\mathbb{A}_v^l$, $v \in V^l$, множество $B \subseteq \mathcal{S}^l$ определено как указано выше; для каждого $k \geq m \geq l$ имеем $H_p'^m = H_p^m$ всякий раз, когда m-ая итерация имеет тип **3**, или когда m-ая итерация имеет тип **2** и $\mathcal{S}^m$ является $\{v^m\}$-прямоугольным по модулю $\mu_{v^m}^m$, и $|H_p'^m| = 1$, если m-ая итерация имеет тип **2** и конгруэнция θ_{v^m} алгебры $\mathbb{A}_{v^m}^m$ является отношением равенства. Тогда B является стандартным базисом множества $\mathcal{S}^l$.*

Координаты кортежа $\mathbf{a}$ в базисе B мы будем обозначать через $K(\mathbf{a})$. Кортеж $K(\mathbf{a})$ состоит из $k - l + 1$ части $K^k(\mathbf{a}), \ldots, K^l(\mathbf{a})$, которые соответствуют частям $B^k, \ldots, B^l$ базиса B. Далее, $K^i(\mathbf{a})$ состоит из $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$, которые в свою очередь соответствуют множествам $B_1^i, \ldots, B_s^i$. Наконец, каждый $K_p^i(\mathbf{a})$ — это кортеж $(\alpha_1, \ldots, \alpha_m)$, компонентами которого являются целые числа. По построению, самое большее один из кортежей $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$ может быть отличен от нулевого кортежа, и этот ненулевой кортеж, $K_p^i(\mathbf{a})$, содержит ровно две отличных от нуля компоненты, -1 и 1. Пусть $K_p^i(\mathbf{a}) = (\alpha_1, \ldots, \alpha_m)$ и $B_p^i = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$. Иногда мы будем использовать обозначение $\mathbf{b} + K_p^i(\mathbf{a}) \cdot B_p^i$. Оно обозначает кортеж $\mathbf{b}$, если $K_p^i(\mathbf{a})$ — нулевой кортеж, и кортеж $\mathbf{d}(\mathbf{b}, \mathbf{a}_i, \mathbf{a}_j)$ в противном случае, где $\alpha_i = -1$, $\alpha_j = 1$. Поскольку не более одного из кортежей $K_1^i(\mathbf{a}), \ldots, K_s^i(\mathbf{a})$ является ненулевым, мы можем определить $\mathbf{b} + K^i(\mathbf{a}) \cdot B^i$ как $\mathbf{b} + K_p^i(\mathbf{a}) \cdot B_p^i$, где $K_p^i(\mathbf{a})$ — ненулевая часть кортежа $K^i(\mathbf{a})$.

Когда мы будем решать уравнения, нам потребуются обозначения для координат неизвестного кортежа. Эти неизвестные координаты мы будем обозначать через $K(x)$.

4.3 Построение базиса

В этом разделе мы опишем вторую стадию работы алгоритма — построение базиса. На этой стадии алгоритм проходит через те же самые этапы, что и на стадии планирования, но в обратном порядке — от тривиальной задачи к исходной, — строя стандартные базисы множеств $\mathcal{S}^k, \mathcal{S}^{k-1}, \ldots, \mathcal{S}^1$. Через $\mathbb{A}^l$ мы обозначаем прямое произведение алгебр $\mathbb{A}^l_v$, $v \in V^l$. На каждой итерации возможны два случая. Если итерация имеет тип **3**, то мы пользуемся предложением 3.3 и алгоритм в этом случае очень прост. Он для каждого кортежа $\mathbf{a}$ из базиса для множества $\mathcal{S}^{l+1}$ находит представителя $\mathbf{b}$ из $\mathcal{S}^l$ такого, что $\mathbf{b}{\uparrow}^{l+1}= \mathbf{a}$ и для каждого элемента алгебры $\mathbb{A}^l_{v^l}$ добавляет один кортеж к этому множеству представителей, чтобы получить базис $\mathcal{S}^l$, описанный в предыдущем разделе. Второй случай, в котором итерация имеет тип **2**, более сложен. В этом случае алгоритм находит базис пространства решений для каждого из классов $H_1, \ldots, H_s$ монолита $\mu^l_{v^l}$ алгебры $\mathbb{A}^l_{v^l}$ отдельно. Для этого он использует базис B_{H_p} множества $\mathcal{S}_{H_p} = \{\mathbf{a} \in \mathcal{S}^{l+1} \colon \mathbf{a} = \mathbf{b}{\uparrow}^{l+1}, \mathbf{b}[v^l] \in H_p\}$, $1 \le p \le s$, которое было найдено на предыдущей итерации, и для каждого $1 \le t \le q$ и каждого $\mathbf{a} \in B_{H_p}$ находит кортеж $\mathbf{a}_t \in \mathbb{A}^l$ такой, что $\mathbf{a}_t|_{\mathbf{s}^l_t} \in \varrho^l_t$ и $\mathbf{a}_t{\uparrow}^{l+1}= \mathbf{a}$. Множество $\{\mathbf{a}_t \colon \mathbf{a} \in B_{H_p}\}$ обозначается через $B_{H_p,t}$. Алгоритм выбирает произвольный вектор $\mathbf{b} \in B_{H_p,t}$ и полагает $D_{p,t}$ равным множеству $a/\mu^l_{v_l}$, где $a = \mathbf{b}[v^l]$, если $v^l \notin \mathbf{s}^l_t$ или ϱ^l_t является v^l-прямоугольным по модулю $\mu^l_{v^l}$, либо равным $\{a\}$ в противном случае. Множество $D'_{p,t}$ затем получается продолжением элементов из $D_{p,t}$ с помощью компонент кортежа $\mathbf{a}$ до кортежей из алгебры $\mathbb{A}^l$. Наконец, алгоритм находит базис пересечения подалгебр, порожденных множествами $B_{H_p,t} \cup D'_{p,t}$, $1 \le t \le q$. Этот базис становится частью искомого базиса множества $\mathcal{S}^l$.

В ходе этого процесса из отношений ограничений некоторые кортежи могут быть удалены. В этом случае алгоритм должен повторить процедуру планирования, поскольку может быть утрачена 3-согласованность или измениться граф G^l. Ниже мы даем формальное описание алгоритма.

Вход. $\mathcal{P} = (V; \{\mathbb{A}_v : v \in V\}; \sigma; \{C_1, \ldots, C_q\})$, где $\mathbb{A}_v$ — алгебры с мальцевской операцией $\mathbf{d}$, $C_t = \langle \mathbf{s}_t, \varrho_t \rangle$.

Выход. Стандартный базис B множества решений $\mathcal{P}$ или "НЕТ" если задача не имеет решений.

АЛГОРИТМ

Шаг 1. **Применить** процедуру разложения к задаче $\mathcal{P}$ и каждой из переменных $v \in V$. Полученную задачу обозначить через $\mathcal{P}'^1 = (W^1; \{\mathbb{A}_v^1 \colon v \in W^1\}; \sigma'; \{C'^1_1, \ldots, C'^1_q\})$, где $C'^1_t = \langle \mathbf{s}'^1_t, \varrho'^1_t \rangle$ для $1 \le t \le q$.

Шаг 2. **Установить** 3-согласованность, **найти** ассоциированную приведенную задачу $\mathcal{P}^1$ с множеством переменных V^1.

Шаг 3. **Применить** процедуру планирования к $\mathcal{P}^1$.

Шаг 4. **Если** $\mathcal{P}^k$ содержит пустое отношение ограничения, то **Вывести** "НЕТ". **Иначе** задача $\mathcal{P}^k$ имеет только одно решение $\mathbf{b}$. **Присвоить** $B = B^k := \{\mathbf{b}\}$.

Шаг 5. **Для каждого** $1 \le l < k$ **выполнять**.

Шаг 5.1. Предположим, что базис $\overline{B} = \overline{B}^k \cup \ldots \cup \overline{B}^{l+1}$ множества $\mathcal{S}^{l+1}$ построен. **Если** l-ая итерация имеет тип **3**, **то выполнять**

Шаг 5.1.1 **Для каждого** $\mathbf{a} \in \overline{B}$ **найти** $\mathbf{a}' \in \mathbb{A}^l$ такой, что $\mathbf{a}'{\upharpoonleft}^{l+1} = \mathbf{a}$. **Присвоить** $B^j := \{\mathbf{a}' : \mathbf{a} \in \overline{B}^j\}$ для $l < j \le k$.

