Московский Государственный Университет
имени М.В. Ломоносова
Российская Академия Наук
Международная Академия Технологических Наук
Российская Академия Естественных Наук

Интеллектуальные Системы.

Теория и приложения

ТОМ **23** ВЫПУСК 2 * **2019**

МОСКВА

ISSN 2411–4448

УДК 519.95; 007:159.955
ББК 32.81

Издается с 1996 г.*

В журнале «Интеллектуальные системы. Теория и приложения» публикуются научные достижения в области теории и приложений интеллектуальных систем, новых информационных технологий и компьютерных наук.

Издание журнала осуществляется под эгидой МГУ им. М. В. Ломоносова, Научного Совета по комплексной проблеме «Кибернетика» РАН, Отделения «Математическое моделирование технологических процессов» АТН РФ, Секции «Информатики и кибернетики» РАЕН.

Учредитель журнала: ООО «Интеллектуальные системы».

Журнал входит в список изданий, включенных ВАК РФ в реестр публикаций материалов по кандидатским и докторским диссертациям по математике и механике.

Спонсором издания является:

ООО «Два Облака»
Разработка корпоративных информационных систем
http://www.dvaoblaka.ru

Индекс подписки на журнал: 64559 в каталоге НТИ «Роспечать».

Адрес редакции: 119899, Россия, Москва, Воробьевы Горы, МГУ, ГЗ, механико-математический факультет, комн. 12-01.
Адрес издателя: 115230, Россия, Москва, Хлебозаводский проезд, д. 7, стр. 9, офис 9. Тел. +7 (495) 939-46-37, e-mail: mail@intsysjournal.org

*) Прежнее название журнала: «Интеллектуальные системы».

ОГЛАВЛЕНИЕ

Часть 1.
Общие проблемы теории интеллектуальных систем

Восстановление нот из двузвучия

Ботхолов А.Ж.

В данной работе рассматривается восстановление нот из одновременного звучания двух нот в терминах амплитуд и частот.

Приведены методы восстановления амплитуд двух нот, которые были одновременно сыграны двумя различными музыкальными инструментами.

Описаны случаи существования и не существования одновременно двух решений для задачи восстановления нот.

Ключевые слова: основной тон, обертон, амплитуда, частота, огибающая ноты, суммарная спектрограмма.

1. Введение

В данной работе рассматривается восстановление нот из двузвучия (одновременного звучания двух нот) в терминах амплитуд и частот. При колебании струны мы можем наблюдать единственный четкий тон звука, который называется основным тоном. Но как известно, большая часть музыкальных инструментов воспроизводит не только основные тона, но также и призвуки, которые называются обертонами, формирующие уникальное звучание для каждого инструмента, поэтому одна и та же нота будет звучать каждый раз уникально при воспроизведении разными инструментами. Обертоны бывают гармоническими и негармоническими. Частоты гармонических обертонов кратны частоте основного тона. Далее будем считать, что в составе звучания ноты, проигрываемой различными инструментами, находятся только гармонические обертоны и основной тон. То есть частоты всех тонов ноты можно записать как набор $(w_0, 2w_0, 3w_0, \ldots, n \cdot w_0)$, где w_0 — частота основного тона, $2w_0$, $3w_0$,..., $n \cdot w_0$ — частоты обертонов.

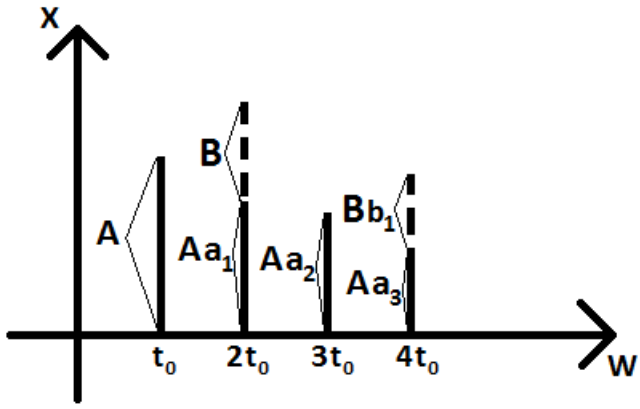
В работе описан случай существования единственного решения для задачи восстановления нот из двузвучия, а также приведен пример, когда возможно существование двух решений.

Автор выражает благодарность проф. Э.Э.Гасанову за постановку задачи.

2. Основные понятия

Пусть A — это амплитуда колебаний основного тона. Каждый i-ый обертон обладает собственной амплитудой колебаний, которая выражается как $a_i \cdot A$, будем считать, что a_i обязательно больше 0. Тогда можем записать амплитуды колебаний всех тонов ноты как набор $(A, a_1 \cdot A, a_2 \cdot A, \ldots, a_n \cdot A)$. Так как все амплитуды кратны A, то можем рассмотреть набор коэффициентов $(1, a_1, a_2, \ldots, a_n)$. Назовем данный набор огибающей ноты.

Допустим, два различных музыкальных инструмента одновременно сыграли по одной произвольной ноте, тогда получаем общий суммарный набор, состоящий из частот тонов от каждой отдельной ноты, а также соответствующие амплитуды, причем некоторые частоты могут как совпадать, так и отличаться. И в случае, если частоты совпали, то амплитуды суммируются. Изобразим пример зависимости частот от амплитуд при звучании одновременно двух нот на графике, где на оси абсцисс отмечены частоты, а на оси ординат амплитуды, обычными линиями изображены амплитуды первой ноты, пунктиром амплитуды второй ноты.



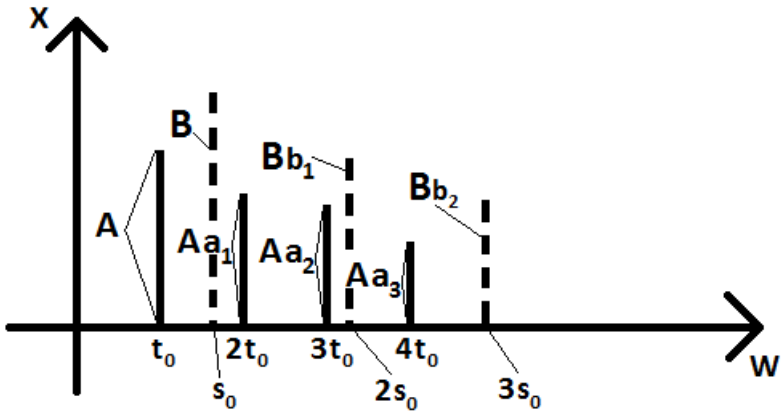
Как можно заметить, в данном примере вторая и четвертая частоты тонов разных нот совпали, поэтому амплитуды у данных частот суммируются. Данный график зависимости частот от амплитуд назовем общей спектрограммой.

3. Существование и единственность решения при вычислении амплитуд в случае конечных огибающих

Теорема 1. *Два различных инструмента одновременно играют по одной ноте. Известны конечные огибающие этих нот, причем отличные друг от друга, также известна суммарная спектрограмма. Тогда существуют единственные амплитуды A и B этих нот, удовлетворяющие данным условиям.*

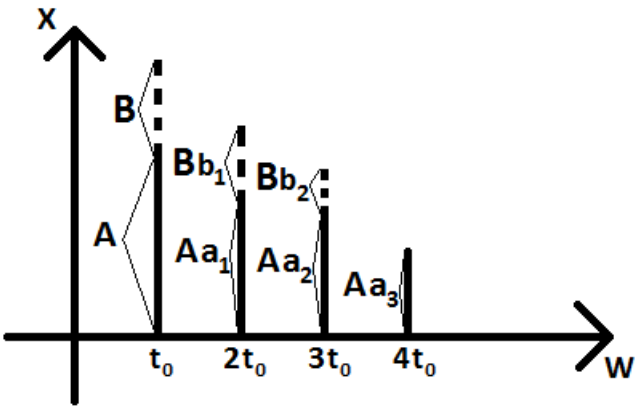
Доказательство. Существование. Обозначим через $(1, a_2, \ldots, a_n)$ огибающую первой ноты, а через $(1, b_2, \ldots, b_m)$ огибающую второй ноты. Также мы знаем суммарную спектрограмму, но не знаем к набору частот какой ноты относится каждая частота на графике. Обозначим через $(t_0, 2t_0, \ldots, n \cdot t_0)$ частоты первой ноты, а через $(s_0, 2s_0, \ldots, m \cdot t_0)$ частоты второй ноты. Данные наборы не известны. Рассмотрим всевозможные случаи расположения этих частот на суммарной спектрограмме.

Случай 1. Ни одна частота из набора $(s_0, 2s_0, 3s_0, \ldots, m \cdot t_0)$ не совпадает ни с одной частотой из набора $(t_0, 2t_0, 3t_0, \ldots, n \cdot t_0)$. То есть не существуют натуральные числа k и l, где $k \geqslant 1$, $l \geqslant 1$, такие что $k \cdot t_0 = l \cdot s_0$, значит количество частот суммарной спектрограммы равно $n + m$. Пример данного случая можно изобразить на графике:



Амплитуды A и B в таком случае равны амплитуде при частоте t_0 и амплитуде при частоте s_0 соответственно.

Случай 2. Частоты основных тонов двух нот равны, то есть $t_0 = s_0$. Следовательно, набор частот одной из нот полностью принадлежит набору частот второй ноты. Значит, количество частот суммарной спектрограммы равно либо n, либо m. Приведем пример такого случая на графике:



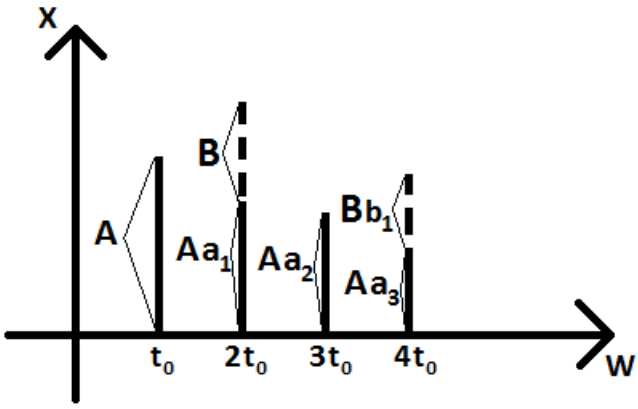
Пусть $n \geqslant m$. Чтобы вычислить амплитуды A и B составим следующую систему из двух уравнений, где R_1 и R_2 амплитуды суммарной спектрограммы для частот t_0 и $2t_0$ соответственно:

$$\begin{cases} A + B = R_1, \\ a_2 \cdot A + b_2 \cdot B = R_2 \end{cases}$$

Получаем, что $A = \dfrac{R_2 - b_2 \cdot R_1}{a_2 - b_2}$, $B = \dfrac{R_1 \cdot a_2 - R_2}{a_2 - b_2}$. Если полученные амплитуды A и B удовлетворяют также уравнениям для оставшихся амплитуд R_3, $\ldots$, R_n суммарной спектрограммы, то решение найдено, в противном случае, полученные A и B не являются решением. Так как огибающие нот отличны друг от друга, то рассмотренная система из двух уравнений линейно независима. То есть для рассматриваемого случая не может быть более одного решения.

Случай 3. Существует такое натуральное число k, где $k > 1$, что $k \cdot t_0 = s_0$, либо $k \cdot s_0 = t_0$. То есть частота основного тона второй ноты совпадает с одной из частот первой ноты, кроме частоты основного тона первой ноты, либо наоборот, частота основного тона первой ноты совпадает с одной из частот второй ноты, кроме частоты основного тона вто-

рой ноты. Следовательно, количество частот суммарной спектрограммы $< n+m$. Изобразим на графике возможный пример для данного случая:



Рассмотрим вариант, когда $k \cdot t_0 = s_0$. Для варианта, когда $k \cdot s_0 = t_0$, поиск решения аналогичен. Рассмотрим сначала следующую систему уравнений:

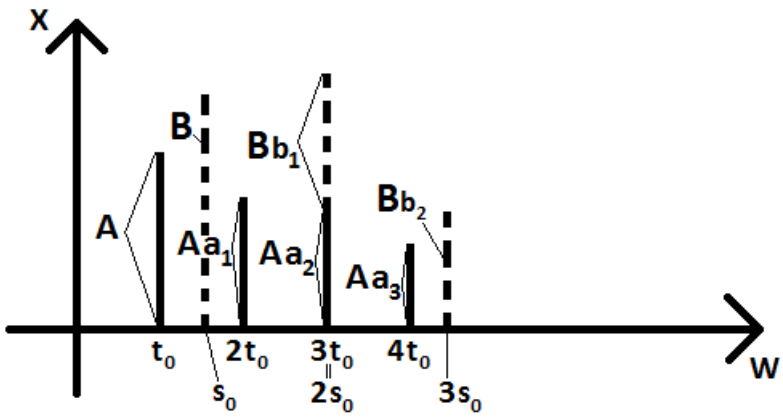
$$\begin{cases} A = R_1, \\ a_2 \cdot A + B = R_2 \end{cases}$$

$\Rightarrow B = R_2 - a_2 \cdot A = R_2 - a_2 \cdot R_1$. Проверяем, полученный $B > 0$, или $B = 0$. Если $B > 0$, то амплитуды A и B найдены, остается только проверить, удовлетворяют ли A и B также уравнениям для оставшихся амплитуд. Если же $B = 0$, то рассматриваем систему уравнений:

$$\begin{cases} A = R_1, \\ a_3 \cdot A + B = R_3 \end{cases}$$

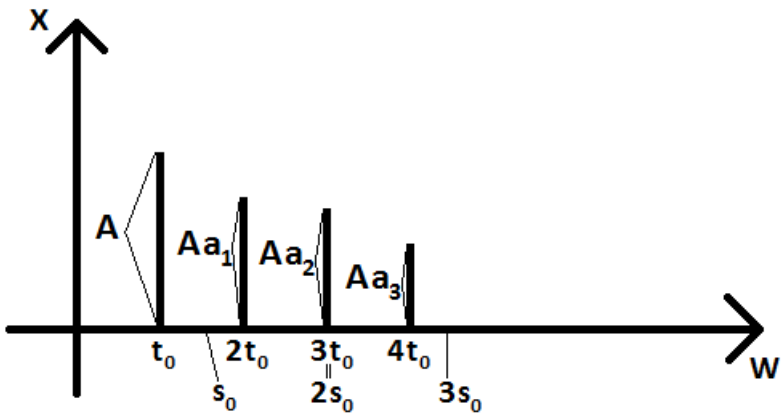
Также проверяем, является ли $B > 0$. В итоге, пытаемся найти такое k, что $a_k \cdot A + B = R_k$, где $B > 0$. Считаем, что $a_k = 0$, если $k > n$. Очевидно, что в рассмотренном случае 3 не может быть более одного решения.

Случай 4. Существуют натуральные числа k и l, где $k > 1$, $l > 1$, такие что $k \cdot t_0 = l \cdot s_0$, и не существует натуральное число p, где $p > 1$, что $p \cdot t_0 = s_0$, либо $p \cdot s_0 = t_0$. Пример данного случая изобразим на графике:



Допустим, что первая частота суммарной спектрограммы принадлежит первой ноте. Значит A будет равно амплитуде суммарной спектрограммы в данной частоте. Для предположения, что первая частота суммарной спектрограммы принадлежит второй ноте, поиск решения аналогичен.

Идем последовательно слева направо по набору частот суммарной спектрограммы и находим первую попавшуюся частоту, которая не кратна начальной частоте. Очевидно, что найденная частота есть частота основного тона второй ноты, и амплитуда B будет равна амплитуде суммарной спектрограммы в данной частоте. Вычтем из амплитуд суммарной спектрограммы, частоты которых кратны частоте основного тона второй ноты, произведения амплитуды B и соответствующего коэффициента огибающей. Тогда получим следующий график:



Проверяем, удовлетворяет ли найденная амплитуда A оставшимся амплитудам на графике суммарной спектрограммы. Если да, то решение найдено. Очевидно, что в рассмотренном случае 4 не может быть более одного решения.

Таким образом, для каждого отдельного случая расположения частот на суммарной спектрограмме мы определили свой метод вычисления амплитуд A и B.

Существование решения доказано.

Единственность. Докажем невозможность существования решения одновременно для нескольких случаев. Очевидно, что если случай 4 удовлетворяет суммарной спектрограмме, и решение для данного случая найдено, то остальные случаи точно не имеют решения. Аналогично, можно сказать и про случай 1. Поэтому для доказательства единственности решения остается рассмотреть только случаи 2 и 3.

Рассмотрим бесконечную последовательность целых неотрицательных чисел 1, a_2, ..., a_n, a_{n+1}, a_{n+2},..., где первые n элементов есть коэффициенты огибающей первой ноты, а последующие элементы равны 0, то есть $a_{n+1} = 0$, $a_{n+2} = 0$, ..., бесконечную последовательность 1, b_2, ..., b_m, b_{m+1}, b_{m+2},..., где первые m элементов есть коэффициенты огибающей второй ноты, а последующие элементы равны 0, то есть $b_{m+1} = 0$, $b_{m+2} = 0$, ..., а также бесконечную последовательность R_1, R_2, ..., где первые элементы есть амплитуды суммарной спектрограммы, а последующие элементы равны 0. Докажем, что не существуют натуральные числа A_1, B_1, A_2, B_2, k, такие что верна система уравнений:

$$\begin{cases} A_1 + B_1 = A_2 = R_1, \\ \vdots \\ a_{k-1} \cdot A_1 + b_{k-1} \cdot B_1 = a_{k-1} \cdot A_2 = R_{k-1} \\ a_k \cdot A_1 + b_k \cdot B_1 = a_k \cdot A_2 + B_2 = R_k \\ a_{k+1} \cdot A_1 + b_{k+1} \cdot B_1 = a_{k+1} \cdot A_2 = R_{k+1} \\ \vdots \\ a_{2k-1} \cdot A_1 + b_{2k-1} \cdot B_1 = a_{2k-1} \cdot A_2 = R_{2k-1} \\ a_{2k} \cdot A_1 + b_{2k} \cdot B_1 = a_{2k} \cdot A_2 + b_2 \cdot B_2 = R_{2k} \\ a_{2k+1} \cdot A_1 + b_{2k+1} \cdot B_1 = a_{2k+1} \cdot A_2 = R_{2k+1} \\ \vdots \end{cases}$$

Данная система состоит из уравнений вида $a_p \cdot A_1 + b_p \cdot B_1 = a_p \cdot A_2 = R_p$, если k не делит p, и уравнений вида $a_p \cdot A_1 + b_p \cdot B_1 = a_p \cdot A_2 + b_r \cdot B_2 = R_p$, если k делит p, и $r = \dfrac{p}{k}$

Допустим, что существуют натуральные числа A_1, B_1, A_2, B_2, k, такие что верна система уравнений из теоремы. Из данной системы рассмотрим первое и (km)-тое уравнения:

$$\begin{cases} A_1 + B_1 = A_2 = R_1, \\ a_{km} \cdot A_1 + b_{km} \cdot B_1 = a_{km} \cdot A_2 + b_m \cdot B_2 = R_{km} \end{cases}$$

Тогда возможны два варианта:

1) $km > n$. Тогда $a_{km} = 0$, $b_{km} = 0$, и система примет вид:

$$\begin{cases} A_1 + B_1 = A_2, \\ 0 = b_m \cdot B_2 \end{cases}$$

Имеем, что $b_m = 0$ — противоречие.

2) $km \leqslant n$. Тогда $a_{km} > 0$, $b_{km} = 0$, и система примет вид:

$$\begin{cases} A_1 + B_1 = A_2, \\ a_{km} \cdot A_1 = a_{km} \cdot A_2 + b_m \cdot B_2 \end{cases}$$

Следовательно, $a_{km} \cdot A_1 = a_{km} \cdot (A_1 + B_1) + b_m \cdot B_2$. Получается, что $0 = a_{km} \cdot B_1 + b_m \cdot B_2$, значит $a_{km} = b_m = 0$ — противоречие.

Теорема доказана.

□

4. Существование двух решений при вычислении амплитуд в случае бесконечных огибающих

Возможно ли существование нескольких решений, если предположить, что огибающие нот состоят из бесконечного числа ненулевых коэффициентов? Рассмотрим следующую теорему.

Теорема 2. *Существуют такие бесконечные огибающие и суммарная спектрограмма двух нот, одновременно сыгранных двумя различными инструментами, которым удовлетворяют две пары амплитуд первой и второй нот A_1 и B_1, а также A_2 и B_2.*

Доказательство. Из условия теоремы следует, что существует натуральное число k, где $k \geqslant 2$, такое что верна система уравнений:

$$\begin{cases} A_1 + B_1 = A_2 = R_1, \\ \vdots \\ a_{k-1} \cdot A_1 + b_{k-1} \cdot B_1 = a_{k-1} \cdot A_2 = R_{k-1} \\ a_k \cdot A_1 + b_k \cdot B_1 = a_k \cdot A_2 + B_2 = R_k \\ a_{k+1} \cdot A_1 + b_{k+1} \cdot B_1 = a_{k+1} \cdot A_2 = R_{k+1} \\ \vdots \\ a_{2k-1} \cdot A_1 + b_{2k-1} \cdot B_1 = a_{2k-1} \cdot A_2 = R_{2k-1} \\ a_{2k} \cdot A_1 + b_{2k} \cdot B_1 = a_{2k} \cdot A_2 + b_2 \cdot B_2 = R_{2k} \\ a_{2k+1} \cdot A_1 + b_{2k+1} \cdot B_1 = a_{2k+1} \cdot A_2 = R_{2k+1} \\ \vdots \end{cases}$$

Данная система состоит из уравнений вида $a_p \cdot A_1 + b_p \cdot B_1 = a_p \cdot A_2 = R_p$, если k не делит p, и уравнений вида $a_p \cdot A_1 + b_p \cdot B_1 = a_p \cdot A_2 + b_r \cdot B_2 = R_p$, если k делит p, и $r = \dfrac{p}{k}$

Из (1)-ого и $(k-1)$-ого уравнений $\Rightarrow a_{k-1} \cdot A_1 + b_{k-1} \cdot B_1 = a_{k-1} \cdot (A_1 + B_1) = R_{k-1} \Rightarrow b_{k-1} = a_{k-1}$. По аналогии для всех натуральных p, таких что k не делит p, имеем $b_p = a_p \Rightarrow$ пусть $b_{t \cdot k+l} = a_{t \cdot k+l} = \dfrac{1}{t \cdot k + l}$, где $1 \leqslant l \leqslant k-1$, $t \geqslant 0 \Rightarrow R_{t \cdot k+l} = \dfrac{A_2}{t \cdot k + l}$.

Пусть $a_k = \frac{1}{k} \Rightarrow R_k = \frac{A_2}{k} + B_2$. Из (1)-ого и (k)-ого уравнений $\Rightarrow$ $a_k \cdot A_1 + b_k \cdot B_1 = a_k \cdot (A_1 + B_1) + B_2 \Rightarrow b_k \cdot B_1 = a_k \cdot B_1 + B_2 \Rightarrow b_k = a_k + \frac{B_2}{B_1}$ $\Rightarrow b_k = \frac{1}{k} + \frac{B_2}{B_1}$

Вычтем из (k)-ого уравнения $(2k)$-ое уравнение, умноженное на $b_2 \Rightarrow$ $(a_k \cdot b_2 - a_{2k}) \cdot A_1 + (b_k \cdot b_2 - b_{2k}) \cdot B_1 = (a_k \cdot b_2 - a_{2k}) \cdot A_2$. Так как $A_1 + B_1 = A_2$ $\Rightarrow (b_k \cdot b_2 - b_{2k}) \cdot B_1 = (a_k \cdot b_2 - a_{2k}) \cdot B_1 \Rightarrow b_k \cdot b_2 - b_{2k} = a_k \cdot b_2 - a_{2k}$ $\Rightarrow b_{2k} = b_2 \cdot (b_k - a_k) + a_{2k} \Rightarrow b_{l \cdot k} = b_l \cdot (b_k - a_k) + a_{l \cdot k}$, где $l \geqslant 2$. Пусть $a_{l \cdot k} = \frac{1}{l \cdot k}$, $l \geqslant 2$, тогда $b_{l \cdot k} = b_l \cdot (\frac{1}{k} + \frac{B_2}{B_1} - \frac{1}{k}) + \frac{1}{l \cdot k} = b_l \cdot \frac{B_2}{B_1} + \frac{1}{l \cdot k}$, где b_l — известно $\Rightarrow R_{l \cdot k} = \frac{A_2}{l \cdot k} + b_l \cdot B_2$.

Таким образом для любого натурального $k \geqslant 2$ мы определили все числа a_i, b_i, R_i, где $i \geqslant 2$.

Теорема доказана.

□

Список литературы

[1] Клюкин И.И., *Удивительный мир звука*, 1978.

[2] Зарипов Р.Х., *Кибернетика и музыка*, «Знание», 1963.

[3] Вахромеев В.А., *Элементарная теория музыки*, «МУЗГИЗ», 1961.

Recovery of two notes sounding simultaneously

Botkholov A.J.

In this work recovery of two notes sounding simultaneously in terms of amplitudes and frequencies is considered.

The methods of recovery of amplitudes of two notes which were played at the same time by two different musical instruments are given.

Cases of existence and not existence of two solutions for a problem of recovery of notes are described.

Keywords: basic tone, overtone, amplitude, frequency, bending around note, total spectrogram.

Персистентные гомологии для марковских цепей и их применение к анализу текста на естественном языке

Кушнарева Л.П., Кузьминых Д.В.

В работе предложен новый метод введения персистентных топологических инвариантов для марковских цепей. Продемонстрирован пример использования этих инвариантов для прикладной задачи классификации текстов.

Ключевые слова: Топологический анализ данных, персистентные гомологии, марковские цепи, текст на естественном языке

Введение

Персистентные гомологии - один из основных инструментов топологического анализа данных - молодой дисциплины, которая исследует возможности выделения внутренней структуры в экспериментальных данных различной природы и введения топологических инвариантов на этой структуре. Это позволяет применять методы из алгебраической топологии для анализа данных и решения связанных с ними прикладных задач. В статье [1] приведен пример того, как можно использовать топологические методы для анализа изображений. В частности, автор сопоставляет каждому небольшому фрагменту изображения вектор в пространстве большой размерности. И оказывается, что векторы, соответствующие фрагментам изображений, полученным из реальных фотографий, лежат в окрестности небольшого подмногообразия пространства векторов, соответствующих произвольным (случайным) фрагментам. Таким образом, появляется возможность описать на языке алгебраической топологии, чем осмысленные изображения отличаются от бессмысленных.

Марковские цепи позволяют моделировать процессы в большом количестве приложений. Однако, по описанию марковских цепей в явном виде может быть трудно оценить "структурное" сходство или различие

таких процессов. Это приводит к вопросу о том, могут ли марковские цепи быть классифицированы аналогично тому, как это сделано для комплексов и поверхностей методами алгебраической топологии. В данной работе мы предлагаем метод введения топологических инвариантов для марковских цепей, в качестве основы используя идеи из статьи [**1**].

Мы преобразуем методологию, используемую в [**1**], так, чтобы она была применима к марковским цепям и введем на них инвариант - аналог персистентных гомологий, который позволяет выделять отличительные признаки различных марковских цепей. В качестве основного примера марковской цепи в данной работе будет использоваться марковская цепь, построенная на основе текста на естественном языке. В частности, будет показано, каким образом введенные на марковских цепях топологические инварианты позволяют отличать цепи, построенные по осмысленным текстам, от цепей, построенных по случайно сгенерированным текстам с той же частотой слов.

1. Предварительные сведения. Персистентность

Для удобства читателя, выпишем базовые определения теории категорий, на которые опирается определение персистентного объекта.

Определение. Категория $\underline{K}$ - это совокупность класса $Ob(\underline{K})$, элементы которого называются объектами категории $\underline{K}$, и класса $Mor(\underline{K})$, элементы которого называются морфизмами категории $\underline{K}$. Объекты и морфизмы категории должны быть связаны между собой следующими условиями:

1) Каждой упорядоченной паре объектов $a, b \in \underline{K}$ сопоставлено некоторое множество $H_{\underline{K}}(a, b)$ морфизмов категории $\underline{K}$.

2) Каждый морфизм категории $\underline{K}$ принадлежит одному и только одному из множеств $H_{\underline{K}}(a, b)$.

3) В классе $Mor(\underline{K})$ введена операция композиции. Композиция морфизмов $\alpha \in H_{\underline{K}}(a, b)$, $\beta \in H_{\underline{K}}(b, c)$ дает морфизм $\alpha\beta \in H_{\underline{K}}(a, c)$. Операция ассоциативна, т.е. $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ для любых трех морфизмов $\alpha \in H_{\underline{K}}(a, b)$, $\beta \in H_{\underline{K}}(b, c)$, $\gamma \in H_{\underline{K}}(c, d)$.

4) В каждом множетве $H_{\underline{K}}(a, a)$ содержится такой морфизм 1_a, что $\alpha 1_a = \alpha$ и $1_a\beta = \beta$, для произвольных морфизмов $\alpha \in H_{\underline{K}}(x, a)$,

$\beta \in H_{\underline{K}}(a, y)$. Такой морфизм 1_a называется тождественным или единичным морфизмом объекта a.

Определение. Одноместным ковариантным функтором из категории $\underline{K}$ в категорию $\underline{L}$ называется отображение $F : \underline{K} \to \underline{L}$, удовлетворяющее условиям:

1) Для всякого $a \in Ob(\underline{K})$, $F(a) \in Ob(\underline{L})$
2) Для всякого $\alpha \in H_{\underline{K}}(a, b)$, $F(\alpha) \in H_{\underline{L}}(F(a), F(b))$
3) Для всякой единицы $1_a \in \underline{K}$, $F(1_a) = 1_{F(a)}$
4) Для $\alpha \in H_{\underline{K}}(a, b)$, $\beta \in H_{\underline{K}}(b, c)$ имеет место равенство $F(\alpha\beta) = F(\alpha)F(\beta)$.

В дальнейшем будем под "функтором"понимать одноместный ковариантный функтор, если не сказано иное.

Определение Пусть $\underline{C}$ - произвольная категория, а P - частично упорядоченное множество. Наделим P категорной структурой следующим образом: возьмем P в качестве множества объектов и будем считать, что из объекта x в объект y из C существует морфизм если и только если $x \leq y$. Тогда функтор $\Phi : \underline{P} \to \underline{C}$ мы будем называть P-персистентным объектом.

Более конкретно, это означает наличие семейства$\{c_x\}_{x \in P}$ объектов в $\underline{C}$ вместе с морфизмами ϕ такими, что $\phi : c_x \to c_y <=> x \leq y$, и $\phi_{yz}\phi_{xy} = \phi_{xz} <=> x \leq y \leq z$.

2. Основная конструкция

Воспользуемся следующими определениями марковской цепи и матрицы переходов из [3] :

Определение. Пусть $(\Omega, \mathcal{A}, P)$ - конечное вероятностное пространство и $M = (\xi_0, ..., \xi_n)$- последовательность случайных величин со значениями в конечном множестве X. Последовательность $(\xi_0, ..., \xi_n)$ называется конечной марковской цепью, если выполнено условие $P(\xi_{k+1} = a_{k+1} | \xi_k = a_k, ..., \xi_0 = a_0) = P(\xi_{k+1} = a_{k+1} | \xi_k = a_k)$ для любых $a_0, ..., a_k$ таких, что $P\{\xi_k = a_k, ..., \xi_0 = a_0\} > 0$.

Определение. Множество X называется пространством состояний цепи, а матрица $||p(x, y)||$, $x, y \in X$, где $p(x, y) = P(\xi_k = y | \xi_{k-1} = x)$ -

матрицей переходных вероятностей. Если матрица переходных вероятностей не меняется со временем, соответствующая ей марковская цепь называется стационарной.

В дальнейшем в данной работе мы будем под "марковской цепью" всегда подразумевать конечную стационарную марковскую цепь M с фиксированным начальным состоянием I, если не сказано иное.

Определение.Путем ω в марковской цепи M назовем произвольную последовательность переходов между её состояниями $I, x_{i_1}, ..., x_{i_n}, ...$, такую, что вероятности переходов $p(x_{i_j}, x_{i_{j+1}}) > 0$ для всех $j \in \mathbb{Z}_+$. Пространство всех путей для данной марковской цепи M с фиксированным начальным состоянием I будем обозначать $\Omega_I(M)$.

Объединение пространств путей со всеми возможными начальными состояниями марковской цепи M будем обозначать $\Omega(M) = \bigcup\limits_{x \in X} \Omega_x(M)$, где X - множество состояний исходной марковской цепи.

Определение. Построим по произвольной марковской цепи M взвешенный ненаправленный граф $\Gamma_i = (V, W_i)$ следующим образом:

- В качестве вершин графа Γ_i возьмем состояния исходной марковской цепи M.

- Определим вспомогательную функцию $\xi(\{x_1, x_2\}) : \Omega_I(M) \to \mathbb{Z}_+ \cup \{\infty\}$, где $\{x_1, x_2\}$ - неупорядоченная пара вершин (состояний) исходной марковской цепи, следующим образом: функция ξ сопоставляет каждому возможному пути с началом в I (лежащему в марковской цепи M), количество раз, которое ребра (x_1, x_2) и (x_2, x_1) (т.е. произвольное ребро с концами в x_1 и x_2 без учета направления) встретились в данном пути.

  Далее, с помощью функции ξ введем весовую функцию на каждом ненаправленном ребре $e = \{x_1, x_2\}$:

  $$\omega_i(e) = \omega_i(\{x_1, x_2\}) = P(\xi(\{x_1, x_2\}) \geq i).$$

  Эта функция сопоставляет каждой паре вершин x_1 и x_2 вероятность пройти по ребру с концами в этих вершинах (в любом из двух направлений) не менее, чем i раз, начиная путь из вершины I.

Определение.Для каждого графа Γ_i, построенного в предыдущем определении и произвольного $p \in [0, 1]$, построим невзвешенный ненаправленный граф Γ_i^p следующим образом:

- В качестве вершин графа Γ_i^p возьмем вершины графа Γ_i (которые, в свою очередь, соответствуют состояниям исходной марковской цепи M).

- Будем считать, что ребро $e = \{x_1, x_2\}$ присутствует в графе Γ_i^p тогда и только тогда, когда вес соответствующего ребра $\{x_1, x_2\}$ в графе Γ_i не меньше, чем p: $w_i(\{x_1, x_2\}) \geq p$.

Полученный таким образом граф Γ_i^p будем называть фильтрацией графа Γ_i по вероятности p.

Лемма 1. *Пусть графы Γ_i^a и Γ_i^b построены по одной и той же марковской цепи с фиксированным начальным состоянием, $i \in \mathbb{N}$, а вероятности a и b удовлетворяют неравенству $0 \leq a < b \leq 1$. Тогда имеет место включение $\Gamma_i^a \supseteq \Gamma_i^b$.*

Доказательство. Графы Γ_i^a и Γ_i^b имеют одно и то же множество вершин по построению. Далее, для каждого произвольно взятого ребра e графа Γ_i^b выполняется неравенство $w_i(e) \geq b > a$. Следовательно, e также является ребром и в Γ_i^a, и мы имеем включение по ребрам. □

Лемма 2. *Пусть графы Γ_i^p и Γ_{i+1}^p также построены по одной и той же марковской цепи с фиксированным начальным состоянием, а $i \in \mathbb{N}$. Тогда для любого $p \in [0, 1]$ имеет место включение $\Gamma_i^p \supseteq \Gamma_{i+1}^p$.*

Доказательство. Множества вершин указанных графов, опять же, совпадают по построению. Далее, если некоторое ребро e принадлежит графу Γ_{i+1}^p, то имеет место неравенство $P(\xi(e) \geq i) \geq P(\xi(e) \geq i + 1) \geq p$. Следовательно, e также присутствует и в графе Γ_i^p, что дает искомое включение.

□

Теорема 1. *Рассмотрим объединение множеств*

$$P_{Th} = \bigcup_{i \in \mathbb{N}} \bigcup_{e \in \Gamma_i} \omega_e = \bigcup_{i \in \mathbb{N}} \bigcup_{e \in \Gamma_i} P(\xi_e \geq i) = \{p_1, \ldots, p_N\},$$

где $0 \leq p_1 \leq ... \leq p_N \leq 1$.

Тогда имеет место таблица включений:

$$\begin{array}{ccccccc}
\Gamma_1^{p_1} & \supseteq & \Gamma_1^{p_2} & \supseteq \ldots \supseteq & \Gamma_1^{p_n} & \supseteq \ldots \\
\cup| & & \cup| & & \cup| & \\
\Gamma_2^{p_1} & \supseteq & \Gamma_2^{p_2} & \supseteq \ldots \supseteq & \Gamma_2^{p_n} & \supseteq \ldots \\
\cup| & & \cup| & & \cup| & \\
\vdots & & \vdots & & \vdots &
\end{array}$$

Доказательство. Вертикальные включения - следствие утверждения 2; горизонтальные включения - следствие утверждения 1. □

Замечание. Из указанных утверждений также следует, что для любых натуральных m и n, таких, что $m \geq n$ и любых вещественных a и b, таких, что $0 \leq a \leq b \leq 1$, имеют место следующие включения:

$$\begin{array}{ccc}
\Gamma_n^a & \supseteq & \Gamma_n^b \\
\cup| & & \cup| \\
\Gamma_m^a & \supseteq & \Gamma_m^b
\end{array}$$

.

Определение. Построим по каждому графу $\Gamma_k^{p_j}$ абстрактный симплициальный комплекс $K_k^{p_j}$ следующим образом:

- Каждой вершине v_i графа $\Gamma_k^{p_j}$ сопоставим (взаимно однозначно) нульмерный симплекс $\{\Delta_i\}$ и включим его в комплекс $K_k^{p_j}$.
- Если вершины $\{v_{i_1}, ..., v_{i_n}\}$ графа $\Gamma_k^{p_j}$ образуют клику, добавим в комплекс $K_k^{p_j}$ $n-1$-мерный симплекс, посмтроенный на соответствующих им вершинах $\{\Delta_{i_1}, ..., \Delta_{i_n}\}$.
- Никаких других симплексов, кроме добавленных по правилам, перечисленным выше, комплекс $K_k^{p_j}$ не содержит.

Замечание. Поскольку каждая клика графа содержит все свои подклики, каждый симплекс комплекса $K_k^{p_j}$ также содержит все свои подсимплексы, а значит, $K_k^{p_j}$ действительно является симплициальным комплексом.

Теорема 2. *Для любых натуральных m и n, таких, что $m \geq n$ и любых $a, b \in [0, 1]$, таких, что $b \geq a$, следующая диаграмма коммутативна:*

$$\begin{array}{ccc} H_l(K_n^a) & \to & H_l(K_n^b) \\ \downarrow & \searrow & \downarrow \\ H_l(K_m^a) & \to & H_l(K_m^b) \end{array} \qquad (*)$$

где H_l - l-я группа симплициальных гомологий с коэффициентами в целых числах.

Доказательство. Доказанные вложения для графов индуцируют вложения клик, а значит, и вложения цепей симплексов соответствующих симплициальных комплексов:

$$\begin{array}{ccc} C_l(K_n^a) & \supseteq & C_l(K_n^b) \\ \cup| & & \cup| \\ C_l(K_m^a) & \supseteq & C_l(K_m^b) \end{array} \qquad (**)$$

где $C_l(K_n^a)$ - группа l-цепей комплекса K_n^a.

Эти вложения, в свою очередь, можно рассматривать как соответствующие гомоморфизмы - проекции. А именно, если $C_l \supseteq C_l'$, то мы имеем отображение $f : C_l \to C_l'$, однозначно определенное следующим образом: f тождественно на элементах базиса C_l' (как подмножестве C_l), а остальные элементы базиса C_l переводит в ноль.

Заметим, что поскольку проекции, очевидно, коммутируют, то при замене вложений в (**) на эти проекции, мы получаем коммутативную диаграмму.

Будем в дальнейшем для простоты обозначать все отображения, построенные таким образом для различных цепей, одним и тем же символом - f. Каждое конкретное построенное по такому принципу отображение, очевидно, восстанавливается однозначно, если мы знаем, какие именно группы цепей представляют собой его область определения и область значения.

Заметим, что для построенного таким образом гомоморфизма - проекции f выполняется соотношение:

$$f\delta(\Delta) = f(\sum_i (-1)^i [v_0, ..., \hat{v_i}, ..., v_n]) =$$
$$\sum_i (-1)^i f([v_0, ..., \hat{v_i}, ..., v_n]) = \delta f(\sigma),$$

где $\Delta = [v_0, ..., v_n]$ - произвольный n-мерный симплекс.

Таким образом, следующие диаграммы коммутативны:

$$
\begin{array}{ccccccccc}
... & \to & C_{k+1}(K_n^a) & \stackrel{\delta}{\to} & C_k(K_n^a) & \stackrel{\delta}{\to} & C_{k-1}(K_n^a) & \stackrel{\delta}{\to} & ... \\
 & & \downarrow f & \searrow & \downarrow f & \searrow & \downarrow f & & \\
... & \to & C_{k+1}(K_m^a) & \stackrel{\delta}{\to} & C_k(K_m^a) & \stackrel{\delta}{\to} & C_{k-1}(K_m^a) & \stackrel{\delta}{\to} & ...
\end{array}
$$

и

$$
\begin{array}{ccccccccc}
... & \to & C_{k+1}(K_n^a) & \stackrel{\delta}{\to} & C_k(K_n^a) & \stackrel{\delta}{\to} & C_{k-1}(K_n^a) & \stackrel{\delta}{\to} & ... \\
 & & \downarrow f & \searrow & \downarrow f & \searrow & \downarrow f & & \\
... & \to & C_{k+1}(K_n^b) & \stackrel{\delta}{\to} & C_k(K_n^b) & \stackrel{\delta}{\to} & C_{k-1}(K_n^b) & \stackrel{\delta}{\to} & ...,
\end{array}
$$

где δ - граничное отображение, $C_k(K_n^a)$ - группа k-мерных цепей комплекса (K_n^a).

По свойству функториальности симплициальных гомологий, указанные цепные отображения индуцируют отображения в гомологиях

$f_* : H_k(K_n^a) \to H_k(K_m^a)$,

$f_* : H_k(K_n^a) \to H_k(K_n^b)$,

и $f_* : H_k(K_n^a) \to H_k(K_m^b) \ \ \forall k \in \mathbb{Z} \cup \{\infty\}$

и коммутативность диаграммы (*).

□

Следствие 1. *Пусть $\underline{C}$ - категория групп гомологий с гомоморфизмами в качестве морфизмов. Далее, пусть $\underline{P}$ - категория вещественных чисел из отрезка $[0, 1]$ с отношением порядка в качестве морфизмов. Тогда существует функтор $\Phi : \underline{C} \to \underline{P}$, являющийся персистентным объектом.*

Доказательство. Непосредственно следует из предыдущей теоремы и определения персистентного объекта (Определение 3).

А именно, для каждой пары вероятностей a, b такой, что $a \leq b$, мы построили соответствующий гомоморфизм $H_l(K_n^a) \to H_l(K_n^b)$ для всех натуральных l и n. Таким образом, мы уже построили искомый функтор, а предыдущая теорема показывает его персистентность.

□

3. Численный эксперимент

3.1. Набор данных

Для эксперимента использовалось 50 первых блогов из открытого набора данных “The Blog Authorship Corpus”. Этот набор данных состоит из текстов интернет-блогов 19,320 авторов с сайта blogger.com. Каждый блог включает в себя не менее 200 вхождений часто используемых английских слов и разбит на отдельные посты. Для более подробной информации о наборе данных отсылаем читателя к [5].

3.2. Предварительная обработка данных

Для всего корпуса (состоящего из выбранных 50 блогов) как цельного объекта, была проделана следующая предварительная обработка:

- Были удалены все дополнительные символы, кроме латинских букв и пробелов;
- Был применен Porter stemming algorithm для нормализации формы слов;
- Был составлен частотный словарь 99 наиболее часто встречающихся в корпусе слов;
- Слова, не попавшие в словарь, были названы “редкими” и заменены всюду в тексте на специальное слово “RARE_WORD”. Это слово было включено в частотный словарь с частотой, равной сумме частот встречаемости отдельных “редких” слов.

