Math-Net.Ru

Общероссийский математический портал

А. В. Черемушкин, Бесповторная декомпозиция сильно зависимых функций, *Дискрет. матем.*, 2004, том 16, выпуск 3, 3–42

DOI: <https://doi.org/10.4213/dm161>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.234.197.8

26 апреля 2023 г., 15:51:05

Бесповторная декомпозиция сильно зависимых функций

© 2004 г. А. В. Черемушкин

Приводится обобщение на k -значный случай результатов по декомпозиции двоичных функций. Описываются свойства групп автотопий и изострофий функций, допускающих нетривиальную декомпозицию, а также предлагается метод вычисления параметров таких функций.

Введение

Проблема описания функционально разделимых двоичных функций, то есть функций, допускающих бесповторную декомпозицию, была поставлена еще К. Шенноном в 1949 г. (см. [1]). Задача о существовании и единственности различных типов декомпозиции исследовалась рядом авторов и получила полное решение в работах [2] и [3]. В [2] вводится отношение близости формул и доказывается, что две бесповторные формулы представляют одну функцию в том и только том случае, когда они являются близкими. В [3] с использованием техники решения функциональных уравнений вводится отношение эквивалентности на множестве переменных и с его помощью осуществляется сведение описания различных декомпозиций у функции к изучению простых декомпозиций.

В дальнейшем внимание многих авторов было сосредоточено в основном на поиске эффективных алгоритмов нахождения простых декомпозиций (см. [4, 5, 6] и др.) для полностью и частично определенных двоичных и k -значных функций, а также на изучении условий существования декомпозиции для функций из конкретных классов (см., например, [7]).

Другое направление исследований, возникшее под влиянием работ А. В. Кузнецова [2] и С. В. Яблонского [8], было посвящено исследованию классов функций, порожденных в различных базисах с помощью операции бесповторной суперпозиции (подробнее см. [9] и монографию [10]).

Следует отметить, что термин “бесповторная” обычно относится к функциям, формулам, суперпозициям, а применительно к декомпозиции обычно используется термин “разделительная”. В данной работе, как и в [13], в интересах единообразия всюду будет использован одинаковый термин, поскольку данное употребление, на взгляд автора, имеет определенное удобство и не должно вызывать разночтений.

Для k -значных функций, являющихся n -арными квазигруппами, решение функциональных уравнений описано в работе В. Д. Белоусова [14]. В работе автора [15] на основе

результата В. Д. Белоусова о решении уравнения общей ассоциативности получено описание неповторной декомпозиции для n -арных квазигрупп, обобщающее на k -значный случай результаты по декомпозиции двоичных функций.

В настоящей статье изучается неповторная декомпозиция сильно зависимых функций. С использованием приведенного в работе Ф. Н. Сохацкого [16] обобщения теоремы В. Д. Белоусова на случай сильно зависимых функций приводится обобщение результатов работы [15]. Показывается, что для каждой сильно зависимой функции можно определить однозначную с точностью до определенного отношения эквивалентности каноническую декомпозицию.

В качестве применения полученных результатов приводится описание свойств групп автотопий и изострофий функций, допускающих нетривиальную неповторную декомпозицию, а также предлагается способ вычисления параметров таких функций.

1. Необходимые определения и результаты

1.1. Сильно зависимые функции

Напомним основные определения (см. [14, 17, 18]).

Пусть $n \geq 0$, $k \geq 2$, и $\Omega = \{0, 1, \dots, k-1\}$. Функцию $f: \Omega^n \rightarrow \Omega$ будем называть k -значной функцией или n -арной операцией на множестве Ω .

Элементарной трансляцией функции $f: \Omega^n \rightarrow \Omega$ (n -арной операции f) над Ω называется унарная операция, полученная из f путем фиксации всех переменных, кроме одного.

Множество с бинарной операцией $(\Omega, \circ)$ называется группоидом. Если все элементарные трансляции операции $\circ$ являются подстановками, то такой группоид называется квазигруппой. Квазигруппа $(\Omega, \circ)$ называется лупой, если она имеет единичный элемент e , то есть $e \circ x = x \circ e = x$ для всех $x \in \Omega$. Если бинарная операция $\circ$ ассоциативна и имеет единичный элемент, то группоид $(\Omega, \circ)$ называется моноидом. Если из контекста ясно, о каком группоиде $(\Omega, \circ)$ идет речь, то будем для удобства использовать термины квазигруппа, лупа и моноид для самой бинарной операции $\circ$.

Контрольный набор элементов n -арной операции на множестве Ω — это такой набор из $n-1$ элементов из Ω , при котором полученная после фиксации ими аргументов элементарная трансляция является подстановкой по оставшемуся переменному.

Сильно зависимая функция (операция) — это такая функция, у которой для любого переменного найдутся контрольные наборы элементов. Данное определение удобно тем, что множество зависимых функций является замкнутым относительно операции неповторной суперпозиции (см. ниже). В случае $k = 2$ сильно зависимая функция — это двоичная функция, существенно зависящая от всех своих переменных. Заметим, что бинарная операция с единичным элементом всегда является сильно зависимой.

Если функция от n переменных при фиксации любых $n-1$ переменных любыми значениями будет подстановкой по оставшемуся переменному, то она называется n -квазигруппой.

1.2. Определение основных групп преобразований

Пусть $\Omega_2^{\Omega_1}$ — множество функций $f: \Omega_1 \rightarrow \Omega_2$, $S(\Omega)$ — симметрическая группа на множестве Ω . Будем использовать обозначение (G, Ω) для группы подстановок множества Ω , то есть $G \leq S(\Omega)$.

Определим основные группы, действующие на множестве функций $\Omega_2^{\Omega_1}$. Всюду ниже для действия групп на множестве функций будем использовать правую (экспоненциальную) запись, а для действия на исходных множествах — левую (функциональную).

Как правило, группы, применяемые для классификации функций, имеют какое-либо стандартное действие. Например, группа подстановок S_n действует на множестве $\{1, 2, \dots, n\}$, а полная линейная группа $GL(n, 2)$ — на множестве n -мерных векторов и т. п. При классификации функций возникает необходимость рассматривать действия этих групп на более сложно устроенных множествах.

Рассмотрим основные способы, позволяющие строить необходимые действия. Исходными для дальнейших построений являются следующие два способа построения новых действий для исходных групп.

Пусть (G_1, Ω_1) и (G_2, Ω_2) — группы, действующие на множествах аргументов и значений функций (если $\Omega_1 = \Omega_2$ и G_1 и G_2 совпадают как группы подстановок, то все равно будем их различать, как действующие на различных множествах: первую — на множестве аргументов, а вторую — на множестве значений функции).

1. Группа $(G_1, \Omega_2^{\Omega_1})$ определяется действием $\pi: f \mapsto f^\pi$, где при всех $x \in \Omega_1$ и $\pi \in G_1$

$$f^\pi(x) = f((\pi^{-1}(x))).$$

2. Группа $(G_2, \Omega_2^{\Omega_1})$ определяется действием $\gamma: f \mapsto f^\gamma$, где при всех $x \in \Omega_1$ и $\gamma \in G_2$

$$f^\gamma(x) = \gamma(f(x)).$$

3. Обобщением двух предыдущих способов построения действий является построение действия прямого произведения $(G_1 \times G_2, \Omega_2^{\Omega_1})$, определяемого следующим образом: при всех $x \in \Omega_1$ и $(\pi, \gamma) \in G_1 \times G_2$

$$f^{(\pi, \gamma)}(x) = \gamma(f(\pi^{-1}(x))).$$

Для определения действия групп на множестве функций $f: \Omega_1^n \rightarrow \Omega_2$ от нескольких переменных необходимо уточнить строение группы, действующей на множестве аргументов Ω_1^n . Пусть, как и выше, заданы две группы подстановок (G_1, Ω_1) и (G_2, Ω_2) . Обычно используются следующие группы:

- группа (G_1^n, Ω_1^n) , состоящая из преобразований $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in G_1$, $i = 1, \dots, n$, и определяемая действием

$$\alpha(x_1, \dots, x_n) = (\alpha_1(x_1), \dots, \alpha_n(x_n)),$$

где $x_i \in \Omega_1$, $i = 1, \dots, n$;

- группа (S_n, Ω_1^n) , состоящая из подстановок

$$\pi = \begin{pmatrix} 1 & \dots & n \\ \pi(1) & \dots & \pi(n) \end{pmatrix}$$

и определяемая действием

$$\pi(x_1, \dots, x_n) = (x_{\pi^{-1}(1)}, \dots, x_{\pi^{-1}(n)}),$$

где $x_i \in \Omega_1$, $i = 1, \dots, n$;

– группа $([G_1]S_n, \Omega_1^n)$ (экспоненцирование групп), состоящая из преобразований (α, π) , где $\pi \in S_n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, и определяемая действием

$$(\alpha, \pi)(x_1, \dots, x_n) = (\alpha_{\pi^{-1}(1)}(x_{\pi^{-1}(1)}), \dots, \alpha_{\pi^{-1}(n)}(x_{\pi^{-1}(n)})),$$

где $x_i \in \Omega_1$, $i = 1, \dots, n$.

Рассматривая эти группы в их действии на множестве Ω_1^n аргументов функций и вводя группу (G_2, Ω_2) , действующую на множестве значений функций, получаем следующие группы, действующие на множестве функций $\{f: \Omega_1^n \rightarrow \Omega_2\} = \Omega_2^{\Omega_1^n}$.

4. Группа $(G_1^n, \Omega_2^{\Omega_1^n})$ определяется действием

$$f^\alpha(x_1, \dots, x_n) = f(\alpha_1^{-1}(x_1), \dots, \alpha_n^{-1}(x_n)),$$

где $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in G_1$, $x_i \in \Omega_1$, $i = 1, \dots, n$.

5. Группа $(S_n, \Omega_2^{\Omega_1^n})$ определяется действием

$$f^\pi(x_1, \dots, x_n) = f(x_{\pi(1)}, \dots, x_{\pi(n)}),$$

где $\pi \in S_n$, $x_i \in \Omega_1$, $i = 1, \dots, n$.

6. Группа $(G_1^n \times G_2, \Omega_2^{\Omega_1^n})$ определяется действием

$$f^{(\alpha, \gamma)}(x_1, \dots, x_n) = \gamma(f(\alpha_1^{-1}(x_1), \dots, \alpha_n^{-1}(x_n))),$$

где $\gamma \in G_2$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in G_1$, $x_i \in \Omega_1$, $i = 1, \dots, n$.

7. Группа $([G_1]S_n \times G_2, \Omega_2^{\Omega_1^n})$ определяется действием

$$f^{(\alpha, \pi, \gamma)}(x_1, \dots, x_n) = \gamma(f(\alpha_{\pi(1)}^{-1}(x_{\pi(1)}), \dots, \alpha_{\pi(n)}^{-1}(x_{\pi(n)}))),$$

где $\gamma \in G_2$, $\pi \in S_n$, $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in G_1$, $x_i \in \Omega_1$, $i = 1, \dots, n$.

Диаграмма, иллюстрирующая вложения введенных выше групп преобразований, приведена на рис. 1.

В случае, когда $\Omega_1 = \Omega_2 = \Omega$ и функции $f: \Omega^n \rightarrow \Omega$ являются n -квазигруппами, обычно рассматривают следующие случаи введенных выше групп.

8. Группа парастрофий $(S_{n+1}, \Omega^{\Omega^n})$ состоит из подстановок

$$\pi = \begin{pmatrix} 1 & \dots & n+1 \\ \pi(1) & \dots & \pi(n+1) \end{pmatrix}$$

и определяется действием

$$f^\pi(x_1, \dots, x_n) = x_{n+1}$$

в том и только том случае, когда

$$f(x_{\pi(1)}, \dots, x_{\pi(n)}) = x_{\pi(n+1)},$$

где $x_i \in \Omega$, $i = 1, \dots, n+1$. Такие преобразования называются парастрофиями n -квазигрупп. В случае $\pi(n+1) = n+1$ парастрофия называется главной.

Рис. 1. Группы преобразований множества функций

9. Группа изострофий $([S_k]S_{n+1}, \Omega^{\Omega^n})$, $k = |\Omega|$, определяется действием

$$f^{(\alpha, \pi)}(x_1, \dots, x_n) = x_{n+1}$$

в том и только в том случае, когда

$$f(\alpha_{\pi(1)}(x_{\pi(1)}), \dots, \alpha_{\pi(n)}(x_{\pi(n)})) = \alpha_{\pi(n+1)}(x_{\pi(n+1)}),$$

где $x_i \in \Omega$, $i = 1, \dots, n+1$. Для удобства преобразования из этой группы при $\pi(n+1) = n+1$ назовем главными изострофиями.

10. Группа изотопий $(S_k^{n+1}, \Omega^{\Omega^n})$ совпадает с группой $(S_k^n \times S_k, \Omega^{\Omega^n})$ (см. п. 6). Преобразования (α, α_{n+1}) , где $\alpha = (\alpha_1, \dots, \alpha_n)$, $\alpha_i \in S_k$, $i = 1, \dots, n+1$, из этой группы при $\alpha_{n+1} = e$ называются главными изотопиями.

В данном случае диаграмма вложения групп имеет вид, изображенный на рис. 2.

Группой инерции G_f функции f в группе G , где G — одна из введенных выше групп, действующих на множестве функций, как обычно, будем называть стабилизатор элемента f в группе G .