Шаг 5.1.2. Пусть $H_1, \ldots, H_s$ — $\mu^l_{v^l}$-классы. **Для каждого** H_p **выбрать** $\mathbf{a}_p \in \mathcal{S}^{l+1}$ такой, что $\mathbf{a}_p\big|_{v^l{\upharpoonleft}^{l+1}} = H_p{\upharpoonleft}^{l+1}$. (*См. раздел 5.3.*) **Положить** B^l_p равным множеству всех кортежей $\mathbf{b} \in \mathbb{A}^l$ таких, что $\mathbf{b}{\upharpoonleft}^{l+1} = \mathbf{a}_p$ **и** $B^l = B^l_1 \cup \ldots \cup B^l_s$.

Шаг 5.2. **Если** l-ая итерация имеет тип **2 то делать**

Шаг 5.2.1. Пусть $H_1, \ldots, H_s$ — $\mu^l_{v^l}$-классы алгебры $\mathbb{A}^l_{v^l}$ и $\mathcal{S}_{H_p}$, $1 \le p \le s$, — множество $\{\mathbf{a} \in \mathcal{S}^{l+1} \colon \mathbf{a} = \mathbf{b}{\upharpoonleft}^{l+1},\ \mathbf{b}[v^l] \in H_p\}$. **Для каждого** $1 \le p \le s$ **пусть** B_{C_p} — базис множества $\mathcal{S}_{H_p}$. (B_{H_p} *найден на предыдущей итерации.*)

Шаг 5.2.2. **Для каждого** $1 \le t \le q$, **каждого** $1 \le p \le s$ и **каждого** $\mathbf{a} \in B_{H_p}$ **выбрать** $\mathbf{a}_t \in \mathbb{A}^l$ такой, что $\mathbf{a}_t{\upharpoonleft}^{l+1} = \mathbf{a}$, $\mathbf{a}_t\big|_{\mathbf{s}^l_t} \in \varrho^l_t$. (*Кортеж* $\mathbf{a}_t$ *с этими свойствами существует, так как* $\mathbf{a}\big|_{\mathbf{s}^{l+1}_t} \in \varrho^{l+1}_t = \varrho^l_t{\upharpoonleft}^{l+1}$.) **Присвоить** $B_{H_p,t} = \{\mathbf{a}_t \colon \mathbf{a} \in B_{H_p}\}$.

Шаг 5.2.3. **Для каждого** $1 \le p \le s$ **зафиксировать** кортеж $\mathbf{a}^p \in B_{H_p}$ и соответствующие кортежи $\mathbf{a}^p_1, \ldots, \mathbf{a}^p_s$ из $B_{H_p,1}, \ldots, B_{H_p,s}$, соответственно. **Для каждого** $1 \le t \le q$, **присвоить** $D_{p,t} := \mathbf{a}^p_t[v^l]/\mu^l_{v^l}$ если $v^l \notin \mathbf{s}^l_t$ или ϱ^l_t является v^l-прямоугольным по модулю $\mu^l_{v^l}$, и $D_{p,t} := \{\mathbf{a}^p_t[v^l]\}$ в противном случае.

Шаг 5.2.4. **Присвоить** $D'_{p,t} := \{\mathbf{b} \in \mathbb{A}^l \colon \mathbf{b}[v^l] \in D_{p,t},\ \mathbf{b}|_{V^l-\{v^l\}} = \mathbf{a}^p_t|_{V^l-\{v^l\}}\}$.

Шаг 5.2.5. **Для каждого** $1 \le p \le s$ **решить** систему уравнений

$$\begin{aligned}
&\mathbf{b}^k_{p,1} + K^{k-1}(x)\cdot B^{k-1}_{H_p,1} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{H_p,1} + y^1_1\mathbf{b}^1_1 + \ldots + y^{n_1}_1\mathbf{b}^{n_1}_1\\
&= \ \mathbf{b}^k_{p,2} + K^{k-1}(x)\cdot B^{k-1}_{H_p,2} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{H_p,2} + y^1_2\mathbf{b}^1_2 + \ldots + y^{n_2}_2\mathbf{b}^{n_2}_2\\
&\qquad\qquad\vdots\\
&\mathbf{b}^k_{p,1} + K^{k-1}(x)\cdot B^{k-1}_{H_p,1} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{H_p,1} + y^1_1\mathbf{b}^1_1 + \ldots + y^{n_1}_1\mathbf{b}^{n_1}_1\\
&= \ \mathbf{b}^k_{p,q} + K^{k-1}(x)\cdot B^{k-1}_{H_p,q} + \ldots + K^{l+1}(x)\cdot B^{l+1}_{H_p,q} + y^1_q\mathbf{b}^1_q + \ldots + y^{n_q}_q\mathbf{b}^{n_q}_q,
\end{aligned}$$

где $B_{H_p,t} = \{\mathbf{b}^k_{p,t}\} \cup B^{k-1}_{H_p,t} \cup \ldots \cup B^{l+1}_{H_p,t}$, $D'_{p,t} = \{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$. Множество решений этой системы обозначается через $\mathcal{S}'_p$, а его стандартный базис — через E_p. Пусть также $\mathcal{S}' = \bigcup_{1 \le p \le s} \mathcal{S}'_p$. (*Алгоритм, решающий указанную систему, описан в разделе 5.1.*)

Шаг 5.2.6. **Если** все E_p пусты, **то Вывести**(“НЕТ”). **Иначе** преобразовать $E_1, \ldots, E_p$ в стандартный базис. (*См. раздел 5.4.*)

Шаг 5.3. **Для каждого** $i \in \{k, \ldots, l-1\}$, **каждого** $v \in V^i$ **и** подалгебры $\mathbb{B}$ из $\mathbb{A}^i_v$ **найти** стандартный базис множества $\mathcal{S}_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i \colon \mathbf{a}[v] \in \mathbb{B}\}$ если $i \ne l-1$, или множества $\mathcal{S}'_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l : \mathbf{a}|_{v\uparrow^l} \in \mathbb{B}{\uparrow}^l\}$ в противном случае. (*См. раздел 5.2.*)

Шаг 5.4. **Для каждого** кортежа **a из каждого** отношения ограничения ϱ^l_t **найти** базис множества $\{\mathbf{b} \in \mathcal{S}^l \colon \mathbf{b}|_{\mathbf{s}^l_t} = \mathbf{a}\}$. Для этого **выполнять**

Шаг 5.4.1. Пусть $\mathbf{s}^l_t = (v_1, \ldots, v_n)$. **Присвоить** $D^0 = B$.

Шаг 5.4.2. **Для каждого** $1 \le j \le n$ **найти** стандартный базис множества $\{\mathbf{b} \in \langle D^{j-1}\rangle : \mathbf{b}[v_j] = \mathbf{a}[v_j]\}$. (*См. раздел 5.2.*)

Шаг 5.4.3. **Присвоить** $D = D^n$.

Шаг 5.4.4. **Если** базис D пуст, то удалить **a** из ϱ^l_t, и все **b** такие, что $\mathbf{b}{\uparrow}^l = \mathbf{a}$, из ϱ^i_t, $1 \le i < l$.

Шаг 5.5. Пусть $\mathcal{P}'^1$ обозначает задачу, полученную из $\mathcal{P}^1$ на предыдущем шаге. **Если** существует 3-элементное множество $W \subseteq V^1$ такое, что множество частичных решений задач $\mathcal{P}'^1$ и $\mathcal{P}^1$ на W различны, то **установить** 3-согласованность $\mathcal{P}'^1$. Обозначить полученную задачу через $\mathcal{P}^1$ **и перейти** на шаг 2.

Шаг 5.6. **В противном случае вычислить** граф $G(\mathcal{P}'^l)$, где $\mathcal{P}'^l$ — задача, полученная из $\mathcal{P}^l$ на шаге 5.4. **Если** $G(\mathcal{P}'^l) \neq G(\mathcal{P}^l)$ **то положить** $\mathcal{P}^1$ равным $\mathcal{P}'^1$, **и перейти** на шаг 2.

5 Описание процедур алгоритма и комментарии

5.1 Решения системы уравнений над стандартным базисом и решения задачи CSP

На шаге 5.2.5 алгоритма из раздела 4.3 была получена некоторая система уравнений, коэффициентами в которой являются компоненты кортежей стандартного базиса. Мы будем обозначать ее через $(*)$. В данном разделе мы покажем, как решения системы $(*)$ соответствуют решениям исходной задачи CSP, а также, как решения этой системы могут быть найдены. Мы используем обозначения, введенные в предыдущем разделе.