  Таким образом, был получен общий для всего корпуса словарь из 100 слов.

После этого для каждого блога в отдельности было проделано следующее:

- Были вычислены частоты встречаемости каждого слова из общего для всего корпуса словаря, включая “редкое слово”, в данном конкретном блоге.

- По полученным частотам был сгенерирован случайный текст с тем же словарем и той же длины, что и данный блог, с той же вероятностью встречаемости каждого слова.

  Отметим, что таким образом, для каждого блога был построен случайный текст, неотличимый от него с помощью простых алгоритмов, не учитывающих порядок слов (таких, как bag of words).

- По каждому тексту - и случайному, и неслучайному - была построена марковская цепь. А именно, каждому слову x частотного словаря было сопоставлено ровно одно состояние марковской цепи, которое мы обозначаем для простоты тем же символом. В качестве вероятности $p(x, y)$ перехода из состояния x в состояние y была назначена вероятность встретить слово y в данном тексте сразу после слова x.

  Но поскольку мы не можем знать точно указанные вероятности, в качестве их приближений были приняты эмпирические вероятности, вычисленные отдельно на основе каждого текста.

- Для каждой полученной таким способом марковской цепи методом Монте-Карло были вычислены матрицы смежностей соответствующего графа Γ_1. Подробности этого вычисления описаны в следующем параграфе.

3.3. Оценка весов графа Γ_1; построение графов Γ_1^p для различных значений p и вычисление их гомологий.

Для вычисления графа Γ_1 для каждой марковской цепи запускалось 100 случайных блужданий из каждого возможного начального состояния. Блуждание останавливалось, если мы пришли в конечное слово (после которого ничего не встречается) или совершили более 1000 шагов (ограничение введено для того, чтобы программа всегда заканчивала работу). Затем подсчитывалось, сколько проходов по каждому ребру было сделано в процессе каждого блуждания. Результаты усреднялись сначала по всем проходам, а затем - по всем начальным состояниям.

Далее, на основе каждого графа Γ_1 были вычислены по 8 графов $\Gamma_1^{p_1}, ...\Gamma_1^{p_8}$ для восьми равно отстоящих друг от друга значений p_i. Затем были вычислены размерности нулевых групп гомологий (то есть, количество компонентов связности) каждого из этих графов. Из этих восьми чисел Бетти был составлен вектор. Каждый такой вектор был дополнен

числом 100 (максимально возможное количество компонент связности) в качестве константы. Далее мы назначили метку 1 векторам, которые соответствуют текстам, написанным человеком, и 0 - векторам, которые соответствуют текстам, сгенерированным случайно.

Таким образом, мы сопоставили каждому тексту 9 целых чисел от 0 до 100 (включая константу) в качестве признаков и один бинарный параметр в качестве метки.

Приведем в качестве примера векторы признаков, полученных на основе текстов пяти первых блогов:

[5, 29, 61, 75, 80, 88, 91, 96, 100],

[1, 43, 65, 77, 86, 93, 94, 97, 100],

[3, 34, 54, 74, 85, 89, 92, 95, 100],

[4, 35, 60, 78, 80, 88, 93, 96, 100],

[4, 41, 67, 81, 86, 91, 93, 95, 100]

И векторы признаков, полученных на основе соответствующих им случайно сгенерированных текстов:

[1, 17, 52, 65, 80, 84, 90, 93, 100],

[2, 23, 63, 72, 78, 87, 92, 93, 100],

[1, 32, 55, 73, 84, 87, 91, 93, 100],

[3, 29, 57, 72, 82, 86, 92, 94, 100],

[3, 37, 64, 76, 81, 88, 91, 94, 100]

Отметим, что каждая отдельная компонента векторов из первой группы в среднем больше соответствующей компоненты векторов из второй группы, что наталкивает на мысль о линейной разделимости соответствующих классов. Поэтому мы использовали их в качестве признаков для обучения линейного классификатора - логистической регрессии.

Мы перемешали все вектора случайным образом и разбили их на два набора - тренировочный и тестовый в отношении 9:1. После этого на тренировочном наборе была обучена логистическая регрессия методом стохастического градиентного спуска с регуляризатором $C = 1$ и максимальным количеством итераций 1000.

3.4. Результат эксперимента

Эксперимент показал, что вектора из тестового множества, соответствующие осмысленным и бессмысленным текстам, линейно разделимы с точностью от 0.96 до 1 с помощью логистической регрессии.

4. Выводы

В данной статье мы ввели новые инварианты - персистетные гомологии на марковских цепях - и доказали их основные свойства. Был также приведен пример их эффективного использования в решении одной из важных прикладных задач, а именно - классификации текстов на естественном языке.

Тем не менее, возможности применения разработанного нами инструмента не ограничиваются только данной конкретной прикладной задачей. Как уже было отмечено, он потенциально может оказаться полезным и во многих других областях, где требуется находить инварианты марковских цепей. Но это уже тема для следующих исследований.

5. Благодарности

Авторы выражают благодарность А.А. Ирматову за поддержку в работе - помощь в уточнении формулировок и определений, а также отдельных деталей доказательств.

Список литературы

[1] G. Carlsson, "Topology And Data", *Bulletin (new series) of the American Mathematical Society*, **46**:2 (April 2009), 255–308.

[2] Н.Бурбаки, *Теория множеств*, пер. с фр. Г.Н.Поварова и Ю.А.Шихановича, ред. В.А.Успенского, Мир, М., 1965.

[3] А.Н. Ширяев, *ВЕРОЯТНОСТЬ*. Т. 1, 4-е изд., переработ. и доп, МЦНМО, М., 2007.

[4] А.Т.Фоменко, Д.Б.Фукс, *Курс гомотопической топологии*, Наука, М., 1989.

[5] J. Schler, M. Koppel, S. Argamon and J. Pennebaker, "Effects of Age and Gender on Blogging", Proceedings of the AAAI Spring Symposia on Computational Approaches to Analyzing Weblogs (2006), 2006.

Persistent homology of Markov chains and its application to natural language processing

Kushnareva L., Kuzminykh D.

In this work we introduce new persistent topological invariants for Markov chains. We also demonstrate the way of using these invariants for natural language processing task.

Keywords: Topology data analysis, persistent homology, Markov chains, natural language processing

Часть 2.
Специальные вопросы теории интеллектуальных систем

Критерий надежности канала с запрещениями

Казаков И.Б.

В работе исследуется возможность надежной передачи информации в ситуации, когда противник в каждой момент времени может блокировать некоторое подмножество символов алфавита. Показано, что гарантированно надежный канал существует тогда и только тогда, когда мощность алфавита n и число разрешенных символов k удовлетворяют неравенству $n \leq 2k - 2$.

Ключевые слова: скрытые каналы, блуждания по плоскости, запрещения алфавитных символов, передаваемый язык

1. Введение

В работе изучается вопрос о том, возможно ли передавать каким-либо образом информацию, используя алфавит из n символов, если при каждом акте передачи какие-то произвольные символы этого алфавита могут быть объявленными запрещенными к передаче. Однако, перед тем, как будет дано формальное точное определение тому, что же это означает, мы приведем мотивировку исследования данного вопроса.

Прежде всего, скажем, что изначальный пункт — это теория скрытых каналов. Скрытым каналом называется называется коммуникационный канал, пересылающий информацию методом, который изначально не был для этого предназначен. То есть существуют злоумышленники, передающие информацию таким образом, что сторонние наблюдатели не могут зафиксировать сам факт передачи.

Исторически первой работой, посвященной теории скрытых каналов, считается статья [1]. Также упомянем о современном обзоре [2], посвященном сетевым скрытым каналам.

Конкретно в данной работе речь идет о скрытом канале блужданий по плоскости. Блуждания по плоскости изучаются в связи с задачей построения скрытых каналов через online-шутеры, то есть многопользовательские игры, в которых некий клиент может передавать игровому

серверу команды о перемещении своего персонажа по плоскости, а другие клиенты могут получать от сервера данные о местоположении (и, следовательно, также о изменениях местоположения) этого персонажа.

Задача построения скрытых каналов через online-шутеры ранее исследовалась в [3]. Там использовался подход, несколько отличающийся от применяемого в настоящей работе, а именно: передача информации осуществлялась через *малые отклонения* от «естественного движения». Также использовался дополнительный параметр «угол зрения персонажа», который исключен здесь из рассмотрения.

Однако, в [3] не изучался вопрос исправления ошибок, а также вопрос о возможности блокирования направлений движения, которому и посвящена настоящая работа.

С технической точки зрения, протокол передачи данных через блуждания по плоскости задан следующим образом. Вся игровая плоскость разбита на квадраты прямыми линиями. Игрок, который хочет передать некое скрытое сообщение, должен находиться в области видимости игрока, которому он хочет передать это сообщение. Актом передачи информации считается пересечение границы квадрата (в котором в данный момент находится передающий игрок) в одном из четырех возможных направлений. Таким образом, на каждом акте могут быть переданы 4 возможных значения, или 2 бита информации.

Как вариант, можно разбивать плоскость не на квадраты, а на шестиугольники. При таком разбиении каждый шестиугольник имеет 6 соседних. Аналогично считая актом передачи переход в соседний шестиугольник, можно передавать уже не 4, а 6 возможных значений.

Однако в реальных online-играх движение персонажей по игровому полю не является абсолютно свободным. Во-первых, у игрового поля есть границы, и персонаж не может находиться за этими границами. Во-вторых, существуют предусмотренные игрой препятствия для перемещения, такие как «камни», «вода» и так далее, которые игрок вынужден обходить. В-третьих, сервер может передавать игроку, принимающему скрытое сообщение, координаты не всех игроков на поле, а лишь тех, которые расположены в «зоне видимости» (то есть где-то недалеко от местонахождения игрока-приемника). Поэтому для игрока-передатчика переход в ячейки, находящиеся за пределами области видимости игрока-приемника, недопустим: это означает разрыв связи в канале. В-четвертых, есть местонахождения, крайне нежелательные по игровым причинам: например, около этой точки на игровом поле находится враг, её просматривающий. Враг начинает атаковать любого игрока, пер-

сонаж которого там находится, и персонаж игрока-передатчика может оказаться слишком слаб для того, чтобы этого врага победить.

Таким образом, на любом шаге может оказаться так, что по некоторым направлениям игроку-передатчику ходить нельзя, то есть невозможно передать некоторые из значений. При этом игрок-приемник может как знать, какие именно направления сейчас запрещены (например, в случае края поля), так и не знать, *куда же игрок-передатчик «не хочет идти»*.

И, следовательно, возникает задача конструирования схемы кодирования информации для передачи в вышеописанных условиях. Мы рассмотрим следующую абстрактную постановку задачи: пусть дан алфавит из n символов, и пусть на каждом шаге может быть запрещено не более, чем $n - k$ из них. При каких n и k гарантированно возможно что-либо передать?

2. Протокол

Для того, чтобы ответить на вышепоставленный вопрос, необходимо дать формальное математическое определение выражению «возможно что-либо передать». Отметим, что если вообще «возможно что-либо передать», то очевидно, что прежде всего возможно передать 1 бит информации.

Уметь передавать 1 бит информации — это значит уметь передавать некие два различных «сигнала». Это означает, что игрок-передатчик сначала выбирает, какое же из двух значений (0 или 1) ему передавать, и соответственно с выбором значения передает символы игроку-приемнику по одному из двух заранее определенных способов. Игрок-приемник, считывая принятые символы, должен уметь распознавать, какой же из двух способов был использован игроком-передатчиком.

Следовательно, нужно далее определить, что же такое «способ передачи» сигнала. Игрок-приемник, считывая изменения местоположения игрока-передатчика, принимает последовательность символов алфавита, соответствующую происходящим перемещениям. В некоторый момент игрок-приемник, очевидно, должен решить, что «сигнал передан».

Игроку-приемнику недоступна никакая другая информация, кроме последовательности получаемых им символов. Следовательно, алгоритм, принимающий решение о том, произошло ли событие «сигнал передан», на одинаковых *конечных последовательностях уже принятых символов* (то есть на одинаковых *словах*) должен выдавать одинаковый ответ.

А это означает ничто иное как то, что «способ передачи сигнала» может быть описан исключительно *как множество слов* (или *язык*). Событие «сигнал передан» тождественно событию «последовательность уже принятых символов образует слово, принадлежащее заданному языку».

Таким образом, для передачи 1 бита информации предзадаются два языка X и Y. Соответственно значению бита выбирается один из них, и игрок-передатчик пытается передавать символы так, чтобы на каком-то шаге было передано какое-то слово из выбранного языка. Заметим, что так как здесь речь идет не об одном языке, а о двух, то для *различаемости* соответствующих «сигналов» необходимо потребовать соблюдения ещё одного условия (далее формально определенного как *кросс-префиксность*): чтобы никакое начало слова, принадлежащего одному из языков, не совпадало с каким-нибудь словом из другого языка. Действительно, если, например, на некотором шаге произошло событие «передано значение 1», то ни на каком предыдущем шаге (а также, разумеется, и на данном) не могло произойти события «передано значение 0».

Замечание. *Можно потребовать не только кросс-префиксности пары языков, но также префиксности каждого из них, то есть того, чтобы никакое слово не являлось началом другого слова этого же языка. Так как, если, например, на каком-то шаге уже «передано значение 1», то на этом передачу следует остановить, и тем самым исключить то, что на каком-то последующем шаге снова произойдет событие «передано значение 1». Это совершенно необходимо, если мы хотим всё же передавать не 1 бит, а сообщения произвольной длины: игрок-приемник должен определять, в какой момент можно считать завершенной передачу очередного бита.*

3. Противодействующий субъект

Осталось учесть только лишь только тот факт, что на каждом шаге некоторые символы (не более чем $n - k$ из них) запрещены к передаче. Для краткости мы будем далее говорить, что в некоторый момент достигнуто состояние, описываваемое словом α (или просто состояние α), если к этому моменту уже была передана конечная последовательность символов, это слово образующая.

Пусть для передачи выбран язык X. Тогда задача игрока-передатчика *при любых запрещениях на всех ходах* прийти в любое из

состояний из X. Возможность этого, очевидно, зависит только от самого языка X. Если это возможно, то такой язык называется *передаваемым*.

Так как запрещения символов могут быть любыми, то нам следует изучать самый худший случай: как будто бы запрещения происходят именно так, чтобы во чтобы то ни стало не дать прийти в состояние из X.

Следовательно, можно представить себе дело так, как будто запрещениями управляет некий третий субъект, пытающийся сорвать передачу, а сама эта передача суть игра между передатчиком и данным субъектом. Далее, следуя сложившийся традиции, мы будем именовать игрока-передатчика — *Алисой*, игрока-приемника — *Бобом*, а мешающего третьего субъекта — *Евой*.

Ход Евы состоит в выборе множества запрещенных символов, причем если этот ход корректен, то количество запрещаемых символов не может превышать $n - k$. Следующий за ним корректный ход Алисы состоит в выборе какого-нибудь не запрещенного Евой символа с последующей отправкой его Бобу. Алиса выигрывает игру на языке X в момент, когда достигается состояние, соответствующее слову из X.

И, следовательно, вопрос о том, передаваем ли язык X, является по существу вопросом о том, существует ли страгегия, выигрышная (относительно языка X) для Алисы. А вопрос о том, возможно ли передача 1 бита, таким образом, сводится к вопросу: существуют ли два кросс-префиксных передаваемых языка при заданных n и k.

Теперь осталось только лишь формально записать уже напрашивающиеся определения, а также установить немедленно следующие из этих определений свойства.

4. Передаваемый язык

Для начал дадим определение языка как такового.

Определение 4.1. *Алфавит $A = \{a_1, a_2, ..., a_n\}$ — это конечное множество (n) символов.*

Определение 4.2. *Слово α, составленное из символов алфавита A — это некая конечная последовательность символов из A. Множество всех таких слов обозначается как A^*. В этом множестве, отдельно отметим, есть последовательность из 0 символов, то есть пустое слово $\Lambda \in A^*$.*

Определение 4.3. *Бесконечное слово — это бесконечная последовательность символов алфавита A. Множество всех бесконечных слов обозначается как A^∞.*

Определение 4.4. *Язык X — это просто некое множество слов: $X \subset A^*$.*

Теперь нужно выразить вышеупомянутые накладываемые на языки условия.

Определение 4.5. *Слово $\alpha\alpha'$ — это конкатенация слов α и α', то есть результат приписывания α' после α.*

Определение 4.6. *Слово α' называется префиксом слова α, если существует такое α'', что $\alpha = \alpha'\alpha''$. Особо отметим, что может быть $\alpha'' = \Lambda$, то есть любое слово согласно данному определению является префиксом самого же себя. Также отметим, что далее полагается допустимым говорить о конечном слове как о префиксе бесконечного.*

Замечание. *Пустое слово Λ считается префиксом любого слова.*

Определение 4.7. *Язык X называется префиксным, если в нем нет двух таких слов $\alpha, \alpha' \in X$, таких что α' — префикс α.*

Определение 4.8. $pr(X) \stackrel{\text{def}}{=} \{\alpha \in A^* | \exists \alpha' \in X : \alpha$ *— префикс* $\alpha'\}$ *— префиксное замыкание, то есть множество всех слов, которые являются префиксом какого-нибудь слова из X.*

Утверждение 4.1. $X \subset pr(X)$

Доказательство. Немедленно следует из того, что любое слово суть префикс самого себя. □

Утверждение 4.2. $pr(pr(X)) = pr(X)$

Доказательство. Немедленно следует из того, что префикс префикса — суть префикс. □

Определение 4.9. *Пара языков X, Y называется кросспрефиксной при выполнении следующих условий:*
1) $pr(X) \cap Y = \emptyset$
2) $pr(Y) \cap X = \emptyset$

Утверждение 4.3. *Если пара X, Y кросспрефиксна, то $X \cap Y = \emptyset$.*

Доказательство.
1. Пусть $\alpha \in X \cap Y$.
2. Так как $X \subset pr(X)$, то $\alpha \in pr(X) \cap Y$, что немедленно противоречит определению кросспрефиксности.

□

Далее нужно приписать Алисе стратегию и определить, что же означает, что Алиса всегда может выиграть игру, то есть определить для стратегии свойство «быть выигрышной». Это возможно сделать, также определив последовательность ходов Евы и задав отношение: побеждает ли Алиса при заданной страгетии, если Ева сделает определённые ходы.

Определение 4.10. *Стратегия Алисы — это функция* $f : A^* \times 2^A \to A$

Определение 4.11. *Корректная стратегия Алисы — это стратегия Алисы, для которой выполнено следующее свойство:* $\forall \alpha \in A^* \ \forall B \in 2^A \ ||B| \geq k| : f(\alpha, B) \in B$

Первый аргумент функции f — это текущее состояние игры, второй — это сделанный Евой ход, значение функции — ответный ход Алисы. Условие корректности, таким образом, означает, что в ответ выбор Евой допустимого множества символов (т.е. любое множество символов, в котором их k и более штук), разрешенных на текущем ходе, Алиса, как и положено, выбрает какой-то символ именно из этого множества.

Что касается Евы, то любое возможное её поведение может быть описано как последовательность множеств символов, которые она оставляет незапрещенными для Алисы.

Определение 4.12. *Последовательность ходов Евы — это отображение* $g : \mathbb{N} \to 2^A$*, то есть попросту последовательность неких подмножеств алфавита* A*.*

По условию, Ева всегда должна оставлять хотя бы k символов незапрещенными, что соответственно накладывает ограничения на последовательности ходов Евы, рассматриваемые как описания её поведения.

Определение 4.13. *Допустимая последовательность ходов Евы — это та, для которой выполнено* $\forall i \ |g(i)| \geq k$*.*

Определение 4.14. *Будем говорить, что бесконечное слово* $\alpha^\infty = \alpha^\infty(1)\alpha^\infty(2)\alpha^\infty(3)... \in A^\infty$ *согласованно с стратегией Алисы* f*, а также последовательностью ходов Евы* g*, если выполнено:*

1) $\alpha^\infty(1) = f(\Lambda, g(1))$
2) $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i+1))$

Утверждение 4.4. *Для любой стратегии Алисы f и любой последовательности ходов Евы согласованное бесконечное слово существует и единственно.*

Доказательство. Очевидно по индукции: определение задает явное посимвольное построение. □

Согласованное слово — это и есть «реально печатаемая Алисой последовательность символов».

Теперь наконец можно дать формальное определение понятию «передаваемый язык», исходя из того, что Алиса по определению выигрывает, если на каком-то шаге последовательность переданных ей символов складывается в слово из искомого языка.

Определение 4.15. *Будем говорить, что некий начальный отрезок бесконечного слова α^∞ лежит в X, если в языке X найдется такое слово α', что α' — префикс α^∞.*

Определение 4.16. *Корректная стратегия Алисы f передает язык X, если для всякой допустимой последовательность ходов Евы g согласованное с такими f и g бесконечное слово α таково, что некий его начальный отрезок лежит в X.*

Определение 4.17. *Язык X — передаваемый, если существует передающая его корректная стратегия.*

5. Особый случай

Рассмотрим отдельно случай $n \leq 2k-2$.

В этом случае дан алфавит $A = \{a_1, ..., a_n\}$. Положим $X = \{a_1, ...a_{n-k+1}\}$, $Y = \{a_{n-k+2}, ..., a_{2n-2k+2}\}$.

Очевидно, что X, Y — кросспрефиксная пара.

Утверждение 5.1. *X, Y – передаваемы (как языки).*

Доказательство. Возьмем для примера X. Так как в X (как множестве символов) более чем $n-k$ символов, то Ева не может запретить всё из X. Следовательно, Алиса может победить за один ход, выбрав символ из X, который оказался разрешенным, и передав его Бобу. □

Таким образом, при $n \leq 2k-2$ передача информации от Алисы к Бобу возможна, и осуществляется весьма *тривиальным* образом: просто среди символов выбираются два непересекающихся множества мощности больше, чем $n-k$.

А возможна ли передача (хотя бы 1 бита) информации при каком-нибудь другом n? Ответ на данный вопрос является отрицательным, и это составляет собственно главный результат данной работы.

6. Вспомогательные понятия

Прежде всего, мы введем некоторые определения технического характера, а также установим немедленно вытекающие из них тривиальные утверждения, которые будут использованы в дальнейших формальных доказательствах.

Здесь $X \subset A^*$ — некий произвольный язык.

Определение 6.1. $succ_X(\alpha) \stackrel{\text{def}}{=} \{a \in A | \alpha a \in X\}$ — *множество «последователей (а точнее их последних символов) слова α в языке X», т.е. множество таких символов a, что αa является словом из языка X.*

Утверждение 6.1. *Если $a \in succ_X(\alpha)$, то $\alpha a \in X$*

Доказательство. Немедленно из определения. □

Утверждение 6.2. $succ_{A^* \setminus X}(\alpha) = A \setminus (succ_X(\alpha))$

Доказательство.

1. $a \in succ_{A^* \setminus X}(\alpha) \Leftrightarrow \alpha a \in A^* \setminus X \Leftrightarrow \alpha a \notin X$.
2. $a \in A \setminus (succ_X(\alpha)) \Leftrightarrow a \notin succ_X(\alpha) \Leftrightarrow \alpha a \notin X$
3. Как видно, условия принадлежности эти двум множествам равносильны. □

Утверждение 6.3. *Пусть $\alpha \in X$ такое, что $|succ_X(\alpha)| \geq k$. Также пусть f — некая корректная стратегия Алисы, и $a = f(\alpha, succ_X(\alpha))$.*

Тогда $\alpha a \in X$.

Доказательство.
1. Согласно определению корректной стратегии, из $|succ_X(\alpha)| \geq k$ и $a = f(\alpha, succ_X(\alpha))$ следует $a \in succ_X(\alpha)$.
2. $a \in succ_X(\alpha) \Rightarrow \alpha a \in X$, по утверждению 6.1. □

Утверждение 6.4. *Пусть* $A_1 \subset A$, $A_2 \subset A$, $|A| = n$, $|A_1| \geq n - k + 1$, $|A_2| \geq n - k + 1$, *а также* $n > 2k - 2$. *Тогда* $A_1 \cap A_2 \neq \emptyset$.

Доказательство.
1. Рассмотрим множество $A_1 \cup A_2$. Из условий немедленно следует $A_1 \cup A_2 \subset A$, и, стало быть, $|A_1 \cup A_2| \leq n$.
2. С другой стороны, согласно общеизвестной формуле включений-исключений, $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2| \geq 2(n-k+1) - |A_1 \cap A_2| = 2n - 2k + 2 - |A_1 \cap A_2|$.
3. Таким образом, $2n - 2k + 2 - |A_1 \cap A_2| \leq n$, откуда $n \leq 2k - 2 + |A_1 \cap A_2|$, и, следовательно, $|A_1 \cap A_2| \geq n - (2k - 2) > 0$.
4. Но $|A_1 \cap A_2| > 0$ и означает, что $A_1 \cap A_2 \neq 0$. □

Утверждение 6.5. *Пусть* $A_1 \subset A$, $B \subset A$, $|A| = n$, $|A_1| \geq n - k + 1$, $|B| \geq k$. *Тогда* $A_1 \cap B \neq \emptyset$

Доказательство.
1. Аналогично предыдущему доказательству: $n \geq |A_1 \cup B| = |A_1| + |B| - |A_1 \cap B| \geq (n - k + 1) + k - |A_1 \cap B| = n + 1 - |A_1 \cap B|$.
2. Откуда немедленно $|A_1 \cap B| \geq 1$, т.е. $A_1 \cap B \neq \emptyset$.

□

7. Необходимое условие передаваемости

Установим достаточное условие того, что некий язык X не является передаваемым. Отрицание данного условия, соответственно, является необходимым условием передаваемости.

Определение 7.1. *Будем говорить, что язык* S *является предблокирующим для языка* X, *если выполнено следующее:*
1) $S \cap X = \emptyset$
2) $\forall \alpha \in S \ |succ_S(\alpha)| \geq k$

Определение 7.2. *Предблокирующий язык* S *блокирует* X, *если также* $\Lambda \in S$.

Интуитивно, условие 2) предблокирования — это условие того, что «если уж Алиса завела игру в какое-то состояние из S, то Ева может больше не выпускать Алису из S». Действительно, пусть $\alpha \in S$, тогда Ева своим ходом может оставить разрешенными лишь символы из $succ_S(\alpha)$. Ответный ход Алисы, таким образом, не выведет из S.

Соответственно, добавление условия 1) означает, что оставаясь в S, нельзя прийти ни к чему из X, а блокирование — что Алиса «ещё не начав игру, уже находится в S — ловушке».

Далее формализуем эти соображения.

Теорема 7.1. *Пусть S блокирует X. Тогда X не является передаваемым языком.*

Доказательство.

1. Предположим обратное. Пусть X — передаваемый язык. Тогда, согласно определению, найдется передающая его корректная стратегия Алисы f.

2. Положим $\hat{f}(\alpha) \stackrel{\text{def}}{=} f(\alpha, succ_S(\alpha))$ — ход Алисы из состояния α, если Ева оставила разрешенным множество символов $succ_S(\alpha)$.

3. Так как по условию блокирования $|succ_S(\alpha)| \geq k$, то согласно утверждению 6.3 $\alpha \in S \Rightarrow \alpha\hat{f}(\alpha) \in S$.

4. Зададим посредством индуктивного определения бесконечное слово $\alpha^\infty \in A^\infty$: $\alpha^\infty(1) \stackrel{\text{def}}{=} \hat{f}(\Lambda) = f(\Lambda, succ_S(\Lambda))$, $\alpha^\infty(i+1) \stackrel{\text{def}}{=} \hat{f}(\alpha^\infty(1)...\alpha^\infty(i)) = f(\alpha^\infty(1)...\alpha^\infty(i), succ_S(\alpha^\infty(1)...\alpha^\infty(i)))$.

5. Докажем по индукции, что $\forall m\ \alpha^\infty(1)...\alpha^\infty(m) \in S$.

5.1. Базис. $\Lambda \in S$. Согласно п.3, $\Lambda\hat{f}(\Lambda) = \alpha^\infty(1) \in S$.

5.2. Шаг индукции. Пусть $\alpha^\infty(1)...\alpha^\infty(m) \in S$. Тогда $\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1) = \alpha^\infty(1)...\alpha^\infty(m)\hat{f}(\alpha^\infty(1)...\alpha^\infty(m)) \in S$, согласно тому же пункту 3.

6. Положим $g : \mathbb{N} \to 2^A$, $g(1) \stackrel{\text{def}}{=} succ_S(\Lambda)$, $g(i+1) \stackrel{\text{def}}{=} succ_S(\alpha^\infty(1)...\alpha^\infty(i))$ — последовательность ходов Евы. По только что доказанному в п.5, а также уже упомянутому условию $\forall\alpha \in S\ |succ_S(\alpha)| \geq k$, эта последовательность ходов Евы является *допустимой*.

7. Очевидно, что выполнено $\alpha^\infty(1) = f(\Lambda, g(1))$, $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i))$, что по определению означает, что α^∞ согласовано с f, g.

8. Так как g — допустимая последовательность ходов Евы, а корректная стратегия f передает X, то некий начальный отрезок α^∞ лежит в X. То есть найдется такое m (в том числе это может быть и $m = 0$, что соответствует пустому слову Λ), такое что $\alpha^\infty(1)...\alpha^\infty(m) \in X$.

9. Таким образом, по п.5 и п.9 получаем: $\alpha^\infty(1)...\alpha^\infty(m) \in S \cap X$, что противоречит условию 1) предблокирования. Следовательно, предположение п.1 неверно, и X не является передаваемым языком.

ч.т.д.

□

8. Достаточное условие передаваемости

Пусть некоторым словам α приписаны какие-то числовые значения, и из состояния α с данным значением (*ненулевым*) Алиса всегда может выполнить ход, приводящий к состоянию, которому приписано меньшее значение. Также предположим, что Алиса не только может, но и всегда делает именно такой ход.

Тогда очевидно, что если пустому слову Λ приписано числовое значение, то за конечное число ходов Алисы состояние игры всегда оказывается среди слов, которым приписан 0. Следовательно, если все такие слова лежат в X, то X оказывается передаваемым языком.

Выразим сказанное формальным образом.

Определение 8.1. *Градуировка — это отображение* $d : A^* \to \{0\} \cup \mathbb{N} \cup \{+\infty\}$

Определение 8.2. $succ_d(\alpha) \stackrel{\text{def}}{=} \{a \in A | d(\alpha a) < d(\alpha)\}$ — *«множество (последних символов) последователей по градуировке», т.е. множество таких символов* a*, что значение градуировки на* αa *меньше, чем на исходном слове* α*.*

Определение 8.3. *Градуировка называется предправильной, если из* $0 < d(\alpha) < +\infty$ *следует* $|succ_d(\alpha)| \geq n - k + 1$

Определение 8.4. *Правильная градуировка — это предправильная, у которой* $d(\Lambda) < +\infty$*.*

Определение 8.5. $bott(d) \stackrel{\text{def}}{=} \{\alpha \in A^* | d(\alpha) = 0\}$ *– дно градуировки* d*. То есть это те слова, на которых она равна* 0*.*

Лемма 8.1. *Пусть* d *— предправильная градуировка. Тогда существует корректная стратегия Алисы* f*, такая что если* $0 < d(\alpha) < +\infty$ *и* $|B| \geq k$*, то* $d(\alpha f(\alpha, B)) < d(\alpha)$*.*

Доказательство.

1. Достаточно определить $f(\alpha, B)$ лишь при $|B| \geq k$, причем так, чтобы в этом случае $f(\alpha, B) \in B$. Во всех остальных случаях значение f можно выбрать произвольным: это не влияет на корректность. Далее рассматриваем только данный случай.

2. При $d(\alpha) = 0$ или $d(\alpha) = +\infty$ в качестве $f(\alpha, B)$ можно выбрать любой символ $a \in B$. ($|B| \geq k \geq 1 \Rightarrow B \neq \emptyset$). Аналогично, далее рассматриваем только случай $0 < d(\alpha) < +\infty$.
3. В обозначенном случае, так как по условию d — предправильно, $|succ_d(\alpha)| \geq n - k + 1$. И так как $|B| \geq k$, то согласно утверждению 6.5 $succ_d(\alpha) \cap B \neq \emptyset$.
4. В качестве $f(\alpha, B)$ выберем любое $a \in succ_d(\alpha) \cap B$.
5. Из определения $succ_d$ немедленно следует, что $d(\alpha a) < d(\alpha)$.
ч.т.д. □

Теорема 8.1. *Пусть d — правильная градуировка, и $bott(d) \subset X$. Тогда X — передаваемый язык.*

Доказательство.

1. Согласно предыдущей лемме, найдется такая корректная стратегия Алисы f, что при $0 < d(\alpha) < +\infty$, $|B| \geq k$ выполнено $d(\alpha f(\alpha, B)) < d(\alpha)$.
2. Зафиксируем $g : \mathbb{N} \to 2^A$ — допустимую последовательность ходов Евы, т.е. $\forall i \in \mathbb{N}\ |g(i)| \geq k$.
3. Пусть α^∞ — бесконечное слово, согласованное с f и g: $\alpha^\infty(1) = f(\Lambda, g(1))$, $\alpha^\infty(i+1) = f(\alpha^\infty(1)...\alpha^\infty(i), g(i+1))$.
4. Предположим, что никакой его начальный отрезок не лежит в X, т.е. $\Lambda \notin X$, $\forall m \in \mathbb{N}\ \alpha^\infty(1)...\alpha^\infty(m) \notin X$.
5. И, следовательно, так как $B(d) \subset X$, то $d(\Lambda) \neq 0$, $d(\alpha^\infty(1)...\alpha^\infty(m)) \neq 0$.
6. Докажем по индукции, что $\forall m \in \mathbb{N}$
$0 < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$ и $d(\alpha^\infty(1)...\alpha^\infty(m)\alpha(m+1)) < d(\alpha^\infty(1)...\alpha^\infty(m))$

6.1. Известно, что $d(\Lambda) < +\infty$, так как d — правильная градуировка, а также $d(\Lambda) \neq 0$ (п.5). Таким образом, $0 < d(\Lambda) < +\infty$. И, следовательно, согласно п.1,2: $d(\Lambda f(\alpha, g(1))) = d(\alpha^\infty(1)) < d(\Lambda) < +\infty$.

6.2. Также по п.5, $0 < d(\alpha^\infty(1))$.

6.3. Шаг индукции. Предположим, что $0 < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$. Тогда, согласно тем же п.1,2: $d(\alpha^\infty(1)...\alpha^\infty(m)f(\alpha^\infty(1)...\alpha^\infty(m), g(m+1))) = d(\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1)) < d(\alpha^\infty(1)...\alpha^\infty(m)) < +\infty$.

6.4. $0 < d(\alpha^\infty(1)...\alpha^\infty(m)\alpha^\infty(m+1))$ по п.5.

7. Таким образом, получаем: $+\infty > d(\Lambda) > d(\alpha^\infty(1)) > d(\alpha^\infty(1)\alpha^\infty(2)) > d(\alpha^\infty(1)\alpha^\infty(2)\alpha^\infty(3)) > ...$ — бесконечная убывающая последовательность натуральных чисел. Но такого не может быть в принципе, поэтому

предположение п.4 является ложным, т.е. некий начальный отрезок α^∞ лежит в X.
8. g было выбрано произольно. То есть для любой допустимой стратегии Евы g некий начальный отрезок согласованного с f и g бесконечного слова α^∞ лежит в X. Что и означает, что корректная стратегия f передает X.
9. И, следовательно, X — передаваемый язык.
ч.т.д.

□

9. Выигрышные состояния

Предположим, что Алиса уже привела игру в состояние α. И что $|succ_X(\alpha)| \geq n - k + 1$. Тогда, какой бы ход не сделала Ева, она не может запретить все символы из $succ_X(\alpha)$, и следовательно, Алиса сможет победить ответным ходом.

Стало быть, о таких α можно говорить как о «заведомо выигрышных для Алисы состояниях». Более того, это рассуждение можно повторять индуктивно: пусть для множества $\{\alpha a_1, ..., \alpha a_n\}$ уже известно, что хотя бы $n-k+1$ из них «заведомо выигрышны для Алисы». Тогда, аналогично, само α тоже может считаться «заведомо выигрышным».

Проведем формальное построение множества «заведомо выигрышных состояний» указанным образом.

Определение 9.1. $X' \stackrel{\text{def}}{=} \{\alpha \in A^* | \ |succ_X(\alpha)| \geq n - k + 1\}$ — *язык X, называемый производной языка X, т.е. ничто иное, как множество состояний, в которых Алиса «находится в одном шаге от X».*

Соответственно множество $X \cup X'$ может быть интерпретировано как множество состояний, в которых «Алиса находится в *не более чем одном* шаге от X».

Находиться в не более чем одном шаге от множества слов, находящихся в не более чем в одном шаге от X, значит находиться в не более чем в *двух* шагах от X. Соответственно, быть в не более чем одном шаге от нахождения в не более чем двух — это нахождение в *трех* шагах, и так далее.

Определение 9.2.
$X^{(0)} \stackrel{\text{def}}{=} X$
$X^{(i+1)} \stackrel{\text{def}}{=} X^{(i)} \cup (X^{(i)})'$

Утверждение 9.1. $X^{(0)} \subset X^{(1)} \subset X^{(2)} \subset X^{(3)} \subset X^{(4)} \subset ...$

Доказательство. Немедленно из определения: $X^{(i)} \subset X^{(i+1)}$ □

Таким образом, «находиться в не более, чем в n шагах от X» означает лежать в $X^{(n)}$.

И, стало быть, теперь можно определить, что значит «находиться в каком-нибудь конечном числе шагов от X». Что и означает «находиться в выигрышном для Алисы состоянии».

Определение 9.3. $X^{(\infty)} \stackrel{\text{def}}{=} \bigcup\limits_{i=0}^{\infty} X^{(i)}$

Все выигрышные состояния лежат в префиксном замыкании.

Утверждение 9.2. *Пусть $Z \subset pr(X)$. Тогда $Z' \subset pr(X)$.*

Доказательство.

1. Пусть $\alpha \in Z'$. Тогда $|succ_X(\alpha)| \geq n - k + 1 \geq 1$.
2. То есть найдется такой символ $a \in A$, что $\alpha a \in Z$.
3. По условию это тут же означает, что $\alpha a \in pr(X)$, т.е. найдется такое $\alpha' \in X$, что αa — префикс α'.
4. Следовательно, α — также префикс $\alpha' \in X$, а значит $\alpha \in pr(X)$.

ч.т.д.

□

Теорема 9.1. $X^{(\infty)} \subset pr(X)$.

Доказательство.

1. Базис индукции. $X = X^{(0)} \subset X^{(\infty)}$.
2. Шаг индукции. Пусть $X^{(i)} \subset pr(X)$. Тогда, по предыдущему утверждению, $(X^{(i)})' \subset pr(X)$, и следовательно, также $X^{(i+1)} = X^{(i)} \cup (X^{(i)})' \subset pr(X)$.
3. Все $X^{(i)} \subset pr(X)$, поэтому $X^{(\infty)} = \bigcup\limits_{i=0}^{\infty} X^{(i)} \subset pr(X)$.

ч.т.д.

□

10. Критерий передаваемости

Теперь можно задаться следующим вопросом: пусть некое $\alpha \in X^{(\infty)}$. В скольких шагах от победы находится Алиса, если она уже привела игру в состояние α?

Из определения очевидно, что если $\alpha \in X^{(\infty)}$, то найдутся такие k, что $\alpha \in X^{(k)}$. Для ответа на вышепоставленный вопрос нужно выбрать минимальное из таких k.

Тем самым, каждому $\alpha \in X^{(\infty)}$ можно приписать некую *степень*, выражаемую конечным числом. Всем остальным словам можно приписать бесконечную степень, и тем самым получить некую *градуировку*.

Определение 10.1. *Градуировка* $deg_X : A^* \to \{0\} \cup \mathbb{N} \cup \{+\infty\}$ *определяется как* $deg_X(\alpha) \stackrel{\text{def}}{=} \begin{cases} min\{k|\alpha \in X^{(k)}\}, & \alpha \in X^{(\infty)} \\ +\infty, & \alpha \notin X^{(\infty)} \end{cases}$

Утверждение 10.1. $bott(deg_X) = X$

Доказательство.

1. Пусть $deg_X(\alpha) = 0$. Из определения deg_X немедленно вытекает, что $\alpha \in X^{(0)} = X$.
2. Обратно, пусть $\alpha \in X = X^{(0)}$. Тогда, очевидно, $deg_X(\alpha) = 0$.

□

Утверждение 10.2. $X^{(\infty)} \setminus X = \{\alpha \in A^* | 0 < deg_X(\alpha) < +\infty\}$

Доказательство.

1. Из определения ясно, что $\alpha \in X^{(\infty)} \Leftrightarrow deg_X(\alpha) < +\infty$.
2. По предыдущему утверждению $\alpha \notin X \Leftrightarrow deg_X(\alpha) > 0$.

□

Установим тривиальные свойства:

Утверждение 10.3. *Пусть* $\alpha \in X^{(k)}$. *Тогда* $deg_X(\alpha) \leq k$.

Доказательство. Очевидно по определению. □

Утверждение 10.4. *Пусть* $deg_X(\alpha) = k$, $k < +\infty$. *Тогда* $\alpha \in X^{(k)}$.

Доказательство. Очевидно по определению. □

А также более сложные:

Утверждение 10.5. *Пусть* $deg_X(\alpha) = k$, $0 < k < +\infty$. *Тогда* $\alpha \in (X^{(k-1)})'$.

Доказательство.

1. Из условий и предыдущего утверждения: $\alpha \in X^{(k)}$.
2. Если бы $\alpha \in X^{(k-1)}$, то было бы $deg_X(\alpha) \leq k-1 < k$. Следовательно, $\alpha \notin X^{(k-1)}$.
3. $\alpha \in X^{(k)} = X^{(k-1)} \cup (X^{(k-1)})'$, $\alpha \notin X^{(k-1)} \Rightarrow \alpha \in (X^{(k-1)})'$.

□

Утверждение 10.6. *Пусть* $deg_X(\alpha) = k$, $0 < k < +\infty$.
Тогда $succ_{deg_X}(\alpha) = succ_{X^{(k-1)}}(\alpha)$

Доказательство.

I. ($\Rightarrow$)
1. Пусть $a \in succ_{deg_X}(\alpha)$. Это означает, что $deg_X(\alpha a) < deg_X(\alpha) = k$. Обозначим $k' = deg_X(\alpha a)$, тогда $k' < k$, что равносильно $k' \leq k-1$.
2. Тогда $\alpha a \in X^{(k')} \subset X^{(k-1)}$.
3. И, следовательно, $a \in succ_{X^{(k-1)}}(\alpha)$.

II. ($\Leftarrow$)
1. Пусть теперь $a \in succ_{X^{(k-1)}}(\alpha)$. Тогда $\alpha a \in X^{(k-1)}$.
2. Следовательно, $deg_X(\alpha a) \leq k-1 < k = deg_X(\alpha)$
3. $deg_X(\alpha a) < deg_X(\alpha) \Rightarrow a \in succ_{deg_X}(\alpha)$

ч.т.д.

□

Всё готово для получения важного промежуточного результата.

Лемма 10.1. *Для любого языка* X *градуировка* deg_X *является предправильной.*

Доказательство.

1. Пусть α — такое слово, что $0 < deg_X(\alpha) < +\infty$.
2. Тогда по утверждению 10.5 $\alpha \in (X^{(k-1)})'$. Это означает, что $|succ_{X^{(k-1)}}(\alpha)| \geq n-k+1$

3. Но по утверждению 10.6 $|succ_{deg_X}(\alpha)| = |succ_{X^{(k-1)}}(\alpha)| \geq n - k + 1$
4. Что и требуется определением предправильной градуировки.
ч.т.д.

□

Дополнение $A^* \setminus X^{(\infty)}$ также обладает интересным свойством:

Лемма 10.2. *$A^* \setminus X^{(\infty)}$ — предблокирует язык X.*

Доказательство.