По аналогии с квазигруппами будем использовать для групп инерции k -значных функций от n переменных (n -арных операций)

$$f: \Omega^n \rightarrow \Omega, \quad k = |\Omega|,$$

следующие термины:

$(S_k^{n+1})_f$ — группа автотопий (обозначаем ее $\text{Atp}(f)$);

$(S_k^n)_f$ — группа главных автотопий (обозначаем ее $\text{Atp}^\circ(f)$);

$(S_n)_f$ — группа главных паратопий;

Рис. 2. Группы преобразований множества n -квазигрупп

$([S_k]S_n \times S_k)_f$ — группа главных автострофий (обозначаем ее $\text{Ast}^\circ(f)$).

Для групп инерции n -квазигрупп f также используются термины:

$(S_{n+1})_f$ — группа паратопий;

$([S_k]S_{n+1})_f$ — группа автострофий (обозначаем ее $\text{Ast}(f)$).

1.3. Бинарные сильно зависимые функции

Приведем некоторые свойства, которые являются обобщениями известных свойств квазигрупп на случай бинарных сильно-зависимых функций. Пусть $z = x * y$ — сильно зависимая бинарная операция на множестве Ω . Обозначим через L_a и R_b трансляции

$$L_a = \begin{pmatrix} x \\ a * x \end{pmatrix}, \quad R_b = \begin{pmatrix} x \\ x * b \end{pmatrix}, \quad a, b \in \Omega.$$

Если a и b — контрольные элементы для операции $*$, то L_a и R_b — подстановки на множестве Ω , которые называются левой и правой регулярными подстановками соответственно. В частности, если $(\Omega, *)$ — квазигруппа, то они всегда являются подстановками.

Аналогично квазигруппам, каждая из которых изотопна некоторой лупе, для сильно зависимых функций справедлива следующая теорема.

Теорема 1. *Всякая сильно зависимая бинарная операция главноизотопна операции с единицей. При этом всякая такая изотопия имеет вид $(R_a^{-1}, L_b^{-1}, \varepsilon)$ при некоторых $a, b \in \Omega$ (ε — единичная подстановка на множестве Ω).*

Доказательство. Пусть a и b — контрольные элементы для x и y соответственно. Рассмотрим операцию

$$x \circ y = R_b^{-1}(x) * L_a^{-1}(y).$$

Покажем, что элемент $c = a * b$ является единицей операции $\circ$. Так как $c = L_a(b) = R_b(a)$, получаем, что

$$\begin{aligned} x \circ c &= R_b^{-1}(x) * L_a^{-1}(c) = R_b^{-1}(x) * b = R_b(R_b^{-1}(x)) = x, \\ c \circ x &= R_b^{-1}(c) * L_a^{-1}(x) = a * L_a^{-1}(x) = L_a(L_a^{-1}(x)) = x. \end{aligned}$$

Обратно, пусть при некоторых α и $\beta \in S(\Omega)$ выполняется равенство

$$x \diamond y = \alpha(x) * \beta(y),$$

причем операция $\diamond$ имеет единицу e . Тогда

$$\begin{aligned} x &= x \diamond e = \alpha(x) \diamond \beta(e), \\ y &= e \diamond y = \alpha(e) \diamond \beta(y), \end{aligned}$$

откуда

$$\alpha(x) = R_{\beta(e)}^{-1}(x), \quad \beta(y) = L_{\alpha(e)}^{-1}(y).$$

Теорема доказана.

Справедлива также следующая теорема.

Теорема 2. Если бинарная операция с единицей $\circ$ изотопна моноиде $*$, то она сама ассоциативна и изоморфна операции $*$.

Воспользуемся следующими хорошо известными свойствами ассоциативных операций (см., например, [18]).

Лемма 1. Если бинарная операция $\circ$ ассоциативна, то

- если существуют левая и правая единицы, то они совпадают;
- если для элемента $a \in \Omega$ существует левый и правый обратный, то они совпадают;
- если в конечном моноиде элемент $a \in \Omega$ имеет левый обратный, то он имеет и правый обратный, и наоборот.

Доказательство теоремы 2. Пусть при некоторых подстановках α , β и γ выполняется равенство

$$\alpha(x) \circ \beta(y) = \gamma(x * y).$$

Сведем задачу к случаю главной изотопии, заменив операцию $*$ на изоморфную ей операцию

$$x \diamond y = \gamma(\gamma^{-1}(x) * \gamma^{-1}(y)).$$

Справедливо равенство

$$\alpha(\gamma^{-1}(x)) \circ \beta(\gamma^{-1}(y)) = x \diamond y,$$

или иначе

$$x \circ y = \gamma(\alpha^{-1}(x)) \diamond \gamma(\beta^{-1}(y)).$$

По теореме 1

$$\alpha^{-1}\gamma = R_b^{-1}, \quad \beta^{-1}\gamma = L_a^{-1}$$

при некоторых контрольных элементах $a, b \in \Omega$, где

$$R_b = \begin{pmatrix} x \\ x \diamond b \end{pmatrix}, \quad L_a = \begin{pmatrix} x \\ a \diamond x \end{pmatrix}.$$

Так как $\diamond$ — моноид, а $a, b \in \Omega$ — контрольные элементы, в силу леммы 1 существуют обратные $a^{-1}, b^{-1} \in \Omega$. При этом в силу ассоциативности операции $\diamond$ и конечности Ω выполняются равенства

$$R_b^{-1} = \begin{pmatrix} x \\ x \diamond b \end{pmatrix}^{-1} = \begin{pmatrix} x \\ x \diamond b^{-1} \end{pmatrix} = R_{b^{-1}},$$

$$L_a^{-1} = \begin{pmatrix} x \\ a \diamond x \end{pmatrix}^{-1} = \begin{pmatrix} x \\ a^{-1} \diamond x \end{pmatrix} = L_{a^{-1}},$$

откуда

$$x \circ y = (x \diamond b^{-1}) \diamond (a^{-1} \diamond x) = x \diamond (a \diamond b)^{-1} \diamond y.$$

Полагая $c = a \diamond b$, непосредственной проверкой убеждаемся, что операция $x \diamond c^{-1} \diamond y$ ассоциативна. Вместе с тем, равенство

$$x \circ y = x \diamond c^{-1} \diamond y$$

после замены переменных можно записать в виде

$$(x \diamond c) \circ (y \diamond c) = (x \diamond y) \diamond c.$$

Отсюда следует, что операции $\circ$ и $\diamond$ изоморфны.

Теорема доказана.

Для случая квазигрупп эта теорема известна как теорема Алберта: если лупа изоморфна группе, то она сама группа, изоморфная этой группе.

Приведенное выше доказательство теоремы 2 не только обосновывает существование искомого изоморфизма, но и указывает его явный вид. Сформулируем одно уточнение этой теоремы, описывающее явный вид компонент для случая главной изотопии, необходимое нам в дальнейшем.

Следствие 1. Если бинарная операция $\circ$ с единицей главноизотопна моноиду $\diamond$, то она ассоциативна и имеет вид $x \circ y = x \diamond c^{-1} \diamond y$ при некотором обратимом элементе $c \in \Omega$ моноида $\diamond$. При этом элемент c является единицей операции $\circ$ и, если x^{-1} — обратный к x относительно операции $\diamond$, то $c \diamond x^{-1} \diamond c$ — обратный к x относительно операции $\circ$. Изоморфизм между операциями $\circ$ и $\diamond$ имеет вид (R_c, R_c, R_c) , где $R_c = \begin{pmatrix} x \\ x \diamond c \end{pmatrix}$.

Из этих двух теорем следует, что классификация с точностью до изотопии сильно зависимых бинарных операций с единицей (квазигрупп) сводится к классификации сильно зависимых операций с единицей (луп) (теорема 1). Классификация же последних распадается на два непересекающихся случая: ассоциативный и неассоциативный (теорема 2).

1.4. Группы главных автострофий моноидов

По аналогии с квазигруппами введем понятие квазиавтоморфизма группоида $G = (\Omega, *)$ как главную компоненту его автотопии (см. [11], [17]), то есть подстановка $\gamma \in S(\Omega)$ — квазиавтоморфизм (обратный квазиавтоморфизм), если найдутся подстановки α и β такие, что

$$\gamma(x * y) = \alpha(x) * \beta(y) \quad (\gamma(x * y) = \beta(y) * \alpha(x)). \quad (1)$$

Все квазиавтоморфизмы образуют группу, которую будем обозначать $\text{Hol}(G)$, а все обратные квазиавтоморфизмы образуют смежный класс по этой группе в группе, которая является их объединением и называется группой диквазиавтоморфизмов.

Опишем строение групп автотопий моноидов.

Согласно лемме 1 множество элементов моноида G , имеющих левые обратные, совпадает с множеством элементов, имеющих правые обратные, и образует группу обратимых элементов моноида. Обозначим ее G^* .

Лемма 2. Подстановка $\gamma \in S(\Omega)$ является квазиавтоморфизмом (обратным квазиавтоморфизмом) моноида $G = (\Omega, *)$ в том и только том случае, когда при некотором обратимом элементе $a \in \Omega$ выполняется тождество

$$\gamma(x * y) = \gamma(x) * a * \gamma(y) \quad (\gamma(x * y) = \gamma(y) * a * \gamma(x)). \quad (2)$$

Доказательство. Пусть $e \in \Omega$ — единица моноида. Подставим в равенство (1) вместо значений переменных единицу моноида:

$$\gamma(x) = \alpha(x) * \beta(e), \quad \gamma(y) = \alpha(e) * \beta(y).$$

Так как γ, α и β — подстановки, то $\beta(e)$ и $\alpha(e)$ — обратимые элементы моноида. Поэтому

$$\alpha(x) = \gamma(x) * \beta(e)^{-1}, \quad \beta(y) = \alpha(e)^{-1} * \gamma(y).$$

Отсюда,

$$\gamma(x * y) = \gamma(x) * \beta(e)^{-1} * \alpha(e)^{-1} * \gamma(y),$$

и

$$a = \beta(e)^{-1} * \alpha(e)^{-1}.$$

Случай обратных квазиавтоморфизмов рассматривается полностью аналогично.

Лемма 3. Пусть γ — квазиавтоморфизм моноида $G = (\Omega, *)$ и a — обратимый элемент из равенства (2). Тогда

- (1) $\gamma R_a \in \text{Aut}(G)$;
- (2) $a = (\gamma(e))^{-1}$, где e — единица моноида G ;
- (3) множество всех квазиавтоморфизмов образует группу $\text{Hol}(G)$ порядка

$$|\text{Hol}(G)| = |G^*| |\text{Aut}(G)|;$$

- (4) $\text{Hol}(G) = \text{Aut}(G)H(G)$, где $H(G) = \{R_a : a \in G^*\}$.

Доказательство. Домножив обе части (2) на a , получаем равенство

$$\gamma(x * y) * a = \gamma(x) * a * \gamma(y) * a.$$

Элемент a обратим, поэтому $\beta = \gamma R_a$ — подстановка, причем

$$\beta(x * y) = \beta(x) * \beta(y).$$

Следовательно, β — квазиавтоморфизм моноида G .

При автоморфизме единичный элемент переходит в единичный, так что $\beta(e) = e$. Отсюда, $a = (\gamma(e))^{-1}$.

Наконец, докажем последнее утверждение. Если γ — квазиавтоморфизм, то $\gamma = \beta R_b$, где $b \in G^*$, $\beta \in \text{Aut}(G)$. Обратно, всякая подстановка такого вида, очевидно, будет квазиавтоморфизмом. Поэтому

$$|\text{Hol}(G)| = |G^*| |\text{Aut}(G)|.$$

Теорема доказана.

Теорема 3. Каждая компонента автотопии моноида является квазиавтоморфизмом. При этом

$$|\text{Atp}(G)| = |G^*|^2 |\text{Aut}(G)|.$$

Доказательство. Пусть $e \in \Omega$ — единица моноида. Рассуждая аналогично доказательству леммы 2, находим, что

$$\gamma(x * y) = \gamma(x) * \beta(e)^{-1} * \alpha(e)^{-1} * \gamma(y),$$

и по лемме 3 $\gamma = \xi R_c$, где $c = \alpha(e) * \beta(e)$, $\xi \in \text{Aut}(G)$. При $b = \beta(e)$ и $a = \alpha(e)$ получаем, что

$$\gamma = \xi R_a R_b, \quad \alpha = \gamma R_b^{-1}, \quad \beta = \gamma R_a R_b L_a^{-1}. \quad (3)$$

Так как $R_a L_a^{-1} \in \text{Aut}(G)$, то $a, b \in \text{Hol}(G)$.

С другой стороны, для произвольных $a, b \in G^*$, $\xi \in \text{Aut}(G)$ тройка подстановок, (α, β, γ) вида (3) является автотопией.

Таким образом,

$$|\text{Atp}(G)| = |G^*|^2 |\text{Aut}(G)|.$$

Теорема доказана.

Приведем теперь описание группы главных автострофий моноида. В данном случае строение группы зависит от наличия у операции $*$ антиизоморфизма. Заметим, что существуют моноиды как имеющие антиизоморфизм, так и не имеющие. Например, полугруппа матриц имеет антиизоморфизм — транспонирование, а симметрическая полугруппа не имеет. С другой стороны, группы всегда имеют антиизоморфизм — обращение элемента.

Лемма 4. Если у моноида $*$ имеется обратный квазиавтоморфизм, то у него есть и антиизоморфизм σ . При этом всякий обратный квазиавтоморфизм γ моноида $G = (\Omega, *)$ имеет вид $\gamma = \sigma \gamma'$, где γ' — квазиавтоморфизм.