5.1.1 Почти стандартное разложение

Нам потребуется обобщенная версия стандартного базиса и разложения по такому базису.

Пусть множество $B = B^k \cup \ldots \cup B^l$ — базис множества $\mathcal{S}^l$, а $K(x)$ — некоторый кортеж, состоящий из целых чисел, и такой, что $K^k(x)$ есть однокомпонентный кортеж (1) и $\sum_{i=1}^m \alpha_i = 0$ для каждого $K_p^j(\mathbf{x}) = (\alpha_1, \ldots, \alpha_m)$. Определим кортеж $\mathbf{b}$ из $\mathbb{A}^l$ следующим образом.

Положим $\mathbf{b}^k = \mathbf{a}$, где $B^k = \{\mathbf{a}\}$.

Далее, предположим, что для $l \le j < k$ кортеж $\mathbf{b}^{j+1}$ уже определен. Пусть $B_1^j, \ldots, B_s^j$ обозначают части базиса B^j, кортежи $\mathbf{b}_0 = \mathbf{b}^{j+1}$, $\mathbf{b}_{p-1}$ уже определены, и $B_p^j = \{\mathbf{a}_1, \ldots, \mathbf{a}_m\}$, $K_p^j(x) = (\alpha_1, \ldots, \alpha_m)$. Аргументы x, z терма $\mathbf{d}(x, y, z)$ называются *четными*, а аргумент y — *нечетным*.

Положим $\mathbf{b}_p = \mathbf{d}(\ldots \mathbf{d}(\mathbf{d}(\mathbf{b}_{p-1}, \mathbf{a}_{i_1}), \mathbf{a}_{i_2}, \mathbf{a}_{i_4}) \ldots)$, где число раз, которое $\mathbf{a}_i$ встречается в качестве четного [нечетного] аргумента обозначается через β_i [соответственно γ_i], и $\beta_i - \gamma_i = \alpha_i$ для $i \in \{1, \ldots, m\}$. (Таким образом, кортеж $\mathbf{b}_p$ для каждого p определен неоднозначно.) Положим $\mathbf{b}^j = \mathbf{b}_s$.

Наконец, положим $\mathbf{b} = \mathbf{b}^l$.

Лемма 5.1. *Кортеж имеет почти стандартное B-разложение тогда и только тогда, когда он имеет стандартное B-разложение.*

В самом деле, если $\mathbf{b}$ имеет почти стандартное B-разложение, то $\mathbf{b}$ принадлежит подалгебре, порожденной B. Следовательно, $\mathbf{b}$ имеет стандартное B-разложение.

5.1.2 Соответствие между решениями систем линейных уравнений и решениями задач CSP

В этом разделе мы прежде всего продемонстрируем связь между решениями систем уравнений вида $(*)$ и решениями задач CSP; как станет ясно, эти решения некоторым образом соответствуют друг другу. Затем мы покажем, что система $(*)$ сводится к системе уравнений над некоторой абелевой группой, а поскольку системы уравнений над абелевыми группами могут быть легко решены, это позволяет решать системы вида $(*)$ и, следовательно, задачи CSP.

Предположим, что базис множества $\mathcal{S}^{l+1}$ уже найден, l-ая итерация алгоритма имеет тип **2** и для класса H_p конгруэнции $\mu^l_{v^l}$ получена система вида $(*)$, где множество $B_{H_p,t} = \{\mathbf{b}^k_{p,t}\} \cup B^{k-1}_{H_p,t} \cup \ldots \cup B^{l+1}_{H_p,t}$ таково, что $B_{H_p,t}\!\restriction^{l+1}$ является базисом множества $\mathcal{S}_{H_p}$ и $D'_{p,t} = \{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$.

Лемма 5.2. *Кортеж $\mathbf{c} \in \mathbb{A}^l$ является решением задачи $\mathcal{P}^l$ тогда и только тогда, когда найдутся кортежи $(K^{k-1}(x), \ldots, K^{l+1}(x), y^1_1, \ldots, y^{n_1}_1, \ldots, y^{n_q}_q)$ такие, что для любого $1 \leq t \leq q$ числа $(K^{k-1}(x), \ldots, K^{l+1}(x), y^1_t, \ldots, y^{n_t}_t)$ являются почти стандартными координатами $\mathbf{c}$ и кортеж $\mathbf{c}|_{\mathbf{s}^l_t}$ может быть представлен в виде $\mathbf{b}^k_{p,t} + K^{k-1}(x) \cdot B^{k-1}_{H_p,t} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{H_p,t} + y^1_t \mathbf{b}^1_t + \ldots + y^{n_1}_t \mathbf{b}^{n_1}_t$, где p таково, что $\mathbf{c}[v^l] \in H_p$.*

Доказательство. Пусть $\mathbf{c} \in \mathcal{S}^l$ и $\mathbf{c}[v^l] \in H_p$. Тогда для любого $1 \le t \le q$ кортеж $\mathbf{c}{\uparrow}^{l+1} \in \mathcal{S}_{H_p}$ может быть разложен следующим образом:

$$\mathbf{c}{\uparrow}^{l+1} = \mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{H_p,t}{\uparrow}^{l+1} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{H_p,t}{\uparrow}^{l+1},$$

где $K^k(\mathbf{c}), \ldots, K^{l+1}(\mathbf{c})$ не зависят от t. Для каждого $1 \le t \le q$ положим $\mathbf{a}_t = \mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{H_p,t} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{H_p,t}$. Заметим, что $\mathbf{a}_t[w] = \mathbf{c}[w]$ для всех переменных $w \ne v^l$. Если множество $D'_{p,t} = \{\mathbf{b}^1_t, \ldots, \mathbf{b}^{n_t}_t\}$ таково, что $\{\mathbf{b}^1_t[v^l], \ldots, \mathbf{b}^{n_t}_t[v^l]\} = H_p$ (см. шаг 5.2.4), то $\mathbf{c} = \mathbf{d}(\mathbf{a}, \mathbf{b}^i_t, \mathbf{b}^j_t)$, где $\mathbf{b}^i_t[v^j] = \mathbf{a}[v^j]$, $\mathbf{b}^j_t[v^j] = \mathbf{c}[v^j]$. Отсюда существуют $y^1_t, \ldots, y^{n_t}_t$ такие, что $\mathbf{c} = \mathbf{b}^k_{p,t} + K^{k-1}(\mathbf{c}) \cdot B^{k-1}_{H_p,t} + \ldots + K^{l+1}(\mathbf{c}) \cdot B^{l+1}_{H_p,t} + y^1_t \mathbf{b}^1_t + \ldots + y^{n_t}_t \mathbf{b}^{n_t}_t$. А именно, $y^i_t = -1$, $y^j_t = 1$ и $y^m_t = 0$ для прочих m. Если $|D'_{p,t}| = 1$, то $\mathbf{c} = \mathbf{a}$ и $y^1_t = 0$.

Обратно, если условия леммы верны, то для любого $1 \le t \le q$ кортеж $\mathbf{c}|_{\mathbf{s}^l_t}$ может быть представлен в виде $\mathbf{b}^k_{p,t}|_{\mathbf{s}^l_t} + K^{k-1}(x) \cdot B^{k-1}_{H_p,t}|_{\mathbf{s}^l_t} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{H_p,t}|_{\mathbf{s}^l_t} + y^1_t \mathbf{b}^1_t|_{\mathbf{s}^l_t} + \ldots + y^{n_t}_t \mathbf{b}^{n_t}_t|_{\mathbf{s}^l_t}$. Каждый кортеж, встречающийся в этом разложении, принадлежит ϱ^l_t, следовательно, кортеж $\mathbf{c}|_{\mathbf{s}^l_t}$ также принадлежит ϱ^l_t, а значит $\mathbf{c}$ является решением $\mathcal{P}^l$.

Из леммы 5.2 следует, что кортеж $\mathbf{c}$ является решением задачи $\mathcal{P}^l$ тогда и только тогда, когда его почти стандартное разложение в базисах $B_{H_p,t}$, $1 \le t \le q$, образует решение системы $(*)$. Покажем теперь, как система $(*)$ может быть преобразована к системе линейных уравнений над некоторой абелевой группой.