1. Так как $X = X^{(0)} \subset X^{(\infty)}$, то $(A^* \setminus X^{(\infty)}) \cap X = \emptyset$. Тем самым, выполнено условие 1) предблокирования.
2. Предположим, что условие 2) не выполнено, тогда найдется $\alpha \in A^* \setminus X^{(\infty)}$ такое, что $|succ_{A^* \setminus X^{(\infty)}}(\alpha)| < k$.
3. Пользуясь утверждением 6.2, это можно переписать как $|succ_{X^{(\infty)}}(\alpha)| > n - k$.
4. И, следовательно, найдутся (хотя бы) $n - k + 1$ различных символов $a_1, ..., a_{n-k+1}$ такие, что $\alpha a_1, ..., \alpha a_{n-k+1} \in X^{(\infty)}$.
5. Стало быть, найдутся также такие $i_1, ..., i_{n-k+1}$, что $\alpha a_1 \in X^{(i_1)}, ..., \alpha a_{n-k+1} \in X^{(i_{n-k+1})}$.
6. Положим $i = \max(i_1, ..., i_{n-k+1})$. Тогда все $\alpha a_1, ..., \alpha a_{n-k+1} \in X^{(i)}$.
7. Из этого вытекает, что $a_1, ..., a_{n-k+1} \in succ_{X^{(i)}}(\alpha)$.
8. Таким образом, $succ_{X^{(i)}}(\alpha) \supset \{a_1, ..., a_{n-k+1}\}$. Откуда, естественно, $|succ_{X^{(i)}}(\alpha)| \geq n - k + 1$.
9. Это означает, что $\alpha \in (X^{(i)})'$. Так как $X^{(i+1)} = X^{(i)} \cup (X^{(i)})'$, то и $\alpha \in X^{(i+1)} \subset X^{(\infty)}$.
10. Согласно п.2, $\alpha \in A^* \setminus X^{(\infty)}$. Согласно п.9, $\alpha \in X^{(\infty)}$. Получившееся противоречие показывает, что предположение из п.2 неверно, т.е. выполнен условие 2) предблокирования.
ч.т.д.

□

Сформулируем фундаментальный критерий (и докажем его, собрав вместе результаты ранее проделанной работы), позволяющий «заменить определение передаваемости» (т.е. необходимое и достаточное условие), и далее при исследовании передаваемых языков не иметь дело с стратегиями Алисы, допустимимыми последовательностями ходов Евы и т.д.

Теорема 10.1. *Язык X передаваем тогда и только тогда, когда $\Lambda \in X^{(\infty)}$.*

Доказательство.

I. ($\Leftarrow$)
1. Пусть $\Lambda \in X^{(\infty)}$.
2. Тогда $deg_X(\Lambda) < \infty$. И, следовательно, $\deg_X$ — правильная градуировка. (предправильной она же уже является по лемме 10.1)
3. Также, согласно утверждению 10.1 $bott(deg_X) = X$. И, следовательно, согласно достаточному условию (теорема 8.1) X — передаваемый язык.

II. ($\Rightarrow$)
1. Пусть $\Lambda \notin X^{(\infty)}$. Переформулируем: $\Lambda \in A^* \setminus X^{(\infty)}$.
2. Тогда $A^* \setminus X^{(\infty)}$ — блокирует X. ($A^* \setminus X^{(\infty)}$ предблокирует X по лемме 10.2)
3. Согласно теореме 7.1 этого достаточно для того, чтобы X не являлся передаваемым языком.
ч.т.д.

□

Замечание. *Из представленных рассуждений можно видеть, как именно должна действовать Алиса, если язык передаваем, и как же должна действовать Ева, если нет. В случае передаваемости Алисе на каждом ходу следует выбирать символ из $succ_{deg_X}(\alpha)$, в случае непередаваемости Еве следует «не пускать Алису в $X^{(\infty)}$»*

11. Одновременно передаваемые языки

В данном разделе будет приведен главный результат настоящей работы. Доказывать мы его начнем с изучения некоторых специфических свойств, относящихся к *парам* языков X, Y (а точнее относящихся к ним предправильных градуировок deg_X, deg_Y).

Лемма 11.1. *Пусть X, Y — произвольные языки, и для некоего слова α выполнено: $0 < deg_X(\alpha) < +\infty$, $0 < deg_Y(\alpha) < +\infty$. А также верно $n > 2k - 2$.*
Тогда найдется символ a такой, что $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$

Доказательство.

1. Так как градуировки deg_X, deg_Y (см. лемму 10.1) предправильны, то $|succ_{deg_X}(\alpha)|, |succ_{deg_Y}(\alpha)| \geq n - k + 1$.
2. Согласно утверждению 6.4, из этого следует, что $succ_{deg_X}(\alpha) \cap succ_{deg_Y}(\alpha) \neq \emptyset$.
3. Выберем некое $a \in succ_{deg_X}(\alpha) \cap succ_{deg_Y}(\alpha)$. Тогда по определению «последователей по градуировке» $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$.
ч.т.д

□

Изучим также свойства $X^{(\infty)}, Y^{(\infty)}$, следующие из кросспрефиксности:

Утверждение 11.1. *Пусть X, Y — кросспрефиксны. Тогда*
1) $(X^{(\infty)} \cap Y^{(\infty)}) \cap X = \emptyset$
2) $(X^{(\infty)} \cap Y^{(\infty)}) \cap Y = \emptyset$

Доказательство.

1. $X^{(\infty)} \subset pr(X) \Rightarrow (X^{(\infty)} \cap Y^{(\infty)}) \cap Y \subset X^{(\infty)} \cap Y \subset pr(X) \cap Y = \emptyset$, согласно кросспрефиксности.
2. $Y^{(\infty)} \subset pr(Y) \Rightarrow (X^{(\infty)} \cap Y^{(\infty)}) \cap X \subset Y^{(\infty)} \cap X \subset pr(Y) \cap X = \emptyset$, аналогично.

□

Оказывается, при выполнении условия $n > 2k - 2$, если существует какое-то общее выигрышное состояние $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$, то существует целый «бесконечный спуск» таких состояний.

Лемма 11.2. *Пусть X, Y — кросспрефиксны, $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$, $n > 2k - 2$. Тогда найдется такое $a \in A$, что $\alpha a \in X^{(\infty)} \cap Y^{(\infty)}$, причем $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$*

Доказательство.

1. По предыдущему утверждению, из условия $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$ следует, что $\alpha \notin X$, $\alpha \notin Y$.
2. Так как $\alpha \in X^{(\infty)}, \alpha \notin X$, то $0 < deg_X(\alpha) < +\infty$. (см. утверждение 10.2)
3. Аналогично $\alpha \in Y^{(\infty)}, \alpha \notin Y \Rightarrow 0 < deg_Y(\alpha) < +\infty$
4. Применяя лемму 11.1, находим символ $a \in A$ такой, что $deg_X(\alpha a) < deg_X(\alpha)$, $deg_Y(\alpha a) < deg_Y(\alpha)$.

5. При этом $deg_X(\alpha a) < deg_X(\alpha) < +\infty$, $deg_Y(\alpha a) < deg_Y(\alpha) < +\infty$, а значит $\alpha a \in X^{(\infty)}$, $\alpha a \in Y^{(\infty)}$
ч.т.д.

□

Однако, «бесконечных спусков» *с убывающей на каждом шаге степенью* не может быть.

Лемма 11.3. *Пусть X, Y — кросспрефиксная пара языков, $n > 2k - 2$. Тогда $X^{(\infty)} \cap Y^{(\infty)} = \emptyset$.*

Доказательство.

1. Пусть $\alpha \in X^{(\infty)} \cap Y^{(\infty)}$.
2. Тогда, индуктивно применяя (это возможно, так как заключение леммы относительно αa «повторяет условие») предыдущую лемму, построим *бесконечную* последовательность слов $\alpha, \alpha a_1, \alpha a_1 a_2, \alpha a_1 a_2 a_3, ... \in X^{(\infty)} \cap Y^{(\infty)}$
3. При этом $deg_X(\alpha) > deg_X(\alpha a_1) > deg_X(\alpha a_1 a_2) > deg_X(\alpha a_1 a_2 a_3) > ...$ и $deg_Y(\alpha) > deg_Y(\alpha a_1) > deg_Y(\alpha a_1 a_2) > deg_Y(\alpha a_1 a_2 a_3) > ...$ — бесконечные убывающие последовательности натуральных чисел.
4. Бесконечных убывающих последовательностей натуральных чисел не существует.
ч.т.д.

□

Замечание. *Сам по себе «бесконечный спуск в $X^{(\infty)}$» (без убывания степени) существовать может. Построим пример.*

Положим $n = 3, k = 2$, $A = \{a_1, a_2, a_3\}$. Язык X составим из слов вида $a_1, a_2a_1, a_2a_2a_1, a_2a_2a_2a_1, ...$, а также вида $a_2, a_2a_3, a_2a_2a_3, a_2a_2a_2a_3, ...$

Тогда все слова $a_2, a_2a_2, a_2a_2a_2... \in X' \subset X^{(1)} \subset X^{(\infty)}$ — образуют «бесконечный спуск».

Это показывает, что вышеприведенные рассуждения «не могут быть упрощены», то есть для получения противоречия, недостаточно продемонстрировать сам факт того, что существует бесконечный спуск (а это может быть сделано без использования понятия степени deg_X)

Финальный результат.

Теорема 11.1. *Пара одновременно передаваемых кросспрефиксных языков X, Y существует тогда и только тогда, когда $n \leq 2k - 2$*

Доказательство.

I. При $n > 2k - 2$
1. Если X, Y передаваемые языки, то согласно критерию (теорема 10.1) $\Lambda \in X^{(\infty)} \cap Y^{(\infty)}$.
2. Однако, это запрещено предыдущей леммой.
II. При $n \leq 2k - 2$.
1. См. пример, построеный в разделе 5 «Особый случай».

□

Замечание. *Таким образом, при выполнении условия $n \leq 2k - 2$ Алиса и Боб могут построить скрытый канал, имеющий пропускную способность 1 бит на каждый передаваемый Алисой символ.*

Полученный результат означает, что передача информации при поставленных условиях или осуществляется весьма тривиальным образом (при $n \leq 2k - 2$ с помощью языков X, Y, в которых все слова являются односимвольными), или же вовсе невозможна. Как видно из представленных в работе рассуждений, для того, чтобы Ева могла гарантированно сорвать передачу информации от Алисы к Бобу, ей достаточно знать используемую пару кросспрефиксных языков и какое именно значение (0 или 1) Алиса в этот раз намеривается передать Бобу.

Другим важным результатом, который может быть использован в дальшейшем, является представленный в работе критерий (теорема 10.1), дающий исчерпывающий ответ на вопрос о передаваемости языка.

В настоящей работе изучался лишь вопрос того, возможна ли *гарантированная* передача при *любых возможных* помехах. Это соответствует тому предположению, что Ева ведёт идеальную игру. Однако, реальные запрещения направлений передвижений по плоскости в online-игре таковыми, разумеется, не являются, так как возникают весьма случайно. Следовательно, в подавляющем большинстве случаев, Алиса успешно пересылает информацию Бобу, а случайный срыв передачи происходит на самом деле с исчезающе малой вероятностью.

Изучение подобных вопросов выходит за рамки настоящей статьи и будет предпринято в последующих работах. Однако, для примера, рассмотрим далее один частный случай.

Позволим Еве *менять* множество запрещенных символов не на каждом ходе, а например, раз в два хода. Это означает, что на ходах с номерами $2s, 2s+1$ Алисе разрешены к передаче *одни и те же* символы. Соответственно принятым ограничениям очевидным образом модифицируется понятие «допустимой последовательности ходов Евы», и, следовательно, понятие «передаваемого языка».

Положим $k = 2, n = 3$, и рассмотрим пару (кросспрефиксных) языков $X = \{a_0a_0, a_1a_1, a_2a_2\}$, $Y = \{a_1a_2, a_2a_0, a_0a_1\}$. На первом ходу Ева может запретить для Алисы лишь какой-то один символ из $\{a_0, a_1, a_2\}$, и *тот же самый* символ она должна запретить и на втором ходу.

Если запрещается a_0, то в языке X есть слово a_1a_1, которое может передать Алиса при данном решении Евы. Соответственно, в Y есть a_1a_2. Аналогично, для a_1: $a_2a_2 \in X$ и $a_2a_0 \in Y$, а для a_2: $a_0a_0 \in X$ и $a_0a_1 \in Y$. Остался лишь случай, когда Ева выбрала вообще не запрещать никаких символов. Однако, он тривиален: тогда Алиса может передать любое из слов в языках X, Y.

Таким образом, X, Y — «передаваемые языки». А следовательно, с принятым ограничением (для прочих n, k подобные языки конструируются аналогично) передача информации осуществима.

Список литературы

[1] Lampson B. W., A Note on the Confinement Problem. *Communications of the ACM* (1973) **16**:10, 613–615.

[2] Llamas D, Allison C, Miller, A., Covert channels in internet protocols: a survey. *Proceedings of the 6th Annual Postgraduate Symposium about the Convergence of Telecommunications, Networking and Broadcasting, PGNET*, 2005.

[3] Zander S., Armitage G., Branch P., Covert channels in multiplayer first person shooter online games, *2008 33rd IEEE Conference on Local Computer Networks, LCN*, 2008, 215–222.

Reliabilty criterion for channels with prohibitions

Kazakov I.B.

We investigate the possibility of reliable transmission in a situation when an adversary can prohibit some characters, and a set of prohibitions can change at every clock cycle. We show that reliable transmission is possible if and only if the cardinality of the alphabet n and the number of allowed characters k satisfy the inequality $n \leq 2k-2$.

Keywords: covert channels, walks in a plane, character prohibition, transmittable language

Сегментация изображений и преобразования, сохраняющие форму фигур

В.Н. Козлов

Изображением в работе называем конечное (непустое) множество точек в евклидовых пространствах разной размерности. Кратко работа состоит в том, чтобы имея изображение, принадлежащую некоторому образу, извлечь из этого изображения то, что можно было бы назвать описанием этого образа.

Ключевые слова: математическое определение изображения, описание зрительного образа, распознавание изображений.

Кратко и на содержательном уровне настоящая работа состоит в том, чтобы имея изображение (фигуру), принадлежащую некоторому образу, извлечь из этого изображения то, что можно было бы назвать описанием этого образа.

Изображением называем конечное (непустое) множество точек в евклидовых пространствах разной размерности. В частности, двумерное изображение – конечное множество точек на плоскости.

Обосновываем это тем, что любую фигуру можно «аппроксимировать» конечным множеством точек , которые уже сами по себе делают фигуру вполне узнаваемой. При этом если точек много, то такая совокупность точек практически неотличима от исходной фигуры. Так же можно представлять и полутоновые, черно-бело-серые изображения, при этом разная плотность точек в разных частях изображения дает разные оттенки «серого цвета». Как известно, цветное изображение можно представлять как наложение трех монохроматических (аналогов черно-бело-серых) изображений. Это означает, что совокупностями точек можно представлять и цветные изображения. Трехмерные изображения – точки в трехмерном евклидовом пространстве. Соотнесение между трехмерным изображением и двумерными, являющимися их проекциями , приводит к задачам восстановления тел по плоским проекциям и смеж-

ным задачам. Наконец, трехмерный мир в динамике можно рассматривать как четырехмерное изображение (последовательность трехмерных сцен).

Далее рассматриваются двумерные изображения, но сказанное несложно обобщается и на случаи большей размерности.

Ранее [**?**, **?**, **?**] было введено понятие кода изображения, который можно трактовать как описание изображения с точностью до аффинных его преобразований. Это значит, что имея изображение – конкретное множество точек на плоскости – мы получаем его же описание при всех его возможных параллельных переносах на плоскости, вращениях, изменениях в размерах, сжатиях и растяжениях. Это можно рассматривать как первый шаг к формированию на основе данного изображения некоторого его обобщения. Однако шаг явно недостаточный, поскольку различия изображений в рамках одного образа явно не сводятся к только аффинным преобразованиям.

Пусть X - некоторое изображение . Точку v из X назовем внутренней, если существуют такие точки p,q,s из X, что v лежит внутри треугольника, образованного точками p,q,s (или на его стороне). Остальные точки из X называем внешними или контурными. В совокупности они есть то, что назовем капсулой $K(X)$. Случаи капсул из одной и двух точек полагаем вырожденными. Ясно, что применительно к $K(X)$ (невырожденной) можно говорить о выпуклом многоугольнике. и , соответственно, о сторонах капсулы как о сторонах в этом многоугольнике.

Обозначим через $W(X)$ выпуклую оболочку для X. Ясно, что $W(X)$ и $W(K(X))$ совпадают . Любое конечное (непустое) множество точек из $W(K(X))$ называем наполнением капсулы $K(X)$. Наполнением второго плана называем любое изображение , аффинно эквивалентное какому-либо из изображений наполнения. Ясно, что само изображение X является одним из наполнений капсулы $K(X)$.

Две капсулы A и B называем непересекающимися, если $W(A)$ и $W(B)$ не имеют общих точек.

Пусть даны капсулы A и L. Обозначим через L' капсулу L после параллельного переноса. Если капсула L такова, что ее параллельным переносом можно поместить на A так, что все точки из A принадлежат W(L'), то говорим , что L накрывает A и называем L чехлом для A.

Назовем произвольную капсулу Z (невырожденную) опорой. Определим понятие размера капсулы A по опоре Z. Пусть задано направление – прямая α . Пусть a_α длина наибольшего отрезка , вмещающегося в A и параллельного α , аналогично и соответственно обозначаем z_α в Z.

Тогда отношение a_α/z_α называем размером A по опоре Z и по направлению α. Строим величины a_α/z_α по всем направлениям. Максимум на этом множестве называем размером A (по опоре Z) и обозначаем через $r_Z(A)$.

Частный случай введенного понятия - размер вырожденной капсулы из точек x и y по опоре Z - можно трактовать как расстояние между точками x и y по опоре Z .

Пусть A – капсула, и $G(A)$ - множество всех изображений из наполнения капсулы. Расстоянием между двумя изображениями X и Y из $G(A)$ называем расстояние Хаусдорфа между ними. Для каждого X из $G(A)$ определяем множество Y изображений из $G(A)$, имеющих максимальное расстояние до X . Это расстояние обозначим через $r(X)$. Этим определена тройка $< X, \{Y\}, r(X) >$. Далее рассматриваем множество $\{< X, \{Y\}, r(X) >\}$ таких троек для всех X из $G(A)$. На этом множестве определяем минимум по $r(X)$, т.е. такую тройку $< X, \{Y\}, r(X) >$, на которой значение $r(X)$ минимально. Соответствующее X называем центром капсулы. Ясно, что X - точка и представляет собой центр описанной окружности для A. Содержательно центр капсулы можно трактовать как изображение , максимальное различие которого с остальными изображениями из наполнения капсулы минимально.

Однако капсулу и ее наполнение мы рассматриваем с точностью до аффинных преобразований. При сжатиях-растяжениях описанная окружность превратится в эллипс, и таких эллипсов можно построить бесконечное множество. Нужно выбрать какой-то один из них. Воспользуемся имеющимся результатом [5, 6] о том , что для выпуклого многоугольника существует и единственен описанный эллипс с наименьшей площадью. Центр этого эллипса и будем называть центром капсулы. При аффинных преобразованиях капсулы A с описанным эллипсом E отношение площадей сохраняется. Это значит, что для преобразованной капсулы A' преобразованный эллипс E' будет по прежнему минимальным из возможных по площади, а центр у E' - центром капсулы A' .

Пусть теперь A^+ есть набор $A_1, \ldots, A_k$, $k \geq 1$, попарно непересекающихся капсул. Капсулу L называем чехлом набора A^+, если L является чехлом для каждой капсулы в A^+. Размер набора A^+ (по опоре Z) – наибольший из размеров капсул в A^+. Наполнением набора A^+ называем совокупность наполнений каждой из капсул в A^+. Наполнение второго плана - любое изображение , аффинно эквивалентное какому-либо из изображений наполнения набора A^+.

Ясно, что набор капсул тоже есть изображение, и, с другой стороны, каждое изображение может рассматриваться как набор вырожденных (до точки) капсул.

Пусть дан набор капсул B^+, состоящий из капсул $K_1, \ldots, K_l$. Пусть выбраны капсулы с номерами i и j $(i, j = 1, \ldots, l, i \neq j)$. Склейкой называем объединение $U(K_i, K_j)$ капсул K_i и K_j и замена их на капсулу $K(U(K_i, K_j))$. Если эта капсула не пересекается с остальными капсулами , то получившийся набор капсул называем укрупнением исходного набора, а саму операцию – операцией укрупнения. Ясно , что к получившемуся укрупнению можно снова применять операцию укрупнения, и т.д. Через $B^{+\times}$ обозначим множество всех укрупнений для B^+ (включая само изображение B^+). Количество t капсул в них может меняться от 1 до l . Через $B_t^{+\times}$ обозначим подмножество множества всех укрупнений, состоящее из наборов с t капсулами.

По сути , футляр A^+ - это своеобразный прогноз, означающий то, что на месте A^+ может оказаться любое изображение из наполнения этого футляра (в том числе и некоторые другие футляры, и исходное изображение A). Футляр $\overset{+}{2}$ назовем сужением футляра $\overset{+}{1}$, если каждое изображение из наполнения $\overset{+}{2}$ аффинно эквивалентно с некоторым изображением из наполнения футляра $\overset{+}{1}$.Ясно, что для этого принадлежать наполнению футляра $\overset{+}{1}$ должно либо изображение $\overset{+}{2}$, либо некоторое его укрупнение.

Пусть H - множество всех изображений из наполнения набора капсул A^+. Максимум различий между изображениями из H будет определяться в целом тем , насколько большим может быть расстояние между точками изображений в одной капсуле, то есть, по сути, размером набора A^+ - чем больше размер A^+, тем в целом более различающимися могут быть изображения в наполнении набора A^+. Это можно трактовать так, что «обобщенная форма» фигуры таким набором капсул задана менее точно, в сравнении с набором, у которого размер меньше.

Для дальнейшего нам понадобятся некоторые понятия и ранее опубликованные результаты [**?**, **?**, **?**]. Содержательный смысл их в том, чтобы обеспечить наложение одного изображения на другое аффинными преобразованиями так, чтобы они "почти совпадали т.е. чтобы различие между изображениями было бы минимальным из возможных.

Пусть изображение A состоит из точек $a_1, \ldots, a_n$, изображение – из точек $b_1, \ldots, b_n$, ψ - одно из возможных взаимно однозначных соответствий между точками изображений A и , которым точке a_i из A сопоставляется точка $b_{\psi(i)}$ из $(i = 1, \ldots, n)$. Обозначим через B^* мно-

жество всех изображений, получаемых из аффинными преобразованиями. Полагаем, что на B' из B^* сохраняется нумерация, порожденная изображением , т.е. через b'_i на B' обозначается точка, в которую переходит при соответствующем преобразовании точка b_i из . Точки a_i и $b_{\psi(i)}$называем соответствующими, соответствующими называем и отрезки $(a_i a_j)$ и $b_{\psi(i)}b_{\psi(j)}$.

Зададимся некоторым положительным числом ε . Обозначим через $\{B\}^{\varepsilon}$ множество всех таких изображений B' из B^*, для которых длина каждого отрезка $(b_i b'_i)$ $(i = 1, \ldots, n)$ не больше ε . Преобразования, переводящие изображения из $\{B\}^{\varepsilon}$ друг в друга , назовем ε -аффинными. Содержательно их можно трактовать как ограниченные, локальные аффинные преобразования для B.

Дадим важное определение искомого (или оптимального) взаиморасположения: через $l_A(B')$ обозначим длину наибольшего из отрезков $a_i b_{\psi(i)}$ $(i = 1, \ldots, n)$. Рассмотрим B_0 – некоторое изображение из B^*, и ψ_0 - одно из взаимно однозначных соответствий между точками изображений A и B. Пусть существует такое ε_1 , что для всех B' из $\{B_0\}^{\varepsilon_1}$ и при всех биекциях ψ минимум величин $l_A(B')$ достигается на изображении B_0 и при биекции ψ_0 . Пусть существует такое ε_2 , что для всякой пары изображений (A', B'_0), получаемой ε_2-аффинными преобразованиями пары (A, B_0) как целого, выполняется аналогичное свойство: для всех B'' из $\{B'_0\}^{\varepsilon_1}$ и при всех биекциях ψ минимум величин $l_{A'}(B'')$ достигается на изображении B'_0 и при биекции ψ_0 . Тогда B_0 называем искомым для изображения A (и взаиморасположение A и B_0 искомым), биекцию ψ_0 - искомым соответствием между точками в A и .

Нетрудно видеть, понятие оптимального взаиморасположения можно рассматривать, как строящееся, в некотором приближении, на основе понятия расстояния Хаусдорфа между множествами.

Из полученных ранее результатов [?] следуют некоторые необходимые условия , которым должны удовлетворять изображения в паре (A, B_0) . Они коротко состоят в следующем . Пусть биекцией ψ точке a_i из A сопоставляется точка $b'_{\psi(i)}$ из $(i = 1, \ldots, n)$. Возьмем на плоскости произвольную точку O и параллельными переносами отрезка $a_i b'_{\psi(i)}$ совместим точку a_i с точкой O. Точку, в которую перейдет при этом $b'_{\psi(i)}$, обозначим через $c_{i\psi(i)}$ и назовем порожденной парой соответствующих точек a_i и $b'_{\psi(i)}$. Изображение из точек $c_{i\psi(i)}$ $(k = 1, \ldots, n)$ называем характеристическим , O – центр характеристического изображения, $c_{i\psi(i)}$ - точки ядра. Окружность наименьшего по радиусу круга, включающего все точки ядра, называем ключевой. Доказано [?], что для пары (A, B_0)

центр характеристического изображения с необходимостью должен совпадать с центром ключевой окружности.

Назовем изображение B' из B^* согласованным с A, если существуют в B' два непараллельных отрезка $(b'_1b'_2)$ и $(b'_3b'_4)$, равные , параллельные и однонаправленные с соответствующими отрезками (a_1a_2) и (a_3a_4) в A. Параллельные отрезки , например , (a_1a_2) и $(b'_1b'_2)$ называем однонаправленными , если, при условии, что (a_1a_2) слева направо сначала идет точка a_1 , а затем a_2 , то и в отрезке $(b'_1b'_2)$ слева направо сначала идет точка b'_1 , затем b'_2 .

Доказано , что если B_0 искомое изображение для A ,то B_0 согласовано с A.

Итак, имеем теперь два необходимых условия для пары (A, B_0): искомое изображение B_0 должно быть согласовано с A , и центр характеристического изображения пары (A, B_0) должен совпадать с центром ключевой окружности. Сочетание этих двух условий позволяет вычленить из $*$ конечное подмножество изображений, среди которых только и может находиться искомое изображение B_0 .

Действительно, согласовывать B' с A можно по разным парам отрезков. Пусть , например, задана пара отрезков (a_1a_2) и (a_3a_4) и эти отрезки равны параллельны и однонаправленны с соответствующими отрезками в B' , т.е. с отрезками $(b'_1b'_2)$ и $(b'_3b'_4)$. Однако этим условием определяется не единственное изображение из B^* , а некоторое их множество, и изображения в этом множестве переводимы друг в друга параллельными переносами. Но, как показано в [?] , среди них существует и единственно такое – обозначим его через B_{1234} – для которого в паре с A центр ключевой окружности совпадает с центром характеристического изображения.

Отрезки (a_1a_2) и (a_3a_4) можно выбрать в A не более чем $(C_n^2)^2$способами. Соответственно не больше будет и изображений B_{1234}. Множество их обозначим через $(A \mid \{B\})_\psi$. Объединим множества $(A \mid \{B\})_\psi$ для всех ψ. Это и будет множеством, в котором находится искомое изображение, обозначим его как $(A \mid \{B\})$, и назовем множеством изображений B, потенциально искомых для A . Заметим, что так определенное $(A \mid \{B\})$ выглядит требующим для своего построения конечного, но довольно большого перебора (главным образом за счет большого числа биекций ψ). Однако этот перебор можно существенно сократить [?]. И здесь уместно сделать некоторое общее замечание: построения тут и далее по тексту предполагают иногда конечный, но большой перебор. Почти всегда его можно кардинально уменьшить, однако здесь мы этим не занимаемся, оставляя на будущее, и довольствуясь здесь конечностью.

Отметим , что в частном случае A может быть, конечно, аффинно эквивалентным с B.

Далее пошагово опишем процедуру, которая для конечной совокупности наборов капсул устраивает на этой совокупности расширения наборов капсул , повышающие их «вместимость», а затем «чистку» совокупности, оставляющую минимально необходимую совокупность наборов капсул .

I. Пусть даны два набора капсул A^+ из капсул $A_1, \ldots, A_n$ и B_+ из капсул $B_1, \ldots, B_n$, и чехол L для A^+ . Называем здесь A^+ подложкой, а изображение B_+ трактуем как предназначенное для наложения аффинными преобразованиями на подложку A^+ . Полагаем, что в изображения A^+ и B_+ включены центры их капсул. Это точки соответственно $a_1, \ldots, a_n$ – обозначаем их совокупность через a_+ - и $b_1, \ldots, b_n$ – обозначаем через b_+ . Далее строим множество $(a^+ \mid \{b^+\})$ преобразованных изображений b_+ , потенциально искомых для a_+ . Изображение a_+ является частью изображения A^+ . Каждому из изображений в $(a^+ \mid \{b^+\})$ соответствует некоторым образом преобразованное изображение B^+ , частью которого оно является. Тем самым , множеству $(a^+ \mid \{b^+\})$ можно сопоставить множество $V(A^+ \mid \{B^+\})$ преобразованных изображений B^+ , по разному расположенных на изображении A^+ .

Возьмем теперь произвольный набор капсул B'^+ из $V(A^+ \mid \{B^+\})$, состоящий из капсул $B'_1, \ldots, B'_n$ причем капсула $B'_{\psi(i)}$ сопоставлена капсуле A_i $(i = 1, \ldots, n)$. Для каждой пары капсул A_i и $B'_{\psi(i)}$ рассматриваем их склейку $U(A_i, B'_{\psi(i)})$ и капсулу $K(U(A_i, B'_{\psi(i)}))$, которую обозначаем через K_i . Если каждая из капсул K_i накрывается чехлом L для A^+ и все капсулы K_i попарно не пересекаются, то набор K_i капсул называем приемлемым расширением подложки A^+ (за счет объединения с набором B'^+ и обозначаем через $(A^+ + B'^+)$ (где B'^+ из $V(A^+ \mid \{B^+\})$.

Трактовка и особенность построенного набора капсул $(A^+ + B'^+)$ в том, что и A^+ , и B'^+ принадлежат наполнению этого набора. Если рассматриваем два любых изображения, являющиеся наполнениями для A^+ и B^+ , то эти A^+ и B^+ можно считать определяющими некоторое деление на «куски» этих изображений, а биекция ψ - соответствие между кусками.

Далее строим приемлемое расширения вида $(A^+ + B'^+)$ подложки A^+ для каждого набора B'^+ из $V(A^+ \mid \{B^+\})$ (если такое расширение есть). Результат процедуры - множество $\{(A^+ + B'^+))\}$ приемлемых расшире-

ний подложки A^+ , и множество ψ соответствий между капсулами в A^+ и B_+ .

Если множество $\{(A^+ + B'^+))\}$ не пустое, то B_+ называем вложимым в A^+ , в противном случае – не вложимым.

II. Мы рассмотрели пару изображений A^+ и B_+. Теперь – некоторое обобщение: пусть вместо одного изображения B_+ имеем некоторую их совокупность $B_1^+, \ldots, B_k^+$, где $k \geq 1$. Для каждого B_i^+ $(i = 1, \ldots, k)$ строим множество $\{(A^+ + B_i'^+)\}$, и пусть Q – объединение всех этих множеств. Далее рассматриваем подмножество q множества Q , обладающее следующими свойствами:

1) каждая расширенная подложка из q состоит из капсул $K_1, \ldots, K_n$. Для каждого s $(s = 1, \ldots, n)$ объединяем (склеиваем) капсулы K_s из всех подложек из q и обозначаем их объединение через K'_s , через K_s^q обозначаем капсулу $K(K'_s)$. Пусть при этом каждая из капсул K_s^q накрывается чехлом L подложки A и капсулы попарно не пересекаются. Тогда подмножество q называем правильным.

2) пусть для любого q' такого, что q является его собственным подмножеством, это q' правильным уже не является. Тогда q называем правильным и полным. Набор капсул $K_1^q, \ldots, K_n^q$ называем расширением исходного набора A^+ , порожденным множеством q, и обозначаем через A_q^+ , а те из $B_1^+, \ldots, B_k^+$, которые в виде соответственно преобразованных $B_i'^+$ вложимы в соответствующие расширенные подложки A'^+ из q, называем вложимыми в A^{+q} .

Итогом описанных процедур для A^+ и $B_1^+, \ldots, B_k^+$ являются расширения $A_1^{+q}, \ldots, A_p^{+q}$ исходного набора капсул A^+ , построенные для каждого возможного правильного и полного подмножества q, и множества $\{B^+\}_1, \ldots, \{B^+\}_p$ вложимых в эти расширения изображений из совокупности $B_1^+, \ldots, B_k^+$. Подчеркнем, что , по построению, для каждого расширения A_i^{+q} ,все наборы капсул из $\{B^+\}_i$ $(i = 1, \ldots, p)$ принадлежат наполнению этого расширения.

Напомним, что последовательность рассмотрений была такой: сначала рассмотрели подложку A^+ и изображение B_+ , которое разными способами пытаемся вложить, «вместить» в A^+ . Если «точного» вложения нет , то расширяем исходный набор капсул A^+ по некоторым правилам, как бы «склеивая» B_+ с A^+ . Итогом этой процедуры была совокупность по разному расширенных A^+ . Затем, следующим шагом, для подложки A^+ мы рассмотрели уже не одно изображение B_+ , а некоторую их совокупность $B_1^+, \ldots, B_k^+$, и которые тоже , как в предшествующей процедуре, мы пытаемся по разному вместить в A^+ . Промежуточным

итогом этой процедуры является множество Q по разному расширенных исходных подложек A^+ , с указанием того, с помощью каких из изображений $B_1^+, \ldots, B_k^+$ это расширение получено. Затем берем подмножество q множества Q со свойствами правильности и полноты: правильность означает, что все наборы в q можно «покапсульно склеить», и в получившемся наборе капсулы будут попарно непересекающимися и вмещающимися (каждая) в чехол для исходного изображения A^+ ; полнота означает, что q «максимален», т.е. его нельзя расширить, и при этом сохранить правильность. В итоге все возможные q дают совокупность m расширенных наборов капсул $A_1^{+q}, \ldots, A_p^{+q}$, с информацией о том, какие из изображений $B_1^+, \ldots, B_k^+$ вложимы в каждый из этих расширенных наборов капсул.

III. Предыдущий шаг – это рассмотрение подложки A^+ и совокупности изображений $B_1^+, \ldots, B_k^+$. Следующий шаг – рассмотрение совокупности наборов капсул $A_1^+, \ldots, A_k^+$. Поочередно берем каждый из этих наборов в качестве подложки , а все $A_1^+, \ldots, A_k^+$, включая выбранную подложку, в качестве $B_1^+, \ldots, B_k^+$. Для каждого такого случая строим совокупность m расширенных наборов капсул с информацией о том, какие из изображений $A_1^+, \ldots, A_k^+$ вложимы в каждый из этих расширенных наборов капсул. Далее рассматриваем множество M – объединение всех совокупностей m. Для каждого A^+ из M через A^{++} обозначаем множество тех из $A_1^+, \ldots, A_k^+$, что вложимы в A^+ .

IV. Заключительный шаг можно условно назвать чисткой множества M. Дело в том, что в M может быть много «лишних» изображений, например, за счет возможной повторяемости изображений в исходном наборе $A_1^+, \ldots, A_k^+$.

Рассматриваем такие совокупности изображений A^+ из M, у которых объединение их множеств A^{++} содержит исходный набор изображений $A_1^+, \ldots, A_k^+$. Среди этих совокупностей выбираем совокупность с наименьшей мощностью (если таких совокупностей не одна, то любую из них). Обозначим эту совокупность через M^*, она и есть искомая. Это есть минимальное множество расширенных наборов капсул таких, что в них вкладываются все изображения исходного набора.

Описанную процедуру обозначим как PROC , исходными для нее являются совокупность наборов капсул $A_1^+, \ldots, A_k^+$ и их чехлов $L_1, \ldots, L_k$ Результат процедуры – 1) совокупность расширенных наборов капсул $A_1^{+q}, \ldots, A_u^{+q}$, 2) для каждого из A_i^{+q} $(i = 1, \ldots, u)$ - множество A_i^{++} тех из исходных изображений $A_1^+, \ldots, A_k^+$, что вложимы в A_i^{+q} , и 3) чехлы для каждого из $A_1^{+q}, \ldots, A_u^{+q}$, обозначим их как $L_1^{+q}, \ldots, L_u^{+q}$.

Пусть теперь дано изображение A (например, некоторая фигура). Это набор вполне конкретных точек на плоскости. Наша цель – создать на базе изображения A такое его описание, которое поднималось бы до описания «образа» A . Первыми шагами в этом направлении было, как отмечалось выше, создание кода изображения A , который определяет изображение с точностью до аффинных преобразований, т.е. независимо от конкретного места на плоскости, от вращений, изменений в размерах, сжатий и растяжений. Однако этого недостаточно, ибо, ясно, к образу A надо относить и изображения, у которых в сравнении с A , например , сделаны некоторые локальные трансформации, и изображения, отличающиеся от A числом точек, и т.д. Мы используем для описания образа A набор капсул A^+ . Капсулы в A^+ полагаем образованными точками из A и включающими как наполнение все точки из A, т.е. это покрытие. Тогда относить (на этом шаге) к образу A можно все изображения из наполнения A^+ (и наполнение второго плана, т.е. все изображения , аффинно эквивалентные наполнению). Сразу вырисовываются ограничения, которые разумно наложить на A^+ : нужна как можно большая одинаковость капсул по размерам. Действительно, капсулы соответствуют разбиению исходного A на «куски», и это разбиение представляет форму изображения A, если «куски» равновелики. В противном случае, например , если есть один огромный «кусок», накрывающий практически все изображение, а остальные «куски» – какие-то точки на периферии, то такое разбиение трудно назвать представляющим форму исходного изображения. Кроме того, как отмечено в замечании выше, чем больше размер наибольшей капсулы в наборе, тем , при том же количестве капсул , больше будут разниться изображения в наполнении, т.е. тем менее «определенную» форму они в совокупности, можно считать, задают.

В качестве опоры для измерения размеров капсул в A^+ используем капсулу $K(A)$ (т.е. «накрывающую» все точки изображения A). Это своеобразная граница изображения A. У этой капсулы есть и та особенность, что какой бы набор капсул A^+ для изображения A мы не использовали, в этом A^+ есть все точки, составляющие $K(A)$.

Будем полагать, что форма чехлов для капсул есть форма капсулы $K(A)$, т.е. каждый чехол представляет собой уменьшенную с надлежащим коэффициентом и с сохранением подобия капсулу $K(A)$. Тогда минимальным возможным коэффициентом для чехла произвольной капсулы , является, нетрудно видеть, ее размер.

Капсул для A – конечное множество . Тем самым возможных размеров капсул – тоже конечное множество . Выстроим эти числа (размеры)

в порядке возрастания : $r_0, r_1, \ldots, r_t$. Здесь, очевидно, всегда $r_0 = 0$, и $r_t = 1$. Из этих капсул выстраиваем все возможные наборы A^+ капсул для изображения A (т.е. из попарно непересекающихся капсул и накрывающих изображение A). Обозначим это множество через $W(A)$. Поскольку размер набора капсул – это размер наибольшей капсулы в нем, то все возможные размеры наборов капсул для изображения A характеризуются той же цепочкой чисел $r_0, r_1, \ldots, r_t$, обозначим ее через r^*.

Множество $W(A)$ – все возможные наборы капсул для A, с разным количеством составляющих набор капсул , и с разными по размерам капсулами в одном наборе. Эти две характеристики – число капсул в наборе и степень разброса капсул по размерам – можно связать в рамках некоторой процедуры, которую можно трактовать, как балансировку. Обозначим через $(W(A), r_i)$ подмножество множества $W(A)$, состоящее из тех наборов капсул, размеры которых не превышают r_i , где r_i из r^*. Далее на $(W(A), r_i)$ рассмотрим все наборы с минимальным числом капсул. Если это число обозначить через n_i , то соответствующее подмножество обозначим через $(W(A), r_i, n_i)$. Такие наборы капсул трактуем как сбалансированные по количеству (капсул) . Ясно, что n_i может принимать значения от 1 до n , где n – число точек в изображении A. Объединим теперь множества $(W(A), r_i, n_i)$ для всех n_i $(n_i = 1, \ldots, n)$ и обозначим через $\{(W(A), r_i, n_i)\}$. Это множество всех сбалансированных по количеству капсул наборов капсул изображения A. Разобьем его на подмножества $F_1, \ldots, F_n$, в каждом F_i содержатся наборы капсул с i капсулами. Далее в каждом F_i оставляем только наборы с наименьшим размером – называем это балансировкой по размеру. Оставшиеся в $F_1, \ldots, F_n$ наборы капсул сбалансированы по количеству и по размерам .

Поскольку в F_i могут быть футляры мало отличающиеся и вложимые в общее для них расширение, то к F_i применим процедуру чистки Proc , введенную выше, и обозначим результат через F_i^* . Изображения из F_i^* (i=1,. . . ,n) называем футлярами для A. Ясно что в F_1^* всего одно изображение, и это капсула $K(A)$, в F_n^* тоже одно изображение, и это изображение A, в F_2^* изображения состоят из двух примерно равных половинок, и т.д

По сути , футляр A^+ - это своеобразный прогноз, означающий то, что на месте A^+ может оказаться любое изображение из наполнения этого футляра (в том числе и некоторые другие футляры, и исходное изображение A). Футляр A_2^+ назовем сужением футляра A_1^+ , если каждое изображение из наполнения A_2^+ аффинно эквивалентно с некоторым изображением из наполнения футляра A_1^+ .

Далее с использованием $F_1^*, \ldots, F_n^*$ построим ярусный граф G_A , который в целом трактуем как очередное приближение к понятию образа , которому принадлежит исходное изображение A. Ярусу с номером i соответствует F_i^* , вершины яруса – футляры из F_i^* . Нижний ярус в графе (с номером 1) состоит всего из одной вершины, соответствующей футляру с одной капсулой $K(A)$, верхний ярус (с номером n) состоит тоже из одной вершины, соответствующей футляру с n капсулами, то есть исходному изображению A . В ярусе с номером i (i=1, ... ,n) вершинам соответствуют футляры, состоящие из i капсул. От каждой вершины в $n-1$ ярусе проводим ребро к вершине в n-ом ярусе. Это обозначает то, что футляр (единственный) из F_n с некоторым укрупнением вкладывается в каждый из футляров в $F_n - 1$. Действительно, исходное изображение A является очевидным сужением для футляров в $F_n - 1$, как, впрочем , и для любых футляров в $F_1^*, \ldots, F_n - 1^*$.

Ребра в графе G_A строим по индукции. Базис индукции – уже построенные ребра между вершинами в ярусах с номерами $n-1$ и n . Ребра считаем направленными, с направлением от вершин в ярусах с меньшими номерами к вершинам в ярусах с большими номерами. Между вершинами в одном ярусе ребер нет.

Пусть теперь уже есть ребра между вершинами в ярусе с номером i (i=2, ... , n-1) и вершинами во всех ярусах с номерами большими i . Строим ребра между вершинами в ярусе с номером $i-1$ и вершинами в ярусах с большими номерами. Это тоже индукция, по k , $k = i, \ldots, n$. Пусть x – одна из вершин яруса $i-1$ и ей соответствует футляр X ,y – одна из вершин яруса k и ей соответствует футляр Y. Если имеется путь из вершины x в вершину y, то ребро между ними не проводим. Если нет , то для Y определяем множество $\{Y^\times\}_i - 1$. Напоминаем – это множество всех укрупнений футляра Y, состоящих из $i-1$ капсул. Футляр X рассматриваем как подложку, наборы капсул из $\{Y^\times\}_i - 1$ - как налагаемые изображения. Если хотя бы один Y' из $\{Y^\times\}_i - 1$ вложим в X , то проводим ребро между вершинами x и y. Описанное проделываем для всех x из яруса i , и всех y из яруса k.