Доказательство. Предположим, что выполняется равенство

$$x * y = \gamma^{-1}(\beta(y) * \alpha(x)).$$

Обозначим символом $\circ$ операцию $x \circ y = y * x$. Тогда

$$x * y = \gamma^{-1}(\alpha(x) \circ \beta(y)),$$

и по теореме 2 должен существовать изоморфизм $\sigma \in S(\Omega)$ такой, что

$$x * y = \sigma^{-1}(\sigma(x) \circ \sigma(y)).$$

Таким образом, моноид $*$ имеет антиизоморфизм σ :

$$x * y = \sigma^{-1}(\sigma(y) * \sigma(x)).$$

Объединяя это равенство с первым, получаем, что

$$\gamma(\sigma^{-1}(x * y)) = \alpha(\sigma^{-1}(x)) * \beta(\sigma^{-1}(y)),$$

откуда и следует, что $\gamma' = \sigma^{-1}\gamma$ — квазиавтоморфизм моноида $*$.

Теорема 4. Пусть $G = (\Omega, *)$ — моноид.

(1) Если операция $*$ коммутативна, то

$$\text{Ast}^\circ(G) = \text{Atp}(G)S_2.$$

(2) Пусть операция $*$ некоммутативна. Если она допускает антиизоморфизм, то

$$|\text{Ast}^\circ(G)| = 2|\text{Atp}(G)|;$$

если операция $*$ не имеет антиизоморфизма, то

$$\text{Ast}^\circ(G) = \text{Atp}(G).$$

Доказательство. Утверждение 1 очевидно. Рассмотрим случай 2. Пусть группа $\text{Ast}^\circ(G)$ содержит преобразование $(\alpha_1, \alpha_2, \alpha_3, \pi)$, где $\alpha_1, \alpha_2, \alpha_3 \in S(\Omega)$, $\pi \in S_2$. Из леммы 4 следует, что случай $\pi = (1, 2)$ возможен в том и только том случае, когда операция $*$ имеет антиизоморфизм. Рассмотрим теперь гомоморфизм $(\alpha_1, \alpha_2, \alpha_3, \pi) \mapsto \pi$ группы $\text{Ast}^\circ(G)$ в группу S_2 . Его ядро совпадает с группой автотопий $\text{Atp}(G)$, а образ, согласно доказанному выше, будет иметь порядок, равный двум, в том и только том случае, когда операция $*$ имеет антиизоморфизм.

Теорема доказана.

1.5. Решение функциональных уравнений

Определение 1. Бесповторной суперпозицией функций A и B называется функция F , удовлетворяющая равенству

$$F(x_1, \dots, x_n) = A(B(x_{i_1}, \dots, x_{i_k}), x_{i_{k+1}}, \dots, x_{i_n}),$$

где $i_l \neq i_m$, $l \neq m$, $1 \leq k \leq n$. Будем говорить, что бесповторная декомпозиция сильно зависимых функций тривиальна, если $k = 1$ или $k = n$.

Заметим, что функция F сильно зависима в том и только том случае, когда функции A , B являются сильно зависимыми. Если ослабить условие сильной зависимости и рассматривать обычную существенную зависимость переменных, то при $|\Omega| \geq 3$ возможны случаи, когда применение операции бесповторной суперпозиции с функциям со всеми существенными переменными дает в результате функцию с несущественными переменными (пример легко построить, взяв нескорректированную функцию B и определив соответствующим образом функцию A).

В общем случае при решении различных задач, связанных с изучением свойств суперпозиции функций, требуется определить условия выполнимости равенств, в правой и левой частях которых стоят суперпозиции функций, или, иначе говоря, найти все решения функционального уравнения.

В случае, когда в качестве операции суперпозиции используется операция бесповторной суперпозиции, задача решения функциональных уравнений произвольного вида сводится к решению одного уравнения, содержащего в общем случае четыре функции и имеющего вид

$$A(B(x_{i_1}, \dots, x_{i_k}), x_{i_{k+1}}, \dots, x_{i_n}) = C(D(x_{j_1}, \dots, x_{j_l}), x_{j_{l+1}}, \dots, x_{j_n}),$$

где $1 \leq k \leq n$, $1 \leq l \leq n$, $\{x_1, \dots, x_n\} = \{x_{i_1}, \dots, x_{i_n}\} = \{x_{j_1}, \dots, x_{j_n}\}$.

Это уравнение называется обобщенным уравнением общей ассоциативности (см. [14]).

Для упрощения записи будем использовать множественную запись для наборов переменных функций и будем вместо $B(x_{i_1}, \dots, x_{i_k})$ писать символ $B(X_1)$, где $X_1 = \{x_{i_1}, \dots, x_{i_k}\} \subseteq X = \{x_1, \dots, x_n\}$. Подчеркнем, что данный символ обозначает функцию, зависящую несущественно от всех переменных из множества $X \setminus X_1$, причем не все переменные из множества X_1 являются существенными. Поскольку множественная запись не фиксирует порядок переменных, формально свободное ее использование может привести к недоразумениям. Однако в нашем случае такая запись будет применяться только для тех уравнений, где уже заранее фиксирован порядок следования переменных. Поэтому для всех функций, которые будут появляться при его решении, можно считать, что порядок выписывания их переменных произволен, но выбирается один раз при первом их появлении и в дальнейшем не изменяется.

С использованием данных обозначений обобщенное уравнение общей ассоциативности можно записать в виде

$$A(B(X_1), X_2) = C(D(Y_1), Y_2),$$

где $X = X_1 \cup X_2 = Y_1 \cup Y_2$ — некоторые разбиения множества X . В зависимости от выбора множеств X_1 , X_2 , Y_1 , Y_2 при решении такого уравнения могут встретиться три принципиально различных случая:

$$\begin{aligned} A(B(Z_1, Z_2), Z_4) &= C(D(Z_2), Z_1, Z_4), & Z_3 &= \emptyset, \\ A(B(Z_1), Z_3, Z_4) &= C(D(Z_3), Z_1, Z_4), & Z_2 &= \emptyset, \\ A(B(Z_1, Z_2), Z_3, Z_4) &= C(D(Z_2, Z_3), Z_1, Z_4), \end{aligned}$$

где

$$Z_1 = X_1 \cap Y_2, \quad Z_2 = X_1 \cap Y_1, \quad Z_3 = X_2 \cap Y_1, \quad Z_4 = X_2 \cap Y_2.$$

Следующая теорема, доказанная Ф. Н. Сохацким в [16], является обобщением аналогичной теоремы В. Д. Белоусова для n -арных квазигрупп из книги [14]. Она дает полное описание решений уравнения общей ассоциативности для сильно зависимых функций.

Теорема 5. Пусть Z_1, Z_2, Z_3, Z_4 — непересекающиеся множества переменных, A, B, C, D — сильно зависимые функции, удовлетворяющие уравнению

$$A(B(Z_1, Z_2), Z_3, Z_4) = C(D(Z_2, Z_3), Z_1, Z_4).$$

Тогда

(i) если $Z_2 \neq \emptyset, Z_3 = \emptyset$, то существует единственная функция T такая, что

$$\begin{aligned} B(Z_1, Z_2) &= T(D(Z_2), Z_1), \\ C(y, Z_1, Z_4) &= A(T(y, Z_1), Z_4), \end{aligned}$$

(ii) если $Z_1 \neq \emptyset, Z_2 = \emptyset, Z_3 \neq \emptyset$, то существует единственная функция T такая, что

$$\begin{aligned} A(y, Z_3, Z_4) &= T(y, D(Z_3), Z_4), \\ C(z, Z_1, Z_4) &= T(B(Z_1), z, Z_4), \end{aligned}$$

(iii) если $Z_1 \neq \emptyset, Z_2 \neq \emptyset, Z_3 \neq \emptyset$, то существуют операции K, F_1, F_2, F_3 и моноид $\circ$ такие, что при некоторой подстановке α выполнены равенства

$$\begin{aligned} A(y, Z_3, Z_4) &= K(\alpha(y) \circ F_3(Z_3), Z_4), \\ B(Z_1, Z_2) &= \alpha^{-1}(F_1(Z_1) \circ F_2(Z_2)), \\ C(z, Z_1, Z_4) &= K(F_1(Z_1) \circ z, Z_4), \\ D(Z_2, Z_3) &= F_2(Z_2) \circ F_3(Z_3). \end{aligned}$$

При этом операция $\circ$ определена однозначно с точностью до изоморфизма.

2. Каноническая декомпозиция

2.1. Отношение эквивалентности на множестве переменных

Определение 2. (Бесповторной) декомпозицией (разложением) функции A называется правая часть равенства

$$A(x_1, \dots, x_n) = F(A_1, \dots, A_s; x_1, \dots, x_n), \quad (4)$$

где F — формула, полученная с помощью операции бесповторной суперпозиции из некоторых операций $A_1, \dots, A_s$, называемых компонентами.

Всюду ниже будем рассматривать декомпозиции только тех функций, которые являются сильно зависимыми. Напомним, что функция A сильно зависима в том и только том случае, когда функции $F, A_1, \dots, A_s$ являются сильно зависимыми.

Определение 3. Разложение вида

$$A(x_1, \dots, x_n) = B(C(x_{i_1}, \dots, x_{i_k}), x_{i_{k+1}}, \dots, x_{i_n}),$$

где $i_l \neq i_m, l \neq m, 1 \leq k \leq n$, называют простой декомпозицией. Назовем простую декомпозицию нетривиальной, если $1 < k < n$.

Как и в предыдущем разделе, будем использовать множественную запись

$$A(X) = B(C(X_1), X_2),$$

где

$$X = \{x_1, \dots, x_n\} = \{x_{i_1}, \dots, x_{i_n}\},$$

$$X_1 = \{x_{i_1}, \dots, x_{i_k}\},$$

$$X_2 = X \setminus X_1 = \{x_{i_{k+1}}, \dots, x_{i_n}\}.$$

В силу пункта (i) теоремы 5 простая декомпозиция однозначно с точностью до некоторой подстановки α определяется подмножеством переменных X_1 . Будем говорить, что простая декомпозиция максимальна (множество X_1 максимально), если не существует нетривиальной простой декомпозиции

$$A(x_1, \dots, x_n) = B'(C'(Y_1), Y_2),$$

где $X_1 \subset Y_1 \subset X$ и $X_1 \neq Y_1 \neq Y$.

Функции (операции), допускающие простые декомпозиции, называются разделимыми. Если функция допускает разложение, в котором все компоненты — бинарные операции, то она называется вполне приводимой.

Покажем, что для всякой сильно зависимой функции существует декомпозиция специального вида, называемая канонической декомпозицией, которая определяется по функции однозначно с точностью до некоторого отношения эквивалентности.

Для заданной операции $F(x_1, \dots, x_n)$ введем на множестве переменных $X = \{x_1, \dots, x_n\}$ бинарное отношение $\sim$, полагая $x_i \sim x_j$ в том и только том случае, когда существует простая декомпозиция $A(X) = B(C(X_1), X_2)$, $1 < |X_1| < n$, такая, что $x_i, x_j \in X_1$. Через $\sim_A$ обозначим транзитивное замыкание этого отношения.

Лемма 5. Для каждой сильно зависимой функции A отношение $\sim_A$ является отношением эквивалентности на множестве переменных.

Доказательство. Симметричность и рефлексивность следуют из определения. Транзитивность отношения $\sim_A$ вытекает из свойств транзитивного замыкания.

Лемма 6. Сильно зависимая функция A с классами эквивалентности $Z_1, \dots, Z_k$ относительно отношения $\sim_A$, $X = \bigcup_{i=1}^k Z_i$, $k \geq 2$, допускает простые декомпозиции вида

$$A(X) = B_i(Z_1, \dots, Z_{i-1}, C_i(Z_i), Z_{i+1}, \dots, Z_k), \quad 1 < i < k.$$

Доказательство. Выберем максимальную простую декомпозицию

$$A(X) = B(C(X_1), X_2)$$

такую, что $X_1 \subseteq Z_1$. Если $X_1 = Z_1$, то эта простая декомпозиция искомая. Если $X_1 \neq Z_1$, то по определению отношения $\sim_A$ найдется еще одна простая декомпозиция $A(X) = B'(C'(Y_1), Y_2)$, у которой $X_1 \cap Y_1 \neq \emptyset$, $X_1 \cap Y_2 \neq \emptyset$, $X_2 \cap Y_1 \neq \emptyset$ и $Y_1 \subseteq Z_1$. По пункту (iii) теоремы 5 найдутся операции K, F_1, F_2, F_3 и моноид $\circ$ такие, что выполнены равенства

$$A(X) = K(F_1(X_1 \cap Y_2) \circ F_2(X_1 \cap Y_1) \circ F_3(X_2 \cap Y_1), X_2 \cap Y_2).$$

В силу максимальной простой декомпозиции с множеством X_1 должно быть $X_2 \cap Y_2 = \emptyset$. Отсюда по определению отношения $\sim_A$ должно быть $k = 1$. Полученное противоречие завершает доказательство леммы.

2.2. Основная теорема

Определение 4. Пусть $\circ$ — ассоциативная бинарная операция. Сильно зависимую функцию A назовем $\circ$ -разложимой, если она допускает нетривиальное разложение вида

$$A(X) = C_1(X_1) \circ C_2(X_2).$$

(Тривиальным считаем случай, когда $X_1 = X$ или $X_2 = X$).

Согласно теореме 1 достаточно ограничиться случаем, когда операция $\circ$ является моноидом.

Приведем описание классов эквивалентности.

Заметим, что если функция A является $\circ$ -разложимой и имеет разложение, в котором содержится не менее трех компонент, например,

$$A(X) = C_1(X_1) \circ C_2(X_2) \circ C_3(X_3),$$

то, расставляя различными способами скобки в разложении и объединяя входящие в них множества переменных, например,

$$A(X) = (C_1(X_1) \circ C_2(X_2)) \circ C_3(X_3) = C_1(X_1) \circ (C_2(X_2) \circ C_3(X_3)),$$

можно построить по крайней мере две простые декомпозиции, соответствующие множествам $X_1 \cup X_2$ и $X_2 \cup X_3$, которые имеют непустое пересечение и дают в своем объединении все множество переменных $X_1 \cup X_2 \cup X_3 = X$. Поэтому в этом случае функция A должна иметь один класс эквивалентности относительно отношения $\sim_A$.