Для каждой переменной $w \in V^l$, $w \ne v^l$ каждое уравнение из $(*)$ выполнено для любых $K^{k-1}(x), \ldots, K^{l+1}(x)$ и $y^1_1, \ldots, y^{n_q}_q$ всякий раз, когда указанные последовательности являются почти стандартными координатами. В самом деле, мы имеем $\mathbf{c}_{t_1}[w] = \mathbf{c}_{t_2}[w]$ для любого кортежа $\mathbf{c} \in B_{H_p}$, любых $t_1, t_2 \in \{1, \ldots, q\}$ и $w \ne v^l$ (напомним, что для кортежа $\mathbf{c} \in B_{H_p}$ через $\mathbf{c}_t$ обозначается кортеж из $B_{H_p,t}$ такой, что $\mathbf{c}_t{\uparrow}^{l+1} = \mathbf{c}$ и $\mathbf{c}_t|_{\mathbf{s}^l_t} \in \varrho^l_t$). Следовательно, $\big(\mathbf{b}^k_{p,t_1} + K^{k-1}(x) \cdot B^{k-1}_{H_p,t_1} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{H_p,t_1}\big)[w] = \big(\mathbf{b}_{p,t_2} + K^{k-1}(x) \cdot B^{k-1}_{p,t_2} + \ldots + K^{l+1}(x) \cdot B^{l+1}_{p,t_2}\big)[w]$. Обозначим кортеж, стоящий в обоих частях этого равенства, через $\mathbf{b}[w]$ и элементы $\mathbf{b}^1_1[w] = \ldots = \mathbf{b}^{n_1}_1[w] = \mathbf{b}^1_2[w] = \ldots = \mathbf{b}^{n_q}_q[w]$ через z. Тогда для любого

$t \in \{1,\dots,q\}$ выражение в правой (левой при $t = 1$) части равенства равно $\mathbf{b}[w]+y_t^1 z+\ldots+y_t^{n_t} z = \mathbf{d}(\ldots(\mathbf{d}(\mathbf{b}[w],z,z),\ldots),z,z) = \mathbf{b}[w]$. Таким образом, для любой переменной $w \neq v^l$ система $(*)$ истинна при любом значении x.

Далее, для любого t и любого кортежа $\mathbf{a} \in B_{H_p,t} \cup D'_{p,t}$ элемент $\mathbf{a}[v^l]$ принадлежит H_p. Пусть $B_{H_p,t} = \{\mathbf{a}_t^1,\dots,\mathbf{a}_t^m\}$, $D'_{p,t} = \{\mathbf{b}_t^1,\dots,\mathbf{b}_t^{n_t}\}$ и $a_t^i = \mathbf{a}_t^i[v^l]$, $b_t^j = \mathbf{b}_t^j[v^l]$. Пусть также $(K^{k-1}(x),\dots,K^{l+1}(x)) = (x_2,\dots,x_{m-1})$. Поскольку l-ая итерация имеет тип **2**, мальцевская операция $\mathbf{d}$ на H_p является операцией $\mathbf{d}(x,y,z) = x-y+z$ абелевой группы $\mathbb{H} = (H_p;\mathbf{d}(x,a,y),\mathbf{d}(a,x,a),a)$, где $a \in H_p$ — произвольный элемент. Тогда каждое уравнение системы $(*)$ может быть переписано в виде

$$\begin{aligned} &a_1^1 + x_2 a_1^2 + \ldots + x_m a_1^m + y_1^1 b_1^1 + \ldots + y_1^{n_1} b_1^{n_1} \\ = \;\; &a_t^1 + x_2 a_t^2 + \ldots + x_m a_t^m + y_t^1 b_t^1 + \ldots + y_t^{n_t} b_t^{n_t}. \end{aligned}$$

Наконец, система $(*)$ сводится к системе

$$\begin{aligned} &x_2(a_1^2 - a_2^2) + \ldots + x_m(a_1^m - a_2^m) + y_1^1 b_1^1 + \ldots + y_1^{n_1} b_1^{n_1} \\ &\qquad + y_2^1 b_2^1 + \ldots + y_2^{n_2} b_2^{n_2} = a_2^1 - a_1^1, \\ &\qquad\qquad \vdots \\ &x_1(a_1^2 - a_q^2) + \ldots + x_m(a_1^m - a_q^m) + y_1^1 b_1^1 + \ldots + y_1^{n_1} b_1^{n_1} \\ &\qquad + y_q^1 b_q^1 + \ldots + y_q^{n_q} b_q^{n_q} = a_q^1 - a_1^1. \end{aligned} \qquad (**)$$

5.1.3 Выбор базиса пространства решений системы линейных уравнений

Для каждого решения $(x_2,\dots,x_m,y_1^1,\dots,y_q^{n_q})$ системы $(**)$ и любого $1 \leq t \leq q$ компоненты кортежа $(x_2,\dots,x_m,y_t^1,\dots,y_t^{n_t})$ являются почти стандартными координатами некоторого решения задачи $\mathcal{P}^l$, представленного в виде $\mathbf{a}_1^1 + x_2 \cdot \mathbf{a}_1^2 + \ldots + x_m \cdot \mathbf{a}_1^m + y_1^1 \cdot \mathbf{b}_1^1 + \ldots y_1^{n^1} \cdot \mathbf{b}_1^{n_1}$. Таким образом, мы должны найти множество решений системы $(**)$, соответствующее кортежам, образующим стандартный базис множества решений. Множество кортежей, почти стандартные координаты которых в базисах $B_{H_p,t} \cup D'_{p,t}$ удовлетворяют уравнениям системы $(*)$ мы будем обозначать через $\mathcal{S}_L$, а стандартный базис этого множества через $\widetilde{B}$. Напомним, что для базиса

$B \subseteq \prod_{v\in V^l} \mathbb{A}_v^l$ множество $B\!\upharpoonright^{l+1}$ является базисом множества решений $\mathcal{S}^{l+1}$, и $\mathbf{a}|_{\mathbf{s}_1^l} \in \varrho_1^l$ для каждого $\mathbf{a} \in B$.

Прежде всего мы строим систему линейных уравнений L' вида $(**)$, как описано в предыдущем разделе и дополняем ее уравнениями вида $x_1 + \ldots + x_m = 0$ для каждого $l \le j < k$ и каждого $1 \le t \le s$, где $B_1^j, \ldots, B_s^j$ являются частями базиса, соответствующего j-ой итерации, а $K_t^j(x) = (x_1, \ldots, x_m)$. Полученная система обозначается через L''. Пусть D обозначает базис множества ее решений, которое является смежным классом в некоторой прямой степени кольца целых чисел. Если эта система несовместна, то системы L' и L также несовместны и задача решений не имеет. В противном случае мы строим базис $\widetilde{B}$, последовательно вычисляя его части. Для $\widetilde{B}^k = \{\mathbf{a}\}$ полагаем $\mathbf{a} = K^k \cdot B^k + \ldots + K^l \cdot B^l$, K — произвольный кортеж из D.

Далее для каждого $l < j < k$ обозначаем через Π смежный класс, натянутый на множество $\{(K^k, \ldots, K^{j+1}) : K \in D\}$, через $H_1', \ldots, H_{s'}'$ — классы конгруэнции $\mu_{v^j}^j$ и полагаем $B^j = B_1^j \cup \ldots \cup B_{s'}^j$. Для каждого класса $H_{p'}'$ проделываем следующие операции. Напомним, что базис $B_{H_{p'}'}$ множества $\mathcal{S}_{H_{p'}'}$, т.е. подмножества из $\mathcal{S}^l\!\upharpoonright^j$, состоящего из кортежей $\mathbf{a}$, удовлетворяющих условию $\mathbf{a}[v^j] \in H_{p'}'$, уже известен. Пусть $D_{p'}$ — множество кортежей $\{(K^k(\mathbf{a}), \ldots, K^{j+1}(\mathbf{a})) : \mathbf{a} \in B_{H_{p'}'}\}$, где $K(\mathbf{a})$ являются координатами кортежа $\mathbf{a}$ в базисе B. Координаты кортежей, являющихся решениями L и приналежащих $\mathcal{S}_{H_{p'}'}$, будут вектора из пересечения множества Π и смежного класса, натянутого на $D_{p'}$. Найдем базис $\overline{D}_{p'}$ этого пересечения.