Граф G_A определен. Он и есть, в некотором приближении, описание (полное) образа, извлекаемое из всего лишь одного изображения A, принадлежащего этому образу. При этом граф в целом скорее можно трактовать как набор описаний, а одним таким описанием считать путь из условного корня графа – вершины, соответствующей футляру из одной капсулы – в вершину с футляром, представляющим собой исходное

изображение A. Чем больше вершин на этом пути, тем более полным можно полагать такое описание образа.

Трактовку такому пути, и соответственно, цепочке футляров , можно дать следующую. Начало пути – футляр из всего одной капсулы. Это максимальное обобщение исходного изображения A, настолько максимальное , что в наполнении этого футляра, нетрудно видеть , находятся любые изображения. Конец пути – максимальная конкретика , т.е. само изображение A (напоминаем, рассматриваемое с точностью до аффинных преобразований), Это значит , что в этот «футляр», т.е. в изображение A, «вкладываются» только изображения, аффинно эквивалентные с A. Пусть теперь x и у из ярусов с номерами i и j $(i < j)$– любые две соседние вершины на этом пути. Им соответствуют футляры X и Y. При этом футляр Y с j капсулами, укрупненный до i капсул , вкладывается в подложку X (возможно, в некоторое ее расширение, ограничиваемое чехлом подложки). Это значит, что футляр Y и все его наполнения можно трактовать как получаемые из наполнения футляра X с последующим его дроблением. В этом смысле Y не противоречит X, и есть его сужение, его «конкретизация».

Отметим, что многое из процедур , описанных выше, можно делать, основываясь не на собственно изображении A , а только на его коде [**?**], определяющем изображение с точностью до аффинных преобразований: это и определение внутренних и контурных точек, и построение капсул и наборов капсул , и пр.

Список литературы

[1] В.Н. Козлов, *Введение в математическую теорию зрительного восприятия*, Издательство Центра прикладных исследований при механико-математическом факультете МГУ, М., 2007.

[2] В.Н. Козлов, “О распознавании аффинно разных дискретных изображений”, *Интеллектуальные системы*, **2**, 1998, 95-122.

[3] В.Н. Козлов, “О зрительном образе, математических подходах к определению этого понятия и о распознавании изображений”, *Журнал вычислительной математики и математической физики*, **39**, 1999, 1929-1946.

[4] V.N. Kozlov, “Visual Pattern and Geometric Transformation of Images”, *Pattern Recognition and Image Analysis*, **10**, 2000, 321-342.

[5] Л. Данцер , Б. Грюнбаум , В. Кли, *Теорема Хелли и ее применения*, Издательство «Мир», М., 1968.

[6] В.Л. Загускин, “Об описанных и вписанных эллипсоидах экстремального объема”, *Успехи математических наук*, **13**, 1958, 89-93.

Image segmentation and shape-preserving transformations

V.N. Kozlov

The image in the paper is a finite (non-empty) set of points in Euclidean spaces of different dimensions. Briefly, the work consists in having an image belonging to a certain image to extract from this image what could be called a description of this image.

Keywords: mathematical definition of the image, image recognition.

Некоторые свойства перестановочной конструкции для параметрического задания квазигрупп

Пивень Н.А.

В работе исследуются свойства так называемой перестановочной конструкции, введенной ранее. Выясняется, что конструкция несколько избыточна, но в результате ее улучшения, она оказывается инъективной для случая линейных правильных семейств булевых функций, и, возможно, инъективной в общем.

Ключевые слова: квазигруппы, правильные семейства булевых функций, латинские квадраты, параметрическое задание

1. Введение

В наши дни разрабатываются различные способы защиты информации, использующие латинские квадраты. Это связано в частности с тем, что К. Шеннон показал, что шифры, построенные на латинских квадратах, обладают свойством “совершенной секретности” ([1]). Латинские квадраты естественным образом связаны с квазигруппами, а именно, в случае конечных квазигрупп, квазигрупповая операция может быть задана таблицей Кэли, являющейся латинским квадратом. Примеры использования квазигрупп для решения различных задач криптографии можно найти в работах [2, 3, 4, 5].

В. А. Носовым в работе [6] был предложен способ задания больших семейств латинских квадратов с помощью так называемых правильных семейств функций. В работе [7] предлагается усиление конструкции В. А. Носова, названное перестановочной конструкцией. При ее использовании удается получить большее количество различных латинских квадратов из того же набора правильных семейств, и более того, на практике было обнаружено, что больший процент из полученных с ее помощью квадратов обладает криптографически важным свойством полиномиальной полноты.

Дальнейшее изложение имеет следующую структуру. В разделе 2 даются основные определения. В разделе 3 анализируются избыточность текущей перестановочной конструкции. В разделе 4 вводится перестановочная конструкция с устранением обнаруженной избыточности и доказывается инъективность полученной конструкции для линейных правильных семейств.

2. Основные понятия

Определение 1. Конечной квазигруппой (Q, f_Q) называется множество Q, $|Q| < \infty$, на котором определена бинарная операция f_Q такая, что для любых элементов $a, b \in Q$ уравнения $f_Q(a, x) = b$ и $f_Q(y, a) = b$ однозначно разрешимы в Q.

В дальнейшем мы будем опускать слово “конечная”.

Определение 2. Латинским квадратом порядка n называется матрица размера $n \times n$, заполненная элементами некоторого n–элементного множества таким образом, что в каждой её строке и в каждом столбце все элементы различны.

Квазигрупповую операцию можно задавать табличным способом: для множества элементов $\{q_1, \ldots, q_m\}$, составляющих квазигруппу Q, выписывается квадратная таблица $m \times m$, такая что на пересечении i–ой строки и j–го столбца стоит $f_Q(q_i, q_j)$. Заметим, что построенная таким образом таблица, в связи с существованием и единственностью решения уравнений $f_Q(a, x) = b$ и $f_Q(y, a) = b$, является латинским квадратом, который мы и называем латинским квадратом, связанным с квазигруппой.

Определение 3. Семейство булевых функций $\mathrm{F}=\{f_i\}_{i=1}^n$, $f_i = f_i(x_1, \ldots, x_n)$, называется правильным, если для любых различных значений аргументов $x' = (x'_1, \ldots, x'_n)$ и $x'' = (x''_1, \ldots, x''_n)$ найдется такой индекс $\alpha \in \{1, \ldots, n\}$, что $x'_\alpha \neq x''_\alpha$, $f_\alpha(x'_1, \ldots, x'_n) = f_\alpha(x''_1, \ldots, x''_n)$

Правильные семейства функций были введены В. А. Носовым в работе [6] для построения латинских квадратов порядка 2^n. Занумеруем элементы множества Q, $|Q| = 2^n$, числами от 0 до $2^n - 1$. Таким образом, каждому элементу $a \in Q$ можно сопоставить n–битный вектор $(a_1, \ldots, a_n)$, задающий двоичную запись номера. В результате квазигрупповая операция f_Q может быть представлена в векторной форме: записи

$z = f_Q(x, y)$ и

$$\begin{aligned} z_1 &= f_Q^1(x_1, \ldots, x_n, y_1, \ldots, y_n), \\ &\vdots \\ z_n &= f_Q^n(x_1, \ldots, x_n, y_1, \ldots, y_n), \end{aligned}$$

где $f_Q^1, \ldots, f_Q^n$ — булевы функции, являющиеся компонентами вектор–функции, порожденной f_Q, эквивалентны.

Пусть $f_1, \ldots, f_n$ — булевы функции от n переменных, $\pi_1, \ldots, \pi_n$ — булевы функции от двух переменных. Рассмотрим следующее семейство функций от $2n$ переменных:

$$\begin{aligned} g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \\ &\vdots \\ g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \ldots, \pi_n(x_n, y_n)), \end{aligned} \tag{1}$$

где операция $\oplus$ означает сложение по модулю 2. В работе [6] показано, что семейство $G = \{g_1, \ldots, g_n\}$ задает латинский квадрат для любых функций $\pi_1, \ldots, \pi_n$ тогда и только тогда, когда семейство $F = \{f_1, \ldots, f_n\}$ правильное.

В работе [7] эта конструкция была усилена следующим образом. Пусть $n \in \mathbb{N}$, $F = \{f_1, \ldots, f_n\}$ — правильное семейство булевых функций, $\alpha, \beta, \gamma \in S_n$ — перестановки на множестве $\{1, \ldots, n\}$. Наложим перестановки α, β, γ на индексы переменных x и y и номера функций g в представлении (1):

$$\begin{aligned} g_{\gamma(1)} &= x_{\alpha(1)} \oplus y_{\beta(1)} \oplus f_1(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})), \\ &\vdots \\ g_{\gamma(n)} &= x_{\alpha(n)} \oplus y_{\beta(n)} \oplus f_n(\pi_1(x_{\alpha(1)}, y_{\beta(1)}), \ldots, \pi_n(x_{\alpha(n)}, y_{\beta(n)})). \end{aligned} \tag{2}$$

Это и было названо перестановочной конструкцией. Заметим, что исходное задание (1) получается из формул (2) при выборе тождественных перестановок в качестве α, β и γ. Также в работе [7] было показано, что после применения перестановочной конструкции к этим равенствам, семейство $G' = \{g_{\gamma(1)}, \ldots, g_{\gamma(n)}\}$ все еще задает латинский квадрат.

3. Избыточность перестановочной конструкции

В ходе практического применения введенной перестановочной конструкции было обнаружено, что, начиная с какого–то момента перебора перестановок, новых латинских квадратов уже не появлялось, что говорит об

избыточности перестановочной конструкции. Для доказательства теоремы о ее избыточности, нам потребуется следующая лемма.

Лемма 1. *При согласованной перестановке индексов функций и переменных правильного семейства, полученное в результате семейство также является правильным.*

Доказательство. Предположим, мы применили перестановку α к индексам функций и переменных правильного семейства F и получили семейство функций F', не являющееся правильным. Тогда из определения правильного семейства, $\exists$ различные $y', y'' : \forall d \in 1 \dots n$ выполнено $y'_d \neq y''_d \implies f'_d(y') \neq f'_d(y'')$.
Пусть D – множество индексов, в которых отличаются y' и y'', тогда это можно переписать как $\exists$ различные $y', y'' : \forall d \in D\ f'_d(y') \neq f'_d(y'')$. (3)
Вернемся теперь к правильному семейству F. Опять же по определению правильного семейства, $\forall$ различных $x', x'' \ \exists i \in 1 \dots n : x'_i \neq x''_i$ и $f_i(x') = f_i(x'')$ возьмем за эти x' и x'' выражения $\alpha^{-1}(y')$ и $\alpha^{-1}(y'')$ соответственно. Они различны, так как α перестановка, тогда $\alpha^{-1}(i) \in D$ и $f'_{\alpha^{-1}(i)}(y') = f'_{\alpha^{-1}(i)}(y'')$, что противоречит выражению (3) $\square$

Перейдем теперь к самой теореме.

Теорема 1. *Любой латинский квадрат, получаемый применением только перестановки γ в перестановочной конструкции, можно получить применением перестановок α, β, взятием другого правильного семейства и других функций π.*

Доказательство. Достаточно доказать утверждение для транспозиции. Без ограничения общности, возьмем транспозицию индексов 1 и 2. Таким образом,

$$\begin{aligned} g'_1 = g_2 &= x_2 \oplus y_2 \oplus f_2(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)) \\ g'_2 = g_1 &= x_1 \oplus y_1 \oplus f_1(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)) \\ &\vdots \\ g'_n = g_n &= x_n \oplus y_n \oplus f_n(\pi_1(x_1, y_1), \dots, \pi_n(x_n, y_n)), \end{aligned}$$

Теперь вместо транспозиции по индексам g применим транспозицию по индексам 1 и 2 для x и y, возьмем правильное семейство, полученное согласованной перестановкой 1 и 2 индекса (такое правильное семейство существует согласно лемме) и возьмем функции π', такие, что $\pi'_1 = \pi_2$ и

$\pi'_2 = \pi_1$, остальные без изменений. Получим:

$$\begin{array}{rcl} g''_1 & = & x_2 \oplus y_2 \oplus f'_1(\pi'_1(x_2,y_2), \pi'_2(x_1,y_1), \ldots, \pi_n(x_n,y_n)) \\ g''_2 & = & x_1 \oplus y_1 \oplus f'_2(\pi'_1(x_2,y_2), \pi'_2(x_1,y_1), \ldots, \pi_n(x_n,y_n)) \\ & \vdots & \\ g''_n & = & x_n \oplus y_n \oplus f'_n(\pi'_1(x_2,y_2), \pi'_2(x_1,y_1), \ldots, \pi_n(x_n,y_n)), \end{array}$$

Запишем это выражение через изначальные функции и получим:

$$\begin{array}{rcl} g''_1 & = & x_2 \oplus y_2 \oplus f_2(\pi_1(x_1,y_1), \ldots, \pi_n(x_n,y_n)) \\ g''_2 & = & x_1 \oplus y_1 \oplus f_1(\pi_1(x_1,y_1), \ldots, \pi_n(x_n,y_n)) \\ & \vdots & \\ g''_n & = & x_n \oplus y_n \oplus f_n(\pi_1(x_1,y_1), \ldots, \pi_n(x_n,y_n)), \end{array}$$

Отсюда несложно заметить, что g'' совпадает с g', что завершает доказательство. □

4. Улучшение перестановочной конструкции

Для доказательства теоремы этого раздела нам потребуется утверждение из [8] о том, что граф существенной зависимости правильного семейства линейных функций не содержит циклов. Графом существенной зависимости семейства линейных функций F вида

$$\begin{array}{rcl} f_1 & = & a_{11}x_1 + \ldots + a_{1n}x_n; \\ & \vdots & \\ f_n & = & a_{n1}x_1 + \ldots + a_{nn}x_n \end{array}$$

назовем ориентированный граф $\Gamma_F(V,E)$ на множестве вершин $V = (1,..,n)$, составляемый по правилу $(i,j) \in E \iff a_{ji} \neq 0$.

В прошлом разделе мы показали избыточность перестановочной конструкции. Заменим ее на конструкцию того же вида, но без применения перестановки γ (ну или просто скажем, что перестановка γ должна быть тождественной, что одно и то же). Перестановочная конструкция такого вида оказалась инъективной для линейных правильных семейств, а именно, верна следующая теорема.

Теорема 2. *Пусть Q' и Q'' – два различных латинских квадрата одного порядка, порожденных линейными правильными семействами методом*

Носова. $S' = (\alpha', \beta', id)$ *и* $S'' = (\alpha'', \beta'', id)$ *– произвольные перестановочные конструкции с* $\gamma = id$*, где* id *– тождественная перестановка. Тогда* $S'(Q') \neq S''(Q'')$

Доказательство. Предположим, что различные квадраты Q' и Q'' перешли в один и тот же квадрат Q с помощью перестановок α', β' и α'', β'' соответственно. Тогда Q' можно перевести в Q'' соответствующей композицией этих перестановок. То есть Q' переходит в Q'' при применении неких перестановок α и β, хотя бы одна из которых нетождественна (Иначе эти квадраты одинаковые. Пусть нетождественна α), к индексам x и y соответственно. Запишем это в виде явных формул (одно из уравнений) учитывая, что функции из F линейны:
$x_1 \oplus y_1 \oplus a_{11}\pi_1(x_1, y_1) \oplus \ldots \oplus a_{1n}\pi_n(x_n, y_n) = x_{\alpha(1)} \oplus y_{\beta(1)} \oplus a'_{11}\pi'_1(x_{\alpha(1)}, y_{\beta(1)}) \oplus \ldots \oplus a'_{1n}\pi'_n(x_{\alpha(n)}, y_{\beta(n)})$
остальные уравнения аналогичны для всех индексов от 2 до n. Рассмотрим равенство, где в левой части первым слагаемым является x_1, то есть выписанное. оно верно для любых наборов x и y. Подставим все нули, кроме $x_{\alpha(1)}$ и соберем все константы в одну. (учитывая, что a_{11} и a'_{11} нулевые из правильности семейств – иначе бы был цикл–петля в графе существенной зависимости). Получим:
$a_{1\alpha(1)}\pi_{\alpha(1)}(x_{\alpha(1)}, 0) = x_{\alpha(1)} \oplus c$
Распишем функцию π как многочлен от 2 переменных с учетом второго аргумента–нуля и занесем константу так же в с:
$a_{1\alpha(1)}ax_{\alpha(1)} = x_{\alpha(1)} \oplus c_0$
Теперь если мы подставим сюда $x_{\alpha(1)} = 0$, то получим, что $c_0 = 0$, а исходя из этого, $a = a_{1\alpha(1)} = 1$
Т.е. в терминах графа существенной зависимости, в нем есть ребро $(\alpha(1), 1)$
Далее рассмотрим такое же равенство, только в котором первым слагаемым является $x_{\alpha(1)}$ и аналогичным образом получим, что в этом графе есть ребро $(\alpha(\alpha(1)), \alpha(1))$ и т.д.
Так как индексов конечное количество, рано или поздно один из них повторится, что означает, что в графе существенной зависимости есть цикл, что противоречит правильности семейства.

□

Из этой теоремы и количества перестановок порядка n очевидным образом получаем

Следствие 1. *Пусть* $(L_1, \ldots, L_k)$ *– множество латинских квадратов порядка* 2^n*, порожденных линейными правильными семействами буле-*

вых функций. Тогда перестановочная конструкция порождает из этого множества $n!^2k$ *попарно различных латинских квадрата.*

Замечание 1. *Во время практической работы с перестановочной конструкцией, было замечено, что это следствие верно вообще говоря для любых семейств булевых функций в случае квадратов порядка 8. В перспективе планируется доказать это утверждение для квадратов произвольного порядка.*

5. Заключение

В работе проведено исследование так называемой перестановочной конструкции, найдена избыточность в ее определении, в определение внесена корректировка для устранения обнаруженной избыточности и доказано, что для нового определения в случае линейности булевых функций, используемых для построения латинских квадратов, избыточность отсутствует.

Список литературы

[1] C. Shannon, "Communication theory of secrecy systems", *Bell System Techn. J.*, **28**:4 (1949), 656–715; имеется перевод: К. Шеннон, "Теория связи в секретных системах", *Работы по теории информации и кибернетике*, Издательство иностранной литературы, Москва, 1963, 333–369.

[2] М.М. Глухов, "О применениях квазигрупп в криптографии", *Прикладная дискретная математика*, 2008, №2, 28–32.

[3] S. Markovski, D. Gligoroski, V. Bakeva, "Quasigroup String Processing: Part 1", *Proc. of Maked. Academ. of Sci. and Arts for Math. And Tech. Sci.*, **XX**:1–2 (1999), 13–28.

[4] S. Markovski, V. Kusacatov, "Quasigroup String Processing: Part 2", *Proc. of Maked. Academ. of Sci. and Arts for Math. and Tech. Sci.*, **XXI**:1–2 (2000), 15–32.

[5] V. Shcherbacov, "Quasigroup based crypto-algorithms", arXiv: 1201.3016v1.

[6] В.А. Носов, "О построении классов латинских квадратов в булевой базе данных", *Интеллектуальные системы*, **4**:3–4 (1999), 307–320.

[7] Н.А. Пивень, "Исследование квазигрупп, получаемых с помощью правильных семейств булевых функций порядка 2", *Интеллектуальные системы. Теория и приложения*, **22**:1 (2018), 21–35.

[8] В. А. Носов, А. Е. Панкратьев, "Латинские квадраты над абелевыми группами", *Фундамент. и прикл. матем.*, **12**:3 (2006), 65–71; *J. Math. Sci.*, **149**:3 (2008), 1230–1234.

Some properties of permutation construction for parametric assignment of quasigroups

Piven N.A.

We analyse so–called permutation construction, introduced before. It turns out, that it's redundant, so we propose an improvement, which makes it injective for linear functions and possibly injective without conditions

Keywords: Quasigroup, Latin square, parametric assignment, proper families of functions

Об алгоритме проверки наличия подквазигруппы в квазигруппе

Собянин П.И.

Рассматривается алгоритм проверки наличия подквазигруппы в квазигруппе. Сравнивается скорость выполнения его последовательной и параллельной версий на вычислительной архитектуре CUDA.

Ключевые слова: квазигруппа, подквазигруппа, GPU, CUDA.

1. Введение

В некоторых задачах криптографии оказывается полезным применение квазигрупп. Примером таких задач могут служить:

- построение кодов аутентификации (A-кодов) [1];
- шифрование [1];
- построение однонаправленных функций [1].

В работе сравнивается производительность последовательной [2] и параллельной версий алгоритма, устанавливающего наличие или отсутствие подквазигруппы в заданной квазигруппе. Вычисления проводились на GPU с архитектурой CUDA[3].

Задача данной статьи – исследовать разницу в производительности двух версий алгоритма. Насколько можно судить по имеющимся публикациям, подобное сравнение еще не проводилось.

Дальнейшая часть статьи построена следующим образом: в разделе 2 рассматривается сам алгоритм поиска подквазигрупп в заданной квазигруппе; раздел 3 посвящен описанию сравнительного эксперимента, его результатам и выводам; в разделе 4 подведены итоги текущей работы и освещены дальнейшие планы в предметной области.

2. Описание алгоритма

Пусть Q – конечная квазигруппа с элементами $q_1, q_2, ..., q_n, n \in N$, и операцией f. Перед запуском алгоритма нормализуем вид квазигруппы, заменяя ее элемент q_i на его индекс i.

Рассмотрим следующую процедуру:

1) Рассмотрим очередной элемент квазигруппы $i_k, 1 \leqslant k \leqslant n$.

2) Инициализируем множество $SQ = \{i_k\}$.

3) Инициализируем множество $SU = \emptyset$.

4) Если $|SQ| = |SU|$ или $|SQ| = |Q|$, то перейти к шагу 6, иначе перейти к шагу 5.

5) Рассмотрим произвольный индекс $j \in SQ \setminus SU$. Рассмотрим всевозможные пары (k, l), такие, что по крайней мере одно из значений k и l равно j, а оставшийся элемент либо равен j, либо принадлежит SU. Для каждой пары вычислим $t = f(k, l)$. Если $t \notin SQ$, то добавляем t к SQ. После рассмотрения всех пар добавляем j к SUи переходим к шагу 4.

6) Если k из шага 1 равен n, то перейти к шагу 7, иначе – к шагу 1, увеличив k на единицу.

7) Конец.

Другими словами, здесь SQ – это множество-кандидат в подквазигруппы, SU – множество просмотренных элементов. Последовательная версия алгоритма поочередно рассматривает элементы квазигруппы в качестве начальных элементов множества-кандидата. Параллельная же версия рассматривает всех кандидатов "одновременно", запуская алгоритм на множествах с разными начальными элементами на соответствующих им разных вычислительных потоках.

Оригинальное описание алгоритма приведено в [3].

3. Эксперимент

Описание. В качестве входных данных эксперимента генерировались наборы из 10 случайных квазигрупп заданного порядка. Порядок квазигрупп варьировался от 4 до 64. Алгоритм запускался на каждой квазигруппе из набора, замерялось время его выполнения в микросекундах.

Таким образом, для каждого набора входных данных на выходе мы получили информацию о времени работы алгоритма на каждом элементе набора. По каждому набору выходных данных брались минимальное, максимальное и среднее время исполнения, и по этим величинам строились сравнительные графики.

Мы тестировали версии алгоритма на видеокарте Tesla C2070, на которой установлен графический процессор Tesla T20 с 448 вычислительными ядрами, работающих на частоте 1.15 ГГц.

Результаты. По оси X на всех рисунках отложен порядок входной квазигруппы. По оси Y на всех рисунках отложено время выполнения операции в микросекундах.

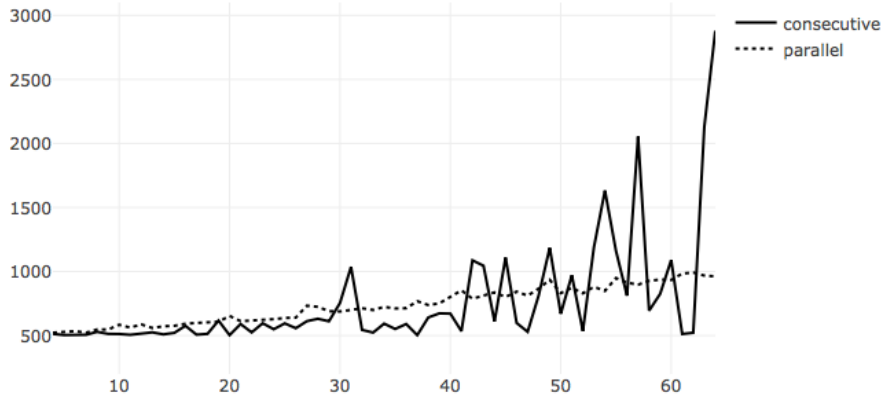


Рис. 1. Быстрейшее время работы двух версий алгоритма в зависимости от порядка квазигруппы.

Результаты тестов показывают, что порядок роста времени совпадает с теоретическим: в параллельном случае рост линейный, а в последовательном – порядка $O(n^2)$, как и ожидалось.

На рис. 1 видно, что зачастую последовательный алгоритм отрабатывает быстрее параллельного. Это объясняется тем, что последователь-

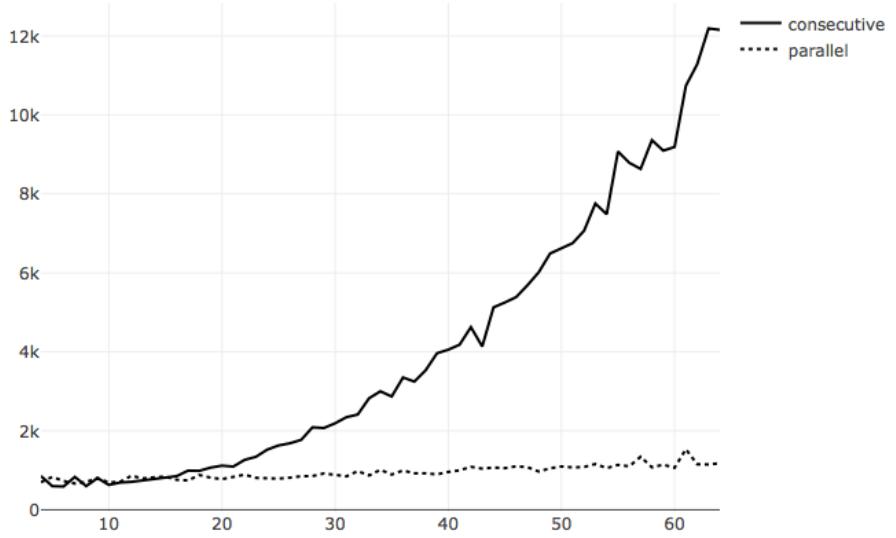


Рис. 2. Наименьшая скорость работы двух версий алгоритма в зависимости от порядка квазигруппы.

ный алгоритм завершает свою работу сразу, как только подквазигруппа будет найдена, т.е. цикл из шага 1 обрывается до его завершения; параллельная же версия дожидается окончания работы процедуры на каждом используемом в данный момент вычислительном потоке и только тогда завершает свою работу. Время работы алгоритма на каждом потоке, вообще говоря, различно – это зависит от входного элемента. Так, например, какой-то поток может найти подквазигруппу за одну итерацию и завершить работу; на другом же потоке алгоритм может установить отсутствие подквазигруппы с входным элементом, и для этого ему потребуется максимум итераций, что влечет за собой увеличение времени работы.

4. Заключение

Параллельная версия алгоритма дает значительное ускорение по сравнению с последовательной версией. В дальнейшем планируется обобщить

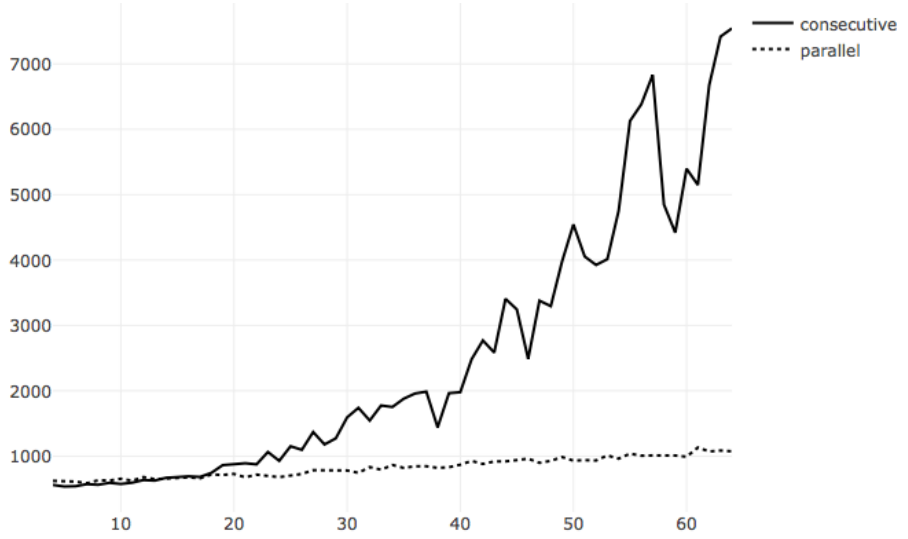


Рис. 3. Среднее время работы двух версий алгоритма в зависимости от порядка квазигруппы.

этот алгоритм на случай n-квазигрупп, проверить его корректность и оценить его сложность.

Автор выражает искреннюю признательность А. В. Галатенко за постановку задачи и обсуждение результатов работы.

Список литературы

[1] М. М. Глухов, "О применениях квазигрупп в криптографии", *ПДМ*, **2**, 2008, 28–32.

[2] "Исходный код алгоритма https://github.com/nikita-toropov/rf/blob/master/main.cpp".

[3] "NVIDIA CUDA http://developer.nvidia.com/object/cuda.html".

[4] Н.А. Торопов, *Алгоритм проверки наличия подквазигрупп в квазигруппе*, Филиал Московского Государственного Университета в г. Ташкенте, 2018.

About algorithm which checks if subquasigroup exists in a given quasigroup

Sobyanin P.I.

Algorithm which checks if subquasigroup exists in a given quasigroup. Performance of its consequent and CUDA parallel versions are compared.

Keywords: quasigroup, subquasigroup, GPU, CUDA.

Часть 3.
Математические модели

Критерий почти полного прогнозирования сверхслова в многозначном алфавите

Ведерников И.К.

Автомат прогнозирует следующий символ входного сверхслова, если он выдает этот символ на выходе в предыдущий момент времени.

В работе для произвольного сверхслова в многозначном алфавите исследуется вопрос его почти полного прогнозирования, т.е. когда прогноз правильный почти всегда. Получен результат, позволяющий сузить класс автоматов, которыми прогнозируется сверхслово, а также доказан критерий почти полной прогнозируемости сверхслова.

Ключевые слова: почти полное прогнозирование, прогнозирующий автомат, автоматное прогнозирование сверхслов, критерий прогнозируемости.

1. Введение

В статье А.Г. Вереникина и Э.Э. Гасанова [1] были введены прогнозирующие автоматы — конечные автоматы, предсказывающие сверхслово или множество сверхслов. Говорят, что автомат прогнозирует сверхслово, если через некоторое конечное время после начала, он начинает в момент времени t выдавать элемент входной последовательности под номером $t + 1$.

Оказалось, что полностью прогнозируемы только периодические сверхслова, изначально это было доказано для двоичного алфавита, но в работе [2] данный результат был обобщен на случай k-значных логик.

В работе [3] А.А. Мастихиной было введено понятие частичного прогнозирования, которое имеет место в случае, когда автомат угадывает следующий символ не обязательно в каждый момент времени, но достаточно часто. В одной из следующих работ А.А. Мастихина [4] предъ-

явила критерий частичной прогнозируемости общерегулярных сверхсобытий в двоичном алфавите. Также вопрос частичного прогнозирования сверхсобытий исследовался в работе [5].

Впервые вопрос прогнозируемости одного сверхслова поднимался А.А. Мастихиной в работе [3], в частности, было доказано, что существует сверхслово не прогнозируемое ни одним автоматом. Однако в поздних работах А.А. Мастихиной акцент делался исключительно на сверхсобытия. В данной работе же исследуется вопрос прогнозирования для одного сверхслова в многозначном алфавите, причем не обязательно общерегулярного. Было введено понятие почти полного прогнозирования – это означает, что автомат угадывает сверхслово почти всегда, т.е. степень частичного прогнозирования равна единице. В результате получено, что наилучшая степень прогнозирования достигается в определенном классе автоматов, а также получен критерий почти полной прогнозируемости одного сверхслова.

Автор выражает благодарность профессору Э.Э. Гасанову за постановку задачи и помощь в работе.

2. Основные понятия и формулировка результата

Введем основные определения.

Пусть $E_k = \{0, 1, \ldots, k-1\}$ – конечный алфавит. Через E_k^* и E_k^∞ обозначим соответственно множество всех слов конечной длины и множество всех сверхслов в алфавите E_k. По определению будем считать, что пустое слово Λ принадлежит E_k^*. Подмножества E_k^* называются *событиями*, а подмножества E_k^∞ — *сверхсобытиями*.

Длину слова α обозначим $|\alpha|$, по определению $|\Lambda| = 0$. Если α — сверхслово, то $|\alpha| = \infty$.

Если α — сверхслово в алфавите E_k, n — натуральное число, то n-ую букву сверхслова α будем обозначать $\alpha(n)$, а через $\alpha\,]_n$ обозначим префикс длины n сверхслова α, т.е. $\alpha\,]_n = \alpha(1)\alpha(2)\ldots\alpha(n)$.

Если α — слово в алфавите E_k, $|\alpha| = m$, n — натуральное число, $n < m$, то через $[_n\,\alpha$ обозначим суффикс длины n слова α, т.е. $[_n\,\alpha = \alpha(m-n+1)\ldots\alpha(m)$. Если $n = 0$, то положим $[_n\,\alpha = \Lambda$.

В работе рассматриваются конечные инициальные автоматы в соответствии с нотацией из [6]:

$$V = (E_k, Q, E_k, \varphi, \psi, q_0),$$

где $E_k = \{0, 1, ..., k-1\}$ – входной и выходной алфавит, Q – множество состояний, которое является конечным подмножеством некоторого фиксированного счетного множества, $\varphi : Q \times E_k \to Q$ – функция переходов, $: Q \times E_k \to E_k$ – функция выходов, q_0 – начальное состояние.

Если на вход инициальному автомату V подается слово или сверхслово $x = x(1)x(2)\ldots$, на выходе получается слово или сверхслово $y = y(1)y(2)\ldots$, и $q(t)$ означает состояние автомата в момент времени t, то функционирование автомата задается системой уравнений

$$\begin{cases} q(1) = q_0, \\ q(t+1) = \varphi\big(q(t), x(t)\big), \\ y(t) = \quad \big(q(t), x(t)\big), \end{cases}$$

где $t \in \mathbb{N}$.

Также определим автомат без выхода $V = (E_k, Q, \varphi, q_0)$, где E_k, Q, φ, q_0 определяются аналогично определению выше, а функционирование задается системой

$$\begin{cases} q(1) = q_0, \\ q(t+1) = \varphi\big(q(t), x(t)\big), \end{cases}$$

где $t \in \mathbb{N}$.

Функции φ и ψ естественно расширяются на $Q \times E_k^*$, а именно, если $\alpha \in E_k^*$, $a \in E_k$, то индуктивно определим

$$\varphi(q, \alpha a) = \varphi(\varphi(q, \alpha), a),$$

$$\psi(q, \alpha a) = \psi(\varphi(q, \alpha), a).$$

Введем также обозначения

$$\overline{\varphi}(q, \alpha) = \varphi(q, \alpha]_1)\varphi(q, \alpha]_2) \ldots \varphi(q, \alpha),$$

$$\overline{\psi}(q, \alpha) = \psi(q, \alpha]_1)\psi(q, \alpha]_2) \ldots \psi(q, \alpha),$$

если α — слово, если же α — сверхслово, то

$$\overline{\varphi}(q, \alpha) = \varphi(q, \alpha]_1)\varphi(q, \alpha]_2) \ldots \varphi(q, \alpha]_n) \ldots,$$

$$\overline{\psi}(q,\alpha) = \psi(q,\alpha]_1)\psi(q,\alpha]_2)\dots\psi(q,\alpha]_n)\dots.$$

Если α — сверхслово в алфавите A, то *пределом* сверхслова α назовем такое множество $A' \subseteq A$, что в сверхслове α бесконечное число раз встречаются символы из A' и только они. Этот факт будем обозначать $A' = \lim\alpha$.

Если есть событие R_1 и событие или сверхсобытие R_2, то через R_1R_2 обозначим их *произведение*, то есть все слова (сверхслова) вида ab, где $a \in R_1, b \in R_2$ (ab – конкатенация слов a и b).

Если R – событие, то обозначим R^* – *итерация* события R, то есть $R^* = R \cup R^2 \cup R^3 \cup ... \cup R^i ...$, а R^∞ – *сверхитерация* события R, $R^\infty = \{a_1a_2a_3...|\ a_i \in R, i = 1,2,3...\}$.

Сверхсобытие R *представимо* автоматом $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ с помощью семейства F, $F \subseteq 2^Q$, тогда и только тогда, когда для любого $\alpha \in R$, существует $Q' \in F$, такое, что $\lim\overline{\varphi}(q_0,\alpha) = Q'$.

Пусть $t \in \mathbb{N}$, скажем, что $(t+1)$-й символ сверхслова $\alpha = \alpha(1)\alpha(2)\dots\alpha(t+1)\dots$ или слова $\alpha = \alpha(1)\alpha(2)\dots\alpha(t')$, $t' > t$, *угадан* автоматом $V = (A, Q, B, \varphi, \psi, q_0)$, если $\psi(q_0,\alpha]_t) = \alpha(t+1)$.

Пусть $\alpha \in E_k^\infty$, обозначим $\sigma_\alpha(V) = \underline{\lim}_{n\to\infty} N_n/n$, где N_n – количество угаданных автоматом V символов в слове $\alpha\,]_n$. Будем говорить, что $\sigma_\alpha(V)$ – *степень прогнозирования сверхслова* α автоматом V. Если $\alpha \in E_k^*$, $|\alpha| = n$, обозначим $\sigma_\alpha(V) = N/n$, где N – количество угаданных автоматом V символов в слове α. Будем говорить, что $\sigma_\alpha(V)$ – *степень прогнозирования слова* α автоматом V.

Считаем, что множество сверхслов R *частично прогнозируемо*, если существует такой автомат V, что степень прогнозирования для каждого сверхслова множества R строго больше нуля. Обозначим $\sigma_R(V) = \inf\limits_{\alpha\in R}\sigma_\alpha(V)$.

Если $\mathfrak{K}$ — некоторый класс автоматов, то степень прогнозирования сверхсобытия R на автоматах из этого класса определим как $\sigma_R(\mathfrak{K}) = \sup\limits_{V\in\mathfrak{K}}\sigma_R(V)$.

Будем говорить, что автомат $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, прогнозирующий сверхсобытие R, лежит в классе представляющих относительно R, если существует автомат $V_0 = (E_k, Q, \varphi, q_0)$, представляющий R с помощью некоторого F, $F \subseteq 2^Q$.

Определим некоторый способ задания выходов, т.е. способ описания функции $\psi : Q \times E_k \to E_k$. Задавать выходную функцию будем, помечая ребра диаграммы Мура – в каждом состоянии отметим одно исходящее

ребро. Тогда функция выхода будет описана следующим образом: если у нас отмечено ребро по символу b, $b \in E_k$, исходящее из некоторого состояния q', то для всех q и a, таких что $\varphi(q,a) = q'$, значение выходной функции $\psi(q,a)$ будет равно b. Понятно, что задавая таким образом функцию ψ для каждого состояния, в итоге мы полностью определим ее. Функцию выхода, полученную таким образом, будем называть *размеченной*.

Заметим, что угадывание происходит, когда выход в предыдущий момент времени равен входу в данный момент времени. Поэтому если автомат проходит по отмеченной стрелке, то угадывание происходит.

Обозначим $\mathfrak{A}$ – класс всех автоматов, $\mathfrak{R}(R)$ — множество автоматов, которые лежат в классе представляющих относительно R, $\mathfrak{M}$ – множество всех автоматов с размеченными функциями выхода, а $\mathfrak{MR}(R)$ — все автоматы из $\mathfrak{R}(R)$ с размеченной функцией выхода.

Будем говорить, что сверхслово α *почти полностью прогнозируемо*, если $\sigma_\alpha(\mathfrak{A}) = 1$.

Будем говорить, что H – *конечное приведенное множество слов* над E_k, если для любых α_1, α_2 из H выполнено, что α_1 не является подсловом α_2 и наоборот. Через $M(H)$ обозначим максимальную длину слова из H.

Представлением сверхслова β назовем последовательность слов $\mathfrak{B} = \{\alpha_i^{s_i}\}$ такую, что $\beta = \alpha_0^{s_0}\alpha_1^{s_1}\dots\alpha_m^{s_m}\dots$. Слово $\alpha_i^{s_i}$ будем называть i-*ым элементом* представления.

Накрытием сверхслова β назовем пару $(\mathfrak{B}, H)$, где $\mathfrak{B}$ – представление сверхслова β, H – конечное приведенное множество слов.

Далее определим некоторые характеристики накрытия:

1) Через $\mathfrak{C}_H(\mathfrak{B})$ обозначим *покрывающее множество* и определим его следующим алгоритмом (опишем i-й шаг): возьмем i-ый элемент $\mathfrak{B}$, если $\alpha_i \in H$, то добавим $\alpha_i^{s_i}$ в $\mathfrak{C}_H(\mathfrak{B})$, если нет – ничего не делаем. После этого перейдем к шагу $i+1$.
   Отметим, что $\mathfrak{C}_H(\mathfrak{B})$ – множество с повторениями, то есть может содержать два и более одинаковых слова.

2) $C(\mathfrak{C}_H(\mathfrak{B}), n)$ – количество элементов покрывающего множества, входящих в префикс сверхслова длины n.

3) $L(\mathfrak{C}_H(\mathfrak{B}), n)$ – суммарная длина всех элементов покрывающего множества, входящих в префикс сверхслова длины n.

Далее сформулируем основные результаты данной работы:

Теорема 1. *Пусть автомат* $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ *прогнозирует сверхсобытие* R *со степенью* σ, ψ *– не размеченная, тогда существует автомат* $\widehat{V} = (E_k, \widehat{Q}, E_k, \widehat{\varphi}, \widehat{\psi}, \widehat{q_0})$, *где* $\widehat{\psi}$ *– размеченная, который прогнозирует* R *со степенью* σ. *Более того, если* $V \in \mathfrak{R}(R)$, *то* $\widehat{V} \in \mathfrak{MR}(R)$.

Теорема 2. *Пусть* $\beta \in E_k^\infty$. *Тогда* β *угадываемо со степенью* 1 *тогда и только тогда, когда существует накрытие* $(\mathfrak{B}, H)$ *такое, что выполнено*

$$\varliminf_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}), n) - M(H) \cdot C(\mathfrak{C}_H(\mathfrak{B}), n)}{n} = 1.$$

Замечание 1. *Условие теоремы 2 эквивалентно следующему:*

$$\lim_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}), n) - C(\mathfrak{C}_H(\mathfrak{B}), n)}{n} = 1.$$

3. Достаточность размеченных функций выхода.

Теорема 1. *Пусть автомат* $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ *прогнозирует сверхсобытие* R *со степенью* σ, *– не размеченная, тогда существует автомат* $\widehat{V} = (E_k, \widehat{Q}, E_k, \widehat{\varphi}, \widehat{\psi}, \widehat{q_0})$, *где* $\widehat{\psi}$ *– размеченная, который прогнозирует* R *со степенью* σ. *Более того, если* $V \in \mathfrak{R}(R)$, *то* $\widehat{V} \in \mathfrak{MR}(R)$.