Оказывается, что имеет место и обратное утверждение, более того, справедлива следующая теорема, показывающая отличия между случаями, когда функция имеет один, два или более классов эквивалентности.

Теорема 6. Пусть сильно зависимая функция A имеет k классов эквивалентности $Z_1, \dots, Z_k$ относительно $\sim_A$. Тогда

(i) $k = 1$ тогда и только тогда, когда

$$A(X) = C_1(X_1) \circ \dots \circ C_s(X_s)$$

при некоторых функциях $C_1, \dots, C_s$, моноиде $\circ$ и разбиении $X = \bigcup_{i=1}^s X_i$, $X_i \neq \emptyset$, $1 \leq i \leq s$ и $s \geq 3$;

(ii) $k = 2$ тогда и только тогда, когда

$$A(X) = C_1(X_1) \circ C_2(X_2)$$

при некоторых функциях C_1, C_2 , операции с единицей $\circ$ и разбиении $X = X_1 \cup X_2$, $X_1 \neq \emptyset$, $X_2 \neq \emptyset$, при этом разбиения $X = X_1 \cup X_2 = Z_1 \cup Z_2$ совпадают и выполняется одно из двух условий:

- (a) $\circ$ — моноид и C_1, C_2 — $\circ$ -неразложимые функции,
- (b) $\circ$ — неассоциативная операция с единицей;

(iii) $k \geq 3$ тогда и только тогда, когда

$$A(X) = B(C_1(X_1), \dots, C_m(X_m))$$

при некоторых функциях C_i , $1 \leq i \leq m \leq n$, неразделимой операции B и $m \geq 3$, при этом $m = k$ и разбиения $X = \bigcup_{i=1}^m X_i = \bigcup_{j=1}^k Z_j$ совпадают.

Доказательство. Пусть $k = 1$ и $A(X) = B(C(X_1), X_2)$ — максимальная простая декомпозиция. Поскольку переменные из множеств X_1 и X_2 эквивалентны, найдется простая декомпозиция $A(X) = B_1(C_1(Y_1), Y_2)$, где $X_1 \cap Y_1 \neq \emptyset$, $X_2 \cap Y_1 \neq \emptyset$. В силу максимальной простой декомпозиции $X_1 \cap Y_2 \neq \emptyset$. Поэтому по пункту (iii) теоремы 5 при некоторых функциях K , F_1 , F_2 , F_3 и моноиде $\circ$ выполнено равенство

$$A(X) = K(F_1(X_1 \cap Y_2) \circ F_2(X_1 \cap Y_1) \circ F_3(X_2 \cap Y_1), X_2 \cap Y_2).$$

Отсюда в силу максимальной простой декомпозиции с множеством X_1 должно быть $X_2 \cap Y_2 = \emptyset$ и $K(y) = \gamma(y)$ — подстановка на множестве Ω . Заменяя операцию $\circ$ на изоморфную ей операцию $x * y = \gamma^{-1}(\gamma(x) \circ \gamma(y))$, получаем требуемое разложение. Обратное утверждение очевидно.

Если $k = 2$, то по пункту (ii) теоремы 5 и лемме 6 должна существовать декомпозиция

$$A(X) = C_1(Z_1) \circ C_2(Z_2).$$

В силу теоремы 1 можно считать, что операция $B(x, y) = x \circ y$ имеет единицу. Если операция $\circ$ ассоциативна, то есть является моноидом, то функции C_1 и C_2 должны быть $\circ$ -неразложимыми, так как иначе $k = 1$. Если операция $\circ$ неассоциативна, то по теореме 2 она не изоморфна никакому моноиду.

Обратно, пусть $A(X) = C_1(X_1) \circ C_2(X_2)$, $X_1 \neq \emptyset$, $X_2 \neq \emptyset$, причем выполняются условия (а) или (б). Если множества X_1 и X_2 не совпадают с классами эквивалентности, то $k = 1$ и найдется простая декомпозиция $A(X) = B(C(Y_1), Y_2)$, у которой $X_1 \cap Y_1 \neq \emptyset$ и $X_2 \cap Y_1 \neq \emptyset$. Поскольку $Y_2 \neq \emptyset$, то либо $X_1 \cap Y_2 \neq \emptyset$, либо $X_2 \cap Y_2 \neq \emptyset$. Пусть, например, $X_1 \cap Y_2 \neq \emptyset$. Тогда аналогично первому случаю

$$A(X) = F_1(X_1 \cap Y_2) * F_2(X_1 \cap Y_1) * F_3(X_2 \cap Y_1)$$

при некотором моноиде $*$, причем $X_2 \subseteq Y_1$. Отсюда,

$$\begin{aligned} F_1(X_1 \cap Y_2) * F_2(X_1 \cap Y_1) &= \gamma_1^{-1} C_1(X_1), \\ F_3(X_2 \cap Y_1) &= \gamma_2^{-1} C_2(X_2) \end{aligned}$$

при некоторых подстановках γ_1 , γ_2 , причем $x \circ y = \gamma_1(x) * \gamma_2(y)$. В силу теоремы 1 должно выполняться равенство $x \circ y = x * a^{-1} * y$ при некотором элементе $a \in \Omega$. Поэтому, подправляя функцию C_2 , можно добиться совпадения операций $x \circ y = x * y$. Получаем противоречие с условием (а).

При $k = n$ функция A неразделима. Пусть $3 \leq k < n$. В силу леммы 6

$$A(X) = B(C_1(Z_1), \dots, C_k(Z_k)).$$

Если B разделима, то получаем противоречие с определением классов эквивалентности.

Обратно, пусть

$$A(X) = B'(C'_1(X_1), \dots, C'_m(X_m)),$$

где $m \geq 3$ и B' неразделима. Докажем, что множества $X_1, \dots, X_m$ совпадают с классами эквивалентности. Предположим, что имеется класс эквивалентности Z_1 , отличный от $X_1, \dots, X_m$. Достаточно рассмотреть случай, когда $Z_1 = X_1 \cup \dots \cup X_t$, $2 \leq t \leq m$.

Если $t < m$, то по лемме 6 существует простая декомпозиция

$$A(X) = B''(C_1''(X_1), X_{t+1}, \dots, X_m).$$

По пункту (ii) теоремы 5 в этом случае должны существовать простые декомпозиции

$$C_1(Z_1) = B_i(X_1, \dots, C_i'(X_i), \dots, X_t), \quad 1 \leq i \leq t,$$

при некоторых функциях $B_1, \dots, B_t$. Применяя пункт (i) теоремы 5, получаем, что

$$B''(y, X_{t+1}, \dots, X_m) = D_i(y, X_{t+1}, \dots, C_i'(X_i), \dots, X_m)$$

при некоторых функциях D_i , $t + 1 \leq i \leq m$. Отсюда с помощью пункта (ii) теоремы 5 и индукции по t и $m - t$ получаем разложения

$$\begin{aligned} C_1(Z_1) &= F(C_1'(X_1), \dots, C_t'(X_t)), \\ B''(y, X_{t+1}, \dots, X_m) &= F'(y, C_{t+1}'(X_{t+1}), \dots, C_m'(X_m)) \end{aligned}$$

при некоторых функциях F и F' . Таким образом, справедливо равенство

$$B'(C_1'(X_1), \dots, C_m'(X_m)) = F'(F(C_1'(X_1), \dots, C_t'(X_t)), C_{t+1}'(X_{t+1}), \dots, C_m'(X_m)),$$

откуда

$$B'(y_1, \dots, y_m) = F'(F(y_1, \dots, y_t), y_{t+1}, \dots, y_m),$$

что противоречит неразделимости функции B' .

Если $t = m$, то $k = 1$. Покажем, что операция A на может быть o -разложимой. Пусть

$$A(X) = F_1(Y_1) \circ F_2(Y_2),$$

где $\circ$ — некоторый моноид и $Y_1 \neq \emptyset$, $Y_2 \neq \emptyset$. Зафиксируем все переменные внутри каждого множества X_i , за исключением одного x_{ji} , $1 \leq i \leq m$. После указанной фиксации функция A будет иметь вид

$$B'(C_1''(x_{j_1}), \dots, C_m''(x_{j_m})).$$

В силу неразделимости операции B' все переменные x_{ji} , $1 \leq i \leq m$, должны попасть в одно и то же множество, например, Y_1 . Изменяя выбор переменного x_{ji} внутри X_i , получаем, что $X_i \subseteq Y_1$ при всех $1 \leq i \leq m$. Отсюда, $Y_2 = \emptyset$. Получаем противоречие. Теорема доказана.

2.3. Каноническая декомпозиция

Определим каноническую декомпозицию функции A следующим образом. Согласно теореме 6 каждая функция имеет одно из четырех разложений, описанных в пунктах (i), (ii)(a), (ii)(b) или (iii) этой теоремы, причем все случаи взаимно исключают друг друга. Объединяя случаи (i) и (ii)(a) в один, поскольку в обоих из них функция o -разложима, как следствие теоремы 6 получаем следующее утверждение.

Рис. 3. Граф канонической декомпозиции

Предложение 1. Произвольная сильно зависимая функция A допускает разложение вида

$$A(X) = B(C_1(X_1), \dots, C_m(X_m)),$$

где B — одна из следующих функций:

- (1) $B(y_1, \dots, y_m) = y_1 \circ \dots \circ y_m$, где $2 \leq m \leq n$, $\circ$ — моноид, причем операции C_i — неразложимы, $i = 1, \dots, m$;
- (2) $B(y_1, y_2)$ — сильно зависимая операция с единицей, не изоморфная моноиду;
- (3) $B(y_1, \dots, y_m)$ неразделима и $m \geq 2$, в частности, при $m = n$ сама функция A неразделима.

Если среди операций $C_1, \dots, C_m$ есть разделимые, то они также имеют разложения

$$C_i(X_i) = B_i(C_{i,1}, \dots, C_{i,m_i}), \quad 1 \leq i \leq m,$$

вида (1), (2) или (3). Если среди операций $C_{i,j}$ есть разделимые, то продолжаем этот процесс до тех пор, пока на некотором шагу t все операции $C_{i_1, \dots, j_t}$ не будут либо неразделимыми, либо функциями одной переменной (в этом случае в силу определения сильной зависимости они должны быть подстановками). Назовем такое разложение канонической декомпозицией функции A .

Поставим в соответствие канонической декомпозиции дерево, узловые вершины которого помечены символами операций $B, B_1, \dots, B_m, \dots$, а висячие вершины помечены символами переменных x_i , либо подстановок $\gamma_i(x_i)$, $i = 1, \dots, n$. Для удобства добавим еще одну вершину x_{n+1} , соединенную ребром с корнем дерева, помеченным символом B (см. рис. 3).

Назовем число t глубиной декомпозиции.

Установим, в какой степени однозначно каждое из разложений (1), (2) и (3).

2.4. Свойство однозначности $\circ$ -разложения

Напомним, что всюду рассматриваются декомпозиции только сильно зависимых функций.

Определение 5. Пусть $\circ$ — моноид. Назовем $\circ$ -разложением операции A разложение вида

$$A(X) = C_1(X_1) \circ \dots \circ C_m(X_m),$$

в котором все операции C_i являются $\circ$ -неразложимыми, $X_i \neq \emptyset$, $i = 1, \dots, m$.

Лемма 7. Пусть $\circ$ — моноид и $A(X) = C_1(X_1) \circ \dots \circ C_m(X_m)$ — $\circ$ -разложение, $m \geq 2$. Тогда если операция $\circ$ абелева, то операция A имеет m максимальных простых декомпозиций, соответствующих множествам

$$X_1 \cup \dots \cup X_{m-i} \cup X_{m+i} \cup \dots \cup X_m, \quad i = 1, \dots, m;$$

если же операция $\circ$ неабелева, то функция A имеет ровно две максимальные простые декомпозиции, соответствующие множествам $X_1 \cup \dots \cup X_{m-1}$ и $X_2 \cup \dots \cup X_m$.

Доказательство. Пусть $A(X) = B(C(Y_1), Y_2)$ — максимальная простая декомпозиция. Покажем, что множество Y_1 есть объединение некоторых множеств X_i , $i \in \{1, \dots, m\}$. Фиксируем число i и докажем, что либо $X_i \subseteq Y_1$, либо $X_i \subseteq Y_2$. Если $X_i \cap Y_1 \neq \emptyset$ и $X_i \cap Y_2 \neq \emptyset$, то $Y_1 \setminus X_i \neq \emptyset$, в противном случае $Y_1 \subseteq X_i$, что противоречит максимальнойности множества Y_1 . В силу пункта (iii) теоремы 5 из максимальнойности множества Y_1 следует, что $Y_2 \setminus X_i = \emptyset$, таким образом, $Y_2 \subseteq X_i$. Итак,

$$X = (X_i \cap Y_1) \cup (Y_1 \setminus X_i) \cup Y_2$$

— разбиение. Для удобства обозначим множества этого разбиения через U , V и W соответственно.

Рассмотрим равенства

$$C_1(X_1) \circ \dots \circ C_i(U \cup W) \circ \dots \circ C_m(X_m) = B(C(U, V), W).$$

Пусть $i = m$ (случай $i = 1$ разбирается аналогично). В силу пункта (iii) теоремы 5

$$\begin{aligned} A(X) &= D_1(V) * D_2(U) * D_3(W), \\ B(y, W) &= \alpha(y) * F_3(W), \\ C(U \cup V) &= \alpha^{-1}(D_1(V) * D_2(U)), \\ C_m(X_m) &= D_2(U) * D_3(W), \end{aligned}$$

и

$$C_1(X_1) \circ \dots \circ C_{m-1}(X_{m-1}) \circ z = D_1(V) * \alpha(z)$$

при некоторых операциях D_1 , D_2 , D_3 и моноиде $*$.