Если пересечение пусто, то полагаем $\widetilde{B}_{p'}^j = \emptyset$. В противном случае пусть $B_{p'}^j = \{\mathbf{b}^1, \ldots, \mathbf{b}^n\}$. Мы выбираем произвольный кортеж $(K_0^k, \ldots, K_0^{j+1}) \in \overline{D}_{p'}$ и находим множество $\overline{\overline{D}}_{p'}$ кортежей $K = (K^k, \ldots, K^{j+1}, K^j)$ из множества частичных решений системы L'', которые имеют вид $K^k = K_0^k, \ldots, K^{j+1} = K_0^{j+1}, K_r^j = (0, \ldots, 0)$ для всех $r \ne p'$. При этом $K_{p'}^j = (x_1, \ldots, x_n)$ таков, что $x_1 = 0$ при $n = 1$, а в случае $n > 1$ найдется $1 \le u \le n$ такой, что $x_i = 1$ при $i = u$, $x_i = -1$ при $i = u'$ и $x_i = 0$ в остальных случаях, где u' удовлетворяет условию $(K^k \cdot B^k + \ldots + K^{j+1} \cdot B^{j+1})[v^j] = \mathbf{b}^{u'}[v^j]$. Наконец, полагаем

$\widetilde{B}^j_{p'} = \{K^k \cdot B^k + \ldots + K^l \cdot B^l : K \in \overline{\overline{D}}_{p'}\}$.

Если $\widetilde{B}^k, \ldots, \widetilde{B}^{l+1}$ уже найдены, то выбираем кортеж $\mathbf{a}$ из объединения этих множеств и находим базис D^l подпространства пространства решений системы L'', состоящего из кортежей $\mathbf{b}$ с условием $K^k(\mathbf{b}) = K^k(\mathbf{a}), \ldots, K^{l+1}(\mathbf{b}) = K^{l+1}(\mathbf{a})$. Для $E = \{K^k \cdot B^k + \ldots + K^l \cdot B^l \colon K \in D^l\}$ множество $M = \{a \in \mathbb{A}^l_{v_l} \colon a = \mathbf{a}[v^l],\ \mathbf{a} \in E\}$ является подмножеством из H_p. Теперь $\widetilde{B}^l$ может быть выбрано равным $\{\mathbf{b} \colon \mathbf{b}[v^l] \in M,\ \mathbf{b}|_{V^l - \{v^l\}} = \mathbf{b}|_{V^l - \{v^l\}}\}$.

Мы завершаем этот раздел доказательством того, что множество $\widetilde{B}$ действительно является стандартным базисом множества $\mathcal{S}_L$.

Лемма 5.3. *Множество $\widetilde{B}$, полученное с помощью описанного выше алгоритма, является стандартным базисом множества $\mathcal{S}_L$.*

Доказательство. По определению, для любого кортежа $\mathbf{a} \in \mathcal{S}_L$ почти стандартные координаты $K(\mathbf{a})$ соответствуют некоторому решению системы L. Поскольку почти стандартные координаты удовлетворяют дополнительным уравнениям, системы L' и L'' имеют одни и те же решения, компоненты которых являются почти стандартными координатами некоторых кортежей. Более того, как показано в разделе 5.1.2, системы L и L' эквивалентны. Следовательно, обозначая множество кортежей, соответствующих решениям системы L'', через $\mathcal{S}_{L''}$, мы получаем $\mathcal{S}_L = \mathcal{S}_{L''}$.

Теперь мы покажем, что для любого $k \geq j \geq l$ множество $(\widetilde{B}^k \cup \ldots \cup \widetilde{B}^j){\uparrow}^j$ является стандартным базисом множества $\mathcal{S}_L{\uparrow}^j$. Это, очевидно, верно для $j = k$, что образует базу индукции. Предположим, что требуемое свойство верно для $j+1$. Для каждого класса $H_{p'}$ конгруэнции $\mu^j_{v^j}$ множество $\widetilde{B}^j_{p'}$ может быть выбрано как произвольное множество, удовлетворяющее условию: $\widetilde{B}^j_{p'}{\uparrow}^j$ имеет вид $\{\mathbf{a}_b : b \in H_{p'},\ b$ является v^j-ой компонентой кортежа из $\mathcal{S}_L{\uparrow}^j\}$ для некоторого $\mathbf{a} \in \mathcal{S}_L{\uparrow}^j$, где $\mathbf{a}_b[w] = b$ если $w = v^j$, $\mathbf{a}_b[w] = \mathbf{a}[w]$ в противном случае. Из построения нетрудно понять, что $\widetilde{B}^j_{p'}$ и в самом деле имеет требуемый вид.

5.2 Нахождение базиса подалгебры

В этом разделе мы опишем метод поиска стандартного базиса $\overline{B}$ множества $\mathcal{S}_{\mathbb{B}} = \{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i\colon \mathbf{a}\big|_J \in \mathbb{B}\}$ кортежей $\mathbf{a}$ из $\mathcal{S}^l$, таких что $\mathbf{a}\big|_J$ принадлежит подалгебре $\mathbb{B}$ из $\prod_{u\in J}\mathbb{A}^i_u$, $l-1 \le i \le k$, $J \subseteq V^i$. Сначала мы сделаем это, предполагая $\mathbb{B} = \{\mathbf{c}\}$ (иными словами, для каждого элемента из $\mathbb{B}$), а затем преобразуем объединение найденных базисов, как это указано в разделе 5.4.

Пусть $J^m = J{\uparrow}^m$ для $i \le m \le k$ и $\mathbf{c}_m = \mathbf{c}{\uparrow}^m$ для $i \le m \le k$. Через $\mathcal{S}_{\mathbf{c}}$ обозначим множество $\{\mathbf{a} \in \mathcal{S}^l{\uparrow}^i\colon \mathbf{a}\big|_J = \mathbf{c}\}$, а через $\mathcal{T}^m_{\mathbf{c}}$ — множество $\{\mathbf{a} \in \mathcal{S}^l{\uparrow}^m\colon \mathbf{a}\big|_{J^m} = \mathbf{c}_m\}$ если $m > i$ и $\mathcal{T}^m_{\mathbf{c}} = \mathcal{S}_{\mathbf{c}}$ если $m = i$. Как и ранее базис $D_{\mathbf{c}}$ множества $\mathcal{S}_{\mathbf{c}}$ строится индуктивно. База индукции задается равенством $D^k_{\mathbf{c}} = B^k{\uparrow}^k$. Далее, если базис $\overline{D}_{\mathbf{c}}$ множества $\mathcal{T}^{m+1}_{\mathbf{c}}$, $i \le m < k$, уже найден, то мы выполняем следующее. Прежде всего находим представителя $\mathbf{a}' \in \mathcal{S}^l{\uparrow}^m$ для каждого $\mathbf{a} \in \overline{D}_{\mathbf{c}}$, т.е. $\mathbf{a}'{\uparrow}^{m+1} = \mathbf{a}$. Например, $\mathbf{a}' = K^k(\mathbf{a}) \cdot B^k{\uparrow}^m + \ldots + K^{m+1}(\mathbf{a}) \cdot B^{m+1}{\uparrow}^m$, где $K^k(\mathbf{a}), \ldots, K^{m+1}(\mathbf{a})$ — координаты $\mathbf{a}$ в базисе $B{\uparrow}^{m+1}$. Множество всех выбранных кортежей будет обозначаться через $\widetilde{D}_{\mathbf{c}}$.