Доказательство. Будем преобразовывать автомат V так, чтобы его функция выхода стала размеченной.

Рассмотрим произвольное состояние q. Пусть $Prev_q = \{(q_0, c_0), \ldots, (q_n, c_n)\}$ – множество пар состояние – символ таких, что в автомате V для любой пары $(q', c) \in Prev_q$ выполняется $\varphi(q', c) = q$.

Если в этом состоянии функция выхода автомата V удовлетворяет требованию размеченности, то есть существует символ b, что для любой пары $(q', c) \in Prev_q$ выполнено, что $\psi(q', c) = b$, то для состояния q условие размеченности выполнено, и мы переходим к рассмотрению другого состояния.

Если не удовлетворяет, то существуют $b_1, \ldots, b_l$, $l \le n, l \le k$, и представление множества $Prev_q = Prev_q^1 \cup \cdots \cup Prev_q^l$ такие, что для любой пары $(q', c) \in Prev_q^s, s \in \{1, \ldots, l\}$, выполнено, что $\psi(q', c) = b_s$.

Далее получим из V некоторый автомат $V' = (E_k, Q', E_k, \varphi', \psi', q_0')$:

1) Заменим состояние q на состояния $\{q^1, \ldots, q^l\}$, то есть $Q' = Q \cup \{q^1, \ldots, q^l\} \setminus \{q\}$.

2) Функции переходов и выходов определим следующим образом:

   а) Для любой пары (q', c) из $Prev_q^s$, $q' \neq q$, положим, что $\varphi'(q', c) = q^s$, а $\psi'(q', c) = b_s$.

   б) Пусть $j \in \{1, \ldots, l\}$, тогда для любого $a \in E_k$, если $\varphi(q, a) \neq q$, положим $\varphi'(q^j, a) = \varphi(q, a)$, $\psi'(q^j, a) = \psi(q, a)$. Если $\varphi(q, a) = q$, то пара (q, a) принадлежит некоторому $Prev_q^s$, тогда положим $\varphi'(q^j, a) = q^s$, $\psi'(q^j, a) = b_s$.

   в) Для остальных случаев положим $\varphi'(q', c) = \varphi(q', c)$, и $\psi'(q', c) = \psi(q', c)$.

3) Если q было начальным состоянием автомата V, то $q'_0 = q^1$, иначе $q'_0 = q_0$.

Заметим, что, исходя из построения, в любой момент времени t и для любого входного сверхслова α выполнено, что $\psi(q_0, \alpha|_t) = \psi'(q'_0, \alpha|_t)$, то есть автомат V' неотличим от V. Следовательно, если автомат V угадывал некоторый символ $\alpha(m + 1)$, то и автомат V' будет угадывать этот символ. Более того в автомате V' в состояних $q^1, \ldots, q^l$ функция выхода ψ' – размеченная, и, если в автомате V было r состояний с не размеченной функцией выхода, то в автомате V' их будет $r - 1$.

Теперь рассмотрим ситуацию, когда $V \in \mathfrak{R}(R)$. Тогда существует автомат $V_0 = (E_k, Q, \varphi, q_0)$, который представляет R с помощью $F = \{Q_1, \ldots, Q_h\}$, $F \subseteq 2^Q$. После операции описанной выше, мы получили автомат $V' = (E_k, Q', E_k, \varphi', \psi', q'_0)$ и далее построим множество F', с помощью которого автомат $V'_0 = (E_k, Q', \varphi', q'_0)$ представляет R. Для этого рассмотрим каждый элемент Q_i множества F и сделаем следующее:

1) Пусть $q \notin Q_i$, тогда добавим Q_i в F'.

2) Пусть $q \in Q_i$. Рассмотрим множества $S_{p,i} = L_p \cup Q_i \setminus \{q\}$, где $L_p \in 2^{\{q^1, \ldots, q^l\}} \setminus \{\varnothing\}$. Далее, если существует такое сверхслово $\alpha \in R$, что $\lim(\alpha) = S_{p,i}$, то добавим $S_{p,i}$ в F'.

Заметим, что если в автомате V_0 предел сверхслова был равен Q_i, то в автомате V'_0 его предел будет равен либо множеству $S_{p,i}$ для некоторого p, либо самому Q_i. В результате получим, что если сверхслово $\alpha \in R$, то $\lim(\alpha) \in F'$. Обратное тоже верно, так как если $\lim(\alpha) = S_{p,i}$ или

$\lim(\alpha) = Q_i$ в автомате V_0', то в автомате V_0 его предел равен Q_i, а значит $\alpha \in R$.

Тем самым мы показали, что в результате операции разделения состояний, сохраняется принадлежность к классу представляющих автоматов.

Далее возьмем V' и проделаем с ним операцию описанную выше, получим автомат V'' с $r-2$ состояниями, в которых функция выхода не размеченная. Проделав эту операцию r раз, получим автомат $\widehat{V}$, у которого функция выхода в каждом состоянии размеченная, и который по построению прогнозирует R со степенью σ. И так как сохраняется принадлежность к классу представляющих автоматов, то итоговый автомат $\widehat{V}$ будет принадлежать классу $\mathfrak{MR}(R)$, если автомат V был из $\mathfrak{R}(R)$.

□

Замечание 2. *Из теоремы явно следует, что для любого сверхслова β выполнено $\sigma_\beta(\mathfrak{A}) = \sigma_\beta(\mathfrak{M})$. Поэтому далее будем рассматривать автоматы только из $\mathfrak{M}$.*

4. Доказательство вспомогательных утверждений и вспомогательные построения.

Введем несколько вспомогательных определений:

Сильно связным множеством назовем такое множество состояний C, $C \subseteq Q$, автомата $V = (E_k, Q, E_k, \varphi, \psi, q_0)$, что для любых $q', q'' \in C$ найдется такое слово α из E_k^*, что $\varphi(q', \alpha) = q''$ и $\overline{\varphi}(q', \alpha) \in C^*$, т.е. по слову α автомат переходит из состояний q' в состояние q'', проходя только состояния из C. Множество, состоящее из одного состояния, по определению считается сильно связным.

Любое сильно связное множество состояний C назовем *автоматным циклом*, если $|C| > 1$. Одноэлементное множество состояний $C = \{q\}$ является *автоматным циклом* только если существует символ a из E_k, что $\varphi(q, a) = q$. *Длиной автоматного цикла* назовем число состояний в автоматном цикле.

Пусть $V = (E_k, Q, E_k, \varphi, \psi, q_0)$ и ψ – размеченная. *Размеченным циклом* в автомате V назовем автоматный цикл автомата V, в котором все переходы по циклу отмечены.

Лемма 1. *Пусть у автомата V, $V \in \mathfrak{M}$, нет размеченного цикла, тогда для любого сверхслова β выполнено, что $\sigma_\beta(V) < 1$.*

Доказательство. Заметим, что функция ψ – размеченная, а значит угадывание происходит только тогда, когда автомат проходит по отмеченной стрелке в диаграмме Мура. По условию, в автомате нет размеченного цикла, следовательно, каждые m тактов, где m – количество состояний автомата V, будет не более $m-1$ угадывания. Отсюда следует, что $\sigma_\beta(V) \leq \frac{m-1}{m} < 1$.

□

Теперь пусть H – конечное приведенное множество слов над E_k, опишем некоторое частичное построение автомата, которое пригодится при доказательстве теоремы:

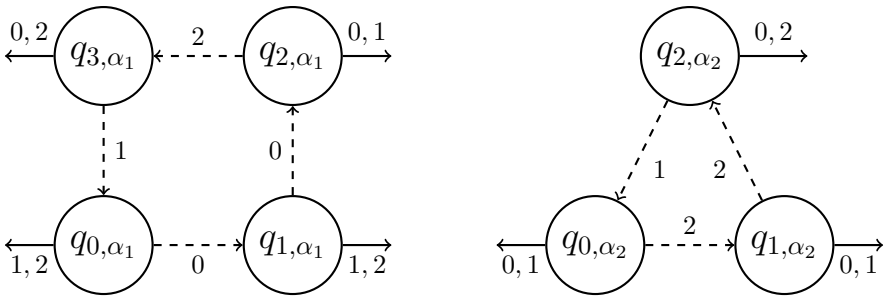


Рис. 1. Пример построения 1.

Построение 1. *Для каждого слова из H построим размеченный автоматный цикл.*

1) Пусть $\alpha \in H$, $\alpha = a_0 \dots a_{l-1}$, тогда в цикле будет l состояний, обозначим их $\{q_{0,\alpha}, \dots q_{l-1,\alpha}\}$.

2) Функцию переходов зададим следующим образом: $\varphi(q_{i,\alpha}, a_i) = q_{i+1,\alpha}$, если $i \in \{0, \dots, l-2\}$. Если $i = l-1$, то $\varphi(q_{l-1,\alpha}, a_{l-1}) = q_{0,\alpha}$. Остальные переходы оставим неопределенными.

3) Функцию выхода зададим с помощью разметки. В каждом состоянии $q_{i,\alpha}$ отметим переход a_i, $i \in \{0, \dots, l-1\}$.

Пример к построению 1. Пусть $H = \{\alpha_1, \alpha_2\}$, $H \subset E_3^*$, где $\alpha_1 = 0021$, $\alpha_2 = 221$. В результате построения получим два цикла, которые изображены на рис. 1, пунктиром обозначены отмеченные переходы.

Далее пусть есть автомат $V = (E_k, Q, \varphi, q)$, и каждому слову из H сопоставлено одно состояние из Q, причем разным словам – разные состояния. Будем говорить, что *автомат V разделяет вход по множеству H*, если для любого слова $\gamma\alpha$, где α из H, а γ такое, что ни одно слово из H не содержится как подслово в слове $\gamma\alpha\,]_{|\alpha|-1}$, выполнено $\varphi(q, \gamma\alpha) = q_\alpha$, где q_α – состояние, сопоставленное слову α. Данное определение означает, что в автомате выделено $|H|$ состояний, и как только во входном слове встречается подслово равное слову из H, то автомат попадает в соответствующее выделенное состояние и не выходит оттуда.

Отметим, что определение выше ставит задачу поиска первого попавшегося слова из некоторого фиксированного множества в качестве подслова. Подобную задачу уже давно рассматривают, и известным результатом в этой области является алгоритм Ахо-Корасик [7], который реализует поиск множества подстрок в некоторой данной строке. Алгоритм строит конечный автомат, которому затем передаёт строку поиска. В лемме 2 описывается построение подобного автомата, но с учетом того, что множество искомых слов приведенное и искать нужно до первого вхождения, эти условия гарантируют, что получится автомат, который разделяет вход по множеству H.

Лемма 2. Пусть H – конечное приведенное множество слов над E_k, тогда существует автомат V, разделяющий вход по H.

Доказательство. Пусть $H = \{\alpha_0, \ldots, \alpha_{p-1}\}$, и пусть префиксное дерево для слов из H имеет m вершин, среди которых p листьев. Обозначим вершины как $U = \{v_0, \ldots, v_{m-1}\}$, причем v_0 – корень дерева, а $\{v_{m-p}, \ldots, v_{m-1}\}$ – листовые вершины.

Далее построим автомат V, разделяющий вход по H. Положим $Q = \{q_0, \ldots, q_{m-1}\}$ – состояния автомата, при этом q_0 – начальное состояние. Каждому состоянию автомата q_i сопоставим вершину v_i из U и зададим функцию переходов:

1) Если в префиксном дереве есть ребро из вершины v_i в вершину v_j по символу a, то положим $\varphi(q_i, a) = q_j$.

2) Если q_i – состояние, которому соответствует листовая вершина, то $\varphi(q_i, a) = q_i$ для любого a из E_k.

3) Если в префиксном дереве из вершины v_0 не выходит ребра с символом a, то $\varphi(q_0, a) = q_0$.

4) Возьмем состояние $q_i,\ i \in \{1,\dots,m-p-1\}$, пусть $\delta,\ |\delta| = l,$ – слово, которое проводит из корня v_0 в вершину v_i, и пусть в пункте 1 в состоянии q_i было задано $k-k'$ переходов, $k' < k$. Без ограничения общности можно предположить, что осталось задать переходы по символам $\{0,\dots,k'-1\}$.

   Рассмотрим произвольный символ $h,\ h \in \{0,\dots,k'-1\}$. Возьмем суффикс $\lfloor_{l-1}\delta$, если существует слово α из H такое, что $(\lfloor_{l-1}\delta)h = \alpha\rfloor_l$, то положим $\varphi(q_i,h) = \varphi(q_0,\alpha\rfloor_l)$. Если не существует, то возьмем суффикс $\lfloor_{l-2}\delta$ и префиксы слов из H длины $l-1$ и т.д.. Если же для любого $l',\ l' \in \{1,\dots,l\}$, и любого слова $\alpha,\ \alpha \in H$, верно, что $(\lfloor_{l-l'}\delta)h \neq \alpha\rfloor_{l-l'+1}$, то положим $\varphi(q_i,h) = q_0$.

Заметим, что множество H приведенное, то есть ни одно слово не является подсловом другого, поэтому построение в пункте 4 корректно. Также заметим, что по построению для любого слова $\gamma,\ \gamma \in E_k^*$, выполнено, что как только первый раз встречается слово α из H в качестве подслова γ, то автомат заходит в состояние $\varphi(q_0,\alpha)$ и уже не выходит оттуда, при этом разным словам из H соответствуют разные состояния. Тем самым мы построили автомат V, который разделяет вход по множеству H.

□

Пример к лемме 2. Пусть $H = \{20, 221, 1110, 1121\},\ H \subset E_3^*$. В результате построения как в лемме 2 получим автомат, изображенный на рис. 2.

5. Доказательство критерия угадываемости.

Теорема 2. *Пусть $\beta \in E_k^\infty$. Тогда β угадываемо со степенью 1 тогда и только тогда, когда существует накрытие $(\mathfrak{B}, H)$ такое, что выполнено*

$$\varliminf_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}),n) - M(H)\cdot C(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 1.$$

Доказательство. Необходимость. Пусть $\sigma_\beta(\mathfrak{A}) = 1$. Возьмем автомат $V = (E_k, Q, E_k, \varphi, \psi, q_0),\ |Q| = m$, такой, что $\sigma_\beta(V) = 1,\ \ V \in \mathfrak{M}$, по условию и теореме 1 такой существует.

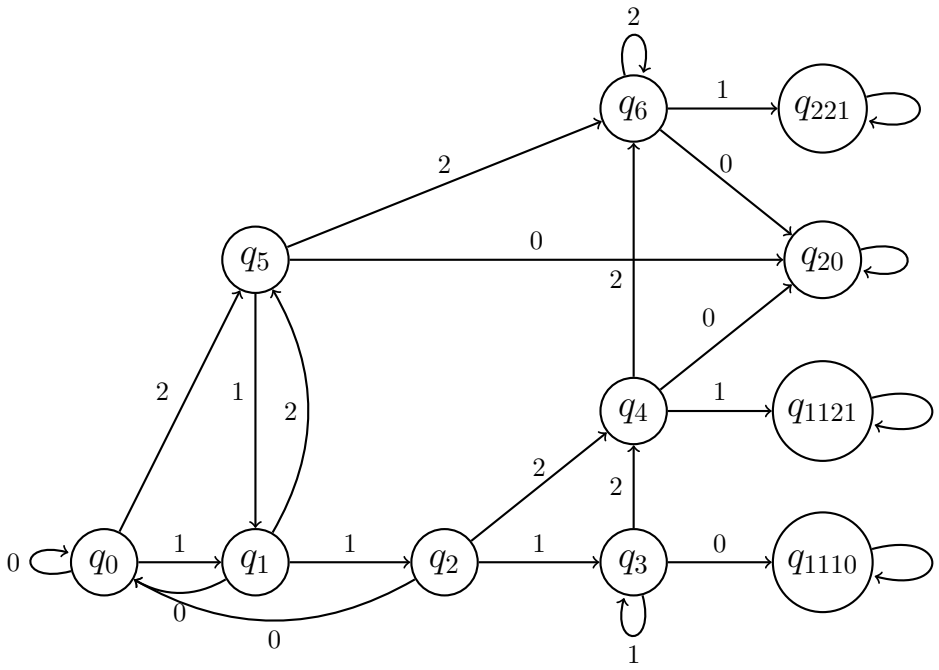


Рис. 2. Пример к лемме 2.

По лемме 1 автомат V имеет хотя бы один размеченный цикл, пусть у него их p штук, обозначим их $\{C_0, \dots C_{p-1}\}$. Зафиксируем у каждого цикла C_i произвольное состояние, которое назовем начальным и обозначим $q_{0,i},\ i \in \{0, \dots, p-1\}$. Теперь пусть слово, которое проводит автомат от начального состояния цикла $q_{0,i}$ до него же – это соответственно α_i. Если среди этих слов есть такие, что $\alpha_i^\infty = \alpha_j^\infty$, то выбросим максимальное по длине, в результате получим множество слов $\{\alpha_0, \dots, \alpha_{p'-1}\},\ p' \le p$. Положим $H = \{\alpha_0^{s_0}, \dots, \alpha_{p'-1}^{s_{p'-1}}\}$, где $\{s_0, \dots, s_{p'-1}\}$ минимальные натуральные числа такие, что для любого i слово $\alpha_i^{s_i}$ не является подсловом $\alpha_j^{s_j},\ j \in \{0, \dots, i-1, i+1, \dots, p'-1\}$. По построению H – приведенное множество слов.

Представление $\mathfrak{B}$ построим по автомату V и сверхслову β следующим алгоритмом:

1) Изначально $\mathfrak{B}$ пусто, и $u = 1$, u – начальная позиция в слове β, $q = q_0,\ q$ – начальное состояние алгоритма.

2) Возьмем u', $u \le u'$ такое, что $\varphi(q, \beta(u)\dots\beta(u')) = q_{0,i}$ для некоторого i, и при этом для любого u'', $u \le u'' < u'$ выполнено, что $\varphi(q, \beta(u)\dots\beta(u'')) \ne q_{0,i}$ для любого i.

3) Пусть $\varphi(q, \beta(u)\dots\beta(u'))$ было равно $q_{0,h}$. Возьмем u''', $u' < u'''$ такое максимальное натуральное число, что

$$\varphi(q_{0,h}, \beta(u'+1)\dots\beta(u''')) = q_{0,h}, \tag{1}$$

и при этом выполняется

$$\forall\ u'' :\ u' < u'' \le u'''\ \Rightarrow\ \varphi(q_{0,h}, \beta(u'+1)\dots\beta(u'')) \in C_h. \tag{2}$$

Если такого u''' не существует возможны два случая:

а) Условия (1) и (2) выполняются бесконечное число раз, то есть максимума не существует. В этом случае β – периодическое с предпериодом, и тогда возьмем $u''' = u' + 2^{u'} \cdot |C_h|$. Данный выбор гарантирует, что условия (1) и (2) будут выполнены.

б) Условия (1) и (2) никогда не выполняются, тогда просто пропустим этот шаг.

4) Добавим слово $\beta(u)\dots\beta(u')$ в $\mathfrak{B}$, затем, если u''' существовал, добавим слово $\beta(u'+1)\dots\beta(u''')$. После добавления обновим значения u и q: если u''' существовал, то $u = u''' + 1$, $q = \varphi(q, \beta(u)\dots\beta(u'''))$, если не существовал, то $u = u' + 1$, $q = \varphi(q, \beta(u)\dots\beta(u'))$.

5) Вернемся к шагу 2.

Так как степень угадывания сверхслова β равна 1, то автомат заходит во множество $\{C_0, \dots, C_{p-1}\}$ бесконечное число раз, следовательно, алгоритм корректен. Также заметим, что по построению сверхслово β равно последовательной конкатенации элементов $\mathfrak{B}$, отсюда получаем, что $\mathfrak{B}$ – представление β. И еще отметим, что множество $\mathfrak{C}_H(\mathfrak{B})$ состоит из элементов вида $\beta(u'+1)\dots\beta(u''')$.

Возьмем накрытие $(\mathfrak{B}, H)$ и покажем, что для него верно условие теоремы.

Рассмотрим два случая, первый – слово β является периодическим с предпериодом. Заметим, что в этом случае с некоторого момента времени

автомат не выходит из размеченного цикла, а в построении $\mathfrak{B}$ число u''' выбиралось таким, что

$$\underline{\lim}_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 1;\ \underline{\lim}_{n\to\infty} \frac{C(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 0.$$

Откуда сразу следует, что

$$\underline{\lim}_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}),n) - M(H)\cdot C(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 1.$$

Пусть теперь β не периодическое с предпериодом. Представим каждый момент времени n как сумму $|T_1(n)|$ и $|T_2(n)|$, где $T_1(n)$ – множество тактов, которые соответствуют элементам построения $\mathfrak{B}$ из пункта 3 до момента n, а $T_2(n)$ – множество всех остальных тактов, то есть тех, которые соответствуют элементам из пункта 2 до момента n. Также обозначим $N_1(n)$ – количество угадываний в такты $T_1(n)$, а $N_2(n)$ – в такты $T_2(n)$, получим, что $N_n = N_1(n) + N_2(n)$.

Заметим, что в такты $T_2(n)$ не может быть больше чем $m-1$ угадывания на каждые m тактов, так как после каждого элемента из пункта 3 представления $\mathfrak{B}$ происходит выход из размеченного цикла, что гарантирует хотя бы одно неугадывание, и, в случае не периодического сверхслова, все проходы по размеченным циклам попадают в такты $T_1(n)$. Следовательно, $N_2(n) \le \frac{m-1}{m}\cdot|T_2(n)|$, и $N_1(n) = |T_1(n)|$, откуда получим

$$\sigma_\beta(V) = 1 = \underline{\lim}_{n\to\infty} \frac{N_1(n)+N_2(n)}{n} \le \underline{\lim}_{n\to\infty} \frac{|T_1(n)| + \frac{m-1}{m}\cdot|T_2(n)|}{n} \le 1,$$

так как $|T_1(n)| + |T_2(n)| = n$, из неравенства следует, что

$$\lim_{n\to\infty} \frac{|T_2(n)|}{n} = 0.$$

По определению верно, что $C(\mathfrak{C}_H(\mathfrak{B}),n) \le |T_2(n)|$, а $M(H)$ – фиксированная константа. Получаем

$$\lim_{n\to\infty} \frac{C(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = \lim_{n\to\infty} \frac{M(H)\cdot C(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 0.$$

Теперь заметим, что $|T_1(n)| \le L(\mathfrak{C}_H(\mathfrak{B}),n) \le n$, следовательно,

$$\sigma_\beta(V) \le \underline{\lim}_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}),n)}{n} = 1.$$

Из двух предыдущих выводов следует, что

$$\underline{\lim}_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}), n) - M(H) \cdot C(\mathfrak{C}_H(\mathfrak{B}), n)}{n} = 1.$$

Необходимость доказана.

Достаточность. Построим автомат $V = (E_k, Q, E_k, \varphi, \psi, q)$, который будет почти полностью прогнозировать β.

Возьмем множество $H = \{\alpha_0, \ldots, \alpha_{p-1}\}$, по построению 1, получим размеченные циклы для каждого слова из H, обозначим их как частично заданные автоматы $C_{\alpha_i} = (E_k, Q_{\alpha_i}, E_k, \varphi_{\alpha_i}, \psi_{\alpha_i}, q_{0,\alpha_i})$, $i \in \{0, \ldots, p-1\}$, $Q_{\alpha_i} = \{q_{0,\alpha_i}, \ldots, q_{|\alpha_i|-1,\alpha_i}\}$. Также из леммы 2 возьмем автомат $A = (E_k, Q_A, \varphi_A, q_0)$, разделяющий вход по H, и обозначим его состояния $Q_A = \{q_0, \ldots, q_{m-1}\}$ и пусть $\{q_{m-p}, \ldots, q_{m-1}\}$ – состояния, сопоставленные словам из H, причем слову α_i сопоставлено состояние q_{m-p+i} для любого i.

Далее приступим к построению автомата V:

1) Положим $Q = Q_{\alpha_0} \cup \cdots \cup Q_{\alpha_{p-1}} \cup Q_A \setminus \{q_{m-p}, \ldots, q_{m-1}\}$, за начальное состояние q примем состояние q_0.

2) Определим функцию переходов, рассмотрим несколько случаев:

   а) Пусть $q' \in Q_A \setminus \{q_{m-p}, \ldots, q_{m-1}\}$ и $\varphi_A(q', a) = q_i$. Если $i \in \{0, \ldots, m-p-1\}$, то положим $\varphi(q', a) = q_i$. Если же $i \in \{m-p, \ldots, m-1\}$, то $\varphi(q', a) = q_{0,\alpha_i}$.

   б) Пусть $q' \in Q_{\alpha_i}$ для некоторого $i \in \{0, \ldots, p-1\}$. Если для символа a, $a \in E_k$, функция $\varphi_{\alpha_i}(q', a)$ определена, то положим $\varphi(q', a) = \varphi_{\alpha_i}(q', a)$.

   в) Теперь рассмотрим случай, когда $q' \in Q_{\alpha_i}$ для некоторого $i \in \{0, \ldots, p-1\}$, и функция $\varphi_{\alpha_i}(q', a)$ не определена. Пусть $q' = q_{j,\alpha_i}$, $j \in \{0, \ldots, |\alpha_i|-1\}$. Рассмотрим значение $\varphi_A(q_0, \alpha_i\,]_j\, a) = q_{i'}$. Если $i' \in \{0, \ldots, m-p-1\}$, то положим $\varphi(q', a) = q_{i'}$. Если $i' \in \{m-p, \ldots, m-1\}$, то положим $\varphi(q', a) = q_{0,\alpha_{i'}}$.

3) Функцию выхода зададим разметкой. В состояниях $Q_{\alpha_0} \cup \cdots \cup Q_{\alpha_{p-1}}$ отметим то же ребро, что и в соответствующем цикле, в остальных состояниях отметим произвольное ребро.

Далее рассмотрим степень прогнозирования автоматом V сверхслова β. Как только в сверхслове β встречается подслово, являющееся эле-

ментом из $\mathfrak{C}_H(\mathfrak{B})$, то не более чем через $M(H)$ тактов автомат начинает угадывать и угадывает на протяжении всей длины элемента $\mathfrak{B}$. Это обеспечивается пунктом 2в построения автомата и тем, что автомат A приходит в состояние, сопоставленное некоторому слову из H, не более чем через $M(H)$ тактов после подачи соответствующего слова. Смена размеченных циклов происходит тоже не более чем за $M(H)$ тактов по пункту 2в и построению автомата A. Отсюда получаем, что $N_n \geq L(\mathfrak{C}_H(\mathfrak{B}), n) - M(H) \cdot C(\mathfrak{C}_H(\mathfrak{B}), n)$, и, следовательно,

$$\sigma_\beta(V) \geq \varliminf_{n\to\infty} \frac{L(\mathfrak{C}_H(\mathfrak{B}), n) - M(H) \cdot C(\mathfrak{C}_H(\mathfrak{B}), n)}{n} = 1.$$

Теорема доказана.

□

Список литературы

[1] Вереникин А.Г., Гасанов Э.Э., "Об автоматной детерминизации множеств сверхслов", *Дискретная математика*, **18**:2 (2006), 84–97.

[2] Гасанов Э.Э., "Прогнозирование периодических сверхсобытий автоматами", *Интеллектуальные системы*, **19**:1 (2015), 23–34.

[3] Мастихина А.А., "О частичном угадывании сверхслов", *Интеллектуальные системы*, **11**:1–4 (2007), 561–572.

[4] Мастихина А.А., "Критерий частичного предвосхищения общерегулярных свехсобытий", *Дискретная математика*, **23**:4 (2011), 103–114.

[5] Ведерников И.К., "Исследование алгоритма, задающего функцию выхода прогнозирующего автомата", *Интеллектуальные системы*, **20**:3 (2016), 103–111.

[6] Кудрявцев В.Б., Алешин С.В., Подколзин А.С., *Введение в теорию автоматов*, «Наука», Москва, 1985, 320 с.

[7] Alfred V. Aho, Margaret J. Corasick, "Efficient string matching: An aid to bibliographic search", *Communications of the ACM*, **18**:6 (1975), 333–340

Criterion for almost complete prediction of a superword in a multi-valued alphabet

Vedernikov I.K.

The machine predicts the next character of the input sequence if it outputs that character the moment before.

The present paper considers whether an arbitrary superword in multivalued alphabet can be almost completely predicted or not.

The paper provides a theorem that enables to restrict the class of machines, with the help of which superwords are predicted. Moreover, the paper presents the criterion for almost complete predicting.

Keywords: almost complete predicting, predicting machine, prediction of superwords by a machine, criterion for predicting.

Верхняя оценка энергопотребления объемных схем, реализующих булевы операторы.

Ефимов А.А.

В данной работе рассматриваются объёмные схемы, являющиеся обобщением плоских схем в пространстве. Был рассмотрен класс схем, реализующих булевы операторы. Для этого класса получена верхняя оценка потенциала — меры мощности, равной количеству элементов схемы, выдающих единицу на данном входном наборе. Показано, что любой оператор от n переменных можно реализовать объемной схемой, потенциал которой не превосходит $\mathcal{O}(m \cdot 2^{n/3})$, если $m \leq n$, и $\mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$, если $m > n$.

Ключевые слова: схемы из функциональных элементов, объёмные схемы, мощность схемы, потенциал.

1. Введение

В ряде работ исследовалась сложность схем из функциональных элементов, реализующих функции алгебры логики от n аргументов. Однако, зачастую в них рассматривались схемы, в которых не накладывалось никаких ограничений на размещение элементов схемы, способ соединения и т.п. На самом деле в любой схеме, когда она располагается в пространстве, функциональные элементы имеют определенную длину, ширину и соединяются проводниками, размеры которых следует учитывать.

Данная работа посвящена объёмным схемам, которые определяются аналогично плоским схемам, но в пространстве. Впервые понятие плоской схемы было введено Кравцовым в 1967 году [1]. Коршунов в работе [2] получил оценку сложности схем из объемных функциональных элементов (l-схем), удовлетворяющим некоторым ограничениям. Развитие теории плоских схем было связано с развитием технологии производства и

укладки реальных микросхем. Идея о том, что схемы можно укладывать друг на друга в пространстве была также известна давно, но не находила широкого применения вплоть до недавнего времени. Лишь несколько лет назад подобная технология начала использоваться, так как у инженеров закончились способы выжать лучшие характеристики из чипов прежнего размера. В частности, речь идёт о том, чтобы в будущем использовать многослойные чипы.

Основной целью данной работы является обобщение результатов Калачева [3, 4] на объёмные схемы и продолжение результатов работы [5] в случае булевых операторов. Как и в его работах, автор использует такое понятие сложности схемы, как максимальный потенциал. Он равен максимальному значению количества единиц на всех внутренних узлах схемы, взятому по всем входным наборам. Неформально говоря, потенциал показывает количество «энергии» схемы, необходимой для её функционирования. В данной работе была получена верхняя оценка потенциала для класса булевых операторов.

Автор выражает глубокую благодарность научному руководителю д.ф.-м.н., профессору Э.Э. Гасанову и Г.В. Калачёву за постановку задачи и внимание к работе.

2. Основные понятия и формулировка результатов

Кубическим элементом будем называть булев оператор, у которого в сумме не более шести входов и выходов, причем каждому его входу и выходу сопоставлена некоторая метка из множества $\{l, t, r, b, f, a\}$, причём метки не повторяются.

Метки будем называть сторонами элемента:

- l – левая сторона;
- r – правая сторона;
- t – верхняя сторона;
- b – нижняя сторона;
- f – передняя сторона;
- a – задняя сторона.

Кубический элемент будем изображать в виде единичного куба в пространстве. При этом входам и выходам элемента сопоставляются грани куба в соответствии с присвоенными им метками.

Метки, присвоенные входам (выходам) оператора будем называть *входами (выходами)* элемента. Метки, не присвоенные ни входам, ни выходам, будем называть *изоляторами*. Множество входов (выходов) элемента e будем обозначать $in(e)$ ($out(e)$). Входы и выходы элемента будем называть его *контактами*.

Если на всех выходах элемента реализуются тождественные функции, то будем называть элемент *коммутационным*, иначе – *логическим*.

Коммутационный элемент соотвествует либо проводнику в микросхеме, либо пересечению проводов, либо тождественной функции, служащей для усиления сигнала.

Описывать элемент можно уравнениями, которые задают его оператор, заменяя все переменные в них на сопоставленные им метки (l, t, r, b, f, a). Тогда в левой части каждого уравнения будет стоять выходная метка, а в правую часть будут входить только входные метки.

Всюду далее значок $:=$ будет обозначать «по определению равно».

За E обозначим множество всех кубических элементов.

Сетью из кубических элементов на множестве $M \subset \mathbb{Z}^3$ будем называть отображение $K : M \to E$.

Элемент $K(x, y, z)$ будем называть *элементом схемы K с координатами (x,y,z)*.

Левой, правой, верхней, нижней, передней и задней стороной элемента e с координатами (x, y, z) будем называть точки с координатами $(x - \frac{1}{2}, y, z), (x + \frac{1}{2}, y, z), (x, y, z + \frac{1}{2}), (x, y, z - \frac{1}{2}), (x, y + \frac{1}{2}, z), (x, y - \frac{1}{2}, z)$ соответственно.

Будем говорить, что сеть K из кубических элементов корректна, если для любых элементов x и y схемы K верно, что если сторона a элемента x совпадает со стороной b элемента y, то выполнено одно из условий:

- один из элементов x, y – изолирующий,
- стороны a и b являются изоляторами,
- среди них одна является входом, другая выходом, например, a – выход, а b – вход, в таком случае будем говорить, что выход a *подключен* ко входу b.

Множество M будем называть *носителем* сети K.

Введём понятие *графа корректной сети из кубических элементов* K (будем обозначать G_K). G_K – ориентированный граф, вершинами которого являются входы и выходы элементов схемы. Если выход одного элемента подключен ко входу другого, то им будет соответствовать одна и та же вершина графа (будем говорить, что эта вершина является выходом первого элемента и входом второго). Из вершины a в вершину b ведет ребро в том и только в том случае, когда существует элемент e такой, что a является его входом, b – выходом, причем функция, реализуемая на выходе b, существенно зависит от входа a.

Объёмной схемой или *схемой из кубических элементов* на множестве $M \subset \mathbb{Z}^3$ будем называть корректную сеть из кубических элементов, в графе которой нет ориентированных циклов. Множество M будем называть *носителем* схемы K.

Длиной схемы K будем называть длину наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $l(K)$.

Шириной схемы K будем называть ширину наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $w(K)$.

Высотой схемы K будем называть высоту наименьшего прямоугольного параллелепипеда, содержащего все непустые элементы схемы K, обозначается $h(K)$.

Если вход (выход) элемента не подключен к выходу (входу) другого элемента, будем его называть *входом (выходом)* схемы. *Контактами* схемы K будем называть её входы и выходы, и обозначать их $In(K), Out(K)$ соответственно.

Узлами схемы K будем называть вершины графа G_K.

Если M – носитель схемы K, то величину $|M|$, равную количеству элементов в множестве M, будем называть *объёмом* схемы K и обозначать $V(K)$.

В графе G_K будем считать, что все ребра имеют вес 1. *Расстоянием между вершинами* в графе G_K будем считать длину наименьшего пути между этими вершинами. *Расстоянием между узлами* схемы будем называть расстояние между соответствующими вершинами в G_K. Расстояние от узла a до узла b на схеме K будем обозначать $\rho_K(a, b)$.

Каждой объёмной схеме K можно сопоставить схему их функциональных элементов $Circ(K)$ следующим образом:

1) каждой функции $f_{s,i}$, которую реализует i-й выход элемента s объёмной схемы, сопоставим функциональный элемент $e_{s,i}$, реализую-

щий $f_{s,i}$; если i-й и j-й выходы являются выходами одной и той же функции, то им будет соответствовать один и тот же функциональный элемент;

2) если i-й выход элемента s_1 подключен к j-му входу элемента s_2, то соединим выход элемента $e_{s_1,i}$ с j-ми входами элементов $e_{s_2,k}$ для всех k, для которых $f_{s_2,k}$ существенно зависит от j-го аргумента;

3) удалим все тождественные функции, присоединив их вход ко всем их выходам.

Будем говорить, что схема K *реализует* булев оператор F, если схема из функциональных элементов $Circ(K)$ реализует F. Через $Impl(F)$ обозначим множество всех объёмных схем, реализующих оператор F.

Назовём схему K *минимальной*, если она обладает минимальным объёмом среди всех объёмных схем, реализующих F_K.

Через $V(F)$ обозначим объём минимальной схемы, реализующей оператор F.

Будем говорить, что объёмные схемы K_1 и K_2 *равны* и писать $K_1 = K_2$, если существует параллельный перенос пространства, который позволяет совместить схемы K_1 и K_2, иначе будем говорить, что они *различны*. Для каждой схемы K зафиксируем некоторую нумерацию её узлов. На i-м узле реализуется некоторая функция g_i от входных переменных схемы K (на входах схемы считаем, что реализуются тождественные функции).

Везде далее будем считать, что схема K имеет n входов, m выходов и l узлов. *Состоянием* схемы K на входном наборе x назовём вектор

$$s_K(x) := (g_1(x), ..., g_l(x)).$$

Если $v = (v_1, ..., v_q) \in \{0,1\}^q$, обозначим $|v| := v_1 + v_2 + ... + v_q$.

Потенциалом схемы K на входном наборе $x \in \{0,1\}^n$ назовём величину $u_K(x) := |s_K(x)|$.

Максимальным потенциалом схемы K назовём величину

$$\hat{U}(K) := \max_{x \in \{0,1\}^n} u_K(x).$$

Пусть $f : \{0,1\}^n \to \{0,1\}^m$ – булев оператор. Тогда

$$\hat{U}(f) := \min_{K \in Impl(f)} \hat{U}(K).$$

Если $Impl(f)$ пусто, то формально полагаем $\hat{U}(f) = \infty$.

Теорема 1 (Основная теорема)**.** *Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$*. Тогда существует объемная схема* W_f *со входами* $x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* f*, причём схема* W_f *обладает следующими характеристиками:*

1) Если $m \le n$*:*

а) $l(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

б) $\hat{U}(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

в) $V(W_f) \le \mathcal{O}(m \cdot 2^n)$.

2) Если $m > n$*:*

а) $l(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;

б) $\hat{U}(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;

в) $V(W_f) \le \mathcal{O}(m \cdot 2^n)$.

Замечание: Отметим, что при $\log_2(m) = o(2^n)$ объем схемы $|W_f|$ является оптимальным по порядку, что легко получить по аналогии с [4, Утв. 1] или нижней оценкой в [2].

3. Реализация булева оператора

3.1. Параметры основных блоков

Для реализации булева оператора нам потребуются несколько различных блоков. Опишем их характеристики.

1) Дешифратор D_n^1 (*Ефимов А.А., [5, лемма 2]*):

$$l(D_n^1) = \mathcal{O}(2^n),\ w(D_n^1) = \mathcal{O}(2^{n/2}),\ h(D_n^1) = 1,\ \hat{U}(D_n^1) = \mathcal{O}(2^n).$$

2) Блок дешифраторов $D'_{n,k}$ (*Калачёв Г.В., [4, лемма 2.19]*):

$$l(D'_{n,k}) = \mathcal{O}(k \cdot 2^n),\ w(D'_{n,k}) = \mathcal{O}(n^2) + \mathcal{O}(nk),\ h(D'_{n,k}) = 1,$$

$$\hat{U}(D'_{n,k}) = \mathcal{O}(kn^2 \cdot 2^n) + \mathcal{O}(k^2 n \cdot 2^n).$$

3) Левый обратный блок $D'^{-1}_{n,k}$ (*Калачёв Г.В., [4, лемма 2.20]*):

$$l(D'^{-1}_{n,k}) = \mathcal{O}(k \cdot 2^n),\ w(D'^{-1}_{n,k}) = \mathcal{O}(kn^2),\ h(D'^{-1}_{n,k}) = 1,$$

$$\hat{U}(D'^{-1}_{n,k}) = \mathcal{O}(k^2 n^2 \cdot 2^n).$$

4) Схема Q_f, реализующая оператор $f : \{0,1\}^n \to \{0,1\}^m, (m \leq n)$ (*Калачёв Г.В., [4, лемма 2.32]*):

$$l(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ w(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ h(Q_f) = 1,$$

$$\hat{U}(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}).$$

5) Схема Q^1_g, такая что схема $D^{-1}_m \circ Q^1_g \circ D'_{k-l,4}$ реализует оператор $g : \{0,1\}^{4k-4l} \to \{0,1\}^m, n = 6k, m = 8^{4l}$:

$$l(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ w(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}),\ h(Q^1_g) = 1,$$

$$\hat{U}(Q^1_g) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

6) Блок $\vee^k_n$, реализующий k дизъюнкций от n переменных:

$$l(\vee^k_n) = 1,\ w(\vee^k_n) = k,\ h(\vee^k_n) = n,\ \hat{U}(\vee^k_n) = \mathcal{O}(nk).$$

3.2. Реализация вспомогательных блоков

В данном параграфе подробно опишем реализацию всех вспомогательных блоков. Будем считать, что если у нас есть плоская схема, то можно естественным образом построить объемную схему такой же длины, ширины, и единичной высоты. При этом ясно, что оценки потенциала такой объемной схемы будут совпадать. Отметим, что некоторые леммы из работы [4] мы переформулируем указанным образом, то есть будем считать, что плоские схемы — это объемные схемы единичной высоты.

Почти все блоки, которые мы будем использовать, будут иметь базис из класса T_0. Также у них будет так называемый *управляющий вход* z. Если $z = 0$ и значения других входов равны 0, то потенциал внутренней части блока равен 0. Отметим, что значения выходов в таком случае также равны 0, то есть реализуемая схемой функция от переменных $z, x_1, \ldots, x_n$ лежит в классе T_0. Таким образом, вход z играет роль «выключателя» блока. Наличие такого входа позволяет достаточно легко оценивать потенциал схем, состоящих из нескольких блоков.

Для удобства введём еще одно обозначение. Пусть $i \in \mathbb{Z}, 0 \leq i \leq 2^n - 1$. Тогда $\bar{i}_1, \bar{i}_2, \ldots \bar{i}_n$ — разложение числа i в двоичном виде, где $\bar{i}_1$ — младший бит разложения, а $\bar{i}_n$ — старший.

Дешифратор D_n^1.

D_n^1 — плоский дешифратор, имеющий оптимальный потенциал.

Лемма 1. *(Ефимов А.А., [5, лемма 2]) Существует объемная схема D_n^1 со входами $z, x_1, \ldots, x_n$ имеющая 2^n выходов, на i-м выходе которой на допустимых наборах $(z \geq x_1 \vee \ldots \vee x_n)$ реализуется функция*

$$z x_1^{\bar{i}_1} x_2^{\bar{i}_2} \ldots x_n^{\bar{i}_n},$$

причём схема D_n^1 обладает следующими характеристиками:

1) $l(D_n^1) = \mathcal{O}(2^n),\ w(D_n^1) = \mathcal{O}(2^{n/2}),\ h(D_n^1) = 1;$

2) $\hat{U}(D_n^1) = \mathcal{O}(2^n).$

Блок дешифраторов $D'_{n,k}$.

Плоский блок дешифраторов $D'_{n,k}$. На вход подаются k групп переменных по n штук + отдельная переменная z. Переменные обозначаем x_j^i, где i — номер группы, а i — номер переменной в этой группе. Каждую группу переменных мы подаем на отдельный дешифратор D'_n, переменную z подаем на все дешифраторы. Объединение выходов всех дешифраторов есть выходы схемы. Основное свойство блока дешифраторов в том, что у него сравнительно небольшой потенциал, а при этом на выходе активны всегда ровно k выходов (по одному с каждого дешифратора).