Из последнего равенства и следствия 1 теоремы 2 вытекает, что при изменении функций D_1 , D_2 , D_3 можно добиться того, чтобы $\circ = *$. Так как при этом $\alpha(x) = b \circ x$, $b \in \Omega$, получаем противоречие с $\circ$ -разложимостью операции C_m .

Случай $2 \leq i \leq m-1$ сводится к предыдущему после фиксации всех переменных из множеств $X_{i+1}, \dots, X_m$.

Итак, для каждого $i \in \{1, \dots, m\}$ либо $X_i \subseteq Y_1$, либо $X_i \subseteq Y_2$.

Если операция $\circ$ абелева, то, очевидно, что все простые декомпозиции, соответствующие множествам

$$X_1 \cup \dots \cup X_{i-1} \cup X_{i+1} \cup \dots \cup X_m$$

будут максимальными, так как иначе Y_1 не является объединением множеств X_i , $1 < i < m$.

Пусть $\circ$ неабелева. Две простые декомпозиции, соответствующие множествам вида $X_1 \cup \dots \cup X_{m-1}$, $X_2 \cup \dots \cup X_m$, будут максимальными по тем же соображениям. Докажем, что других нет.

Пусть $Y_1 = X_{i_1} \cup \dots \cup X_{i_s}$, $1 \leq s < m$. Если $X_1 \subseteq Y_2$ ($X_m \subseteq Y_2$), то в силу максимальности по включению множества Y_1 справедливо равенство $X_1 = Y_2$ ($X_m = Y_2$), и утверждение доказано. Рассмотрим случай $X_1 \cup X_m \subseteq Y_1$. Пусть $X_i \subseteq Y_2$, $1 < i < m$. Зафиксировав все переменные в множествах $X_2, \dots, X_{i-1}, X_{i+1}, \dots, X_{m-1}$ так, чтобы выполнялись равенства $C_2 \circ \dots \circ C_{i-1} = e$ и $C_{i+1} \circ \dots \circ C_{m-1} = e$, где e — единица моноида $\circ$, получаем равенство

$$C_1(X_1) \circ C_i(X_i) \circ C_m(X_m) = B'(C'(X_1, X_m), X_i).$$

Фиксируя теперь сначала все переменные из множества X_1 так, чтобы $C_1 = e$, а затем из множества X_m так, чтобы $C_m = e$, получаем соответственно равенства

$$C_i(X_i) \circ C_m(X_m) = B'(C'_1(X_m), X_i),$$

$$C_1(X_1) \circ C_i(X_i) = B'(C'_2(X_1), X_i).$$

Учитывая пункт (i) теоремы 5, убеждаемся, что при некоторых подстановках γ_1 и γ_2 должны выполняться равенства

$$C_i(X_i) \circ \gamma_1(y) = B'(y, X_i),$$

$$\gamma_2(z) \circ C_i(X_i) = B'(z, X_i).$$

Отсюда при $z = y$ и $u = C_i(X_i)$ получаем равенство

$$u \circ \gamma_1(y) = \gamma_2(y) \circ u.$$

При $u = e$ получаем равенство $\gamma_1 = \gamma_2$, что противоречит коммутативности операции $\circ$. Лемма доказана.

Теорема 7. Пусть $\circ$ — моноид и

$$A(X) = C_1(X_1) \circ \dots \circ C_m(X_m)$$

— некоторое $\circ$ -разложение, $m \geq 2$. Тогда

(1) функция A $\ast$ -разложима только относительно тех моноидов $\ast$, которые получаются из $\circ$ по правилам $x \ast y = x \circ a \circ y$ или $x \ast y = y \circ b \circ x$, $a, b \in \Omega$.

(2) Любое другое $\circ$ -разложение функции A имеет вид

$$A(X) = B_1(Y_1) \circ \dots \circ B_m(Y_m),$$

где

- (а) если операция $\circ$ абелева, то при некоторой подстановке $\pi = (\pi(1), \dots, \pi(m))$ и некоторых элементах $a_i \in \Omega$, $1 \leq i \leq m$, $a_1 \circ \dots \circ a_m = e$, где e — единичный элемент моноида $\circ$, выполняются равенства

$$B_i(Y_i) = C_{\pi(i)}(X_{\pi(i)}) \circ a_i, \quad 1 \leq i \leq m;$$

- (б) если операция $\circ$ неабелева, то при некоторых $a_i, b_i \in \Omega$, $a_1 = b_m = e$, $a_i = b_{i-1}^{-1} = e$, $2 \leq i \leq m$, выполняются равенства

$$B_i(Y_i) = a_i \circ C_i(X_i) \circ b_i, \quad 1 \leq i \leq m.$$

Доказательство. Докажем первое утверждение. Пусть $A(X) = B_1(Y_1) * \dots * B_k(Y_k)$ — некоторое другое разложение, $k \geq 2$, $*$ $\neq \circ$.

Сначала покажем, что разбиения

$$X = \bigcup_{i=1}^m X_i, \quad X = \bigcup_{j=1}^k Y_j$$

совпадают.

Если число максимальных простых декомпозиций функции A больше двух, то моноиды $*$ и $\circ$ абелевы. В этом случае подмножества из обоих разбиений соответствуют максимальным простым декомпозициям, и поэтому разбиения совпадают. Следовательно, $k = m$ и $Y_i = X_{\pi(i)}$, $1 \leq i \leq m$, при некоторой перестановке $\pi = (\pi(1), \dots, \pi(m))$.

Пусть имеется ровно две максимальные простые декомпозиции. Если они соответствуют непересекающимся множествам, то $k = m = 2$ и доказательство аналогично.

Рассмотрим случай, когда максимальные простые декомпозиции соответствуют пересекающимся множествам. В этом случае по лемме 7 $k \geq 3$, $m \geq 3$ и моноиды $\circ$ и $*$ неабелевы. При этом либо $X_1 = Y_1$ и $X_m = Y_k$, либо $X_1 = Y_k$ и $X_m = Y_1$. Фиксируя все переменные из множества X_1 и применяя индукцию, убеждаемся, что $k = m$ и разбиения совпадают.

Найдем соотношение между операциями $\circ$ и $*$.

Если обе операции абелевы, то не уменьшая общности, можно положить $X_i = Y_i$, $1 \leq i \leq m$. Зафиксируем все переменные из множества

$$X_2 \cup \dots \cup X_{m-1} = Y_2 \cup \dots \cup Y_{m-1}$$

так, чтобы

$$B_2(Y_2) * \dots * B_{m-1}(Y_{m-1}) = e^*,$$

где e^* — единица моноида $*$. Получаем равенство

$$C_1(X_1) * c * C_m(X_m) = B_1(Y_1) * B_m(Y_m) \quad (5)$$

при некотором $c \in \Omega$. Фиксируя теперь контрольными элементами все переменные, кроме одного, из каждого из множеств X_1 и X_m с помощью пункта (i) теоремы 5 и следствия 1 теоремы 2 убеждаемся, что $x * y = x \circ a \circ y$ при некотором $a \in \Omega$.

Если обе операции неабелевы, то возможен случай $X_1 = Y_m$ и $X_m = Y_1$. В этом случае из равенства (5) аналогично получаем равенство $x * y = y \circ b \circ x$ при некоторых $a, b \in \Omega$.

Докажем второе утверждение. Пусть имеется другое $\circ$ -разложение функции A

$$A(X) = B_1(Y_1) \circ \dots \circ B_m(Y_m).$$

Если операция $\circ$ абелева и $Y_i = X_{\pi(i)}$, $1 \leq i \leq m$, то применяя пункт (i) теоремы 5 и следствие 1 теоремы 2 получаем, что

$$B_i(Y_i) = C_{\pi(i)}(X_{\pi(i)}) \circ a_i,$$

причем $a_1 \circ \dots \circ a_m = e$.

Если операция $\circ$ неабелева, то по пункту (ii) теоремы 6 должны выполняться равенства $X_i = Y_i$, $1 \leq i \leq m$ (случай $x \circ y = y \circ a \circ x$ невозможен, так как в этом случае $a = e$ и операция $\circ$ должна быть абелевой). Отсюда с помощью фиксации переменных убеждаемся, что

$$B_i(Y_i) = a_i \circ C_i(X_i) \circ b_i, \quad 1 \leq i \leq m,$$

при некоторых $a_i, b_i \in \Omega$, причем должны выполняться равенства $a_1 = b_m = e$, $a_i = b_{i-1}^{-1} = e$, $2 \leq i \leq m$.

Теорема доказана.

Следствие 2. С точностью до главной изострофии m -моноида $y_1 \circ \dots \circ y_m$ $\circ$ -разложение однозначно.

Строение групп главных автострофий m -моноидов будет приведено ниже.

2.5. Свойство однозначности канонической декомпозиции

Покажем, что в двух оставшихся случаях (2) и (3) из предложения 1 разложение также будет однозначным с точностью до главной изострофии операции $B(y_1, \dots, y_m)$.

Теорема 8. Пусть $\circ$ — неассоциативная бинарная операция и

$$A(X) = C_1(X_1) \circ C_2(X_2)$$

— $\circ$ -разложение, причем функции C_1 и C_2 $\circ$ -неразложимы. Тогда всякое другое $*$ -разложение функции A имеет вид

$$A(X) = B_1(Y_1) * B_2(Y_2),$$

где либо

$$X_1 = Y_1, \quad X_2 = Y_2, \quad x * y = (x * a) \circ (b * y), \quad C_1 = B_1 * a, \quad C_2 = b * B_2,$$

либо

$$X_1 = Y_2, \quad X_2 = Y_1, \quad x * y = (y * b) \circ (a * x), \quad C_1 = a * B_1, \quad C_2 = B_2 * b.$$

Теорема 9. Если сильно зависящая функция A допускает разложение вида

$$A(X) = B(C_1(X_1), \dots, C_m(X_m)),$$

где $B(y_1, \dots, y_m)$ неразделима и $3 \leq m < n$, то всякое другое разложение функции A имеет вид

$$A(X) = B'(D_1(Y_1), \dots, D_k(Y_k)),$$

где $B'(y_1, \dots, y_k)$ неразделима, $k = m$ и выполняются равенства

$$D_i(Y_i) = \gamma_i C_{\pi(i)}(X_{\pi(i)}), \quad 1 \leq i \leq m,$$

при некоторой перестановке $\pi = (\pi(1), \dots, \pi(m))$, причем

$$B(y_1, \dots, y_m) = B'(\gamma_1(y_{\pi(1)}), \dots, \gamma_m(y_{\pi(m)})).$$

Утверждения обеих теорем также вытекает из теоремы 5 и пункта (iii) теоремы 6.

Следствие 3. В условиях предложения 1 σ -разложение однозначно с точностью до главной изострофии операции $B(y_1, \dots, y_m)$.

Таким образом, хотя одной сильно зависимой функции может соответствовать несколько различных канонических декомпозиций, из приведенных выше условий однозначности следует, что двум различным каноническим декомпозициям соответствуют изоморфные деревья, причем соответствующие при изоморфизме вершины отвечают главноизотопным операциям. Более общо, этот факт можно сформулировать следующим образом.

Теорема 10. Пусть A и A' — две главноизострофные сильно зависимые n -арные операции. Тогда их каноническим декомпозициям соответствуют изоморфные деревья, причем соответствующим друг другу при изоморфизме вершинам отвечают главноизострофные компоненты.

Доказательство. Воспользуемся индукцией по глубине канонической декомпозиции операций. Пусть (σ, α) — главная изострофия и выполняется равенство

$$A(x_1, \dots, x_n) = \alpha_{n+1}^{-1} A'(\alpha_1(x_{\sigma(1)}), \dots, \alpha_n(x_{\sigma(n)})),$$

где $\alpha = (\alpha_1, \dots, \alpha_{n+1})$ — изотопия, а $(\sigma(1), \dots, \sigma(n))$ — перестановка. Рассмотрим те разложения этих операций

$$A(X) = B(C_1(X_1), \dots, C_m(X_m)),$$

$$A'(X) = B'(C'_1(X_1), \dots, C'_{m'}(X_{m'})),$$

в которых операции B и B' соответствуют корневым вершинам деревьев их канонических декомпозиций. В силу определения изострофии и условий (1), (2) и (3) предложения 1, определяющих вид канонического разложения, получаем, что $m = m'$, причем операции B и B' должны быть связаны соотношением

$$B(y_1, \dots, y_m) = \alpha_{n+1}^{-1} B'(\gamma_1(y_{\pi(1)}), \dots, \gamma_m(y_{\pi(m)})),$$

где $\gamma_1, \dots, \gamma_m$ — подстановки множества Ω , а $(\pi(1), \dots, \pi(m))$ — некоторая перестановка. При этом должны выполняться равенства

$$C'_i(Y_i) = \gamma_i^{-1} C_{\pi(i)}^{(\sigma, \alpha)}, \quad 1 \leq i \leq m,$$

где операции $C_{\pi(i)}^{(\sigma, \alpha)}$ получены из операций $C_{\pi(i)}$ применением изострофии (σ, α) , то есть вместо переменных x_j стоят $\alpha_j(x_{\sigma(j)})$, $j = 1, \dots, n$. В силу предположения индукции деревья канонических декомпозиций операций C'_i и $C_{\pi(i)}^{(\sigma, \alpha)}$ (а следовательно, и $C_{\pi(i)}$) изоморфны, $1 \leq i \leq m$. Поэтому деревья канонических декомпозиций операций A и A' также изоморфны. Теорема доказана.