Пусть $H_1, \ldots, H_s$ — классы конгруэнции $\mu^m_{v^m}$, для которых $H_p \cap \widetilde{D}_{\mathbf{c}}\big|_{\{v^m\}} \ne \emptyset$. Для каждого $1 \le p \le s$, выберем $\mathbf{a}_p \in \widetilde{D}_{\mathbf{c}}$ такой, что $\mathbf{a}_p[v^m] \in H_p$ (см. раздел 5.3). Предположим сначала, что $v^m \notin J^m$. Если m-ая итерация имеет тип **3**, то новое значение $\overline{D}_{\mathbf{c}}$ может быть выбрано равным $\widetilde{D}_{\mathbf{c}} \cup E_1 \cup \ldots \cup E_s$, где $E_p = \{\mathbf{a}_b\colon b \in H_p\}$ и $\mathbf{a}_b[w] = b$ если $w = v^m$ и $\mathbf{a}_b[w] = \mathbf{a}^p[w]$ в противном случае. По лемме 3.3 $\overline{D}_{\mathbf{c}} \subseteq \mathcal{S}^l{\uparrow}^m$. Если m-ая итерация имеет тип **2**, то полагаем $D^m = D^m_1 \cup \ldots \cup D^m_s$, где $D^m_p = \{\mathbf{a}'^{\,1}_p, \ldots, \mathbf{a}'^{\,k_p}_p\}$, $\mathbf{a}'^{\,j}_p = \mathbf{d}(\mathbf{a}_p, \mathbf{a}^1_p, \mathbf{a}^j_p)$, и $\{\mathbf{a}^1_p, \ldots, \mathbf{a}^{k_p}_p\} = B^m_p$ является частью базиса B_{H_p} множества $\mathcal{S}_{H_p}$, а также $\mathbf{a}^1_p[v^m] = \mathbf{a}_p[v^m]$. Наконец, мы заменяем $\overline{D}_{\mathbf{c}}$ множеством $\widetilde{D}_{\mathbf{c}} \cup D^m$. Поскольку $m \ge i$, базис множества $\mathcal{S}_{H_p}$ уже известен, см. шаг 5.3 алгоритма из раздела 4.3. Так как для любых $\mathbf{a} \in D^m_p$ имеем $\mathbf{a}\big|_{J^m} = \mathbf{a}_p\big|_{J^m} = \mathbf{c}_m$, имеем $D^m_p \subseteq \mathcal{T}^m_c$ для всех p.

Пусть теперь $v^m \in J^m$. Если m-ая итерация имеет тип **3**, то $D_{\mathbf{c}} = \{\mathbf{a}' \mid \mathbf{a} \in \widetilde{D}_{\mathbf{c}}\}$, где $\mathbf{a}'[w] = \mathbf{c}_m[v^m]$ если $w = v^m$ и $\mathbf{a}'[w] = \mathbf{a}[w]$ в противном случае. Вновь по лемме 3.3 каждый кортеж $\mathbf{a}'$ принадлежит $\mathcal{T}^m_{\mathbf{c}}$.

Если m-ая итерация имеет тип **2**, то пусть H_p — класс конгруэнции $\mu^m_{v^m}$, содержащий $\mathbf{c}_m[v]$. Заметим, что $\prod_{v\in J_m}\mathbb{A}^m_v$ является гомоморфным образом алгебры $\prod_{u\in J}\mathbb{A}^i_u$, а следовательно "маленькой" алгеброй, для которой вся необходимая информация известна. Поэтому мы можем найти $\mathbf{a}\in\mathbb{S}^m$ такой, что $\mathbf{a}\big|_{J^m}=\mathbf{c}_m\big|_{J^m}$. Положим $E_p=\{\mathbf{a}'^1,\ldots,\mathbf{a}'^n\}$, где $\mathbf{a}'^j=\mathbf{d}(\mathbf{a},\mathbf{a}^1_p,\mathbf{a}^j_p)$ и $\{\mathbf{a}^1_p,\ldots,\mathbf{a}^n_p\}=B^m_{H_p}$ (поскольку $m\geq i$, базис множества $\mathbb{S}_{H_p}$ уже найден), и решим уравнение $K^k(x)\cdot\widetilde{D}^k_{\mathbf{c}}[v^m]+\ldots+K^{m+1}(x)\cdot\widetilde{D}^{m+1}_c[v^m]+y_1\mathbf{a}'^1[v^m]+\ldots+y_n\mathbf{a}'^n[v^m]=\mathbf{c}_m[v^m]$, где $\widetilde{D}_{\mathbf{c}}=\widetilde{D}^k_{\mathbf{c}}\cup\ldots\cup\widetilde{D}^{m+1}_{\mathbf{c}}$. Пусть $D_{\mathbf{c}}$ — стандартный базис множества его решений.

Уравнение из предыдущего абзаца может быть решено следующим образом. Обозначим $\mathbf{c}_m[v^m]$ через c и для $\mathbf{a}'^i\in E_p$ обозначим $\mathbf{a}'^i[v^m]$ через a'_i. Так же как и в разделе 5.1.2 это уравнение может быть сведено к линейному уравнению $x_2b_2+\ldots+x_rb_r+y_1a'_1+\ldots+y_na'_n=c-b_1$, где $\{b_1\}=\widetilde{D}^k_{\mathbf{c}}[v^m]$, $\{\mathbf{b}_2,\ldots,\mathbf{b}_r\}=\widetilde{D}^{k-1}_{\mathbf{c}}\cup\ldots\cup\widetilde{D}^{m+1}_{\mathbf{c}}$. Далее это уравнение может быть решено аналогично системе из раздела 5.1.3. Заметим еще, что в процессе нахождения стандартного базиса пространства решений системы линейных уравнений алгоритм из раздела 5.1.3 использует базисы множеств вида $\mathbb{S}_{\mathbb{C}}$. Однако это не приводит к недоразумениям, поскольку $\mathbb{C}$ является подалгеброй алгебры $\mathbb{A}^j_v$ для некоторой переменной $v\in V^j$, где $j>i$, и, следовательно, базис множества $\mathbb{S}_{\mathbb{C}}$ уже известен.

Нетрудно проверить, что множество $\overline{B}$, полученное данным алгоритмом для данного $l-1\leq i\leq k$, множества $J\subseteq V^i$ и подалгебры $\mathbb{B}$ из $\prod_{u\in J}\mathbb{A}^i_u$, является стандартным базисом множества $\mathbb{S}_{\mathbb{B}}$.

5.3 Нахождение представителя подалгебры и разложение по базису

Даны кортежи $\mathbf{a}_1,\ldots,\mathbf{a}_n$ из $\mathbb{A}^l$, множество $J\subseteq V^l$ и кортеж $\mathbf{a}\in\mathbb{B}=\prod_{u\in J}\mathbb{A}^l_u$. Требуется найти кортеж $\mathbf{b}$ из алгебры, порожденной кортежами $\mathbf{a}_1,\ldots,\mathbf{a}_n$, такой, что $\mathbf{b}\big|_J=\mathbf{a}$.

Заметим, что за линейное время может быть проверено, принадлежит ли элемент $\mathbf{a}$ подалгебре из $\mathbb{B}$, порожденной $\mathbf{a}_1\big|_J,\ldots,\mathbf{a}_n\big|_J$. Более того, в случае, когда $\mathbf{a}$ принадлежит этой подалгебре, терм $f(\mathbf{a}_1\big|_J, \ldots, \mathbf{a}_n\big|_J) = \mathbf{a}$, выражающий этот элемент, также может быть найден за линейное время. Следовательно, в качестве искомого может быть выбран кортеж $\mathbf{b} = f(\mathbf{a}_1, \ldots, \mathbf{a}_n)$.

Чтобы найти стандартные координаты заданного кортежа $\mathbf{a} \in \mathbb{A}^l$ в данном базисе B множества решений $\mathbb{S}^l$, мы строим последовательные приближения $\mathbf{a}$, используя начальные части $B^k, \ldots, B^m$ базиса. В качестве начального приближения выбираем $\mathbf{b}$, где $B^k = \{\mathbf{b}\}$, и $K^k(\mathbf{a}) = (1)$. Если $K^k(\mathbf{a}), \ldots, K^{m+1}(\mathbf{a})$ уже построены, то вычисляем очередное приближение $\mathbf{a}' = \mathbf{b}{\upharpoonright}^m + K^{k-1}(\mathbf{a}) \cdot B^{k-1}{\upharpoonright}^+ \ldots + K^{m+1}(\mathbf{a}) \cdot B^{m+1}{\upharpoonright}^m$. Предположим, что $H_1, \ldots, H_s$ — классы конгруэнции $\mu^m_{v^m}$. Для каждого $\mathbf{b} \in \mathbb{S}^l$ имеем $\mathbf{b}{\upharpoonright}^m [v^m] \notin \{\mathbf{c}[v^m] \colon \mathbf{c} \in B^m{\upharpoonright}^m\}$. Поэтому если $\mathbf{a}{\upharpoonright}^m [v^m]$ не принадлежит этому множеству, то $\mathbf{a} \notin \mathbb{S}^l$. В противном случае пусть $\mathbf{a}{\upharpoonright}^m [v^m] \in H_p$. Если $|B^m_p| = 1$ и $\mathbf{a}{\upharpoonright}^m \neq \mathbf{a}'$, то вновь $\mathbf{a} \notin \mathbb{S}^l$. В остальных случаях, если $\mathbf{a}{\upharpoonright}^m [v^m] = \mathbf{a}'[v^m]$, полагаем $K^m_j(\mathbf{a}) = (0, \ldots, 0)$ для всех j. Если это не так, то $K^m_p(\mathbf{a}) = (x_1, \ldots, x_m)$, где $H_p = \{a_1, \ldots, a_m\}$, и $x_i = 1$ если $a_i = \mathbf{a}{\upharpoonright}^m [v^m]$, $x_i = -1$ если $a_i = \mathbf{a}'{\upharpoonright}^m [v^m]$, $x_i = 0$ в остальных случаях. Для $i \neq p$ полагаем $K^m_i(\mathbf{a}) = (0, \ldots, 0)$. Корректность алгоритма вытекает из определения базиса.