Лемма 2. *(Калачёв Г.В., [4, лемма 2.19]) Существует объемная схема $D'_{n,k}$ со входами $z, x_1^1, \ldots, x_n^1, x_1^2 \ldots, x_n^2, \ldots x_n^k$ имеющая $k \cdot 2^n$ выходов, на (i,j)-м выходе которой реализуется функция*

$$(x_1^i)^{\bar{j}_1} (x_2^i)^{\bar{j}_2} \ldots (x_n^i)^{\bar{j}_n},$$

причём схема $D'_{n,k}$ обладает следующими характеристиками:

1) $l(D'_{n,k}) = \mathcal{O}(k \cdot 2^n),\ w(D'_{n,k}) = \mathcal{O}(n^2) + \mathcal{O}(nk),\ h(D'_{n,k}) = 1;$

2) $\hat{U}(D'_{n,k}) = \mathcal{O}(kn^2 \cdot 2^n) + \mathcal{O}(k^2 n \cdot 2^n).$

Обратный блок дешифраторов $D'^{-1}_{n,k}$.

Плоский левый обратный блок дешифраторов $D'^{-1}_{n,k}$ к блоку $D'_{n,k}$.

Лемма 3. *(Калачёв Г.В., [4, лемма 2.20]) Существует объемная схема* $D'^{-1}_{n,k}$ *со входами* $z, x^1_1, \ldots, x^1_{2^n}, x^2_1 \ldots, x^2_{2^n}, \ldots x^k_{2^n}$ *имеющая* $k \cdot n$ *выходов, причём схема* $D'^{-1}_{n,k}$ *обладает следующими характеристиками:*

1) $l(D'^{-1}_{n,k}) = \mathcal{O}(k \cdot 2^n),\ w(D'^{-1}_{n,k}) = \mathcal{O}(kn^2),\ h(D'^{-1}_{n,k}) = 1;$

2) $\hat{U}(D'^{-1}_{n,k}) = \mathcal{O}(k^2 n^2 \cdot 2^n).$

Блок Q_f.

Плоский блок Q_f. Прямоугольный блок, который выдает значения данного булева оператора f и имеет оптимальные параметры (на плоскости). Лемма, используемая в работе [4], сформулирована для частичных операторов и в общем виде. Мы воспользуемся следствием из неё для случая $m \leq n$. Также в самой формулировке леммы не указаны оценки для длины и ширины схемы, но при этом они явно указаны в доказательстве.

Лемма 4. *(Калачёв Г.В., [4, лемма 2.32]) Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$*, где* $m \leq n$*. Тогда существует объемная схема* Q_f *со входами* $z, x_1, x_2, \ldots, x_n$ *на* m *выходах которой реализуется оператор* $f'(z, \vec{x}) = zf(x)$*, причём схема* Q_f *обладает следующими характеристиками:*

1) $l(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ w(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^{n/2}),\ h(Q_f) = 1;$

2) $\hat{U}(Q_f) = \mathcal{O}(\sqrt{m} \cdot 2^n).$

Блок $\vee^k_n$.

Объемный блок $\vee^k_n$ (см. рис. 1), реализующий k дизъюнкций от n переменных.

Лемма 5. *Существует объемная схема* $\vee^k_n$ *с* nk *входами* x^j_i $(i = 1 \ldots n, j = 1 \ldots k)$ *на* l *выходе* $(l = 1 \ldots k)$ *которой реализуется функция* $y_l = x^l_1 \vee x^l_2 \vee \ldots \vee x^l_n$*, причём схема* $\vee^k_n$ *обладает следующими характеристиками:*

1) $l(\vee^k_n) = 1,\ w(\vee^k_n) = k,\ h(\vee^k_n) = n;$

2) $\hat{U}(\vee^k_n) = \mathcal{O}(nk).$

Доказательство. На рис. 1 изображена схема $\vee^k_n$, которая по столбцам собирает дизъюнкцию входов и выдает результат на соответствующий выход; при этом схема имеет требуемые характеристики. □

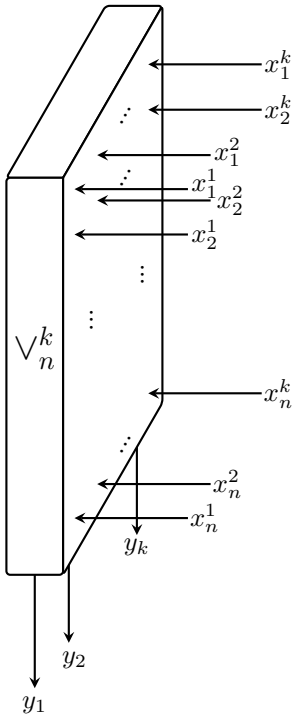


Рис. 1. Реализация блока $\vee_n^k$.

3.3. Реализация булева оператора в случае $m \leq n$

Итак, пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$. Будем считать, что $n = 6k, m = 8^{4l}, m \leq n$. Разложим оператор f по последним $2k + 4l$ переменным:

$$f(x_1, x_2, \ldots, x_{6k}) = \bigvee_{i=0}^{2^{2k+4l}-1} x_{4k-4l+1}^{\bar{i}_1} x_{4k-4l+2}^{\bar{i}_2} \ldots x_{6k}^{\bar{i}_{2k+4l}} f_i(x_1, \ldots, x_{4k-4l}), \tag{1}$$

где

$$f_i(x_1, \ldots, x_{4k-4l}) = f(x_1, \ldots, x_{4k-4l}, \bar{i}_1, \bar{i}_2, \ldots, \bar{i}_{2k+4l}).$$

Для каждого оператора f_i от $4k-4l$ переменных построим вспомогательный блок $Q_{f_i}^1$ (см. рис. 2, где $g = f_i$), реализующий данный оператор. Особенностью данного блока является тот факт, что на вход ему мы подаем выходы из блока дешифраторов $D'_{k-l,4}$, а выходы подсхемы Q_{f_i} мы

подаем на блок дешифраторов, чтобы уменьшить потенциал проводов. Таким образом, если вход z неактивен, то потенциал всей схемы равен 4. Подробно посчитаем характеристики схемы, воспользовавшись следующей леммой, где $g = f_i$.

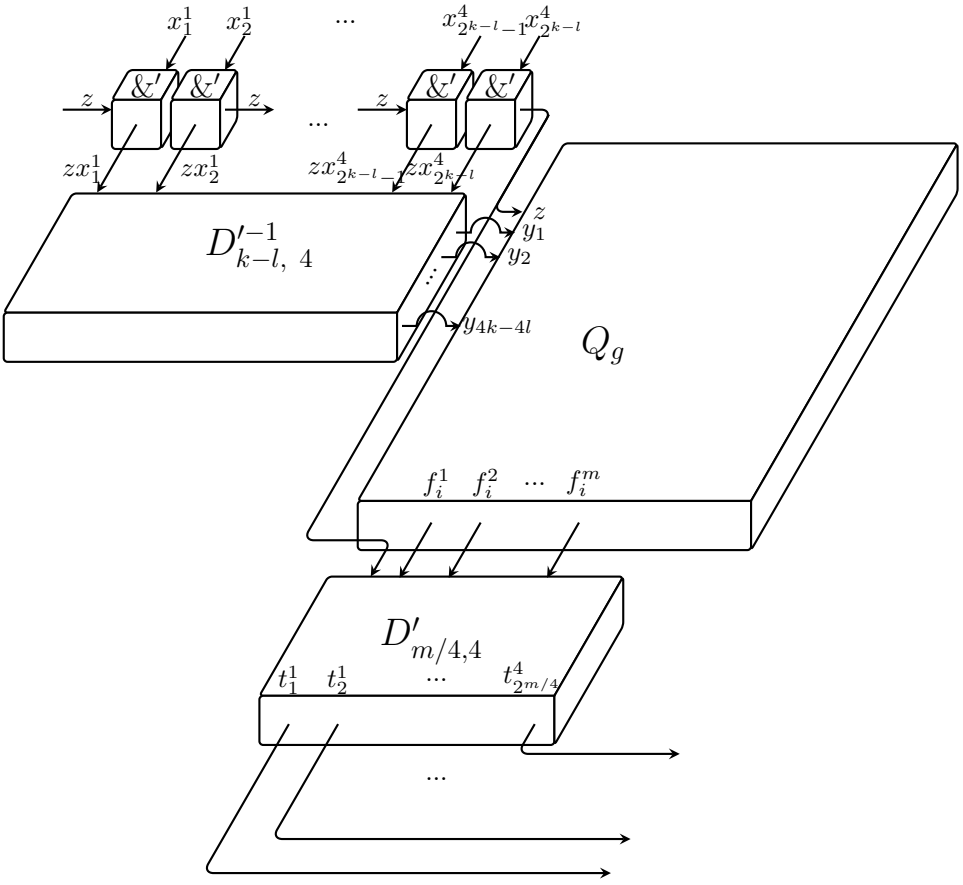


Рис. 2. Реализация блока Q_g^1.

Лемма 6. *Пусть дан частичный булев оператор* $g : G \to \{0,1\}^m, n = 6k, m = 8^{4l}$*; где* G *— множество значений блока* $D'_{k-l,4}$*, т.е.* $G = \{D'_{k-l,4}(x) | x \in \{0,1\}^{4 \cdot 2^{k-l}}\}$*. Тогда существует объемная схема* Q_g^1*, такая, что схема* $D_m^{-1} \circ Q_g^1 \circ D'_{k-l,4}$ *со входами* $z, x_1, x_2, \ldots, x_{4k-4l}$ *на* m

выходах реализует оператор $g'(z,\vec{x}) = z \cdot g(\vec{x})$, *причём схема* Q_g^1 *обладает следующими характеристиками:*

1) $l(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $w(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $h(Q_g^1) = 1$;

2) $\hat{U}(Q_g^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, *если* $z = 1$; *и* $\hat{U}(Q_g^1) = 4$, *если* $z = 0$.

Доказательство. Оценим размеры схемы Q_g^1:

$$l(Q_g^1) = l(D_{k-l,4}^{-1})+1+w(Q_g) = \mathcal{O}(4{\cdot}2^{k-l})+\mathcal{O}(\sqrt{m}{\cdot}2^{2k-2l}) = \mathcal{O}(\sqrt{m}{\cdot}2^{2k-2l}) =$$

$$= \mathcal{O}\left(\frac{\sqrt{m} \cdot 2^{2k}}{\sqrt[6]{m}}\right) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$w(Q_g^1) = l(Q_g) + 1 + w(D'_{m/4,4}) + \mathcal{O}(4 \cdot 2^{m/4}) = \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) + \mathcal{O}(m)+$$

$$+\mathcal{O}(m^2/16) + \mathcal{O}(4 \cdot 2^{m/4}) = \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$h(Q_g^1) = 1.$$

Оценим потенциал, если $z = 1$. Общий потенциал схемы Q_g^1 складывается из потенциала блоков $D_{k-l,4}^{\prime -1}, Q_g, D'_{m/4,4}$ и площади проводов. Здесь мы учитываем, что на выходе блока $D'_{m/4,4}$ будут активны только 4 провода, а значит потенциал той области можно оценить как 4 полупериметра: $4 \cdot (4 \cdot 2^{m/4} + w(Q_g))$. Получаем оценку:

$$\hat{U}(Q_g^1) = \mathcal{O}(4 \cdot 2^{k-l}) + \hat{U}(D_{k-l,4}^{-1}) + l(Q_g) + w(Q_g) + \hat{U}(Q_g) + l(D'_{m/4,4})+$$

$$+\hat{U}(D'_{m/4,4}) + 4 \cdot (4 \cdot 2^{m/4} + w(Q_g)) = \mathcal{O}(4 \cdot 2^{k-l}) + \mathcal{O}(16(k-l)^2 \cdot 2^{k-l})+$$

$$+\mathcal{O}(2^{2k-l}) + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l}) + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l})+$$

$$+\mathcal{O}(m^2 \cdot 2^{m/4}) + 4 \cdot (4 \cdot 2^{m/4} + \mathcal{O}(\sqrt{m} \cdot 2^{2k-2l})) =$$

$$= \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Если $z = 0$, то активны ровно 4 входа схемы Q_g^1, так как G — множество значений блока $D'_{k-l,4}$, а значит потенциал $\hat{U}(Q_g^1) = 4$. □

Лемма 7 (Основная лемма)**.** *Пусть дан булев оператор* $f : \{0,1\}^n \to \{0,1\}^m$, $(m \leq n)$. *Тогда существует объемная схема* W_f^1 *со входами* $z, x_1, x_2, \ldots, x_n$ *на* m *выходах которой на допустимых наборах* $(z \geq x_1 \vee \ldots \vee x_n)$ *реализуется оператор* $f'(z,\vec{x}) = zf(\vec{x})$, *причём схема* W_f^1 *обладает следующими характеристиками:*

1) $l(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $w(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $h(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

2) $\hat{U}(W_f^1) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

3) $V(W_f) \leq \mathcal{O}(m \cdot 2^n)$.

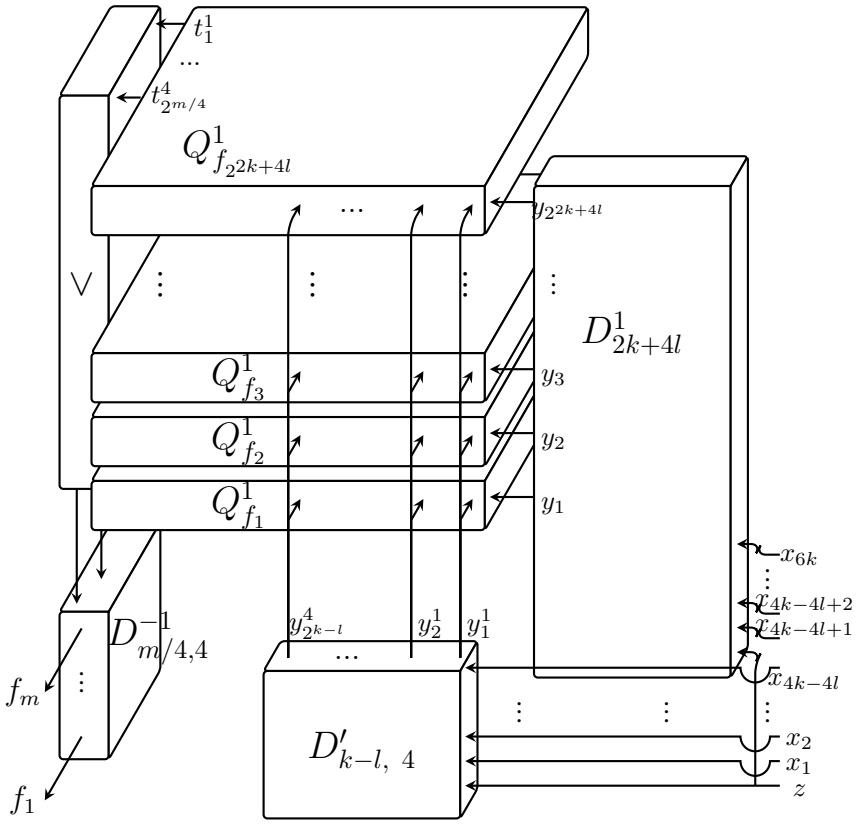


Рис. 3. Реализация основного блока W_f^1.

Доказательство. Покажем, что схема W_f^1 (см. рис. 3) реализует оператор f согласно формуле (1).

Дешифратор D^1_{2k+4l} реализует все элементарные конъюнкции

$$y_i = x_{4k-4l+1}^{\bar{i}_1} x_{4k-4l+2}^{\bar{i}_2} \dots x_{6k}^{\bar{i}_{2k+4l}},$$

причем при любом значении переменных ровно один выход будет активным, а остальные нет. Это означает, что среди блоков $Q^1_{f_i}$ активным будет только один. Оставшиеся переменные $x_1, \ldots, x_{4k-4l}$ отправляются на блок дешифраторов $D'_{k-l,4}$, где в «зашифрованном» виде отправляются на все блоки $Q^1_{f_i}$. В каждом блоке $Q^1_{f_i}$ они «расшифровываются», то есть преобразуются обратно в переменные $x_1, \ldots, x_{4k-4l}$, после чего реализуется оператор $f_i(x_1, \ldots, x_{4k-4l})$. А так как управляющим входом в блок $Q^1_{f_i}$ является $y_i = x^{\bar{i}_1}_{4k-4l+1} x^{\bar{i}_2}_{4k-4l+2} \ldots x^{\bar{i}_{2k+4l}}_{6k}$, то фактически на внутри блока $Q^1_{f_i}$ реализуется оператор

$$x^{\bar{i}_1}_{4k-4l+1} x^{\bar{i}_2}_{4k-4l+2} \ldots x^{\bar{i}_{2k+4l}}_{6k} f_i(x_1, \ldots, x_{4k-4l}).$$

Таким образом, если мы возьмем дизъюнкцию всех выходов блоков $Q^1_{f_i}$ (с помощью блока $\vee^m_{2^{2k+4l}}$, на рис. 1 он для удобства обозначен просто $\vee$), то получим верное значение согласно формуле (1). Но в таком случае мы не получим верной оценки потенциала, поэтому внутри каждого блока $Q^1_{f_i}$ мы сначала «зашифруем» выходы с помощью блока $D^1_{m/4,4}$, а после взятия дизъюнкции «расшифруем» с помощью блока $D^{-1}_{m/4,4}$. Поскольку при любом наборе входных переменных активным будет только один блок $Q^1_{f_i}$, то на выходе блока $\vee$ будут «зашифрованные» выходы $Q^1_{f_i}$, а значит на выходе $D^{-1}_{m/4,4}$ будут верные значения согласно формуле 1.

Теперь оценим параметры схемы W^1_f в случае $n = 6k, m = 8^{4l}$.

$$l(W^1_f) = 1 + w(D^1_{2k+4l}) + l(Q^1_{f_i}) + 1 = \mathcal{O}(2^{k+2l}) + \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$w(W^1_f) = 1 + w(Q^1_{f_i}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{2k}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

$$h(W^1_f) = \max(w(D'_{k-l,4}) + l(D^1_{2k+4l}) - 1, h(\vee) + h(D^{-1}_{m/4,4})) =$$

$$= \max(\mathcal{O}((k-l)^2 + 4(k-l)) + \mathcal{O}(2^{2k+4l}), \mathcal{O}(2^{2k+4l}) + \mathcal{O}(4m^2)) =$$

$$= \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Для оценки объёма схемы $V(W^1_f)$ воспользуемся тем фактом, что для любой объёмной схемы K верно неравенство:

$$V(K) \leq l(K) \cdot w(K) \cdot h(K).$$

Таким образом, имеем оценку:

$$V(W^1_f) \leq l(W^1_f) \cdot w(W^1_f) \cdot h(W^1_f) \leq \mathcal{O}(m \cdot 2^n).$$

Оценим потенциал схемы.

1) Входы $z, x_1, x_2, \ldots x_{4k-4l}$ подводим к блоку $D'_{k-l,4}$. Эту часть схемы оцениваем через объем:

$$U_1 \leq 6{\cdot}(4k{-}4l{+}1){\cdot}(w(D^1_{2k+4l}){+}1) \leq \mathcal{O}((4k{-}4l{+}1){\cdot}2^{k+2l}) \leq \mathcal{O}(2^{2k+4l}).$$

2) Оценим потенциал блока $D'_{k-l,4}$:

$$U_2 \leq \hat{U}(D'_{k-l,4}) \leq \mathcal{O}(4\cdot(k-l)^2\cdot 2^{k-l}) + \mathcal{O}(16\cdot(k-l)\cdot 2^{k-l}) \leq \mathcal{O}(2^{k+2l}).$$

3) На выходах блока $D'_{k-l,4}$ будут активны ровно 4 провода, подводим их к блокам $Q^1_{f_i}$ и оценим потенциал:

$$U_3 \leq 4 \cdot l(D^1_{2k+4l}) \leq 4 \cdot \mathcal{O}(2^{2k+4l}) = \mathcal{O}(2^{2k+4l}).$$

4) Подводим провода $z, x_{4k-4l}, x_{4k+1}, \ldots, x_{6k}$ к дешифратору D^1_{2k+4l} и оценим потенциал:

$$U_4 \leq \mathcal{O}(2k + 4l).$$

5) Оценим потенциал дешифратора D^1_{2k+4l}:

$$U_5 \leq \hat{U}(D^1_{2k+4l}) \leq \mathcal{O}(2^{2k+4l}).$$

6) Так как среди выходов дешифратора D^1_{2k+4l} будет активным только один, и все его выходы будут подключены к управляющим входам блоков $Q^1_{f_i}$, то только 1 из блоков будет активен, а остальные $2^{2k+4l} - 1$ будут иметь потенциал 4:

$$U_6 \leq 4 \cdot (2^{2k+4l} - 1) + \hat{U}(Q^1_{f_i}) \leq \mathcal{O}(2^{2k+4l}).$$

7) Так как ровно 4 выхода одного блока $Q^1_{f_i}$ будут активны, то потенциал внутри блока $\vee$ можно оценить через объем 4 столбцов схемы $\vee$:

$$U_7 \leq 6 \cdot 4 \cdot h(\vee) \leq \mathcal{O}(2^{2k+4l}).$$

8) Осталось оценить потенциал блока $D^{-1}_{m/4,4}$:

$$U_8 \leq \hat{U}(D^{-1}_{m/4,4}) \leq \mathcal{O}(m^2 \cdot 2^{m/4}).$$

В итоге, имеем следующую оценку потенциала схемы W_f^1:

$$\hat{U}(W_f^1) = U_1 + U_2 + U_3 + U_4 + U_5 + U_6 + U_7 + U_8 \leq \mathcal{O}(2^{2k+4l}) + \mathcal{O}(2^{k+2l}) +$$

$$+\mathcal{O}(2^{2k+4l}) + \mathcal{O}(2k+4l) + \mathcal{O}(2^{2k+4l}) + \mathcal{O}(2^{2k+4l}) + \mathcal{O}(2^{2k+4l}) + \mathcal{O}(m^2 \cdot 2^{m/4}) \leq$$

$$\leq \mathcal{O}(2^{2k+4l}) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3}).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 6k, m = 8^{4l}$. Если же $n = 6k+r, m = 8^{4l}+t$, где $r = 1 \ldots 5, t = 1 \ldots (8^{4(l+1)} - 8^{4l} - 1)$, то построим схему для $n = 6k + 6, m = 8^{4(l+1)}$ и на последние $6-r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в $16 \cdot 4 = 64$ раза, а значит оценки по порядку останутся верными. □

3.4. Реализация булева оператора в случае $m > n$

Лемма 8. *Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$, $(m > n)$. Тогда существует объемная схема W_f^1 со входами $z, x_1, x_2, \ldots, x_n$ на m выходах которой реализуется на допустимых наборах $(z \geq x_1 \vee \ldots \vee x_n)$ реализуется оператор $f'(z, \vec{x}) = zf(\vec{x})$, причём схема W_f^1 обладает следующими характеристиками:*

1) $l(W_f^1) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $w(W_f^1) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $h(W_f^1) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;
2) $\hat{U}(W_f^1) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;
3) $V(W_f) \leq \mathcal{O}(m \cdot 2^n)$.

Доказательство. Рассмотрим случай, когда $n = 8t, m = kn$. Покажем, что тогда схема, изображенная на рис. 4 реализует оператор f.

Мы подаем входные переменные $z, x_1, \ldots, x_n$ на вход блоку дешифраторов $D'_{n/8,8}$, далее все эти провода подводим к каждому из k блоков обратных дешифраторов $D^{-1}_{n/8,8}$. «Расшифрованные» переменные $z, x_1, \ldots, x_n$ мы подаем на соответствующий блок $W^1_{f_i}$, который реализует оператор f_i от n переменных. Далее, собирая все выходы блоков $W^1_{f_i}$, получаем выходы оператора f.

Оценим параметры схемы W_f^1.

$$l(W_f^1) = l(W^1_{f_i}) + w(D^{-1}_{n/8,8}) + \mathcal{O}(8 \cdot 2^{n/8}) + w(D'_{n/8,8}) \leq$$

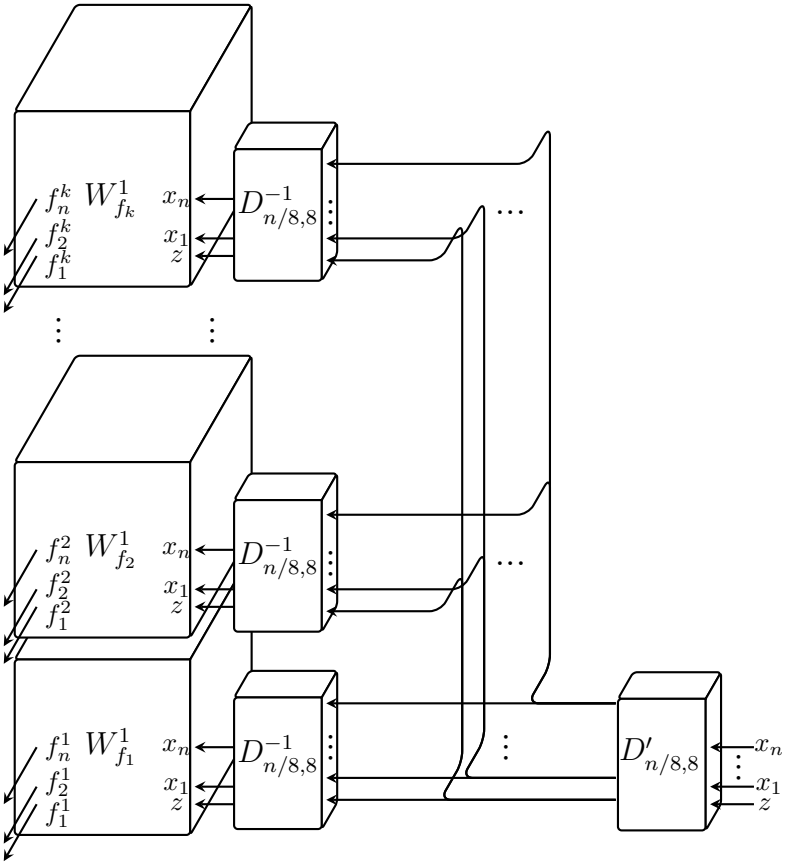


Рис. 4. Реализация основного блока W_f^1 при $m > n$.

$$\leq \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3}) + \mathcal{O}(n^2/8) + \mathcal{O}(8 \cdot 2^{n/8}) + \mathcal{O}(n^2/16 + n) \leq \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3}).$$

$$w(W_f^1) = w(W_{f_i}^1) \leq \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3}).$$

$$h(W_f^1) = k \cdot h(W_{f_i}^1) \leq \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3}\right).$$

Аналогично доказательству из леммы 7 оценим объём схемы W_f^1:

$$V(W_f^1) \leq l(W_f^1) \cdot w(W_f^1) \cdot h(W_f^1) \leq \mathcal{O}(m \cdot 2^n).$$

Оценим потенциал схемы.

1) Блок дешифраторов $D'_{n/8,8}$.

$$U_1 \leq \hat{U}(D'_{n/8,8}) \leq \mathcal{O}(8n \cdot 2^{n/8} + n^2/8 \cdot 2^{n/8}) = \mathcal{O}(n^2 \cdot 2^{n/8}).$$

2) Далее на выходе из блока дешифраторов $D'_{n/8,8}$ будут активны 8 проводов, которые мы подводим к блокам $D^{-1}_{n/8,8}$. Таким образом, имеем оценку:

$$U_2 \leq 8 \cdot (h(W_f^1) + k \cdot \mathcal{O}(8 \cdot 2^{n/8})) \leq \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right).$$

3) Оценим потенциал всех k блоков $D^{-1}_{n/8,8}$:

$$U_3 \leq k \cdot \hat{U}(D^{-1}_{n/8,8}) \leq k \cdot \mathcal{O}(n^2 \cdot 2^{n/8}) \leq \mathcal{O}(mn \cdot 2^{n/8}).$$

4) Оценим потенциал всех k блоков $W^1_{f_i}$:

$$U_4 \leq k \cdot \hat{U}(W^1_{f_i}) \leq k \cdot \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3}) \leq \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right).$$

В итоге, имеем следующую оценку потенциала схемы W^1_f:

$$\hat{U}(W_f^1) = U_1 + U_2 + U_3 + U_4 \leq$$

$$\leq \mathcal{O}(n^2 \cdot 2^{n/8}) + \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right) + \mathcal{O}(mn \cdot 2^{n/8}) + \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right) \leq$$

$$\leq \mathcal{O}\left(\frac{m}{n^{2/3}} \cdot 2^{n/3}\right) = \mathcal{O}\left(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3}\right).$$

Таким образом, получаем верное утверждение теоремы в случае $n = 8t, m = kn$. Если же $n = 8t + r, m = kn + l$, где $r = 1 \ldots 7, l = 1 \ldots (n-1)$, то построим схему для $n = 8t+8, m = (k+1)n$ и на последние $8-r$ входов подадим константу 0. Заметим, что в данном случае получим искомую схему и константы в оценках увеличатся не более, чем в константу раз, а значит оценки по порядку останутся верными. □

В качестве следствия из леммы 7 и леммы 8 докажем основную теорему.

Теорема 2 (Основная теорема)**.** *Пусть дан булев оператор $f : \{0,1\}^n \to \{0,1\}^m$. Тогда существует объемная схема W_f со входами $x_1, x_2, \ldots, x_n$ на m выходах которой реализуется оператор f, причём схема W_f обладает следующими характеристиками:*

1) Если $m \leq n$:

а) $l(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

б) $\hat{U}(W_f) = \mathcal{O}(\sqrt[3]{m} \cdot 2^{n/3})$;

в) $V(W_f) \leq \mathcal{O}(m \cdot 2^n)$.

2) Если $m > n$:

а) $l(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $w(W_f) = \mathcal{O}(\sqrt[3]{n} \cdot 2^{n/3})$, $h(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;

б) $\hat{U}(W_f) = \mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$;

в) $V(W_f) \leq \mathcal{O}(m \cdot 2^n)$.

Доказательство. Построим схему W_f^1, используя лемму 7 при $m \leq n$ или лемму 8 при $m > n$. Подадим в схеме W_f^1 на вход z константу 1. Полученная таким образом схема W_f реализует оператор $f(x_1, x_2, \ldots, x_n)$ на всех наборах $x_1, x_2, \ldots, x_n$ и его параметры остаются такими же по порядку, как и у схемы W_f^1. □

Список литературы

[1] Кравцов С. С., "О реализации функций алгебры логики в одном классе схем из функциональных и коммутационных элементов", *Проблемы кибернетики*, **19** (1967), 285–293.

[2] Коршунов А. Д., "Об оценках сложности из объемных функциональных элементов и объемных схем из функциональных элементов", *Проблемы кибернетики*, **19** (1967), 275–283.

[3] Калачёв Г. В., "Порядок мощности плоских схем, реализующих булевы функции", *Дискретная математика*, **26**:1 (2014), 49–74.

[4] Калачёв Г. В., "Об одновременной минимизации площади, мощности и глубины плоских схем, реализующих частичные булевы операторы", *Интеллектуальные системы. Теория и приложения*, **20**:2 (2016), 203–266.

[5] Ефимов А. А., "Верхняя оценка энергопотребления в классе объемных схем", *Интеллектуальные системы. Теория и приложения*, **23**:1 (2019), 117–132.

The upper estimate of the volumetric power consumption of the circuits that implement boolean operators.

Efimov A.A.

In this work volume schemes which are generalization of plane schemes in space are considered. The class of the schemes implementing boolean operators was considered. For this class upper assessment of potential — a measure of the power equal to quantity of the circuit elements giving unit on this input pattern is received. It is shown that any operator of n variables can be realized with a volume scheme whose potential does not exceed $\mathcal{O}(m \cdot 2^{n/3})$ if $m \leq n$ and $\mathcal{O}(\frac{m}{n} \cdot \sqrt[3]{n} \cdot 2^{n/3})$ if $m > n$.

Keywords: schemes from functional elements, volume schemes, scheme power, potential.

Вопросы выразимости в классе согласованных функций

Кан А. Н.

В настоящей работе рассматривается 2-полнота в классе P согласованных функций. Данный класс был рассмотрен ранее в работах [3, 4]. Он является предполным в классе PL кусочно-линейных функций. В нем было найдено два 2-предполных класса: класс CPL непрерывных функций, класс PF согласованных финитных функций.

Ключевые слова: Класс кусочно-линейных функций, класс кусочно-линейных непрерывных функций, класс согласованных функций, класс финитных функций, класс согласованных финитных функций, 2-предполнота, функция Хэвисайда.

1. Основные понятия и определения.

Рассмотрим следующие функции действительных аргументов:
1) Функция $\Theta(x)$ (Хэвисайда):

$$\Theta(x) = \begin{cases} 0, & \text{если } x < 0 \\ 1, & \text{иначе} \end{cases} \tag{1}$$

2) Функция $\Theta'(x)$:

$$\Theta'(x) = 1 - \Theta(-x) = \begin{cases} 0, & \text{если } x \leq 0 \\ 1, & \text{иначе} \end{cases} \tag{2}$$

3) Функция $F(x, y)$:

$$F(x, y) = \begin{cases} 0, & \text{если } y \leq 0 \\ x, & \text{иначе} \end{cases} \tag{3}$$

Введем некоторые обозначения:

1) Запись вида $f(\overline{a} \cdot t + \overline{b})$ равняется записи $f(a_1 \cdot t + b_1, ..., a_n \cdot t + b_n)$, где $\overline{a} = (a_1, ..., a_n)$ и $\overline{b} = (b_1, ..., b_n)$.

2) Под операцией " $\cdot$ " примененной к векторам, подразумевается операция скалярного произведения векторов.

3) Пусть $M \subset PL$, тогда $M^{(2)}$ это множество состоящие из всех двухместных функций множества M.

4) В данной статье рассматривается замыкание по операциям супер позиции. Замыкание множества $M \in PL$ по операциям суперпозиции, будем обозначать через $[M]$. [1]

Определение 1. *Функция $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ называется линейной, если найдутся $\overline{a} \in \mathbb{R}^n$ и $c \in \mathbb{R}$, такие что $f(\overline{x}) = \overline{x} \cdot \overline{a} + c$. Множество всех линейных функций обозначим через L.*

Пусть l_i - гиперплоскость, задаваемая уравнением $\overline{x} \cdot \overline{a_i} + c_i = 0, a_i \in \mathbb{R}^n \backslash \{\overline{0}\}, c_i \in \mathbb{R}, i = 1, ..., k$. Для каждой точки $\overline{x} \in \mathbb{R}^n$ рассмотрим вектор $\sigma(\overline{x}) = (\sigma_1, ..., \sigma_k)$ с компонентами из множества $\{-1, 0, 1\}, \sigma_i = sgn(\overline{x} \cdot \overline{a_i} + c_i)$, где

$$sgn(b) = \begin{cases} -1, & \text{если } b < 0 \\ 0, & \text{если } b = 0 \\ 1, & \text{если } b > 0. \end{cases} \tag{4}$$

Определение 2. *Две точки $\overline{x}, \overline{y} \in \mathbb{R}$ эквивалентны относительно гиперплоскостей $l_1, ..., l_k$ тогда и только тогда, когда $\sigma(\overline{x}) = \sigma(\overline{y})$, обозначим это через $\overline{x} \sim \overline{y}$.*

Легко проверить, что отношение " $\sim$ " является отношением эквивалентности. Таким образом, пространство $\mathbb{R}^n$ разбивается на классы эквивалентности $R_1, ..., R_s$.

Определение 3. *Сигнатурой класса R называется вектор $\sigma(R) = \sigma(\overline{x})$, где $\overline{x}$ точка класса R.*

Пусть $R_1, ..., R_s$ - все классы эквивалентности на которые гиперплоскости $l_1, ..., l_k$ разбивают $\mathbb{R}^n$.

Определение 4. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется кусочно-линейной, если* $\forall j \in \{1, ..., s\}$ *найдутся* $b_j \in \mathbb{R}^n$ *и* $d_j \in \mathbb{R}$, *что для всех* $\overline{x} \in R_j$ *выполняется* $f(\overline{x}) = \overline{x} \cdot \overline{b_j} + d_j$. *Линейную функцию* $\overline{x} \cdot \overline{b_j} + d_j$, *реализуемую на множестве* R_j, *обозначим* $f_{R_j}(\overline{x})$. *Множество всех кусочно-линейных функций обозначим через* PL.

Определение 5. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется кусочно-постоянной, если* $f \in PL$ *[1] и* $\forall j \in \{1, ..., s\}, \exists d_j \in \mathbb{R}$ *такие, что* $\forall \overline{x} \in R_j$ *(где* R_j *классы эквивалентности [1]),* $f(\overline{x}) = d_j$,. *Класс всех кусочно-постоянной функций обозначим* PC.

Определение 6. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется согласованной, если* $f \in PL$ *и* $\forall \overline{a}, \overline{b}, \overline{d} \in \mathbb{R}^n, \exists N \in \mathbb{R}_+$ *такие, что* $f(\overline{a} \cdot t + \overline{b}) - f(\overline{a} \cdot t + \overline{d}) = const$, $\forall t > N$. *Класс всех согласованных функций обозначим* P.

Определение 7. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется финитной, если* $f \in PL$ *и* $\forall \overline{a}, \overline{b} \in \mathbb{R}^n, \exists A, B, N \in \mathbb{R}$ *такие, что* $f(\overline{a} \cdot t + \overline{b}) = A \cdot t + B$, $\forall |t| > N$. *Класс всех финитных функций обозначим* Φ.

Классы P и Φ замкнуты по операциям суперпозиции и образуют критериальную систему в классе PL кусочно-линейных функций.[3]

Определение 8. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется кусочно-линейной непрерывной, если* $f \in PL$ *и непрерывна. Класс всех кусочно-линейных непрерывных функций обозначим через* CPL.

Далее введем понятие 2-предполных классов.

Определение 9. *Пусть* A *замкнутый класс и* $A \subset B$. A *2-предполный в классе* B, *если*
$B^{(2)} \subset [A \cup \{f\}]$, *где* $f \notin B \backslash A$.

Оказывается, класс непрерывных кусочно-линейных функций является 2-предполным в классе согласованных функций.

2. 2-предполнота непрерывных кусочно-линейных функций.

Пусть $M \subset P$ и $M \not\subset CPL$, тогда верна следующая теорема.

Теорема 1. $P^{(2)} \subset [M \cup CPL]$.

Доказательство.

У нас имеется все непрерывные кусочно-линейные функции и функция $f \notin CPL$ не принадлежащая данному классу. Нам нужно доказать что класс CPL 2-предполный в классе P. Будем строить произвольную функцию из $P^{(2)}$ согласованных функций. Доказательство разобьем на две части.

1) Сначала покажем что мы можем построить функцию, которая совпадает с исходной на всех конечных классах эквивалентности, а на бесконечных классах эквивалентности равняется нулю.

Выделим функцию $g(x) \in CPL \backslash \Phi$:

$$g(x) = \begin{cases} 0, & \text{если } x < 0 \\ x, & \text{иначе} \end{cases} \tag{5}$$

Легко видеть, что функция $g(x)$ не содержится в классе финитных функций. Из курсовой работы [3] следует, что из функции f являющейся разрывной и функции g не являющейся финитной, можно получить функцию $\Theta(x)$. Также выделим функцию $\overline{F}^o(x, y)$:

$$\overline{F}^o(x, y) = \begin{cases} 0, & \text{если } y \leq 0 \\ x, & \text{если } y > |x| \\ y, & \text{если } y > 0, y \leq x \\ -y, & \text{если } y > 0, y \leq -x \end{cases} \tag{6}$$

Легко проверить что функция (5) непрерывна.

$\forall N \in \mathbb{R}_+$, определим функцию $F_N^o(x, y) = \overline{F^o}(x, N \cdot \Theta'(y))$:

$$F_N^o(x, y) = \begin{cases} 0, & \text{если } y \leq 0 \\ x, & \text{если } y > 0, |x| < N \\ c(x, y), & \text{иначе} \end{cases} \tag{7}$$

Функция (6) ведет себя как функция $F(x, y), \forall |x| < N$.

В работе [1] было доказано, что любая функция $f(\overline{x}) \in PL$ может быть представлена в следующем виде:

$$f(\overline{x}) = \sum_{j=1}^{s} F(\overline{b}_j \cdot \overline{x} + d_j, \sum_{i=1}^{k} \chi(sgn(\overline{a}_i \cdot \overline{x} + c_i), \sigma_j^i) - k + 1) \tag{8}$$

Где $s \in \mathbb{N}$ это количество классов эквивалентности, а $k \in \mathbb{N}$ количество разделяющих гиперплоскостей.

Давайте подробнее разберем почему это так. Данное выражение

$$\sum_{i=1}^{k} \chi(sgn(\overline{a}_i \cdot \overline{x} + c_i), \sigma_j^i) - k + 1 \tag{9}$$

из уравнения (7) поэлементно сравнивает вектор сигнатуры класса R_j с вектором сигнатуры точки $\overline{x}$ и если они совпадают (т.е. точка лежит в данном классе эквивалентности) то выражение (8) равно единице в противном случае данное выражение меньше либо равно нулю. Следовательно все выражение в правой части уравнения (7) равно линейной функции соответствующей некому классу эквивалентности R_j если точка $\overline{x}$ лежит в данном классе эквивалентности и равно нулю если точка не принадлежит ни одному классу эквивалентности. Так как мы описываем только конечные классы эквивалентности и функции $F(x, y)$ и $F_N^o(x, y)$ совпадают (при $|x| < N$). Следовательно в уравнении (7) функцию $F(x, y)$ можно заменить на функцию $F_N^o(x, y)$.

$$f(\overline{x}) = \sum_{j=1}^{s} F_N^o(\overline{b}_j \cdot \overline{x} + d_j, \sum_{i=1}^{k} \chi(sgn(\overline{a}_i \cdot \overline{x} + c_i), \sigma_j^i) - k + 1) \tag{10}$$

Аналогично, с помощью уравнения (9) можно представить любую функцию, которая на бесконечных классах эквивалентности равняется нулю.

$$\chi(a, b) = \begin{cases} 1, & \text{если } a = b \\ 0, & \text{иначе} \end{cases} \tag{11}$$

$$sgn(x) = \begin{cases} -1, & x < 0 \\ 0, & x = 0 \\ 1, & x > 0 \end{cases} \tag{12}$$

Функции (10) и (11) принадлежат классу PC кусочно-постоянных функций, а следовательно могут быть получены из функции $\Theta(x)$ и линейных функций. [1]

2) Теперь построим функцию, которая совпадает с исходной на всех бесконечных классах эквивалентности.

$\forall N > 0 \in \mathbb{R}$, определим функцию $F_N(x,y)$: $F_N(x,y) = F_N^o(x, \chi(sgn(x-N),-1) + \chi(sgn(x+N),1)$
$+ \chi(sgn(y),1) - 2)$.

$$F_N(x,y) = \begin{cases} x, & \text{если } y > 0, |x| \leq N \\ 0, & \text{иначе} \end{cases} \tag{13}$$

Докажем вспомогательное утверждение.

Утверждение 1. *$\forall f \in P^{(2)}, \exists g \in [CPL^{(2)} \cup F^N(x,y) \cup \Theta(x)]$ такая, что на всех бесконечных классах эквивалентности $f = g$.*

Доказательство.