Для n -квазигрупп с учетом их обратимости по каждой переменной данный результат можно сформулировать в виде следующего утверждения.

Теорема 11. Деревья канонических декомпозиций изострофных квазигрупп являются изоморфными графами, причем в случае главной изострофии корень одного дерева переходит в корень другого.

Доказательство аналогично.

3. Группы инерции бесповторной суперпозиции

Рассмотрим общее описание групп автотопий и автострофий разделимых сильно зависимых k -значных функций. При $k = 2$ эта задача сводится к описанию групп инерции двоичных функций, представимых в виде бесповторной суперпозиции, в группах инвертирования и перестановок переменных.

3.1. Группы автотопий бесповторной суперпозиции

Всюду в этой главе предполагаем, что все рассматриваемые функции являются сильно зависимыми.

В основе описания групп инерции разделимых функций лежит следующая теорема.

Теорема 12. Если функция f допускает бесповторную декомпозицию

$$f(x_1, \dots, x_n) = A(B(x_1, \dots, x_k), x_{k+1}, \dots, x_n), \quad 1 \leq k \leq n,$$

то группа автотопий $\text{Atp}(f)$ состоит из таких преобразований $(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$, для которых при некоторой подстановке $\beta \in S(\Omega)$

$$\begin{aligned} (\alpha_1, \dots, \alpha_k, \beta) &\in \text{Atp}(B), \\ (\beta, \alpha_{k+1}, \dots, \alpha_{n+1}) &\in \text{Atp}(A). \end{aligned}$$

Доказательство получается путем применения теоремы 5 (случай (i)) к равенству

$$\begin{aligned} f(x_1, \dots, x_n) &= A(B(x_1, \dots, x_k), x_{k+1}, \dots, x_n) \\ &= \alpha_{n+1}^{-1} A(B(\alpha_1(x_1), \dots, \alpha_k(x_k)), \alpha_{k+1}(x_{k+1}), \dots, \alpha_n(x_n)). \end{aligned}$$

Следствие 4. Если $X = \bigcup_{i=1}^m X_i$ — разбиение и

$$f(X) = A(B_1(X_1), \dots, B_m(X_m)), \quad (6)$$

то группа автотопий $\text{Atp}(f)$ состоит из тех и только тех преобразований

$$(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) = (\alpha^{(1)}, \dots, \alpha^{(m)}, \alpha_{n+1}),$$

где $\alpha^{(j)}$ — вектор, составленный из компонент вектора $(\alpha_1, \dots, \alpha_n)$, соответствующих переменным из множества X_j , $j = 1, \dots, m$, для которых при некоторых подстановках $\beta_1, \dots, \beta_m \in S(\Omega)$ выполняются включения

$$\begin{aligned} (\alpha^{(i)}, \beta_i) &\in \text{Atp}(B_i), \quad i = 1, \dots, m, \\ (\beta_1, \dots, \beta_m, \alpha_{n+1}) &\in \text{Atp}(A). \end{aligned}$$

Утверждение очевидным образом вытекает из теоремы 12.

Замечание 1. При описании групп главных автотопий $\text{Atp}(f)$, состоящих из преобразований вида $(\alpha_1, \dots, \alpha_n, \varepsilon)$, для функций вида (6) приходится изучать группы $\text{Atp}^\circ(A)$ и $\text{Atp}(B_1), \dots, \text{Atp}(B_m)$, а не $\text{Atp}^\circ(B_1), \dots, \text{Atp}^\circ(B_m)$.

Следствие 5. При выполнении условий предыдущего следствия соответствие

$$(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) \mapsto (\beta_1, \dots, \beta_m, \alpha_{n+1})$$

задает гомоморфизм группы $\text{Atp}(f)$ в группу $\text{Atp}(A)$, ядром которого является прямое произведение групп главных автотопий операций $B_1, \dots, B_m$. В частности, справедливы верхние оценки

$$|\text{Atp}(f)| \leq |\text{Atp}(A)| \prod_{i=1}^m |\text{Atp}(B_i)|,$$

$$|\text{Atp}^\circ(f)| \leq |\text{Atp}^\circ(A)| \prod_{i=1}^m |\text{Atp}(B_i)|.$$

Если группы (главных) автотопий функций $A, B_1, \dots, B_m$ тривиальны, то тривиальна и группа (главных) автотопий функции $f(X) = A(B_1(X_1), \dots, B_m(X_m))$.

Следствие 6. Если функция f допускает итеративную декомпозицию вида

$$f(X) = A_m(X_m, A_{m-1}(\dots A_2(X_2, A_1(X_1)), \dots),$$

где $X = \bigcup_{i=1}^m X_i$ — разбиение, то группа $\text{Atp}(f)$ состоит из тех и только тех преобразований

$$(\alpha_1, \dots, \alpha_n, \alpha_{n+1}) = (\alpha^{(1)}, \dots, \alpha^{(m)}, \alpha_{n+1}),$$

для которых при некоторых подстановках $\beta_1, \dots, \beta_{m-1} \in S(\Omega)$ выполняются включения

$$(\alpha^{(1)}, \beta_1) \in \text{Atp}(A_1),$$

$$(\beta_{i-1}, \alpha^{(i)}, \beta_i) \in \text{Atp}(A_i), \quad i = 2, \dots, m-1,$$

$$(\beta_{m-1}, \alpha^{(m)}, \alpha_{n+1}) \in \text{Atp}(A_m).$$

Как и в предыдущем случае, справедливы оценки

$$|\text{Atp}(f)| \leq |\text{Atp}(A_1)| \dots |\text{Atp}(A_m)|,$$

$$|\text{Atp}^\circ(f)| \leq |\text{Atp}^\circ(A_1)| \dots |\text{Atp}^\circ(A_m)|.$$

3.2. Вполне приводимые сильно зависимые функции

Вполне приводимые функции — это функции, построенные с помощью операции бесповторной суперпозиции из бинарных операций.

Заметим, что с точностью до главной изотопии можно считать, что все бинарные операции, участвующие в записи этой функции, имеют единичные элементы.

Теорема 13. Всякая вполне приводимая сильно зависимая функция $f(x_1, \dots, x_n)$, заданная бесповторной формулой $A(x_1, \dots, x_n, *_2, \dots, *_n)$ с бинарными операциями $*_2, \dots, *_n$, главноизотопна вполне приводимой функции, которую можно задать формулой $A(x_1, \dots, x_n, o_2, \dots, o_n)$, полученной из предыдущей формулы путем замены операций $*_2, \dots, *_n$ на некоторые бинарные операции с единицей $o_2, \dots, o_n$ соответственно.

Доказательство проводится индукцией по рангу формулы с применением теоремы 1.

В случае, когда операции $*_i$, $i = 2, \dots, n$, ассоциативны, можно получить более подробное описание строения их групп автотопий. Рассмотрим такое описание на примере итеративной декомпозиции.

Теорема 14. Если функция f имеет вид

$$f(x_1, \dots, x_n) = (\dots (x_1 *_2 x_2) \dots *_n x_n),$$

где $*_2, \dots, *_n$ — моноиды, то группа $\text{Atp}(f)$ состоит из тех и только тех преобразований $(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$, для которых выполняются следующие свойства:

- (а) $\alpha_i \in \text{Hol}(*_i)$, то есть $\alpha_i(x) = \xi_i(x) *_i a_i$, где $\xi_i(x) \in \text{Aut}(*_i)$, $\alpha_i \in \Omega^{*i}$ — обратимый элемент моноида $*_i$, $i = 2, \dots, n$,
- (б) при некоторых $b_2 \in \Omega^{*2}, \dots, b_n \in \Omega^{*n}$ для постановок $\beta_1, \dots, \beta_n$, определяемых равенствами

$$\begin{aligned} \beta_1 &= \alpha_1, \\ \beta_i(x) &= b_i *_i \xi_i(x) *_i a_i, \quad i = 2, \dots, n-1, \\ \beta_n &= \alpha_{n+1}, \end{aligned}$$

выполняются тождества

$$\beta_i(x) = \beta_{i-1}(x) *_i a_i, \quad i = 2, \dots, n.$$

Доказательство. Положим $\beta_1 = \alpha_1$, $\beta_n = e$. Согласно следствию 6 найдутся подстановки $\beta_2, \dots, \beta_{n-1} \in S(\Omega)$ такие, что

$$(\beta_{i-1}, \alpha_i, \beta_i) \in \text{Atp}(*_i), \quad i = 2, \dots, n,$$

или

$$\beta_i(x_{i-1} *_i x_i) = \beta_{i-1}(x_{i-1}) *_i \alpha_i(x_i), \quad i = 2, \dots, n. \quad (7)$$

Отсюда,

$$\beta_i(x) = \beta_{i-1}(e_i) *_i \alpha_i(x),$$

где через e_i обозначена единица моноида $*_i$, $i = 2, \dots, n$. Положим b_i равными $\beta_{i-1}(e_i)$, $i = 2, \dots, n$.

Учитывая строение групп $\text{Atp}(*_i)$, $i = 2, \dots, n$ (см. теорему 3), получаем, что

$$\alpha_i(x) = \xi_i(x) *_i a_i, \quad i = 2, \dots, n,$$

где $\xi_i \in \text{Aut}(*_i)$, $i = 2, \dots, n$, — обратимый элемент моноида $*_i$, откуда

$$\beta_i(x) = b_i *_i \xi_i(x) *_i a_i, \quad i = 2, \dots, n.$$

С другой стороны, из равенства (7) получаем, что

$$\beta_i(x) = \beta_{i-1}(x) *_i \alpha_i(e_i) = \beta_{i-1}(x) *_i a_i, \quad i = 2, \dots, n.$$

Теорема доказана.

Эта теорема позволяет вычислить группы инерции итеративных сильно зависимых функций данного вида в различных подгруппах группы изотопий.

Следствие 7. Пусть $G = (\Omega, *)$ — моноид и

$$f(x_1, \dots, x_n) = x_1 * \dots * x_n.$$

Тогда если операция $*$ неабелева, то группа $\text{Atp}(f)$ имеет порядок $|G^*|^{n+1} |\text{Aut}(G)|$ и состоит из преобразований вида $(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$, где

$$\begin{aligned}\alpha_i(x) &= a_i^{-1} * \xi(x) * a_{i+1}, & i &= 1, \dots, n, \\ \alpha_{n+1}(x) &= a_1^{-1} * \xi(x) * a_{n+1}\end{aligned}$$

при некоторых $a_1, \dots, a_{n+1} \in G^*$, $\xi \in \text{Aut}(G)$; если же операция $*$ абелева, то группа $\text{Atp}(f)$ имеет порядок $|G^*|^n |\text{Aut}(G)|$ и состоит из преобразований вида $(\alpha_1, \dots, \alpha_n, \alpha_{n+1})$, где

$$\begin{aligned}\alpha_i(x) &= \xi(x) * a_i, & i &= 1, \dots, n, \\ \alpha_{n+1}(x) &= \xi(x) * a_1 * \dots * a_n\end{aligned}$$

при некоторых $a_1, \dots, a_n \in G^*$, $\xi \in \text{Aut}(G)$.

Утверждение непосредственно вытекает из теоремы 14.

3.3. Группы автострофий бесповторной суперпозиции

В отличие от случая групп автоотопий, для описания групп инерции сильно зависимых функций в группе изострофий и ее подгруппах приходится, по существу, использовать свойство единственности разложения функции в бесповторную суперпозицию заданного вида.

Теорема 15. Пусть сильно зависимая функция f при некотором нетривиальном разбиении $X = \bigcup_{i=1}^m X_i$ представима в виде

$$f(x_1, \dots, x_n) = A(B_1(X_1), \dots, B_m(X_m)),$$

где операции $A, B_1, \dots, B_m$ удовлетворяют одному из трех условий:

- (а) $m \geq 2$, $A(y_1, \dots, y_m) = y_1 * \dots * y_m$, где $(\Omega, *)$ — моноид, а операции $B_1, \dots, B_m$ $*$ -неразложимы;
- (б) $A(y_1, y_2) = y_1 * y_2$, где $\circ$ — неассоциативная бинарная операция с единицей, неизотопная моноиду, B_1, B_2 — произвольные операции;
- (в) $A(y_1, \dots, y_m)$ неразделима, $m \geq 3$, $B_1, \dots, B_m$ — произвольные операции.

Тогда существует гомоморфизм группы $([S(\Omega)]S_n \times S(\Omega))_f$ в группу $([S(\Omega)]S_m \times S(\Omega))_A$, ядро которого есть прямое произведение групп $([S(\Omega)]S_{n_i})_{B_i}$, $n_i = |X_i|$, $i = 1, \dots, m$.

Доказательство. Как вытекает из теорем 7, 8 и 9, при выполнении условий (а)–(в) для любой автострофии вида

$$((\alpha_1, \alpha_2, \dots, \alpha_n, \alpha_{n+1}), \pi) = ((\alpha, \alpha_{n+1}), \pi) \in ([S(\Omega)]S_n \times S(\Omega))_f$$

из равенства

$$A(B_1, \dots, B_m) = \alpha_{n+1}^{-1} A(B_1^{(\alpha, \pi)}, \dots, B_m^{(\alpha, \pi)})$$

следует, что при некоторой главной изотопии $\beta = (\beta_1, \dots, \beta_m)$ и парастрофии

$$\bar{\pi} = \begin{pmatrix} 1, & \dots & m \\ \text{bar } \pi(1) & \dots & \bar{\pi}(m) \end{pmatrix}$$

должны выполняться равенства

$$\begin{aligned} A(y_1, \dots, y_m) &= \alpha_{n+1}^{-1} A(\beta_1(y_{\bar{\pi}(1)}), \dots, \beta_1(y_{\bar{\pi}(m)})), \\ B_j^{(\alpha, \pi)}(X_j) &= \beta_j^{-1} B_{\bar{\pi}(j)}(X_{\bar{\pi}(j)}), \quad j = 1, \dots, m. \end{aligned}$$

Отсюда получаем, что

$$((\beta, \alpha_{n+1}), \bar{\pi}) \in ([S(\Omega)]S_m \times S(\Omega))_A.$$

Наконец, очевидно, что соответствие

$$((\alpha, \alpha_{n+1}), \pi) \mapsto ((\beta, \alpha_{n+1}), \bar{\pi})$$

является гомоморфизмом, ядром которого является прямое произведение групп $([S(\Omega)]S_{n_i})_{B_i}$, $i = 1, \dots, m$.