5.4 Преобразование базиса

В этом разделе мы представим метод поиска по стандартным базисам $E_1, \ldots, E_u$ некоторых подалгебр из $\mathbb{A}^l$ базиса B подалгебры, порожденной множеством $E_1 \cup \ldots \cup E_s$. Этот метод используется в двух случаях: шаг 5.2.6 алгоритма из раздела 4.3, а также в разделе 5.2. В первом случае базисы $E_1, \ldots, E_u$ удовлетворяют условию $\{\mathbf{a}[v] \colon \mathbf{a} \in E\} = \mathbb{A}^l_v$, где $E = E_1 \cup \ldots \cup E_u$, во втором случае базис множества $\mathbb{S}^l$ известен.

Как обычно, базис строится индуктивно. Положим $B^k = E^k_1$. Предположим, что множества $B^k, \ldots, B^{j+1}$ уже найдены и $B^k \cup \ldots \cup B^{j+1} = \{\mathbf{b}_1, \ldots, \mathbf{b}_r\}$. Пусть $H_1, \ldots, H_s$ — классы конгруэнции $\mu^j_{v^j}$ и $\overline{E}^j = \bigcup_{1 \le i \le u} E^j_i$. Для каждого $1 \le p \le s$ пусть $E'_p = \{\mathbf{a} \in \overline{E}^j \colon \mathbf{a}{\upharpoonright}^j [v^j] \in H_p\}$ и пусть $\mathbf{a}_1, \ldots, \mathbf{a}_t$ — список элементов этого множества. Через $\mathbf{a}_i{\upharpoonright}^{j+1}=$

$f_i(\mathbf{b}_1{\upharpoonright}^{j+1}, \ldots, \mathbf{b}_r{\upharpoonright}^{j+1})$ мы обозначаем разложение кортежа $\mathbf{a}_i{\upharpoonright}^{j+1}$ по базису $(B^k \cup \ldots \cup B^{j+1}){\upharpoonright}^{j+1}$, пусть также $\mathbf{a}_i' = f_i(\mathbf{b}_1{\upharpoonright}^j, \ldots, \mathbf{b}_r{\upharpoonright}^j)$, $\mathbf{a}_i'' = f_i(\mathbf{b}_1, \ldots, \mathbf{b}_r)$.

Если $\mathcal{S}^j$ не является v^j-прямоугольным по модулю $\mu^j_{v^j}$, т.е. для всех $i \in \underline{t}$ справедливо $\mathbf{a}_i{\upharpoonright}^j = \mathbf{a}_i'$, то можно принять $B^j_p = \{\mathbf{b}\}$, где $\mathbf{b}$ — произвольный кортеж из B^{j+1} такой, что $\mathbf{b}{\upharpoonright}^j [v_j] \in H_p$ (такой кортеж существует по определению базиса).

В противном случае для некоторого i имеем $\mathbf{a}_i \upharpoonright^j [v^j] \neq \mathbf{a}_i'[v^j]$ (без ограничения общности можно считать, что $i = 1$). Пусть C — подалгебра из $\mathbb{A}^j_{v^j}$, порожденная элементами $\{\mathbf{a}_1 \upharpoonright^j [v^j], \ldots, \mathbf{a}_t \upharpoonright^j [v^j]\}$. Если $\{\mathbf{a}[v] \colon \mathbf{a} \in E\} = \mathbb{A}^l_v$ для всех $v \in V^l$, то положим $a = \mathbf{a}_1{\upharpoonright}^j [v^j]$, $a' = \mathbf{a}_1'{\upharpoonright}^j [v^j]$. По предложению 3.2 для любого элемента $c \in C$ найдется термальная операция $f_c(x, y_1, \ldots, y_m)$ и элементы $e_1, \ldots, e_m \in \mathbb{A}^j_{v^j}$ такие, что $f_c(a, e_1, \ldots, e_m) = a, f_c(a', e_1, \ldots, e_m) = c$. Поскольку $e_1, \ldots, e_m$ принадлежат множеству $\{\mathbf{b} \upharpoonright^j [v^j] \colon \mathbf{b} \in E\}$, найдутся кортежи $\mathbf{e}_1, \ldots, \mathbf{e}_m \in E$, удовлетворяющие условию $\mathbf{e}_i[v^j] = e_i$. Пусть теперь $\mathbf{b}_1 = (a, \mathbf{b}') = f_c(\mathbf{a}_1 \upharpoonright^j, \mathbf{e}_1 \upharpoonright^j, \ldots, \mathbf{e}_m \upharpoonright^j) = f_c((a, \overline{\mathbf{a}}_1), (e_1, \mathbf{e}_1'), \ldots, (e_m, \mathbf{e}_m'))$; $\mathbf{b}_2 = (c, \mathbf{b}') = f_c(\mathbf{a}_1' \upharpoonright^j, \mathbf{e}_1 \upharpoonright^j, \ldots, \mathbf{e}_m \upharpoonright^j) = f_c((a', \overline{\mathbf{a}}_1), (e_1, \mathbf{e}_1'), \ldots, (e_m, \mathbf{e}_m'))$; $\mathbf{b}_1'' = f_c(\mathbf{a}_1, \mathbf{e}_1, \ldots, \mathbf{e}_m)$; $\mathbf{b}_2'' = f_c(\mathbf{a}_1', \mathbf{e}_1, \ldots, \mathbf{e}_m)$; $\mathbf{a}_c = (c, \overline{\mathbf{a}}_1) = \mathbf{d}(\mathbf{a}_1{\upharpoonright}^j, \mathbf{b}_1, \mathbf{b}_2) = \mathbf{d}((a, \overline{\mathbf{a}}_1), (a, \mathbf{b}'), (c, \mathbf{b}'))$; $\mathbf{a}_c'' = \mathbf{d}(\mathbf{a}_1, \mathbf{b}_1'', \mathbf{b}_2'')$. Наконец, $B^j_p = \{\mathbf{a}_c'' \colon c \in C_p\}$.

Если мы находимся в ситуации раздела 5.2 и стандартный базис $\overline{B}$ множества $\mathcal{S}^l$ известен, то для каждого $c \in C$ полагаем $\mathbf{c}_c = \mathbf{d}(\mathbf{a}_1, \overline{\mathbf{b}}_b, \overline{\mathbf{b}}_c)$, где $\overline{\mathbf{b}}_b, \overline{\mathbf{b}}_c \in \overline{B}^j_p$ таковы, что $\mathbf{b}_b{\upharpoonright}^j [v^j] = \mathbf{a}_1{\upharpoonright}^j [v^j]$, $\mathbf{b}_c{\upharpoonright}^j [v^j] = c$. Наконец, $B^j_p = \{\mathbf{c}_c \colon c \in C\}$.

5.5 Корректность и вычислительная сложность

Алгоритм, описанный выше, для произвольной частной задачи $\mathcal{P} \in \mathrm{CSP}(\mathcal{A})$ выдает некоторое множество $B \subseteq \prod_{v \in V} \mathbb{A}_v$. Осталось доказать, что B является стандартным базисом множества решений такой задачи $\mathcal{P}$.