У нас имеются все непрерывные кусочно-линейные функции, все *кусочно-постоянные* функции (порождаются $\Theta(x)$ и *линейными* функциями [1]) и функция $F^N(x,y)$. Пусть f произвольная функция из $P^{(2)}$ и $\{R_i\}$, $i = 1, ..., s$ все бесконечные классы эквивалентности функции f. Построим функцию g, которая бы совпадала на всех бесконечных классах эквивалентности. Так как мы работаем в двумерном случае, то любой бесконечный класс эквивалентности можно представить в виде луча или плоской бесконечной фигуры, которая имеет две (левая и правая) бесконечные границы (в случае луча левая и правая границы совпадают. Границы могут как принадлежать так и не принадлежать своей плоской фигуре). *Соседними классами* эквивалентности будет называть такую пару классов эквивалентности (R_i, R_j) чьи границы имеют общий луч и данный луч входит в одни из этих классов эквивалентности. Без ограничения общности можно считать что R_1 это класс с параллельными оси Y границами (так как добавление фиктивных разделяющих гиперплоскостей не меняют функцию). Пусть $\{R_i^{'}\}$, $i = 1, ..., s$ новый порядок имеющихся классов эквивалентности. Где $R_1^{'} = R_1$, а пары $(R_1^{'}, R_s^{'})$ и $(R_i^{'}, R_{i+1}^{'}), i = 1, .., s-1$ являются соседними классами эквивалентности. Рассмотрим $\{f_{R_i^{'}}\}$, $i = 1, ..., s$ линейные функции, которые реализуются в соответствующих классах эквивалентности. Будем поочередно соединять функции $\{f_{R_i^{'}}\}$ так чтобы получить непрерывную функцию $g_c \in CPL^{(2)}$. Начнем с пары (R_1, R_2). Из определения *согласованных* функций следует, что функции определенные на любых двух параллельных прямых, при достаточно большом значении аргумента, совпадают с точностью до константы. Отсюда следует что прямая, которая является

значением функции на границе и плоскость, которая является значением функции на соседнем, относительно границы, классе эквивалентности параллельны. Следовательно существует константа $c \in \mathbb{R}$, что $f_{R_1'}(t_{1,2}) = f_{R_2'}(t_{1,2}) + c$, где $t_{1,2}$ граница классов (R_1, R_2). Константу c можно добавить с помощью *кусочно-постоянных* функций. Определим функцию $f_{c_{1,2}} \in PC$.

$$f_{c_{1,2}} = \begin{cases} c, & x \in R_2' \\ 0, & \text{иначе} \end{cases} \tag{14}$$

Прибавим $f_{c_{1,2}}$ к функции f: $g_{c_{1,2}} = f + f_{c_{1,2}}$. Функция $g_{c_{1,2}}$ будет непрерывна на $R_1' \cup R_2'$. Аналогично, проделав все операции для пар (R_i', R_{i+1}'), $i = 2, ..., s-1$. Получим функцию $g_{c_{s-1,s}}$. Возможны два случая:

а) Функция $g_{c_{s-1,s}}$ непрерывна на границе $t_{s,1}$. Тогда с помощью уравнения (9) из первой части теоремы мы можем получить функцию $g_c \in CPL^{(2)}$, которая является непрерывной. Следовательно существует некая непрерывная функция $g_c \in CPL^{(2)}$ такая, что проделав все операции в обратном порядке и со знаком «-» мы получим функцию g, которая совпадала бы на всех бесконечных классах эквивалентности с функцией f. Что нам и нужно.

б) Функция $g_{c_{s-1,s}}$ разрывна на границе $t_{s,1}$. Нам известно что границы класса R_1' параллельны. Следовательно, функции которые реализуются на этих границах параллельны. Из курса геометрии известно, что любые две параллельные прямые можно соединить плоскостью. С помощью Функции $F_N(x, y)$ можно соединить две границы плоскостью. Т.е. переходим к случаю «а». **Утверждение доказано.**

Следовательно, мы можем получить функцию, которая совпадает на бесконечных классах эквивалентности, а далее изменить в ней функции, которые реализуются на конечных классах эквивалентности на произвольные функции. Отсюда следует, что мы может получить любую двухместную согласованную функцию. **Теорема доказана.**

3. 2-предполнота согласованных финитно-параллельных функций.

Определение 10. *Функция* $f : \mathbb{R}^n \Rightarrow \mathbb{R}$ *называется согласованной финитно-параллельной функцией, если* $f \in P$ *и* $\forall \overline{a}, \overline{b} \in \mathbb{R}^n, \exists N \in \mathbb{R}$ *та-*

кое, что $f(\overline{a}\cdot t+\overline{b})+f(\overline{a}\cdot(-t)+\overline{b})=const$, *для* $t>N$. *Множество всех согласованных финитно-параллельных функций обозначим через* PFP.

Определение 11. *Функция* $f:\mathbb{R}^n\Rightarrow\mathbb{R}$ *называется непрерывной финитно-параллельной функцией, если* $f\in CPL$ *и* $\forall\overline{a},\overline{b}\in\mathbb{R}^n,\exists N\in\mathbb{R}$ *такое, что* $f(\overline{a}\cdot t+\overline{b})+f(\overline{a}\cdot(-t)+\overline{b})=const$, *для* $t>N$. *Множество всех непрерывных финитно-параллельных функций обозначим через* CFP. *[4]*

Класс PFP *согласованных финитно-параллельных* функций замкнут по операциям суперпозиции, и верно следующее вложение $CFP\subset PFP$.

Следующая теорема говорит что класс *согласованных финитно-параллельных* функций 2-предполный в классе согласованных функций.

Пусть $M\subset P$ и $M\not\subset PFP$, тогда верна следующая теорема.

Теорема 2. $P^{(2)}\subset[M\cup PFP]$.

Доказательство.

Из предыдущей теоремы следует, что если мы получим все двухместные *кусочно-линейные непрерывные* функции и функцию $F_N(x,y),N\in\mathbb{R}$, то мы докажем 2-предполноту класса PFP. Функция $F_N(x,y),N\in\mathbb{R}$ имеется так, как она принадлежит классу *согласованных финитно-параллельных* функций. Рассмотрим функцию $f\notin PFP$. Данная функция не содержится в классе PFP *согласованных финитно-параллельных* функций, а следовательно не содержится в классе CFP *непрерывных финитно-параллельных* функций. Из работы [4] следует, что из функции f и множества L *линейных* функций можно получить все двухместные *кусочно-линейные непрерывные* функции. Т.е. мы доказали 2-предполноту класса PFP. **Теорема доказана.**

Теорема 3. *Класс* P *согласованных функций содержит только два 2-предполных класса: класс* PFP *согласованных финитно-параллельных функций и класс* CPL *непрерывных кусочно-линейных функций.*

Доказательство.

Пусть у нас имеются функции $f_1\notin PFP$ и $f_2\notin CPL$. Докажем что $P^{(2)}\subset[f_1\cup f_2\cup L]$. Из теорем 1 и 2 следует что $P^{(2)}\subset[f_1\cup f_2\cup L]$ если

$(\Theta(x) \cup CPL) \subset [f_1 \cup f_2 \cup L]$. Из функции $f_1 \notin PFP$, функции $f_2 \notin CPL$ и L линейных функций, можно получить $\Theta(x)$ (теорема 1). Все двухместные кусочно-линейные непрерывные функции можно получить из функции $f_1 \notin CFP \subset PFP$ и L линейных функций (теорема 2). **Теорема доказана.**

4. Заключение.

В данной статье мы рассмотрели полноту согласованных функций и только в двумерном случай. Дальнейшей задачей станет обобщения доказательства на n-мерный случай. А также расширение решетки замкнутых классов кусочно-линейных функций.

Автор выражает искреннюю признательность А. А. Часовских за постановку задачи, обсуждение результатов, советы и замечания.

Список литературы

[1] В. С. Половников, *Об оптимизации структурной реализации нейронных сетей*, дисс. ... канд. физ.-матем. наук, Москва, 2007.

[2] В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин, *Введение в теорию автоматов*, Наука, Москва, 1985, 320 pp.

[3] А. Н. Кан, "Вопросы выразимости в классе нейронных функций", *Интеллектуальные системы. Теория и приложения*, **19**:1 (2015), 15–21

[4] А. Н. Кан, "Вопросы полноты в классе кусочно-линейных непрерывных функций", *Интеллектуальные системы. Теория и приложения*, **21**:4 (2017), 46–56

Questions of expressibility in the class of matched functions

Kan A. N.

In this paper we consider the 2-completeness in the class of matched functions P. This class was considered earlier in [3, 4]. It is precomplete in the class PL of piecewise-linear functions. There are two precomplete classes: the class of continuous fucnton, the class of matched finite function.

Key words: Class of piecewise-linear functions, the class of piecewise-linear continuous functions, the class of matched functions, class of finite functions, the class of mathced finite function, 2-precompleteness, the Heaviside function.

Об элементарной выразимости в логике предикатов

Капустин Ю.С.

В математике часто новые понятия вводятся с помощью некоторых кванторных определений. При наличии достаточно большого запаса таких понятий они могут позволить переформулировать новые кванторные определения бескванторным образом. Это делает заслуживающей рассмотрения задачу отыскания базисных понятий в заданной предметной области, которые делают избыточным дальнейшее кванторное определение. Интересной также является задача создания компьютерных программ, автоматически вводящих такие базисы.

В данной работе рассматриваются 3 простых случая сведения кванторной выразимости к бескванторной. Исследуются предикаты и функции, определенные через $\in$ и заданные на множестве $Z \cup 2^Z$, где Z — множество целых чисел. Кроме того, рассматриваются предикаты, выразимые через тот же предикат на множестве точек плоскости и прямых, лежащих в ней. Также рассмотрены предикаты, выразимые на множестве натуральных чисел с отношением делимости на нем. Во всех случаях удалось найти базисы бескванторной выразимости.

Ключевые слова: кванторная выразимость, логика предикатов.

1. Общие определения, используемые в работе

Пусть M — некоторое множество, содержащее $\varnothing$. Интерпретацией сигнатуры S над M будем называть отображение $\Sigma : S \to F$, сопоставляющее элементам множества символов S предикаты и операции, определенные на M. Множество M с заданной на нём системой операций и предикатов будем называть универсумом. Формулы и термы в интерпретации Σ определяются следующим образом:

1) x_i, где x_i – переменная из фиксированного счетного списка – терм.

2) Если $\Sigma(s) = f$ – n—местная операция на M, $t_1, \ldots, t_n$ – термы, то слово $s(t_1, \ldots, t_n)$ – терм.

3) Если $\Sigma(s) = p$ – n—местный предикат, определенный на M, $t_1, \ldots, t_n$– термы, то слово $s(t_1, \ldots, t_n)$ – терм.

4) Если $P_1, \ldots P_k$ — формула, то слова $(P_1 \bigvee \cdots \bigvee P_k), (P_1 \& \ldots \& P_k)$, $\neg P_1, P_1 \to P_2$ – формулы.

5) Если P – формула, $x_1, \ldots, x_n$ — символы переменных, то слова $\forall x_1, \ldots, x_n(P), \exists x_1, \ldots, x_n(P)$ – формулы.

6) Если P – формула, x – переменная, S содержит $\in$, то $set_x(P)$ — терм.

Каждая формула определяет естественным образом некоторый предикат, заданный на наборах элементов множества M. Каждый терм определяет естественным образом некоторую операцию, заданную на наборах элементов M, и принимающий значения в M. $set_x(P)$, где P – формула от свободной переменной x и свободных переменных $x_1, \ldots, x_n$ $set_x(P)$ интерпретируется как $\{y \in M : P(y) = \text{И}\}$ — операция от переменных $x_1, \ldots, x_n$, значение которой равно множеству всех x, на которых верен предикат, задаваемый формулой P. Если это множество при некоторых значениях свободных переменных, входящих в формулу P, не принадлежит M, то на этом значении переменных значение $set_x(P)$ равно $\varnothing$.

Если предикат или операция f определяется какой-либо формулой или термом в сигнатуре $\Sigma : S \to F$, то говорим, что f логически выразимо над F (через F). Если f определяется формулой или термом в Σ, не содержащим кванторов и описателей set, то говорим, что f элементарно выразимо над F.

2. Элементарная выразимость в универсуме U_1

Определим универсум U_1:

Пусть U_0 — произвольное счетное множество элементов, не являющихся множествами, $U_1 = 2^{U_0} \bigcup U_0$, и отношение $\in$ определяется на U_1 следующим образом:

— Если $x_1 \in U_1 \backslash U_0$ или $x_2 \in U_0$, то $x_1 \in x_2 = \text{Л}$

— Иначе значение $x_1 \in x_2$ определено естественным образом.

В данном простейшем случае оказалось возможным найти такой набор предикатов и операций, что все предикаты и операции, выразимые через $\in$ в U_1, элементарно выражаются через него. Верна теорема:

Теорема 1. *Все предикаты и операции, логически выразимые в U_1 через $\in$ – это те и только те, которые элементарно выражаются над Q=$\{a = \varnothing, \varnothing, U_0 \backslash a, a \bigcup b, \{a\}, Card_n(a)\}$, где первые пять предикатов и операций определены естественным образом:*

$U_0 \backslash a = set_x(\neg(x \in a)\&(x \in U_0))$

$a \bigcup b = set_x((x \in a)\&(x \in b))$ — *то есть, если один из операндов не является множеством, то с точки зрения значений операции он считается пустым множеством.*

$\{x\} = \varnothing$, *если* $\neg(x \in U_0)$, *иначе определяется стандартным образом. То есть* $\{z\} = set_x(x \in U_0\&(x = z))(= set_x(x \in U_0\&(\forall y(z \in y) \to (x \in y))))$

$Card_n(x) = U_0$ - *счетный набор операций с параметром n, проверяющих, является ли множество x n-элементным:*

$Card_n(x) = U_0$, *если n—элементно,* $\varnothing$ *иначе.*

Доказательство:

Доказательство теоремы можно разбить на несколько шагов:

1) Докажем, что $\in$ элементарно выразимо над данным набором.

2) Докажем, что все описанные предикаты и операции выразимы.

3) Докажем, что множество предикатов и операций, элементарно выразимых над данным набором, замкнуто относительно однократного применения квантора общности.

4) Докажем, что множество предикатов и операций, элементарно выразимых над данным набором, замкнуто относительно однократного применения описателя set_x.

Тогда из 3) и 4) будет следовать, что множество предикатов и операций, элементарно выразимых над Q, замкнуто относительно применения set_x и кванторов. Кроме того, по определению оно замкнуто относительно элементарной выразимости. Значит, оно замкнуто относительно выразимости. Так как оно согласно 1) включает $\in$, все предикаты и операции, выразимые над $\in$, будут содержаться в этом множестве. Из 2) будет следовать обратное включение, и теорема будет доказана.

В доказательстве будут использоваться предикаты $Crd_n(x)$ (которые не следует путать с операциями $Card_n(x)$), определяемые следующим образом:

$Crd_n(x)$ =И, если x n-элементно.

Иначе $Crd_n(x)$ =Л.

Эти предикаты элементарно выразимы над Q:

$Crd_n(x) \equiv (Card_n(x) = \varnothing)$

Также отметим, что операция $a \bigcap b$ элементарно выразима над Q:

$a \bigcap b = U_0 \backslash ((U_0 \backslash a) \bigcup (U_0 \backslash b))$

Лемма 1. $\in$ *элементарно выразимо над данным набором.*

Действительно:

$a \in b \equiv (a \in U_0)\&(\neg(b \in U_0))\&Crd_1(b \bigcap \{a\})$. При этом:

$(a \in U_0) \equiv (Crd_1(\{a\})) \equiv (\neg((Card_1(\{a\})) = \varnothing)$

(так как для элементов не из U_0 $\{x\} = \varnothing$ по определению)

$Crd_1(b \bigcap \{a\}) \equiv Crd_1(U_0 \backslash ((U_0 \backslash b) \bigcup (U_0 \backslash \{a\}))) \equiv$

$\neg((Card_1(U_0 \backslash ((U_0 \backslash b) \bigcup (U_0 \backslash \{a\})))) = \varnothing)$

Следовательно, отношение $a \in b$ - выразимо.

Так как $a \in b \equiv (a \in U_0)\&(\neg(b \in U_0))\&Crd_1(b \bigcap \{a\})$, подставляя выражения для конъюнктов, получим бесквантерную формулу, задающую $\in$, что доказывает лемму.

Лемма 2. *Все описанные предикаты и операции выразимы через* $\in$.

Действительно, $U_0 = set_x(\exists y(x \in y))$

Пусть f_1 и f_2– выразимы. Тогда описанные операции можно выразить так:

$U_0 \backslash f_1 \equiv set_x(\neg(x \in f_1)\&x \in U_0)$

$f_1 \bigcup f_2 \equiv set_x(x \in f_1\&x \in f_2\&x \in U_0)$

$Card_m(f) \equiv set_x(Crd_m(F)\&x \in U_0)$, где x не является свободной переменной терма f (выразимость предиката $Crd_m(F)$ покажем далее)

$(f = \varnothing) \equiv (\neg(\exists x(f \in x)))\&(\neg(\exists x(x \in f)))$ (f не из U_0 и f не содержит элементов)

$\varnothing = set_x(x \in x)$

$\{z\} = set_x(x \in U_0\&(\forall y(z \in y) \to (x \in y)))$

Покажем выразимость всех предикатов $Crd_n(x)$

Докажем ее индукцией по n:

$Crd_0(x) \equiv \forall y(\neg y \in x)$

$Crd_1(x) \equiv \exists y(y \in x\&\forall z((z \in x) \to \forall u((z \in u) \to (y \in u)))$

(в x есть элемент y такой,что любой элемент x ему равен)

$Crd_{n+1}(x) \equiv \exists y, z(\forall a(((a \in y) \to ((a \in x)\&\neg(a \in z)))\&$

$((a \in z) \to (a \in x)))\&(Crd_n(y))\&Crd_1(z))\&$

$\forall a((a \in x) \to ((a \in y) \bigvee (a \in z))$

(у x есть два непересекающихся подмножества – n—элементное y и 1—элементное z – такие, что их объединение включает x)

Следовательно, все данные предикаты и операции выразимы над $\{\in\}$, а значит, и любое отношение или операция, выразимое бесквантерной формулой или термом над этими предикатами и операциями, выразима над $\{\in\}$. Лемма доказана.

Покажем, что система предикатов и операций, элементарно выразимых через данное множество, замкнута относительно применения квантора, то есть ей принадлежат все предикаты, выразимые через нее однократным применением квантора.

Докажем утверждение для предикатов:

Лемма 3. *Система Q замкнута относительно кванторной выразимости формулой с одним квантором.*

Без ограничения общности можно считать, что используется квантор всеобщности. Необходимо доказать, что $q(x_1, \ldots, x_n)$, выражающийся как $\forall x(p(x, x_1, \ldots, x_n))$, где $p(x, x_1, \ldots, x_n)$ – элементарно выразимый через Q предикат, элементарно выражается через Q.

Заметим, что любое вхождение условной операции $Card_n(f)$ можно исключить из p, добавив предикаты $Crd_n(f)$: $p(x, x_1, \ldots, x_n) \equiv p_1(x, x_1, \ldots, x_n)\&(Crd_n(f)) \bigvee p_2(x, x_1, \ldots, x_n)\&\neg(Crd_n(f))$, где p_1 - формула p, в которой все вхождения $Card_n(f)$ заменены на U_0, а p_2 - формула p, в которой все вхождения $Card_n(f)$ заменены на $\varnothing$. Исключим все такие вхождения в порядке вложенности, начиная с самых вложенных. Устранив по индукции все вложения условных операций, получим формулу $\forall x(p'(x, x_1, \ldots, x_n))$, равносильную исходной, где формула p' не содержит условных операций $Card_n$ (который мог быть вложенным), но содержит предикаты Crd_n (которые не могут быть вложены друг в друга, так как в них вложены только операции).

Пример Пусть $p(x, x_1, \ldots, x_n)$ имеет вид $Card_3(x_1 \bigcup x \bigcup U_0 \backslash (Card_2(x_2))) = \varnothing$. Тогда результаты последовательно примененных преобразований будут иметь вид:

$Card_3(x_1 \bigcup x \bigcup (U_0 \backslash (Card_2(x_2)))) = \varnothing$

$\equiv Card_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) = \varnothing \& Crd_2(x_2) \bigvee Card_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing)) = \varnothing \& \neg Crd_2(x_2)$

$\equiv U_0 = \varnothing \& Crd_2(x_2) \& Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) \bigvee$

$\varnothing = \varnothing \& Crd_2(x_2) \& \neg Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash U_0)) \bigvee$

$U_0 = \varnothing \& \neg Crd_2(x_2) \& Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing)) \bigvee$

$\varnothing = \varnothing \& \neg Crd_2(x_2) \& \neg Crd_3(x_1 \bigcup x \bigcup (U_0 \backslash \varnothing))$

Так как любой элемент U_1 принадлежит либо U_0, либо $U_1 \backslash U_0$, полученная формула $\forall x(p'(x, x_1, \ldots, x_n))$ эквивалентна формуле

$\forall x((x \in U_0) \to p'(x, x_1, \ldots, x_n)) \& \forall x(\neg(x \in U_0) \to p'(x, x_1, \ldots, x_n))$.

Так как любой элемент из U_0 при применении операций $U_0 \backslash$ и $\bigcup$, а также при применении предиката $Crd_n(x)$ ведет себя как $\varnothing$, то в консеквенте в первом конъюнкте вхождение x в эти операции в этой формуле

можно заменить на $\varnothing$ (кроме случая, когда x не вложен ни в какую операцию, и p имеет вид $x = \varnothing$ или $Crd_n(x)$, в случае чего весь квантор равен Л или И, если $n = 0$), и останутся только вхождения в виде $\{x\}$. Формулу $\forall x((x \in U_0) \to p'(\{x\}, x_1, \ldots, x_n))$ можно заменить эквивалентной:

$\forall y((Crd_1(y)) \to p'(y, x_1, \ldots, x_n))$. (произведена замена переменных: $y = \{x\}$, биективно отображающая U_0 на множество одноэлементных множеств)

Что эквивалентно следующей формуле:

$\forall x((\neg(x \in U_0)) \to ((Crd_1(x)) \to p'(x, x_1, \ldots, x_n)))$.

Под вторым квантором, в подформуле $\forall x(\neg(x \in U_0) \to P_2(x, x_1, \ldots, x_n))$, все вхождения $\{x\}$ можно заменить на $\varnothing$, так как $\{x\} = \varnothing$ для любого x из $U_1 \backslash U_0$

Так как образ всех операций из множества Q включается в $U_1 \backslash U_0$, а для любого элемента оттуда $\{x\} = \varnothing$, все подформулы вида $\{g(x, x_1, \ldots, x_n)\}$ можно заменить на $\varnothing$, кроме подформул вида $\{x_i\}$

Пример Пусть формула p' имеет вид

$Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash x) \bigvee Crd_2(x_2 \backslash x))$.

Применим к формуле $\forall x(p'(x, x_1, \ldots, x_n))$ указанные преобразования:

$\forall x Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\}))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash x \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2 \backslash \{x\})))\&$

$\&\forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Card_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\})))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash \varnothing \backslash (x_2 \backslash \varnothing) \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2(x_2 \backslash \{x\})))\&$

$\&\forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Crd_3(x_2 \backslash \varnothing) \bigvee Card_2(x_2 \backslash \varnothing)))$;

$\forall x(x \in U_0 \to Crd_2(x_1 \backslash x_2 \& (Crd_3(x_2 \backslash \{x\}) \bigvee Crd_2 \backslash \{x\})))\&$

$\&\forall x(\neg x \in U_0 \to Crd_2(x_1 \backslash x) \backslash (x_2 \backslash x) \& (Crd_3(x_2) \bigvee Crd_2(x_2)))$.

Таким образом, достаточно показать элементарную выразимость предикатов, задаваемых формулами:

$\forall x(\neg(x \in U_0) \to q(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}))$, где q элементарно выражается через $U_0 \backslash a, a \bigcup b, \varnothing$ и $Crd_n(a)$.

Рассмотрим (для произвольных $x_1, \ldots, x_n$) алгебру множеств, порожденную множествами $U_0, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}$. Все элементы этой алгебры множеств выразимы как дизъюнктное объединение множеств вида $U_0 \bigcap(\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$, где $A \sqcup B = \{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$ (через $A \sqcup B$ обозначено дизъюнктное объединение множеств A и B, то есть в каждом выражении $U_0 \bigcap(\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$ встречаются все элементы $\{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$ по одному разу.)

Действительно, два различных множества такого вида не пересекаются ни при каких значениях $x_1, \ldots, x_n$, так как если $a \in A$, $\neg a \in A'$, то множество $v_{AB} = U_0 \bigcap(\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$ включается в a, а множество

$v_{A'B'} = U_0 \bigcap (\bigcap_{a \in A'} a) \backslash (\bigcup_{a \in B'} a)$ не пересекается с a, а следовательно, и с v_{AB}.

Покажем, что любой элемент алгебры множеств выразим в виде объединения множеств заданного вида (вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a)$). Действительно, применим к терму $F(x_1 \dots x_n)$ над $U_0 \backslash$ и $\bigcup$ преобразования, заданные следующими эквивалентностями:

$U_0 \backslash (a \bigcup b) \equiv (U_0 \backslash a) \bigcap (U_0 \backslash b)$

$U_0 \backslash (a \bigcap b) \equiv (U_0 \backslash a) \bigcup (U_0 \backslash b)$

$U_0 \backslash (U_0 \backslash b) \equiv b$

$(b \bigcup a) \bigcap c \equiv (b \bigcap c) \bigcup (a \bigcap c)$, получим формулу с внешней операцией $\bigcup$, затем$\bigcap$, и внутренней операцией $U_0 \backslash$.

Проведя обратное преобразование $(U_0 \backslash a) \bigcup (U_0 \backslash b) \equiv U_0 \backslash (a \bigcap b)$, приведем выражение к виду:

$\bigcup_k (U_0 \backslash (a_{ki_1} \bigcup \dots \bigcup a_{ki_n}))$, что выражается как объединение множеств заданного вида (вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash (\bigcup_{a \in B} a)$).

Пользуясь данным утверждением докажем, что формула вида

$(1) \forall x (\neg (x \in U_0) \to F(Crd_{m_1}(f_1(x, x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\})), \dots,$

$Crd_{m_k}(f_k(x, x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\})))$,

где f_i – операции, выразимые через $U_0 \backslash$ и $\bigcup$, истинна или ложна только в заисимости от числа элементов в множествах вида $U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a$, причем найдется M такое, что если среди чисел элементов множеств $v_{AB} = U_0 \bigcap (\bigcap_{a \in A} a) \backslash \bigcup_{a \in B} a$ и множеств $v_{A'B'} = U_0 \bigcap \bigcap (\bigcap_{a \in A'} a) \backslash \bigcup_{a \in B} a$ для любых A, B, где:

— $A \sqcup B = \{x_1, \dots, x_n, \{x_1\}, \dots, \{x_n\}\}$,

$A' \sqcup B' = \{x'_1, \dots, x'_n, \{x'_1\}, \dots, \{x'_n\}\}$,

— $x_1, \dots, x_n, x'_1, \dots, x'_n$ — произвольные элементы U_1

— $x_j \in A \equiv x'_j \in \backslash A'$, $\{x_j\} \in A \equiv \{x'_j\} \in A'$,

различаются только те, которые больше M, то значения формулы совпадают на наборах x_j и x'_j.

Возьмем $M = 2max_k m_k + 3$. Тогда по любому множеству x из $U_1 \backslash U_0$, для которого консеквент в формуле(1) ложен (зафиксируем), можно построить множество x', содержащее:

— по столько элементов из каждого из множеств $v_{A'B'}$, сколько элементов x содержится в соответствующем множестве v_{AB}, для v_{AB}, пересечение которых с x содержит не более $max_k m_k$ элементов;

— из множеств $v_{A'B'}$, для которых это число больше $max_k m_k$ – по столько элементов, чтобы число элементов в дополнении x' до этих множеств было таким же, как в дополнении до соответствующего множества v_{AB};

— если же и пересечение с v_{AB}, и дополнение x до v_{AB}содержат более $max_k m_k$ элементов, то из соответствующего $v_{A'B'}$ в x' добавляем по $max_k m_k + 1$ элементов.

(Так как различные множества вида $v_{A'B'}$ не пересекаются, мы всегда можем взять множество, содержащее по данному числу элементов из каждого такого множества, если это число не превосходит мощности множества, что в данном случае выполнено).

Так как $f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$ выражается как дизъюнктивное объединение множеств вида v_{AB}, то значение предиката $Crd_{m_i}(f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$ – булева функция от значений предикатов $Crd_n(v_{AB})$, где v_{AB} выразимо через $U_0\backslash$ и $\bigcup$, а n принимает все значения от 0 до m_i (так как зная значения всех этих предикатов, мы или сможем назвать число элементов в $f_i(x, x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\})$, или сказать, что это число больше m_i, если одна из компонент вида v_{AB} содержит более m_i элементов).

Следовательно, по x такому, что неверен консеквент формулы (1), мы построим x' такое, что оно становится неверным при замене на x' и x_j на x'_j при условии, что числа элементов множеств v_{AB}и $v_{A'B'}$ для каждого различаются только для пар тех множеств, мощность каждого из которых больше $2max_k m_k + 3$.

Отсюда следует, что формула (1) эквивалентна некоторой булевой функции от предикатов $(Crd_n(v_{AB}))$, где $v_{AB} = U_0 \bigcap (\bigcap_{a\in A} a)\backslash(\bigcup_{a\in B} a)$, $A \sqcup B = \{x_1, \ldots, x_n, \{x_1\}, \ldots, \{x_n\}\}$, $n < M$. Следовательно, предикат, ей задаваемый, элементарно выражается через них, а значит, (учитывая, что $a \bigcap b \equiv U_0\backslash(U_0\backslash a \bigcup \backslash U_0\backslash b)$ и $Crd_n(a) \equiv \neg(Card_n(a)) = \varnothing$), и через Q, так как $a \bigcap b$ и $Crd_n(a)$ элементарно выражается через Q. Лемма 3 доказана.

Пример Пусть необходимо элементарно выразить предикат
$\forall x(\neg(x \in U_0) \to (\neg Crd_2(x \bigcup (U_0\backslash x_1) \bigcup \{x_2\}))))$.

Для этого рассмотрим все возможные значения мощностей множеств $U_0\backslash x_1\backslash\{x_2\}, U_0\backslash x_1 \bigcap \{x_2\}, U_0\backslash\{x_2\} \bigcap x_1, \{x_2\} \bigcap x_1$, не различая значения больше 6. Например, для U_0 - множества целых чисел, $x_1 = U_0\{1, 2\}, x_2 = 1$, предикат не выполнен - например, при $x = 2$ подкванторное выражение ложно. Следовательно, для любых x_1, x_2, для которых мощность $U_0\backslash x_1\backslash\{x_2\}$ равна 1, мощность $U_0\backslash x_1 \bigcap \{x_2\}$ равна 1, мощность $U_0\backslash\{x_2\} \bigcap x_1$ больше 6 (выразимый предикат - мощность не равна 0,1,2,3,4, 5, 6), мощность $\{x_2\} \bigcap x_1$ равна 0, можно выбрать x состоящий из одного элемента - элемента множества $U_0\backslash x_1\backslash\{x_2\}$, следовательно, все такие x_1, x_2 не удовлетворяют предикату. Рассмотрев все возможные варианты возможных мощностей множеств

$U_0\backslash x_1\backslash\{x_2\}, U_0\backslash x_1 \bigcap \{x_2\}, U_0\backslash\{x_2\} \bigcap x_1, \{x_2\} \bigcap x_1$, не различая значения больше 6, элементарно выразим $\forall x(\neg(x \in U_0) \to (\neg Crd_2(x \bigcup (U_0\backslash x_1) \bigcup \{x_2\})))$ через предикаты, выражающие мощности этих множеств, а значит, и через Q.

Докажем утверждение для операций.

Лемма 4. *Система Q замкнута относительно выразимости термом без кванторов с одним описателем set_x.*

Нужно доказать, что через данный набор выражаются все операции вида $set_x p(x, x_1, \ldots, x_n)$, где p элементарно выражается через Q.

Сначала заметим, что операция, задаваемая этой формулой, выразима через Q с использованием описателя вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$. Действительно, если существует x не из U_0, для которого выполнено $p(x, x_1, \ldots, x_n)$, то значение операции $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$ равно $\varnothing$, иначе равно значению операции $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$. По доказанному ранее, предикат, выражающийся формулой $\exists x(\neg(x \in U_0) \& p(x, x_1, \ldots, x_n))$ элементарно выражается через предикаты вида $Crd_n(f(x_1, \ldots, x_n))$ только с использованием булевых функций $\bigvee$ и $\neg$, так как они образуют базис булевых функций. Заменяя в выражающей формуле подформулы вида $Crd_n(f(x_1, \ldots, x_n))$ на $Card_n(f(x_1, \ldots, x_n))$, $\neg$ на $U_0\backslash$, и $\bigvee$ на $\bigcup$, получим выражение g, равное $\varnothing$ на значениях $x, x_1, \ldots, x_n$, на которых $\exists x(\neg(x \in U_0) \& p(x, x_1, \ldots, x_n))$ ложно, и U_0, если эта формула истинна. Следовательно, $set_x p(x, x_1, \ldots, x_n) = set_x(x \in U_0 \& p(x, x_1, \ldots, x_n)) \bigcap g$, и истинность утверждения достаточно проверить для операций, выразимых термом вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$, где элементарно выразимо над Q.

Пример Рассмотрим терм $set_x(Card_2(\{x\} \bigcup x_1) = \varnothing)$. Так как $Card_2(\{x\} \bigcup x_1) = \varnothing$ аналогично началу доказательства предыдущей леммы можно привести к виду $Crd_2(\{x\} \bigcup x_1)$ - виду без описателей Card, а $\exists x(\neg(x \in U_0) \& Crd_2(\{x\} \bigcup x_1))$ равносильно бескванторной формуле $Card_2(x_1)$, терм $set_x(Crd_2(\{x\} \bigcup x_1) = \varnothing)$ равносилен терму

$set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap U_0\backslash(Card_2(x_1))$

Путем преобразований, задаваемых данными формулами (заменяя выражения из левой части формул на выражения из правой части формул):

$set_x(x \in U_0 \& f \& g) = set_x(x \in U_0 \& f) \bigcap set_x(x \in U_0 \& g)$,

$a \bigcap b = U_0\backslash((U_0\backslash a) \bigcup (U_0\backslash b))$

$set_x((x \in U_0) \& (f \bigvee g)) = set_x((x \in U_0) \& f) \bigcup set_x((x \in U_0) \& g)$

$set_x(x \in U_0 \& \neg f) = U_0\backslash set_x(x \in U_0 \& f)$

заменим терм вида $set_x(x \in U_0 \& p(x, x_1, \ldots, x_n))$ на эквивалентный ему терм вида $f(set_x(x \in U_0 \& Crd_{n_i}(f_i(x, x_1, \ldots, x_n))))$, где f - операция от i переменных, выразимая через $U_0 \backslash a$, $a \bigcup b$.

Осталось выразить $set_x(x \in U_0 \& Crd_{n_i}(f_i(x, x_1, \ldots, x_n)))$ через Q.

Если x входит в f_i, то во всех его вхождениях, кроме его вхождения в виде $\{x\}$, его можно заменить на $\varnothing$, так как все остальные операции из Q действуют на элементы U_0 так же, как на $\varnothing$.

Если после этого x не входит в полученный терм вида f, то значение этого терма равно значению терма $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$. Иначе его можно записать в равносильном виде:

$\bigcup_{\sigma \in B^{2n}}(Card_{n_i} f_i(x, x_1, \ldots, x_n))) \bigcap(\bigcap_{i=1}^{n}(x \in x_i)^{\sigma_i}) \bigcap(\bigcap_{i=1}^{n}(x = x_i)^{\sigma_i})$,

где B^{2n} – булев куб,

$(x \in y)^{\sigma_i} = (x \in y)?$ при $\sigma = 1$,$U_0 \backslash (x \in y)?$ иначе

(где $x \in y?$ определяется как $Card_1(U_0 \backslash (U_0 \backslash \{x\} \bigcup (U_0 \backslash y))$ — выразимая операция)

$(x = y)^{\sigma_i} = (x = y)?$ при $\sigma = 1$, $U_0 \backslash (x = y)?$ иначе

$(x = y? Card_1(U_0 \backslash (U_0 \backslash \{x\} \bigcup (U_0 \backslash \{y\})))$ — выразимая операция)

Пример $set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1))$ можно записать в виде

$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (x = x_1)? \bigcap (x \in x_1)?) \bigcup$

$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (x = x_1)? \bigcap (U_0 \backslash (x \in x_1)?))$

$\bigcup (set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$

$\bigcup (set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (U_0 \backslash (x \in x_1)?))$

Введем новое обозначение — пусть $[a \backslash \{x\}]$ означает $a \backslash \{x\}$, подразумевая, что $x \in a$ (аналогично тому, как дизъюнктное объединие означает объединение множеств, подразумевая, что они не пересекаются). Преобразуем каждое вхождение $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$ при соответствующих условиях (то есть при условиях на равенство и принадлежность множествам, обозначенным свободными переменными, заданных выражениями $(x \in x_i)^{\sigma_i}$ и $(x = x_i)^{\sigma_i}$, с которыми данное вхождение выражения $Card_{n_i}(f_i(x, x_1, \ldots, x_n))$ связано через $\bigcap$) и на принадлежность и равенство элементам $x_1, \ldots, x_n$ следующим образом:

$a \backslash \{x\}$ заменим на a там, где $\neg(x \in a)$; $a \backslash \{x\}$ заменим на $[a \backslash \{x\}]$ там, где $(x \in a)$;

$\{x\} \backslash a = \varnothing$ там, где $(x \in a)$; $\{x\} \backslash a = \{x\}$ там, где $\neg(x \in a)$;

$\{x\} \bigcup a = a$ там, где $(x \in a)$; $\{x\} \backslash a = a \sqcup \{x\}$ там, где $\neg(x \in a)$; (здесь $\sqcup$ обозначает дизъюнктивное объединение)

$b \backslash [a \backslash \{x\}] = b \backslash a \sqcup x$ или $b \backslash a$

$b \backslash (a \sqcup \{x\}) = b \backslash a \backslash x$ или $b \backslash a$

$b \bigcup (a \sqcup \{x\}) = b \bigcup a \sqcup x$ или $b \bigcup a$

$\{x\} \bigcup [a \backslash \{x\}] = a$
$\{x\} \bigcup (a \sqcup \{x\}) = a \sqcup x$
$\{x\} \backslash [a \backslash \{x\}] = \{x\}$
$\{x\} \backslash (a \sqcup \{x\}) = \varnothing$
$b \backslash \{x\} \bigcup (a \backslash \{x\}) = (a \bigcup b) \backslash \{x\}$
$(b \bigcup \{x\}) \backslash (a \bigcup \{x\}) = b \backslash a$ или $[(b \backslash a) \backslash \{x\}]$
$(b \bigcup \{x\}) \backslash (a \backslash \{x\}) = (b \backslash a) \bigcup \{x\}$
И т.д.

С помощью этих преобразований выражение $f(x, x_1, \ldots, x_n)$ можно привести к одному из видов: $g(x_1, \ldots, x_n)$, $[g(x_1, \ldots, x_n) \backslash \{x\}]$, или $g(x_1, \ldots, x_n) \sqcup \{x\}$.

Тогда:

$set_x(x \in U_0 \& g(x_1, \ldots, x_n) = m)$ можно заменить на тождественно равный терм $Card_m g(x_1, \ldots, x_n)$

$set_x(x \in U_0 \& [g(x_1, \ldots, x_n) \backslash \{x\}] = m)$ можно заменить на тождественно равный терм $Card_{m+1} g(x_1, \ldots, x_n)$

$set_x(x \in U_0 \& (g(x_1, \ldots, x_n) \sqcup \{x\}) = m)$ можно заменить на тождественно равный терм $Card_{m-1} g(x_1, \ldots, x_n)$, считая, что $Card_{-1}(g(x_1, \ldots, x_n))$ равно $\varnothing$.

Пример Терм

$(set_x(x \in U_0 \& Crd_2(\{x\} \bigcup x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$

преобразуется к виду

$(set_x(x \in U_0 \& Crd_2(x_1)) \bigcap (U_0 \backslash (x = x_1)?) \bigcap (x \in x_1)?)$,

так как в рамках данного терма $set_x(x \in U_0 \& Crd_2(x_1))$ можно рассматривать при условии $x \in x_1$ (и $\neg(x = x_1)$).

Лемма доказана.

Как уже было показано ранее, доказательство лемм доказывает теорему.

Выделим базис в системе предикатов и операций, элементарно выразимых над Q.

$\varnothing = \{U_0 \backslash \{x\}\}$ для любого x.

ПримерОстальные элементы системы Q образуют базис:

Нужно доказать, что никакой из этих предикатов и операций не выразим через другие.

$a = \varnothing$ – единственный предикат

$\{a\}$ – единственная операция, различающая элементы U_0

$a \bigcup b$ – единственная многоместная операция.

$Crd_n(x)$ – остальные операции, примененные к элементу x, вне зависимости от того, n—элементный он или счетный со счетным допол-

нением, сохраняют $\{U_0, U_0\backslash x, x, \varnothing\}$ и какое множество из этих является результатом этих операций не зависит от того, n—элементно x или счетно. То есть, если некоторая формула от одной переменной, элементарно выраженная через $Q\backslash Crd_n(x)$, примененная к произвольному n-элементному множеству, дает несчетное множество, то и при применении к счетному множеству со счетным дополнением она также должна давать счетное множество, следовательно, она не может выражать $Crd_n(x)$.

$U_0\backslash a$ – остальные операции склеивают счетные множества.

Следовательно, получен базис.

3. Элементарная выразимость в универсуме натуральных чисел с отношением делимости.

Теперь рассмотрим в качестве множества M множество всех натуральных чисел с предикатом “a|b”. Так как это множество не содержит $\varnothing$, мы не будем рассматривать формулы, содержащие описатель set_x, и будем рассматривать только предикаты, выразимые с использованием кванторов. Каждый элемент этого множества – это конечное произведение простых в каких-то степенях, то есть его можно рассматривать как набор простых с некоторыми индексами. Следовательно, некоторые операции над U_1 имеют аналоги здесь. Например, a$\bigcap$b соответствует операция , а $a\backslash b$ соответствует операция “произведение простых, входящих в a, но не в b, со степенями, с которыми они входили в a". Оказывается, для (M,|) верна теорема, в чем—то аналогичная теореме для U_1:

Теорема 2. *Любой предикат, выразимый в N с использованием кванторных формул (не содержащих описателя set_x) над $\{|\}$ элементарно выражается над следующим счетным набором R предикатов и операций:*

— $aУЧb$, где $aУЧb$ – это произведение простых, входящих в a, но не в b, со степенями, с которыми они входили в a (усеченное частное). Например: $100УЧ15 = 4, 8УЧ2 = 1$

— $НОД(a, b)$

— $aПЧ_nb$, где n—параметр, $aПЧ_nb$ = (произведение простых, входящих в разложение a в большей степени, чем b, как минимум на n.) Например: $8ПЧ_22 = 2, 100ПЧ_15 = 10$

— $ЧП_n(a)$, так обозначим предикат, истинный, если в разложении a ровно n простых, n – параметр (число простых).

Доказательство.

Доказательство можно разбить на те же три шага, что и в прошлом разделе:

— Выразимость отношения делимости через R;

— Выразимость R через отношение делимости;

— Замкнутость R относительно выразимости.

1) Отношение делимости выражается через данный набор. Действительно, $(a|b) \equiv (\text{ЧП}_0(a\text{ПЧ}_1 b))$.

2) Все предикаты, элементарно выразимые через данный набор, выражаются через $|$.

Для этого достаточно показать, что каждый из заданных предикатов и операций выразим формулой, где под выразимостью операции $u(x_1, \ldots, x_n)$ имеется в виду существование формулы $f(x, x_1, \ldots, x_n)$ со свободными переменными $x, x_1, \ldots, x_n$, которая при любых значениях $x_1, \ldots, x_n$ принимает значение И только при $x = u(x_1, \ldots, x_n)$. Покажем, что этого достаточно.

Действительно, в этом случае от любого вхождения в формулу $p(u)$ операции u, выразимой формулой $f(x, x_1, \ldots, x_n)$, можно избавиться с сохранением равносильности:

$p(u(x_1, \ldots, x_n)) \equiv (\exists x(f(x, x_1, \ldots, x_n)\&p(x)))$. Поэтому если все предикаты и операции из R выражаются формулой над $|$, то и все предикаты, элементарно выразимые над R, также будут выразимы формулой над $|$.