Следствие 8. В условиях теоремы 15 справедливы оценки

$$\begin{aligned} |[S(\Omega)]S_n \times S(\Omega)]_f| &\leq |[S(\Omega)]S_m \times S(\Omega)]_A| \left| \prod_{i=1}^m ([S(\Omega)]S_{n_i})_{B_i} \right|, \\ |[S(\Omega)]S_n]_f| &\leq |[S(\Omega)]S_m]_A| \left| \prod_{i=1}^m ([S(\Omega)]S_{n_i})_{B_i} \right|, \\ |(S_n)_f| &\leq |[S(\Omega)]S_m]_A| \left| \prod_{i=1}^m (S_{n_i})_{B_i} \right| \end{aligned}$$

Теорема 15 позволяет описывать строение групп автострофий произвольных разделенных сильно зависимых функций по их канонический декомпозиции. Точнее, с ее помощью удастся свести задачу описания группы главных автострофий (и ее подгрупп) к задачам описания строения групп главных автострофий и проверке эквивалентности функций относительно группы главных изострофий функций, являющихся компонентами канонической декомпозиции.

Случай вычисления произвольных (не главных) автострофий для n -арных квазигрупп описывает следующая теорема.

Теорема 16. Соответствие, при котором каждой автострофии (α, π) n -квазигруппы f ставится в соответствие ее компонента паратопии π , задает гомоморфизм группы $\text{Ast}(f)$ автострофий операции f в группу автоморфизмов дерева D_f ее канонической декомпозиции

$$\text{Ast}(f) \mapsto \text{Aut}(D_f),$$

ядром которого является группа автоморфизмов $\text{Atp}(f)$.

Доказательство проводится аналогично доказательству теоремы 15 с учетом теоремы 10.

3.4. Группы автострофий $*$ -разложимых функций

Особо рассмотрим описание групп изострофий для $*$ -разложимых сильно зависимых функций.

Здесь оказывается полезной следующая теорема.

Теорема 17. Пусть функция имеет вид

$$A(y_1, \dots, y_m) = y_1 * \dots * y_m,$$

где $(\Omega, *)$ — моноид и $\text{Ast}^\circ(A) = ([S(\Omega)]S_m \times S(\Omega))_A$ — группа главных автострофий функции A . Тогда

(а) если операция $*$ абелева, то выполняется равенство

$$\text{Ast}^\circ(A) = \text{Atp}(A)S_m,$$

(б) если операция $*$ неабелева и не имеет антиизоморфизма, то выполняется равенство

$$\text{Ast}^\circ(A) = \text{Atp}(A),$$

если антиизоморфизм существует, то

$$|\text{Ast}^\circ(A)| = 2|\text{Atp}(A)|.$$

Доказательство. В случае (а) утверждение очевидно.

Докажем, что в случае (б) все автострофии имеют вид (α, π) , где $\pi = \varepsilon$ или

$$\pi = \begin{pmatrix} 1 & 2 & \dots & m-1 & m \\ m & m-1 & \dots & 2 & 1 \end{pmatrix}. \quad (8)$$

Рассмотрим равенство

$$y_1 * \dots * y_n = \alpha_{m+1}^{-1}(\alpha_1(y_{\pi(1)}) * \dots * \alpha_m(y_{\pi(m)})).$$

Так как операция $*$ неабелева, имеется ровно две максимальные простые декомпозиции (см. лемму 7). Поэтому либо $\pi(1) = 1, \pi(m) = m$, либо $\pi(1) = m, \pi(m) = 1$. Фиксируя значения переменных $y_{\pi(1)}$ и $y_{\pi(m)}$ и применяя индукцию, получаем, что либо $\pi = \varepsilon$, либо π имеет вид (8).

Если операция $*$ не имеет антиизоморфизма, то для всех подстановок (α, π) из $\text{Ast}^\circ(A)$ справедливо равенство $\pi = \varepsilon$ и поэтому

$$\text{Ast}^\circ(A) = \text{Atp}(A).$$

Пусть найдется преобразование $(\alpha, \pi) \in \text{Ast}^\circ(A)$, для которого подстановка π имеет вид (8). Покажем, что это возможно в том и только том случае, когда операция $*$ имеет антиизоморфизм. Зафиксируем переменные $y_2, \dots, y_{m-1}$ так, чтобы

$$y_2 * \dots * y_{m-1} = e,$$

где e — единица моноида $*$. Тогда должно выполняться равенство

$$y_1 * y_m = \alpha_{m+1}^{-1}(\alpha_m(y_m) * \alpha'_1(y_1))$$

при некоторой подстановке α'_1 . По лемме 4 это равенство равносильно существованию антиизоморфизма у моноида $*$.

Поскольку при гомоморфизме $(\alpha, \pi) \mapsto \pi$ ядром является группа $\text{Atp}(A)$, в данном случае

$$|\text{Ast}^\circ(A)| = 2|\text{Atp}(A)|.$$

Теорема доказана.

Приведем для иллюстрации доказанных выше результатов описание групп главных автострофий сильно зависящих функций, допускающих декомпозицию вида

$$f(X) = A(X_1) * A(X_2) * \dots * A(X_m),$$

где $X = \bigcup_{i=1}^m X_i$ — некоторое разбиение, $|X| = n$, $*$ — коммутативный моноид, а функция A является $*$ -неразложимой.

Опишем группу главных автострофий

$$\text{Ast}^\circ(f) = ([S(\Omega)]S_n \times S(\Omega))_f.$$

Согласно теореме 15, группа $\text{Ast}^\circ(f)$ допускает гомоморфизм в группу $\text{Ast}^\circ(\bar{f})$, где $\bar{f} = y_1 * y_2 * \dots * y_m$, ядром которого является прямое произведение групп

$$([S(\Omega)]S_{n_1})_A \times \dots \times ([S(\Omega)]S_{n_m})_A.$$

Найдем образ гомоморфизма.

По теореме (15) каждой автострофии вида

$$(\alpha, \alpha_{n+1}, \pi) \in ([S(\Omega)]S_n \times S(\Omega))_f$$

при гомоморфизме соответствует изострофия $(\beta, \alpha_{n+1}, \bar{\pi})$ для некоторых главной изотопии $\beta = (\beta_1, \dots, \beta_m)$ и парастрофии

$$\bar{\pi} = \begin{pmatrix} 1 & \dots & m \\ \bar{\pi}(1) & \dots & \bar{\pi}(m) \end{pmatrix},$$

причем выполняются равенства

$$\begin{aligned} y_1 * \dots * y_m &= \alpha_{n+1}^{-1}(\beta_1(y_{\bar{\pi}(1)}), \dots, \beta_m(y_{\bar{\pi}(m)})), \\ A_j^{(\alpha, \pi)}(X_j) &= \beta_j^{-1} A_{\bar{\pi}(j)}(X_{\bar{\pi}(j)}), \quad j = 1, \dots, m. \end{aligned}$$

Сначала покажем, что достаточно ограничиться случаем $\bar{\pi} = \varepsilon$. Действительно, при гомоморфизме группы $\text{Ast}^\circ(f)$ в группу S_m , задаваемом соответствием

$$(\alpha, \alpha_{n+1}, \pi) \mapsto (\beta, \alpha_{n+1}, \bar{\pi}) \mapsto \bar{\pi},$$

образом является вся группа S_m . Это объясняется тем, что, как легко вытекает из вида функции f , всегда выполняется включение

$$([S(\Omega)]S_{n_1})_A S_m \leq ([S(\Omega)]S_n)_f,$$

где $n_i = |X_i|$, $i = 1, \dots, m$, $n_1 = \dots = n_m$ (равенство здесь выполняется не всегда и зависит как от вида преобразований из группы $\text{Ast}^\circ(A)$, так и от строения группы квазиавтоморфизмов $\text{Hol}(*)$). Поэтому достаточно описать только ядро этого гомоморфизма (обозначим его R), которое содержится в прямом произведении групп автострофий:

$$R \leq ([S(\Omega)]S_{n_1} \times S(\Omega))_A \times \dots \times ([S(\Omega)]S_{n_m} \times S(\Omega))_A \cong (\text{Atp}^\circ(A))^m.$$

Найдем порядок группы R . При указанном в теореме (15) гомоморфизме образ группы R будет содержаться в группе $\text{Atp}(\bar{f})$. Учитывая следствие 7, можно описать строение группы $\text{Atp}(\bar{f})$, которая имеет порядок $|G^*|^m |\text{Aut}(G)|$, где $G = (\Omega, *)$, и состоит из преобразований $(\beta, \alpha_{n+1}) = ((\beta_1, \dots, \beta_m), \alpha_{n+1})$, где

$$\begin{aligned}\beta_i(x) &= \xi(x) * a_i, & i &= 1, \dots, m, \\ \alpha_{n+1}(x) &= \xi(x) * a_1 * \dots * a_m, & a_1, \dots, a_m &\in G^*, \quad \xi \in \text{Aut}(G).\end{aligned}$$

Поэтому $\beta_1, \dots, \beta_m, \alpha_{n+1} \in \text{Hol}(G)$. Заметим, что у всех подстановок $\beta_i, i = 1, \dots, m$, и α_{n+1} должен быть один и тот же автоморфизм $\xi \in \text{Aut}(G)$, причем квазиавтоморфизм α_{n+1} однозначно находится по квазиавтоморфизмам $\beta_1, \dots, \beta_m$.

Обозначим через $\tilde{R}$ образ группы R при гомоморфизме

$$R \rightarrow \text{Aut}(G),$$

задаваемом соответствием

$$(\alpha_1, \dots, \alpha_m, \alpha_{n+1}, \pi) \mapsto \alpha_{n+1} \mapsto \xi.$$

Ядро R_0 этого гомоморфизма содержится в группе

$$([S(\Omega)]S_{n_1} \times \Sigma(G))_A \times \dots \times ([S(\Omega)]S_{n_m} \times \Sigma(G))_A,$$

где $\Sigma(G)$ — группа регулярных подстановок моноида $(\Omega, *)$.

Заметим, что элементы a_i , которые могут появляться в компонентах $\beta_i(x) = x * a_i$, $i = 1, \dots, m$, соответствующих элементам ядра R_0 , образуют подгруппу H в группе G^* , причем

$$|R_0| = |H|^m |([S(\Omega)]S_{n_1})_A|^m.$$

Поэтому порядок группы $\text{Ast}^\circ(f)$ равен

$$|\tilde{R}| |R_0| m! = |\tilde{R}| |([S(\Omega)]S_{n_1})_A|^m |H|^m m!,$$

где $|\tilde{R}| \leq |\text{Aut}(G)|$, $|H| \leq |G^*| \leq |\Omega|$. Таким образом, задача нахождения порядка группы $\text{Ast}^\circ(f)$ свелась к задаче вычисления порядков групп $([S(\Omega)]S_{n_1})_A$, $\tilde{R}$ и H , которые зависят от вида операций A и $*$.

Найдем порядок группы $([S(\Omega)]S_n)_f$. Данный случай легко получается из предыдущего с учетом дополнительного условия, что $a_{n+1} = e$ — единица моноида $(\Omega, *)$. Отсюда, $\xi = \varepsilon$ и $|\tilde{R}| = 1$, причем $a_1 * \dots * a_n = e$. По произвольным элементам $a_1, \dots, a_{m-1} \in H$ однозначно находится элемент $a_m \in H$, поэтому

$$|([S(\Omega)]S_n)_f| = |([S(\Omega)]S_{n_1})_A|^m |H|^{m-1} m!.$$

Для групп главных паратопий

$$|\text{Par}(f)| = |(S_n)_f| = |(S_{n_1})_A|^m m!,$$

точнее,

$$\text{Par}(f) = [(S_{n_1})_A] S_n.$$

4. Локальное вычисление параметров неповторной суперпозиции функций

4.1. Матричный подход к получению различных способов задания функций

Пусть $|\Omega| = k \geq 2$, $n \geq 1$, R — произвольное коммутативное кольцо. Выберем произвольное упорядочение элементов из Ω и продолжим его до лексикографического порядка на множестве Ω^n .

Для произвольной функции

$$f: \Omega^n \rightarrow R$$

обозначим через $f^\downarrow$ столбец ее значений при данном упорядочении аргументов.

Выберем произвольную обратимую матрицу $B = (b_{ai})$, $a \in \Omega$, $i = 0, 1, \dots, k-1$, размера $k \times k$ над кольцом R .

Обозначим через ϕ_i , $i = 0, 1, \dots, k-1$, функции

$$\phi_i: \Omega \rightarrow R,$$

табличное задание которых совпадает со столбцами матрицы B ,

$$B = (b_{ai}) = (\phi_0^\downarrow, \dots, \phi_{k-1}^\downarrow),$$

то есть $\phi_i(a) = b_{ai}$ при $a \in \Omega$, $i = \{0, 1, \dots, k-1\}$.