Предложение 5.1. *Множество B, полученное с помощью алгоритма, описанного в разделах 4,5, для частной задачи $\mathcal{P} \in \mathrm{CSP}(\mathcal{A})$, является стандартным базисом множества решений $\mathcal{S}$ задачи $\mathcal{P}$.*

Доказательство. Рассмотрим алгоритм построения базиса из раздела 4.3. Корректность его подпрограмм была проверена в разделах 5.1–5.4. Ясно, что для доказательства корректности самого алгоритма достаточно показать, что множество $B^k \cup \ldots \cup B^l$, полученное на l-ой итерации является стандартным базисом множества решений $\mathcal{S}^l$ задачи $\mathcal{P}^l$ для каждого $1 \leq l \leq k$. Заметим прежде всего, что процедура планирования не изменяет множество решений первоначальной задачи, поскольку установление 3-согласованности не изменяет это множество. В частности, если $\mathcal{P}$ имеет решение, то $\mathcal{P}^k$ имеет решение. Если это так, то, очевидно, множество B^k является стандартным базисом множества $\mathcal{S}^k$. В противном случае, если $\mathcal{P}^k$ несовместна, то алгоритм выдает “НЕТ”, что и требовалось.

Если $\mathcal{P}^{l+1}$ несовместна, то $\mathcal{P}^l$ также не имеет решения. Предположим поэтому, что множество $\overline{B}^k \cup \ldots \cup \overline{B}^{l+1}$, полученное на $l+1$-ой итерации, является стандартным базисом множества $\mathcal{S}^{l+1}$, и докажем, что $B^k \cup \ldots \cup B^l$, полученное на l-ой итерации, является стандартным базисом $\mathcal{S}^l$.

Случай 1. l-ая итерация имеет тип **3**.
По предложению 3.3, для любого кортежа $\mathbf{a} \in B^k \cup \ldots \cup B^l$ и любого $1 \leq t \leq q$ имеем $\mathbf{a}|_{\mathbf{s}_t^l} \in \varrho_t^l$. Таким образом, $B^k \cup \ldots \cup B^l \subseteq \mathcal{S}^l$.

Обратно, если $\mathbf{a} \in \mathcal{S}^l$, то $\mathbf{a}{\uparrow}^{l+1} \in \mathcal{S}^{l+1}$. Следовательно, кортеж $\mathbf{a}{\uparrow}^{l+1}$ может быть разложен по базису $(B^k \cup \ldots \cup B^{l+1}){\uparrow}^{l+1}$. Пусть $K'(\mathbf{a}{\uparrow}^{l+1})$ — координаты $\mathbf{a}{\uparrow}^{l+1}$. Полагая $\mathbf{b} = K'(\mathbf{a}{\uparrow}^{l+1}) \cdot (B^k \cup \ldots \cup B^{l+1})$, получаем $\mathbf{b}[w] = \mathbf{a}[w]$ всякий раз, когда $w \neq v^l$ и $(a, b) \in \mu_{v^l}^l$, где $a = \mathbf{a}[v^l], b = \mathbf{b}[v^l]$. Пусть C_p — класс конгруэнции $\mu_{v^l}^l$, содержащий a, b. Тогда $\mathbf{a} = \mathbf{d}(\mathbf{b}, \mathbf{a}_b, \mathbf{a}_a)$ для $\mathbf{a}_b, \mathbf{a}_a \in B_p^l$.

Случай 2. l-ая итерация имеет тип **2**.
В этом случае достаточно проверить, что для каждого $1 \leq p \leq s$ множество E_p образует стандартный базис множества $\mathcal{S}'_p$. Это, однако, непосредственно вытекает из комментариев в разделе 5.2 и лемм 5.2, 5.3.

Далее мы оценим временну́ю сложность этого алгоритма. Пусть $n = |V|$ и пусть m — общее число кортежей в отношениях ограничений, пусть также r — наибольшая арность отноешений ограничений.

Несмотря на то, что число переменных может возрасти в ходе работы алгоритма, это число не превосходит Cn, где C — некоторая константа, зависящая только от класса $\mathcal{A}$ (можно проверить, что в качестве C можно взять наибольшее число конгруэнций в алгебрах из $\mathcal{A}$). Следовательно, число k итераций в процедуре планирования не превосходит $O(n)$. Каждый вызов этой процедуры, кроме самого первого, вызван тем, что некоторый кортеж был удален из некоторого отношения ограничения. Таким образом, процедура планирования и шаги 4,5 алгоритма из раздела 4.3 выполняются не более $m+1$ раз. Процедура планирования — полиномиальный алгоритм, рассмотрим поэтому оставшиеся шаги алгоритма.

В ходе каждой итерации алгоритм выполняет следующие основные действия: (1) решает систему уравнений (если итерация имеет тип **3**, этот шаг относительно прост и его сложностью можно пренебречь), (2) проверяет все кортежи из отношений ограничений, являются ли они частью решения, (3) находит базисы подалгебр определенного типа.

(1) Число кортежей в части стандартного базиса, соответствующей l-ой итерации, не превосходит $|\mathbb{A}^l_{v_l}|$, а значит общее число элементов базиса не превосходит $O(n)$. Следовательно, система уравнений, полученная на шаге 5.2.5 и затем преобразованная в разделе 5.1.2, содержит $O(n)$ переменных, $O(q)$ уравнений, а значит может быть решена за время $O(qn^2)$. В алгоритме из раздела 5.1.3 эта система должна быть решена не более одного раза для каждой части стандартного базиса, т.е. $O(n)$ раз. Таким образом, сложность решения данной системы уравнений есть $O(qn^3)$.

(3) Для каждой переменной существует постоянное число D подалгебр, базис которых требуется найти. Число D зависит только от класса $\mathcal{A}$. Таким образом, на каждой итерации алгоритм должен найти базисы $O(n)$ подалгебр. Чтобы получить базис подалгебры, алгоритм из раздела 5.2 просматривает элементы подалгебры (число которых ограничено константой) и требует $O(n)$ повторений процедуры планирования. Таким образом, общее время, требуемое на этом шаге, полиномиально.

(2) Наконец, алгоритм проверяет какие из m кортежей длины не более r являются частью решения. Для этого он mr раз применяет процедуру

нахождения базиса подалгебры.

Таким образом, общее время работы алгоритма полиномиально.

Список литературы

[1] A.A. Bulatov. Three-element Mal'tsev algebras *Accepted to Acta Sci. Math.*

[2] A.A. Bulatov and P.G. Jeavons. Algebraic approach to multi-sorted constraints. Technical Report PRG-RR-01-18, Computing Laboratory, University of Oxford, UK, 2001.

[3] A.A. Bulatov and P.G. Jeavons. Algebraic structures in combinatorial problems. Technical Report MATH-AL-4-2001, Technische universität Dresden, Germany, 2001.

[4] A.A. Bulatov and P.G. Jeavons. An algebraic approach to multi-sorted constraits. In *Proceedings of CP'03*, 197–202, 2003.

[5] A.A. Bulatov, P.G. Jeavons, and A.A. Krokhin. Classifying complexity of constraints using finite algebras. *SIAM J. of Comp.*, 34, N3 (2005), 720-742.

[6] A.A. Bulatov, P.G. Jeavons, and A.A. Krokhin. Constraint satisfaction problems and finite algebras. In *Proceedings of ICALP'00*, Springer-Verlag, *LNCS*, 1853 (2000), 272–282.

[7] T. Feder. Constraint satisfaction on finite groups with near subgroups. Submitted to J. of Algebra.

[8] T. Feder and M.Y. Vardi. The computational structure of monotone monadic SNP and constraint satisfaction: A study through datalog and group theory. *SIAM J. of Comp.*, 28, N1 (1998), 57–104.

[9] R. Freese and R. McKenzie. *Commutator theory for congruence modular varieties*, *London Math. Soc. Lecture Notes*, 125. London, 1987.

[10] D. Hobby and R.N. McKenzie. *The Structure of Finite Algebras.* American Mathematical Society, Providence, R.I., 1988.

[11] P.G. Jeavons. On the algebraic structure of combinatorial problems. *Theoretical Computer Science*, 200 (1998), 185–204.

[12] P.G. Jeavons, D.A. Cohen, and M. Gyssens. Closure properties of constraints. *J. of the ACM*, 44 (1997), 527–548.

[13] A.K. Mackworth. Consistency in networks of relations. *Artificial Intelligence*, 8 (1977), 99–118.

[14] T.J. Schaefer. The complexity of satisfiability problems. In *Proceedings of STOC'78*, 216–226, 1978.

Булатов Андрей Арнольдович

Кафедра алгебры и дискретной математики

Уральский государственный университет

ул. Ленина 51

г.Екатеринбург, 620083

andrei.bulatov@usu.ru

тел: (343) 350-7579