Покажем, что все предикаты и операции из R выразимы через отношение делимости:

НОД(a, b) выражается формулой $(x|a\&x|b\&(\forall y((y|a\&y|b) \to y|x)))$

aУЧb – формулой $(\text{НОД}(x, b) = 1\&(x|a)\&\forall y((\text{НОД}(y, b) = 1\&(y|a)) \to y|x)))$, где единица выражается формулой $(\forall y(x|y))$

Предикат “x—простое” – формулой $\forall y(y|x \to (y = x \bigvee y = 1))$

(Предикат $x = y$ выражает формула $\forall z((z|x \to z|y)\&(z|y \to z|x)))$

Предикат $\text{ЧП}_n(a)$ выразим формулой $\exists x_1, \ldots, x_n$ ($x_1, \ldots, x_n$— попарно не равные, простые, делители a и $\forall x_{n+1}(x_{n+1}$или равен одному из x_i, или не простой, или не делитель a)).

$a\text{ПЧ}b(n)$, где n—параметр, $a\text{ПЧ}b(n)$ = (произведение простых, входящих в разложение a в большей степени, чем b, как минимум на n.) выражается так:

$\exists x_1, \ldots, x_n$ ($x_1, \ldots, x_n$— попарно различные простые, каждый из них входит в разложение a в степени минимум на n большей, чем в b, и $\forall x_{n+1}(x_{n+1}$ или совпадает с одним из x_i, или не простое, или не входит в разложение a в степени минимум на n большей, чем в b),

где предикат “x – простое, входящее в a в большей степени, чем в b, как минимум на n” можно выразить таким образом:

$\exists x_0, x_1, \ldots, x_n$ (x—простое&$\forall y((y|x_0$&y—простое$)\to y = x)$&$\ldots$&

$\forall y((y|x_n$&y—простое$) \to y = x)$&$(x_0|x_1$&$\neg(x_0 = x_1))$&$\ldots$&

$(x_{n-1}|x_n$&$\neg(x_{n-1} = x_n))$&$\forall y((\forall z(z|y$&z—простое$\to z = x))$&

$y|b \to (y|x_0))$&$(x_n|a))$

(то есть существуют $n-1$ различных степеней простого числа x, образующие цепочку по делимости, причем первая степень – как минимум та степень, в которой x входит в b, а последняя делит a)

Следовательно, все предикаты и операции из набора R выразимы над $|$, а следовательно, и все операции, элементарно выразимые над R, выразимы над $|$.

3) Остается доказать, что система операций и предикатов, элементарно выразимых над R, замкнута относительно однократного применения квантора.

Докажем это утверждение таким образом. Рассмотрим систему R', состоящую из операций НОД, УЧ и предикатов $\text{ЧП}_m(a\text{ПЧ}_n b)$. Как было указано в пункте 1), отношение $|$ выражается через данный набор. Так как этот набор элементарно выражается через R, он логически выразим над $|$. Следовательно, если мы докажем полноту этого набора, то отсюда будет следовать вывод, что все предикаты, выразимые над $|$, это те и только те, которые выразимы над R'. Так как R' элементарно выразим над R, а R выразим над $|$, отсюда будет следовать утверждение теоремы для R.

Без ограничения общности будем считать, что формула, выразимость которой над R мы хотим доказать, имеет вид: $\exists x p(x, x_1, \ldots, x_n)$, где p – дизъюнкция элементарных формул или их отрицаний. Так как $\text{ЧП}_m(a\text{ПЧ}_n b)$ - единственные предикаты в R', каждая элементарная формула имеет вид $\text{ЧП}_m(a\text{ПЧ}_n b)$, где a – операция, элементарно выразимая над НОД и УЧ. Для удобства в дальнейшем будем обозначать УЧ как $\backslash$.

Рассмотрим систему всех чисел вида

$a_k = (\text{НОД}(x_{11} \ldots x_{1n})\backslash x_{21}\backslash \ldots \backslash x_{2n})$,

где $x_{11}, \ldots, x_{1n}, x_{21}, \ldots, x_{2n}$ – все переменные, входящие в формулу, включая x (если под НОДом нет переменных, считаем, что выражение равно $1 = x\backslash x$ – тоже элементарно выразимая операция). Если рассматривать каждое число только как множество простых, не учитывая степеней, то любая операция, выразимая над $\backslash$ и НОД, будет тождественно

равна дизъюнктному объединению данных множеств. Чтобы учесть и степени, поступим таким образом:

Заметим, что $x = \text{ДНОК}_k(x\backslash(x\backslash a_k))$, где ДНОК обозначает НОК попарно взаимно простых чисел, a_k - взаимно простые и каждый простой делитель x является простым делителем некоторого a_k, и заменим все вхождения переменных в терм такими выражениями.

Пример Если x - это x_1 или x_2, или выразимый через них с помощью НОК и УЧ терм, то $x = \text{ДНОК}(x\backslash(x\backslash(x_1\backslash x_2)), x\backslash(x\backslash(x_2\backslash x_1)), x\backslash(x\backslash(x_1, x_2)))$, так как любой простой делитель x является простым делителем $(x_1\backslash x_2)$, $(x_2\backslash x_1)$ или (x_1, x_2). Например, если $x = x_1 = 15, x_2 = 6$, $\text{ДНОК}(x\backslash(x\backslash(x_1\backslash x_2)), x\backslash(x\backslash(x_2\backslash x_1)), x\backslash(x\backslash(x_1, x_2))) = \text{ДНОК}(5, 1, 3) = 15 = x_1$

Преобразуем полученные термы, используя следующие преобразования:

$\text{ДНОК}_k(x_{1k}\backslash(x_{1k}\backslash(a_k)))\backslash\text{ДНОК}_k(x_{2k}\backslash(x_{2k}\backslash(a_k))) =$

$= \text{ДНОК}(x_{3k}\backslash(x_{3k}\backslash(a_k)))$, где: $x_{3k} = x_{1k}$, если терм x_{2k} не содержит a_k в своем дизъюнктном разложении по a_i

(так как по термам a_i можно разложить терм – формальное выражение – а не его значение при конкретных x, то содержание a_k в разложении терма можно определить, посмотрев на терм, и оно не зависит от значения переменных), иначе $x_{3k} = 1$.

$\text{НОД}(\text{ДНОК}_k(x_{1k}\backslash(x_{1k}\backslash a_k)), \text{ДНОК}_k(x_{2k}\backslash(x_{2k}\backslash a_k))) =$

$= \text{ДНОК}((x_{1k}\text{НОД}x_{2k})\backslash((x_{1k}\text{НОД}x_{2k})\backslash a_k))$.

(Все a_k взаимно простые, и все $(\text{ДНОК}_k(x\backslash(x\backslash a_k)))$ имеют общие делители только с a_k и взаимно просты с a_n, если n не равно k)

Получим, что любое выражение для a или b (где

$\forall x(\text{ЧП}_m(a\text{ПЧ}_n b) = p)$ - предикат, элементарную выразимость которого нам нужно доказать) можно записать в виде

$\text{ДНОК}_k(\text{НОД}_j(x_{ijk})\backslash(\text{НОД}_j(x_{ijk})\backslash a_k))$

(i=1 в выражении для a, i=2 в выражении для b). Тогда предикат $\text{ЧП}_m(a\text{ПЧ}_n b)$ равносилен предикату

$\text{ЧП}_m(\text{ДНОК}_k(\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash a_k))$

$\text{ПЧ}_n\text{ДНОК}_k(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash a_k)))$.

Так как каждое из чисел, входящих в ДНОК, содержит в разложение те и только те простые, которые содержатся в разложении a_k, причем все a_k взаимно простые, $\text{ЧП}_m(\text{ДНОК}_k(\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash a_k))$

$\text{ПЧ}_n\text{ДНОК}_k(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash a_k)))$ тождественно равен

$\text{ЧП}_m(\text{ДНОК}_k((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k)))$.

Число простых делителей ДНОК – это просто сумма чисел простых делителей операндов ДНОК. Рассмотрев все возможные разложения числа m на $2^{\text{число переменных}}$ слагаемых, получим, что подкванторную формулу можно записать, как формулу над элементарными формулами

$\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k))$.

Следовательно, нужно доказать, что над R' выразим предикат, задаваемый формулой: $\exists x(A_1\& \ldots \&A_n)$, где a_i – элементарная формула вида $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash$

$((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash a_k)) = m$ или её отрицание.

Покажем существование таких M, N, что истинность или ложность формулы $\exists x(A_1\& \ldots \&A_n)$ зависит только от значений предикатов вида $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\ \text{НОД}_j(x_{2jk}))\backslash((\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk}))\backslash b_k))$

(что равно $\text{ЧП}_m((\text{НОД}_j(x_{1jk})\backslash(\text{НОД}_j(x_{1jk})\backslash b_k))\text{ПЧ}_n$

$(\text{НОД}_j(x_{2jk})\backslash(\text{НОД}_j(x_{2jk})\backslash b_k)))$ - выразимо над R')

и $\text{ЧП}(b_k) = m$, где b_k определяются как a_k, но только над множеством свободных переменных, все $n < N$, все $m < M$, и формулы не содержат x. (Таких формул конечное число, и если зависимость есть, то она задается булевой функцией).

Действительно, пусть значения всех таких формул совпадают для наборов x_i и x'_i, и для набора x_i существует такой , что $(A_1\& \ldots \&A_n)$ =И. Докажем, что тогда существует и x'_i, такой, что $(A'_1\& \ldots \&A'_n)$ =И, где a'_i получены заменой первого набора на второй.

В качестве x' нужно взять такое число, чтобы число простых в разложении $\text{НОК}(x', b'_k)$ совпадало с числом простых в разложении $\text{НОК}(x, b_k)$, а число простых в разложении $b_k\backslash x$ с числом простых в разложении $\text{НОК}(x', b'_k)$, если эти числа не больше максимального m, содержащегося в формулах a_i. Получим $M >= 2m + 2$.

Посмотрим, от чего зависит вхождение простого в разложение $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$. Если x входит в левый НОД, то простое делит $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$ тогда и только тогда, когда оно делит значение аналогичного выражения без , и выражения $x\text{ПЧНОД}_j(x_{2jk})$ (x из правого НОДа, если он там есть, можно убрать с сохранением вхождения простых). Если только в правый – то тогда и только тогда, когда оно входит или в разложение выражения $\text{НОД}_j(x_{1jk})\text{ПЧ}_n(x)$ или выражения $\text{НОД}_j(x_{1jk})\text{ПЧ}_n\text{НОД}_j(x_{2jk})$, где из правого а изъято x.

Посмотрим, в какой степени может входить простое число в разложении x на множители. Степень, в которой p входит в разложение в $\text{НОД}_j(x_{1jk})$ и в $\text{НОД}_j(x_{2jk})$ — это одна из степеней, в которой p входит

в одно из x_i или в x. С точки зрения значения всех предикатов важно лишь, входит ли простое в x в степени, большей или меньшей, чем степень каждого x_i, а также взаимное расположение степеней, в которых в них входят p (это определяет, в чьей именно степени p входит в этот предикат), и разница между степенью вхождения p в x и каждый из x_i, но только в том случае, если она не больше n.

Следовательно, если взять x', который содержит столько же простых из каждой категории b'_k (если их не больше m) в степенях, на столько же больших или меньших каждого вхождения в x'_k (если эти разности степеней не больше n), на сколько это выполнено для . Получим, что достаточно взять $N = 2n + 2$, $M = (2^{\text{число свободных переменных}} * (\text{число свободных переменных}+1) * (2n + 2)) * (m + 1)$ (т.к. всего возможно максимум $2^{\text{число свободных переменных}}$ расстановки свободных переменных в порядке убывания степени вхождения заданного простого, и имеет значение, находится ли степень между заданными 2 числами, меньше ли она большего на заданное число, не большее n, или больше меньшего на заданное число, меньшее n, — всего не более $=((2^{\text{число свободных переменных}} * (\text{число свободных переменных}+1) * (2n+2))$ позиций – и важно, чтобы числа простых на каждой позиции совпадали, если хоть одно меньше m – максимум на каждую "позицию" придется "поместить" по $m + 1$ простому делителю из соответствующего b_k). Теорема доказана.

4. Элементарная выразимость в универсуме точек плоскости.

Два разобранных множества были во многом схожи. Их можно было рассматривать как набор "простых" элементов и набор "составных", которые могут быть "составлены" из любых простых. Возникает вопрос: что может происходить, если "составные" имеют определённую структуру. Например, рассмотрим в качестве универсума множество прямых и точек плоскости, и, как и в первом случае, множеством операций будет $\{\in\}$. Для того, чтобы можно было рассматривать операции, образованные при помощи описателя set_x, добавим к универсуму $\varnothing$ и множества, состоящие только из одной точки, для того, чтобы результатом операции могла быть точка. Обозначим полученный универсум W.

Какие операции можно выразить таким образом, используя только set_x, причем однократно (достаточно проверить это, так как тогда любой оператор set_x можно будет заменить на соответствующее выражение)? Эти формулы будут иметь вид:

$set_x(P(A_1, \ldots, A_n))$, где P – формула, задающая некоторую булеву функцию от предикатов $A_1, \ldots, A_n$. Заменим формулу P на КНФ булевой функции, задаваемой P:

$set_x((A_{11}\& \ldots \& A_{1m}) \bigvee \cdots \bigvee (A_{k1}\& \ldots \& A_{km}))$, где a_{ij} – атомарные формулы или их отрицания.

Рассмотрим множества точек x, для которых верны атомарные формулы или их отрицания (не учитывая, что кроме точек предикатам могут удовлетворять другие объекты):

$set_x(x \in a) = a$. a может быть пустым множеством, одноточечным множеством или прямой. Если a – точка, то значение предиката равно $\varnothing$.

$set_x(\neg(x \in a))$ =$\Pi \backslash a$, где Π – плоскость, в которой мы рассматриваем точки и прямые.

$set_x(\neg(a \in x))$ =Π, $set_x(a \in x) = \varnothing$

$set_x(a \in b) = (a \in b)?$

$set_x(\neg(a \in b)) = (\neg a \in b)?$

Теперь рассмотрим все возможные пересечения таких множеств, соответствующие описателю set_x, примененному к описателю класса .

1) Если пересечение содержит хоть один элемент $\varnothing$, то и все пересечение будет равно $\varnothing$.

2) Иначе, если оно содержит только тождественные операторы, то это пересечение – $A_1 \bigcap \cdots \bigcap A_n$.

3) Если оно содержит только условные операторы $(a \in b)?$ или $(\neg a \in b)?$, то это пересечение условных операторов.

4) Если оно содержит и условные операторы, и хоть один тождественный, но не содержит элементов вида $\Pi \backslash a$, то оно элементарно выражается через$\bigcap$ и операторы видов $(a \in b?)$ и $(\neg a \in b?d)$, где:

$(a \in b?c) = c$, если $a \in b$, $\varnothing$ иначе.

$(\neg a \in b?d)$= $\varnothing$, если a$\in$b, d иначе.

5—6) Если пересечение содержит элемент вида $\Pi \backslash a$, то:

5)Если есть хоть один тождественный оператор, то пересечение имеет вид $O \backslash A_1 \ldots \backslash A_n$, где O – оператор, выразимый над$\bigcap$, $(a \in b?)$ и $(\neg a \in b?d)$,

6)Иначе оставим его в виде пересечения.

Теперь рассмотрим объединения множеств шести полученных типов, соответствующие дизъюнкциям в формуле

$set_x((A_{11}\& \ldots \& A_{1m}) \bigvee \cdots \bigvee (A_{k1}\& \ldots \& A_{km}))$.

Это прямая в том случае, если одно из этих множеств – прямая, а другие – такие же прямые, или одно – прямая без точек, принадлежащих

другим множествам, причем все точки из остальных множеств принадлежат этой прямой. Точка – если одно из множеств — точка, остальные пустые или эта же точка. Иначе значение оператора, заданного описателем set_x будет равно $\varnothing$.

Прямой или прямой без точек может являться только значение операторов типов 5), 4) или 2). Иначе в случае 1) оно пустое, в случаях 3 и 6) – пустое, если хоть один входящий туда условный оператор принимает значение $\varnothing$, иначе является плоскостью без нескольких точек. Чтобы объединение было прямой или точкой, хотя бы один из операторов должен иметь вид 2), 4) или 5). Введём новую операцию – $diz(A_1, \dots, A_n)$, равную $\varnothing$ во всех случаях, кроме случая, когда среди множеств ровно одно непустое; в этом случае она равна этому множеству. Тогда $set_x(x \in b_1 \bigvee \dots \bigvee x \in B_n \bigvee x \in (\Pi \backslash A_1 \backslash \dots \backslash a_m \bigcap (b_1 \in c_1)? \bigcap \dots \bigcap (B_n \in c_p)) = set_x(\bigvee in = 1(x \in diz((b_1 \in c_1?B_i), \neg(b_1 \in c_1?B_i) \bigcap (b_2 \in c_2?B_i), \dots, \neg(b_1 \in c_1?B_i) \bigcap \dots \bigcap (b_{p-1} \in c_{p-1}?B_i) \bigcap (b_p \in c_p?B_i)))$.

Добавим условные предикаты (b—прямая)? = b, если b прямая, $\varnothing$ иначе. (a=b)? , (a—точка)?, (a—одноточечное множество)? – аналогично.

Заменим операции $(a \in b?)$ и $(\neg a \in b?)$ на операции $(a \subset b?)$, $(\neg a \subset b?)$ и $\{a\}$.

Используя пересечения этих операций и diz полученных пересечений, можно получить операцию, которая в случае, если один из этих элементов – прямая или прямая без точек, которыми являются результаты других операций, или прямая без точек, которые лежат в результате другой операции – такой же прямой, а остальные элементы – такая же прямая или пустые множества, или точки, лежащие на этой прямой, равна этой прямой; в случае, когда один из элементов – точка, а другой – такие же точки или пустые множества, равна $\varnothing$; в остальных случаях равна $\varnothing$.

Следовательно, доказано утверждение:

Утверждение. Любой терм, выразимый над $\in$ в универсуме W термом, содержащим одно вхождение set_x и не солержащим кванторов, элементарно выразим через следующие операции:

$a \bigcap b = set_x(\ \in a \& x \in b)$, $(a -$ прямая$)?$, $(a = b)?$, $(a -$ точка$)?$, $(a -$ одноточечное множество$)?$, $\{a\}$, $diz(a_1, \dots, a_n)$, $(a \subset b?)$, $(\neg a \subset b?)$.

Как видно, использование только описателя set_x приводит к появлению большого числа условных операторов, но почти не добавляет существенных операций в случае, когда универсум содержит не все множества данных элементов. Поэтому рассмотрим, какие предикаты выразимы формулами над универсумом W, не использующими set_x.

Сначала рассмотрим, какие аналоги операций из U_n выражаются в данном универсуме. Аналогом пересечения двух множеств здесь является точка пересечения двух прямых. Аналогом объединения множеств – прямая, проходящая через две данные точки. Аналогом числа элементов – предикаты а—прямая, а—одноточечное множество. Аналогом $\{a\}$ – также операция $\{a\}$. Аналогов разности здесь нет. Также можно ввести предикат принадлежности одноточечного множества прямой. Все эти предикаты выразимы над $\in$:

$(a \bigcap b)$ задается формулой $\exists x((x \in a)\&(x \in b))$

$(a \subset b)$ задается формулой $\exists x(x \in a \& x \in b \& a$—точка$\& b$—прямая$)$

$(a \bigcup b)$ задается формулой $\exists x((a \subset x)\&(b \subset x) \bigvee \neg\exists y((a \subset x)\&$
$(b \subset x))\&x = \varnothing)$

(а—прямая) задается формулой $\exists xyz(\in a \& x \in z \& y \in a \& \neg y \in z)$

(а—одноточечное множество) задается формулой $\exists x(x \in a \&$
$\neg(a$—прямая$))$

а—точка задается формулой ({а} – одноточечное множество).

$\{a\}$ задается формулой $\exists x(x$—одноточечное множество$\& a \in x)$.

С помощью этих предикатов элементарно выражается довольно большой класс отношений. Например, $a \setminus = b$ эквивалентно $a \bigcap b$—точка. Или три точки лежат на одной прямой – $a \in (\{b\} \bigcup \{c\})$ Однако не все отношения, элементарно выразимые через $\in$, элементарно выражаются через данный набор предикатов.

На самом деле верна теорема:

Теорема 3. *Все предикаты, выразимые в W через $\in$ – это те и только те, которые элементарно выразимы через следующие предикаты и операторы:*

1—7)($a \bigcap b$), ($a \bigcup b$), (а—прямая), (а—одноточечное множество), ($a \subset b$), {a}, (прямая, проходящая через точку одноточечного подмножества а параллельно прямой b),

8)(точки из одноточечных множеств $A_1, A_2, A_3, \ldots A_n$ лежат на одной прямой, $A_1, A_2, A_3, \ldots, A_n$ различны, и x_i такие, что $(A_1 - A_i) = x_i(A_1, A_2)$, m>2, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

9)(прямые $A_1, A_2, A_3, \ldots A_n$ параллельны, $A_1, A_2, A_3, \ldots, A_n$ различны, и x_i такие, что отношения направленных расстояний между прямыми $l(A_1 - A_i) = x_i l(A_1, A_2)$, m>2, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

10)(прямые $b_0, b_1, b_2, b_3, \dots b_n$ проходят через одну точку, $b_0, b_1, b_2, b_3 \dots, b_n$ различны, и если провести прямую, параллельную b_0, и обозначить за $A_1, A_2, A_3, \dots A_n$ точки её пересечения с $b_1, b_2, b_3, \dots b_n$, то x_i такие, что вектор $(A_1 - A_m) = x_i(A_1, A_2)$, m>2, лежат в полуалгебраическом множестве A, задаваемом алгебраическими неравенствами с рациональными коэффициентами).

Данная теорема представляет собой лишь перенос теоремы Тарского-Зайденберга[1] на множества точек плоскости. Далее представлена схема её доказательства. В ней не прописывается каждый раз,что все вырожденные случаи можно рассмотреть отдельно. Например, если мы рассматриваем точку пересечения двух прямых в предикате $p(a \bigcup b)$, мы можем задать ему любое значение в случае, если a и b параллельны, или a и b не прямые - (a—прямая)&(b—прямая)& $(a \bigcup b)$ — одноточечное множество & $p(a \bigcup b) \bigvee$ (a—прямая)&(b—прямая)& $\neg(a \bigcup b)$ — одноточечное множество & $p_2 \bigvee \neg$ (a—прямая)&$p_3 \bigvee \neg$ (b—прямая)&p_4

Доказательство.

1)$a \in b = \{a\} \subset b$. В дальнейшем, чтобы не оговаривать специально, не будем различать точку и одноточечное множество (предикат $\{a\}$ ставит в соответствие точке одноточечное множество, а остальные предикаты "работают" с одноточечными множествами), а также не будем проверять операции на корректность, то есть неравенство пустому множеству их результатов, так как случай равенства всегда можно рассматривать отдельно – $((P(U))\&(\neg(U = \varnothing))) \bigvee (U = \varnothing \& \dots)$. Специально вырожденные случаи описывать не будем.

2) Покажем, что все данные предикаты и операции выразимы формулой над $\in$. Выразимость первых шести была показана ранее. Седьмой выражается так: $\exists x$(x—прямая&a—одноточечное множество&b—прямая&$a \subset x \& x \setminus = b$).

Девятые тривиально выражаются с использованием восьмых: (прямые $A_1, A_2, A_3, \dots A_n$ параллельны) & $(A_1, A_2, A_3, \dots, A_n$ различны) &$\exists x(x -$ прямая&$\neg(x = A_1)\&(x \bigcap A_1, \dots, x \bigcap A_n$ удовлетворяют соответствующему восьмому предикату). Десятые выражаются через восьмые аналогично.

Покажем выразимость остальных предикатов. Для этого нам необходимо показать, как строя однозначно заданные прямые со свойствами, выразимыми формулами (т.е. добавляя кванторы $\exists x_1 \dots x_n$ (f$(x_1 \dots x_n)\& \dots)$)

— Умножить данный вектор на целый коэффициент. (то есть задать свойство: вектор, заданный данными двумя точками, равен n*вектор, заданный другими двумя данными точками).

— Сложить данные два коллениарных вектора

— Умножить вектор на отношение двух коллениарных векторов

— Определить сонаправленность данных двух векторов с общим началом.

Пункт II) (пункт 1 из него легко выводится). Пусть мы хотим сложить коллениарные векторы OA и XY. Построим на отрезке OA параллелограмм OABC, и обозначим за D точку пересечения прямой XY с прямой, проходящей через C параллельно XY. Отрезок XC будет требуемой суммой.

Пункт III) Отложим(как в пункте 2) все векторы от одной точки O. Пусть OB нужно умножить на отношение OC и OD. Рассмотрим прямую, не параллельную этим векторам, и проходящую через O. Пусть E, F – точки пересечения этой прямой с двумя параллельными прямыми, проходящими через OC и OD соответственно. Точка пересечения прямой OB и прямой, проходящей через F параллельно ED, и будет концом требуемого вектора.

Пункт IV) OB и OC сонаправленны, если существует D такое, что OB=c(OD) и OD=c(OC). Следовательно, все данные предикаты выразимы.

3) Докажем замкнутость данной системы предикатов.

По теореме Тарского-Зайденберга[1] любая формула над множеством вещественных чисел, кванторно выразимая через операции принадлежности полуалгебраическому множеству, элементарно выразима через эти операции.

Пусть некоторый предикат P задается формулой p. Без ограничения общности можно считать, что в формуле P содержатся условия на классы всех входящих в него переменных (точка/прямая), все прямые, проведенные через любую пару точек, взаимное положение всех точек и прямых и параллельность любой пары прямых. Тогда возможны случаи:

— Имеется только одна точка, пара точек и прямая, проходящая через них, три попарно пересекающиеся прямые, пара параллельных или пересекающихся прямых, на одной из которых, возможно, отмечена точка, три прямые, проходящие через одну точку, возможно, с одной отмеченной точкой. В этом случае данную совокупность прямых и точек можно перенести аффинным преобразованием в любую другую совокупность прямых и точек с таким же попарным расположением. Следовательно,

все выразимые предикаты выражаются через взаимное расположение прямых. Так как три точки, лежащие на одной прямой, не отмечены,

— Имеется хотя бы пара пересекающихся прямых и пара отмеченных на них точек (возможно, точек пересечения с другими прямыми). Рассмотрим все переменные, входящие в формулу – и свободные, и связанные. Можно ввести систему координат с двумя осями – двумя прямыми и единичными отрезками с концами в данной точке. В этом случае точками на этих прямых можно задать координаты каждой точки и каждой прямой (под координатами прямой подразумеваются координаты её пересечения с координатными осями или с одной осью, если она параллельна другой оси). Рассмотрим прямую, проходящую через концы единичных отрезков, и перенесём параллельно ей все отмеченные соответствующие координатам точки с одной из прямых на другую. Все соотношения, задаваемые данным наборов предикатов и отношений полуалгебраические относительно координат в любой аффинной системе координат. По теореме Тарского—Зайденберга любая проекция полуалгебраического множества полуалгебраическая, то есть любая кванторная формула над (+, *, =) имеет равносильную ей бескванторную формулу. Так как при условии, что на плоскости задана декартова система координат, каждая прямая однозначно задается координатами точек её пересечения с осями или фактом её параллельности одной из осей и координатой точки пересечения с другой из осей, а точка задается своими координатами, причем все операции из условия теоремы являются алгебраическими операциями над координатами. Следовательно, от кванторов можно избавиться, сохранив выразимость через данный набор предикатов.

— Имеется только набор параллельных прямых, возможно, на одной из них отмечена точка, или проведена прямая, их пересекающая. Тогда можно взять систему координат, содержащую одну из этих прямых (содержащую отмеченную точку, если есть) и прямую, их пересекающую. Тогда все данные параллельные прямые будут иметь только одну координату, поэтому все предикаты (по теореме Тарского – Зайденберга) можно выразить через алгебраические соотношения отношений только этих координат, то есть через предикаты 8—го типа и предикаты 1)—6).

— Имеется набор прямых, проходящих через одну точку. На одной из них выбираем начало координат, и берем её в качестве первой оси. Вторую координатную ось направляем параллельно одной из прямых. В качестве одного единичного отрезка берем отрезок от начала координат до точки пересечения прямых, в качестве второго – отрезок от начала координат до точки пересечения соответствующей оси до третьей

заданной прямой. В этом случае соотношения координат прямых полностью задаются вторыми координатами прямых, следовательно, отношения координат прямых в полученной системе координат выражаются через предикаты 9—го типа и предикаты 1)—6).

Итак, данная система предикатов и операций замкнута, ч.т.д.

5. Благодарности.

Выражаю благодарность проф. А.С.Подколзину за постановку задачи и помощь в работе.

Список литературы

[1] Н. К. Верещагин, А. Шень, *Языки и исчисления*, МЦНМО, М., 2012.

On the elementary expressibility in predicate logic

Kapustin I.S.

New mathematics concepts are often introduced with some quantifier definitions. If we have a sufficiently large stock of such notions, it can allow to reformulate the new quantifier definitions in a quantifier-free form. This makes the problem of finding basic concepts, which make further quantifiable definition redundant, worth considering. Creating computer programs that automatically introduce such bases is also worth considering.

In this paper we observe 3 simple cases of reducing the quantifier expressions to the quantifier-free ones. We investigate predicates and functions defined by $\in$ predicate on the set $Z \cup 2^Z$, where Z is the set of integers. We consider predicates expressed by $\in$ predicate on the set of points of the plane and the lines lying in it. Finally, predicates expressed on the set of natural numbers by the $|$ predicate on it are also considered. Bases were found in all 3 cases.

Keywords: predicate logic, quantifier definitions

Некорректность теории множеств Цермело-Френкеля относительно конструктивной семантики, основанной на гиперарифметических видах

Коновалов А. Ю.

Определяется семантика реализуемости для формул языка теории множеств, основанная на гиперарифметических видах. Исследуется вопрос о корректности аксиом теории множеств Цермело-Френкеля относительной этой семантики.

Ключевые слова: конструктивная семантика, реализуемость, аксиоматическая теория множеств, гиперарифметические виды.

1. В интуиционистской математике одним из аналогов понятия множества является *вид* как точно сформулированное условие, которому могут удовлетворять некоторые математические объекты (см. [1]), называемые в этом случае *членами* вида. При этом существенно, что условие, задающее вид, само должно пониматься интуиционистски. Это означает, что объект x является членом вида y ($x \in y$), если имеется обоснование того факта, что x удовлетворяет условию, задающему вид y. Следуя идее Клини, лежащей в основе *рекурсивной реализуемости* (см. [2, §82]), будем считать, что объект x может рассматриваться как член данного вида y только вместе с числом e, кодирующим обоснование утверждения $x \in y$, так что на самом деле речь должна идти об упорядоченной паре $\langle e, x\rangle$. Используя данный подход, в работе [3] мы определили конструктивную семантику языка теории множеств, основанную на гиперарифметических видах. В настоящей статье мы продолжим исследование этой семантики.

2. Фиксируем примитивно рекурсивную взаимно-однозначную функцию c, кодирующую пары натуральных чисел натуральными числами. Например, определим c как в [4, §5.3]:

$$\mathsf{c}(u, v) = \frac{1}{2}(u^2 + 2uv + v^2 + 3u + v).$$

Тогда одноместные обратные функции p_1 и p_2, где $\mathsf{p}_1(x)$ и $\mathsf{p}_2(x)$ суть первая и вторая компоненты пары с кодом x, т. е. $\mathsf{c}(\mathsf{p}_1(x), \mathsf{p}_2(x)) = x$, также примитивно рекурсивны. Для любого натурального $n > 0$ с помощью функции c индуктивно определяется функция c^n, взаимно-однозначно отображающая $\mathbb{N}^n$ на $\mathbb{N}$:

$$\mathsf{c}^1(x) = x; \quad \mathsf{c}^{n+1}(x_1, \ldots, x_{n+1}) = \mathsf{c}(\mathsf{c}^n(x_1, \ldots, x_n), x_{n+1}).$$

В выражениях вида $\mathsf{g}(t)$ мы иногда будем опускать скобки и писать просто $\mathsf{g}t$. Кодирование всех конечных кортежей (включая пустой) натуральных чисел τ^* определим как в [4, §5.6]. А именно,

$$\tau^*(\varnothing) \rightleftharpoons 0, \quad \tau^*(\langle x_1, \ldots, x_n\rangle) \rightleftharpoons \mathsf{c}(\mathsf{c}^n(x_1, \ldots, x_n), n-1) + 1.$$

Если f — всюду определенная одноместная функция натурального аргумента, то, согласно [4, с. 482], функция $\overline{f}$ определяется так:

$$\overline{f}(n) \rightleftharpoons \begin{cases} \tau^*(\langle f(0), \ldots, f(n-1)\rangle), & \text{если } n > 0 \\ 0, & \text{если } n = 0. \end{cases}$$

Рекурсивные отношения $T^*_{k,l}(z, y_1, \ldots, y_l, x_1, \ldots, x_k)$ определяются в [4, §16.1, с. 483]. Определим отношение $U(z, x_1, x_2)$ следующим образом:

$$U(z, x_1, x_2) \rightleftharpoons \forall f\, \exists w\, T^*_{1,2}(z, \overline{f}(w), x_1, x_2).$$

Отношения на множестве натуральных чисел, принадлежащие классу Π^1_1 аналитической иерархии [4, §16.1], назовем Π^1_1-предикатами. Согласно [4, §16.1, теорема V], отношение $U(z, x_1, x_2)$ является универсальным для класса всех 2-местных Π^1_1-предикатов. Натуральное число z назовем Π^1_1-индексом отношения $P(x_1, x_2)$, если имеет место $P(x_1, x_2) \iff U(z, x_1, x_2)$. Будем говорить, что отношение $P(x_1, \ldots, x_n)$ является гиперарифметическим, если $P(x_1, \ldots, x_n)$ и $\neg P(x_1, \ldots, x_n)$ суть Π^1_1-предикаты. Натуральное число z назовем Δ^1_1-индексом отношения $P(x_1, x_2)$, если $z = \mathsf{c}(z_1, z_2)$, где z_1 — Π^1_1-индекс отношения $\neg P(x_1, x_2)$, а z_2 — Π^1_1-индекс отношения $P(x_1, x_2)$. Пусть I — множество всех Δ^1_1-индексов всех 2-местных гиперарифметических отношений, а $D_z(x_1, x_2)$ — гиперарифметическое отношение, Δ^1_1-индекс которого есть z.

3. Посредством трансфинитной индукции для каждого ординала α определим множество Δ_α следующим образом:

$$\Delta_\alpha \rightleftharpoons \{z \in I \mid \neg\, \exists s\, \exists x\, D_z(s,x)\},\ \text{если } \alpha = 0;$$
$$\Delta_\alpha \rightleftharpoons \{z \in I \mid \forall s, x\, (D_z(s,x) \to x \in \Delta_\beta)\},\ \text{если } \alpha = \beta + 1;$$
$$\Delta_\alpha \rightleftharpoons \bigcup_{\beta<\alpha} \Delta_\beta,\ \text{если } \alpha \text{ — предельный ординал.}$$

Через Δ обозначим объединение всех множеств Δ_α, для которых ординал α конечен либо счетен. Справедливы следующие утверждения:

1) $\Delta \subseteq I$;

2) если $\alpha < \beta$, то $\Delta_\alpha \subseteq \Delta_\beta$;

3) если $a \in I$, то $a \in \Delta \iff \forall s, x\, (D_a(s,x) \Rightarrow x \in \Delta)$.

4. Формулы языка теории множеств строятся из предметных переменных, констант элементов множества Δ, двухместных предикатных символов $=$ и $\in$, логических констант $\bot, \top$, логических связок $\wedge, \vee, \to$, кванторов $\forall, \exists$ и скобок по обычным правилам. Формулы, которые не содержат свободных вхождений предметных переменных, будем называть замкнутыми. При записи формул будем использовать следующие сокращения:

- $\neg\Phi \rightleftharpoons \Phi \to \bot$;
- $\exists x{\in}t\ \Phi(x) \rightleftharpoons \exists x(x{\in}t \wedge \Phi(x))$;
- $\forall x{\in}t\ \Phi(x) \rightleftharpoons \forall x(x{\in}t \to \Phi(x))$;
- $\exists! x\ \Phi(x) \rightleftharpoons \exists x\, (\Phi(x) \wedge \forall y\, (\Phi(y) \to y = x))$;
- $\forall x_1, \ldots, x_n(\Phi \leftrightarrow \Psi) \rightleftharpoons \forall x_1, \ldots, x_n(\Phi \to \Psi) \wedge \forall x_1, \ldots, x_n(\Psi \to \Phi)$.

5. Для каждого натурального числа n фиксируем вычислимую нумерацию всех n-местных частично-рекурсивных функций: $\varphi_1^n, \varphi_2^n, \ldots$.

Согласно [3], для всякого натурального числа e и произвольной замкнутой формулы Φ языка теории множеств определим отношение «e реализует Φ» (обозначение: $e\ \mathbf{r}\ \Phi$) следующим индуктивным образом:

- $e\ \mathbf{r}\ (a = b) \rightleftharpoons a = b$;
- $e\ \mathbf{r}\ (a \in b) \rightleftharpoons D_b(e,a)$;
- $e\ \mathbf{r}\ (\Phi \wedge \Psi) \rightleftharpoons \mathsf{p}_1 e\ \mathbf{r}\ \Phi$ и $\mathsf{p}_2 e\ \mathbf{r}\ \Psi$;

- $e\ \mathbf{r}\ (\Phi \vee \Psi) \rightleftharpoons (\mathsf{p}_1 e = 0$ и $\mathsf{p}_2 e\ \mathbf{r}\ \Phi)$ или $(\mathsf{p}_1 e = 1$ и $\mathsf{p}_2 e\ \mathbf{r}\ \Psi)$;
- $e\ \mathbf{r}\ \exists x\, \Phi(x) \rightleftharpoons \mathsf{p}_1 e \in \Delta$ и $\mathsf{p}_2 e\ \mathbf{r}\ \Phi(\mathsf{p}_1 e)$;
- $e\ \mathbf{r}\ \forall x_1, \ldots, x_n\, (\Phi(x_1, \ldots, x_n) \to \Psi(x_1, \ldots, x_n)) \rightleftharpoons$ [для всех[1] натуральных чисел s и $a_1, \ldots, a_n \in \Delta$, если $s\ \mathbf{r}\ \Phi(a_1, \ldots, a_n)$, то определено $\varphi_e^{n+1}(a_1, \ldots, a_n, s)$ и верно $\varphi_e^{n+1}(a_1, \ldots, a_n, s)\ \mathbf{r}\ \Psi(a_1, \ldots, a_n)$], при этом список переменных $x_1, \ldots, x_n$ может быть пустым;
- $e\ \mathbf{r}\ \forall x_1, \ldots, x_n\, \Phi(x_1, \ldots, x_n) \rightleftharpoons [e\ \mathbf{r}\ \forall x_1, \ldots, x_n\, (\top \to \Phi(x_1, \ldots, x_n))]$, если список переменных $x_1, \ldots, x_n$ непуст, формула $\Phi(x_1, \ldots, x_n)$ не начинается с квантора $\forall$, и логическая связка $\to$ не является главной в $\Phi(x_1, \ldots, x_n)$.

Будем говорить, что замкнутая формула Φ языка теории множеств является *реализуемой*, если найдется такое натуральное число e, что имеет место $e\ \mathbf{r}\ \Phi$.

Теория множеств Цермело-Френкеля имеет следующие аксиомы и схемы аксиом:

$$\forall x, y\, (\forall z\, (z \in x \leftrightarrow z \in y) \to x = y); \tag{Ext}$$
$$\exists z\, \forall x\, (x \in z \to \bot); \tag{$\varnothing$}$$
$$\forall x\, \exists z\, (x \in z \wedge \forall u {\in} z\, \exists u' {\in} z\, \forall y\, (y \in u' \leftrightarrow y = u)); \tag{Inf}$$
$$\forall x, y\, \exists z\, \forall u\, (u \in z \leftrightarrow (u = x \vee u = y)); \tag{Pair}$$
$$\forall x\, \exists z\, \forall u\, (u \in z \leftrightarrow \exists y\, (y \in x \wedge u \in y)); \tag{Un}$$
$$\forall y\, \exists z\, \forall x\, (x \in z \leftrightarrow \forall u\, (u \in x \to u \in y)); \tag{Pow}$$
$$\forall z\, (\exists u\, (u \in z) \to \exists y {\in} z\, \forall x\, (x \in y \wedge x \in z \to \bot)); \tag{Reg}$$
$$\forall x\, \exists y\, \forall u\, (u \in y \leftrightarrow u \in x \wedge \Phi(u)); \tag{Sep}$$
$$\forall x\, [\forall v {\in} x\, \exists! u\, \Phi(v, u) \to \exists y\, \forall v {\in} x\, \exists u {\in} y\, \Phi(v, u)]. \tag{Rep}$$

Верны следующие теоремы.

Теорема 1. *Следующие аксиомы теории множеств Цермело-Френкеля являются реализуемыми:* ($\varnothing$), (Inf), (Pair), (Un), (Rep).

Теорема 2. *Следующие аксиомы теории множеств Цермело-Френкеля не являются реализуемыми:* (Ext), (Pow), (Reg).

[1] Однако, если в списке $x_1, \ldots, x_n$ на некоторых позициях i и j стоят одинаковые переменные x_i и x_j, то мы не допускаем рассмотрение тех списков $a_1, \ldots, a_n$, в которых $a_i \neq a_j$.

Список литературы

[1] Гейтинг А., *Интуиционизм*, Мир, М., 1965.

[2] Клини С. К., *Введение в метаматематику*, Мир, М., 1957.

[3] Коновалов А. Ю., "Семантика реализуемости для конструктивной теории множеств, основанная на гиперарифметический предикатах", *Вестн. Моск. ун-та. Матем. Механ.*, **3**, 2017, 59–62.

[4] Роджерс Х., *Теория рекурсивных функций и эффективная вычислимость*, Мир, М., 1972.

The Zermelo–Fraenkel set theory is not sound with respect to the constructive sematics based on hyperarithmetic sorts

Konovalov A. Yu.

A semantics of the realizability based on hyperarithmetical sorts for formulas of the language of set theory is introduced. The soundness of axioms of the Zermelo–Fraenkel set theory with respect to this semantics is studied.

Keywords: constructive semantics, realizability, axiomatic set theory, hyperarithmetical sorts.

К сведению авторов публикаций в журнале «Интеллектуальные системы. Теория и приложения»

В соответствии с требованиями ВАК РФ к изданиям, входящим в перечень ведущих рецензируемых научных журналов и изданий, в которых могут быть опубликованы основные научные результаты диссертаций на соискание ученой степени доктора и кандидата наук, статьи в журнал «Интеллектуальные системы. Теория и приложения» предоставляются авторами в следующей форме:

1. Статьи, набранные в пакете LaTeX, предоставляются к загрузке через WEB-форму http://intsysjournal.org/generator_form .
2. К статье прилагаются файлы, содержащие название статьи на русском и английском языках, аннотацию на русском и английском языках (не более 50 слов), список ключевых слов на русском и английском языках (не более 20 слов), информация об авторах: Ф.И.О. полностью, место работы, должность, ученая степень и/или звание (если имеется), контактные телефоны (с кодом города и страны), e-mail, почтовый адрес с индексом города (домашний или служебный).
3. Список литературы оформляется в едином формате, установленном системой Российского индекса научного цитирования.
4. За публикацию статей в журнале «Интеллектуальные системы. Теория и приложения» с авторов (в том числе аспирантов высших учебных заведений) статей, рекомендованных к публикации, плата не взимается. Оттиски статей авторам не предоставляются. Журнал распространяется по подписке, экземпляры журнала рассылаются подписчикам наложенным платежом. Условия подписки публикуются в каталоге НТИ «Роспечать», индекс журнала 64559.
5. Доступ к электронной версии последнего вышедшего номера осуществляется через НЭБ «Российский индекс научного цитирования». Номера, вышедшие ранее, размещаются на сайте http://intsysjournal.org, и доступ к ним бесплатный. Там же будут размещены аннотации всех публикуемых статей.

Подписано в печать: 16.05.2019
Дата выхода: 23.05.2019
Тираж: 200 зкз.
Цена свободная
Свидетельство о регистрации СМИ: ПИ № ФС77–58444 от 25 июня 2014 г., выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций(Роскомнадзор).