Обозначим через $B^{[n]}$ тензорную n -ю степень этой матрицы

$$B^{[n]} = B \otimes B \otimes \dots \otimes B.$$

Тогда вектор $h^\downarrow$, определяемый равенствами

$$f^\downarrow = B^{[n]} h^\downarrow, \quad h^\downarrow = (B^{-1})^{[n]} f^\downarrow, \quad (9)$$

можно рассматривать как новое задание функции f , представляющее собой разложение f в ряд относительно базиса, состоящего из k^n функций $\phi_{i_1, \dots, i_n}(x_1, \dots, x_n)$, табличное задание которых совпадает со столбцами матрицы $B^{[n]}$. При этом выполнено равенство

$$\phi_{i_1, \dots, i_n}(x_1, \dots, x_n) = \phi_{i_1}(x_1) \dots \phi_{i_n}(x_n), \quad i_1, \dots, i_n \in \{0, 1, \dots, k-1\}.$$

Действительно, векторное равенство (9) можно записать в координатном виде

$$\begin{aligned} f(x_1, \dots, x_n) &= \sum_{i_1, \dots, i_n} \phi_{i_1}(x_1) \dots \phi_{i_n}(x_n) h(i_1, \dots, i_n) \\ &= \sum_{i_1, \dots, i_n} b_{x_1 i_1} \dots b_{x_n i_n} h(i_1, \dots, i_n). \end{aligned} \quad (10)$$

Быстрое вычисления вектора $h^\downarrow$ основано на известной формуле

$$B^{[n]} = (B \otimes E \otimes \dots \otimes E)(E \otimes B \otimes \dots \otimes E) \dots (E \otimes E \otimes \dots \otimes B) \quad (11)$$

с n сомножителями и заключается в выполнении n последовательных умножений вектора $f^\downarrow$ на матрицу размера $k^n \times k^n$, у которой в каждой строке не более k ненулевых элементов. Трудоемкость такого алгоритма составляет $O(M(k)k^{n-1}n)$ арифметических операций в кольце R , где $M(k)$ — сложность умножения матрицы размера $k \times k$ на вектор.

Данной схемой описывается переход к многим способам задания. Рассмотрим их более подробно.

4.1.1. Многочлены над конечным полем

Пусть $\Omega = R = GF(q)$ и $f: GF(q)^n \rightarrow GF(q)$ — некоторая функция. Выпишем столбец ее значений в лексикографическом порядке в соответствии со следующим порядком элементов поля $GF(q)$:

$$GF(q) = \{0, 1, \theta, \theta^2, \dots, \theta^{q-2}\},$$

где θ — некоторый примитивный элемент поля. Определим также лексикографический порядок на множестве одночленов многочлена над полем $GF(q)$ функции $f(x_1, \dots, x_n)$ с помощью соответствия

$$(j_1, \dots, j_n) \mapsto x_1^{j_1} \dots x_n^{j_n},$$

где $x_i^0 = 1$, $j_s \in \{0, 1, \dots, q-1\}$, $s = 1, \dots, n$.

С учетом введенных упорядочений при $n = 1$ столбец значений функции

$$f(x) = \sum_{i=0}^{q-1} h(i)x^i$$

можно записать в виде

$$f^\downarrow = \sum_{i=0}^{q-1} h(i)(x^i)^\downarrow = Bh^\downarrow,$$

где столбцы $q \times q$ матрицы B представляют собой табличные задания функций $\phi_i(x) = x^i$, $i = 0, 1, \dots, q-1$:

$$B = (b_{ai}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & \theta & \theta^2 & \dots & \theta^{q-2} & 1 \\ & & & \dots & & \\ 1 & \theta^{q-2} & \theta^{2(q-2)} & \dots & \theta^{(q-2)^2} & 1 \end{pmatrix}.$$

Здесь $b_{ai} = a^i$ при $a \in GF(q)$, $i = 0, 1, \dots, q-1$. Обратная матрица имеет вид

$$B^{-1} = (b'_{ia}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & -1 & -\theta^{-1} & \dots & -\theta^{(q-3)(-1)} & -\theta^{(q-2)(-1)} \\ 0 & -1 & -\theta^{-2} & \dots & -\theta^{(q-3)(-2)} & -\theta^{(q-2)(-2)} \\ 0 & \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & -\theta^{-(q-2)} & \dots & -\theta^{-(q-3)(q-2)} & -\theta^{-(q-2)(q-2)} \\ -1 & -1 & -1 & \dots & -1 & -1 \end{pmatrix}.$$

Здесь $b'_{ia} = -a^{-i}$ при $a \in GF(q)$, $i = 1, \dots, q-1$. То, что матрица B^{-1} имеет такой вид, вытекает из равенств

$$\sum_{j=1}^{q-1} \left(\frac{x}{a}\right)^j = \begin{cases} -1, & x = a, \\ 0, & x \neq a. \end{cases}$$

В частности, при $i \neq 0$ имеет место формула

$$h(i) = - \sum_{0 \neq a \in GF(q)} \frac{f(a)}{a^i}. \quad (12)$$

Аналогично, при $n \geq 2$ получаем формулы (9) и

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n=0}^{k-1} x_1^{i_1} \dots x_n^{i_n} h(i_1, \dots, i_n). \quad (13)$$

Заметим, что аналогичное разложение использовалось в [20] при изучении аналитических свойств взаимно-обратных преобразований.

4.1.2. Многочлен над полем действительных чисел

Пусть $\Omega = \{0, 1, \dots, k-1\}$, $R = \mathbf{R}$. Будем считать, что $\Omega \subset \mathbf{R}$. В дальнейшем все определяется полностью аналогично предыдущему случаю, за исключением вида матриц B и B^{-1} . Теперь матрица B имеет вид

$$B = (b_{ai}) = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 2 & 2^2 & \dots & 2^{k-2} & 2^{k-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & (k-1) & (k-1)^2 & \dots & (k-1)^{k-2} & (k-1)^{k-1} \end{pmatrix}.$$

4.1.3. Разложение Ньютона

Пусть $\Omega = R = \mathbf{Z}_k$ — кольцо вычетов. Определим элементы матрицы B равенствами

$$b_{a0} = \binom{a}{0} = 1, \quad b_{ai} = \binom{a}{i} = \frac{a(a-1)\dots(a-i+1)}{i!}, \quad i = 1, \dots, k-1, \quad a \in \Omega.$$

Заметим, что $B^{-1} = (b'_{ia})$, где

$$b'_{ia} = (-1)^{i+a} \binom{a}{i}.$$

В результате получается разложение Ньютона функции f

$$f(x) = \sum_{i=0}^{k-1} h(i) \binom{x}{i},$$

где коэффициент $h(i)$ совпадает со значением i -й конечной производной функции f в точке $x = 0$,

$$h(i) = \frac{\Delta^i}{\Delta x} f(0),$$

при

$$\frac{\Delta}{\Delta x} f(x) = f(x+1) - f(x).$$

Для n переменных аналогично получаем, что

$$f(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n=0}^{k-1} h(i_1, \dots, i_n) \binom{x_1}{i_1} \dots \binom{x_n}{i_n},$$

где

$$h(i_1, \dots, i_n) = \frac{\Delta^{i_1}}{\Delta x_1} \dots \frac{\Delta^{i_n}}{\Delta x_n} f(0, \dots, 0), \quad i_1, \dots, i_n \in \{0, 1, \dots, k-1\}.$$

Более подробные сведения о разложении Ньютона можно найти, например, в книге [21].

4.1.4. Спектральное разложение

В этом случае $\Omega = G$ — произвольная группа, $R = \mathbb{C}$ — поле комплексных чисел. Множество характеров группы G

$$\{\chi_a(x) : a \in G\}$$

образует группу, изоморфную группе G . Рассмотрим матрицу B вида

$$B = (b_{ai}), \quad b_{ai} = \chi_a(i), \quad a, i \in G.$$

Как известно, в этом случае

$$B^{-1} = \frac{1}{|G|} (b'_{ia}), \quad b_{ia} = \overline{\chi_a(i)}, \quad a, i \in G.$$

Для произвольного $j \in G$ функция $\chi_j(f(x_1, \dots, x_n))$ принимает значения в поле $\mathbb{C}$. Поэтому, применяя к ней формулу (9), получаем спектральное разложение

$$\chi_j(f(x_1, \dots, x_n)) = \sum_{i_1, \dots, i_n \in G} h_j(i_1, \dots, i_n) \chi_{i_1}(x_1) \dots \chi_{i_n}(x_n), \quad (14)$$

коэффициенты которого определяются равенствами

$$h_j(i_1, \dots, i_n) = \frac{1}{|G|^n} \sum_{x_1, \dots, x_n \in G} \chi_j(f(x_1, \dots, x_n)) \overline{\chi_{i_1}(x_1)} \dots \overline{\chi_{i_n}(x_n)}, \quad (15)$$

где $j, i_1, \dots, i_n \in G$. Понятие спектрального разложения функции впервые изучалось в [22], а данное определение введено А. Б. Ремизовым.

4.2. Матрица коэффициентов функции и ее свойства

Во многих случаях оказывается удобным рассматривать разложение вида (10) не для самой функции f , а для функций $\phi_i(f)$, базисных функций ϕ_i , определяемых матрицей B , $i = 0, 1, \dots, k-1$. Рассмотрение векторов значений $(\phi_0(f), \dots, \phi_{k-1}(f))$ дает возможность не только единым способом записывать в матричном виде соотношения между коэффициентами, но и в отдельных случаях находить более эффективные способы вычисления, чем при применении быстрого алгоритма, основанного на соотношении (11). В частности, ниже будет показано, что вычисление каждого заданного коэффициента разложения функции можно проводить быстрее, если воспользоваться наличием у функции бесповторной декомпозиции.

Для произвольной k -значной функции $f: \Omega^n \rightarrow \Omega$ и произвольной обратимой матрицы $B = (b_{ai})$ над кольцом R , столбцы которой рассматриваются как табличные задания

функций $\phi_i: \Omega \rightarrow R, i = 0, 1, \dots, k-1$, рассмотрим $k^n \times k$ матрицу $T(f)$ над кольцом R , столбцами которой являются табличные задания функций

$$\begin{aligned} \phi_i(f(x_1, \dots, x_n)), \quad i = 0, 1, \dots, k-1, \\ T(f) = (\phi_0(f)^\downarrow, \dots, \phi_{k-1}(f)^\downarrow). \end{aligned}$$

Определим матрицу коэффициентов $[f]$ равенством

$$[f] = (B^{-1})^{[n]} T(f).$$

Ее столбцами являются упорядоченные наборы коэффициентов (обозначаемые через $h_j(i_1, \dots, i_n)$) разложений функций $\phi_j(f(x_1, \dots, x_n)), i = 0, 1, \dots, k-1$, в базисе функций $\phi_{i_1, \dots, i_n}(x_1, \dots, x_n), i_1, \dots, i_n \in \{0, 1, \dots, k-1\}$,

$$\phi_j(f(x_1, \dots, x_n)) = \sum_{i_1, \dots, i_n} \phi_{i_1, \dots, i_n}(x_1, \dots, x_n) h_j(i_1, \dots, i_n). \quad (16)$$

Уточним смысл элементов матрицы коэффициентов для рассмотренных выше примеров.

Для многочленов над конечным полем и полем действительных чисел коэффициенты $h_j(i_1, \dots, i_n)$ при $j, i_1, \dots, i_n \in 0, 1, \dots, k-1$, соответствуют представлению

$$f(x_1, \dots, x_n)^j = \sum_{i_1, \dots, i_n=0}^{k-1} x_1^{i_1} \dots x_n^{i_n} h_j(i_1, \dots, i_n). \quad (17)$$

Для разложения Ньютона аналогично получаем, что элементы матрицы коэффициентов в данном случае соответствуют представлению

$$\binom{f(x_1, \dots, x_n)}{j} = \sum_{i_1, \dots, i_n=0}^{k-1} h_j(i_1, \dots, i_n) \binom{x_1}{i_1} \dots \binom{x_n}{i_n}$$

и имеют вид

$$h_j(i_1, \dots, i_n) = \frac{\Delta^{i_1}}{\Delta x_1} \dots \frac{\Delta^{i_n}}{\Delta x_n} \binom{f}{j}(0, \dots, 0), \quad j, i_1, \dots, i_n \in \{0, 1, \dots, k-1\}.$$

Для спектрального разложения коэффициенты (15) разложения (14) в точности совпадают с элементами матрицы коэффициентов функции f .

Изучим свойства матрицы коэффициентов. Для функций от одного переменного свойства матрицы коэффициентов описывает следующая лемма.

Лемма 8. Пусть $n = 1$ и $f(x) = \gamma(x)$, тогда справедливы следующие утверждения:

- (1) если $\gamma(x) = e(x) = x$, то $[f] = B$,
- (2) если $P(\gamma) = (p_{ab})$ — матрица размера $k \times k$ с коэффициентами

$$p_{ab} = \begin{cases} 1, & \gamma(a) = b, \\ 0, & \gamma(a) \neq b, \end{cases}$$

то $T[\gamma] = P(\gamma)B$ и $[\gamma] = B^{-1}P(\gamma)B$,

(3) если $f(x) = \gamma_2(\gamma_1(x)) = \gamma_1\gamma_2(x)$, то $[\gamma_1][\gamma_2] = [\gamma_1\gamma_2]$.

Доказательство первого и второго утверждений вытекает из определения матрицы $T(f)$. Доказательство третьего утверждения вытекает из легко проверяемого равенства $P(\gamma_1\gamma_2) = P(\gamma_1)P(\gamma_2)$.

Обозначим через $[f]_{i_1, \dots, i_{n-1}}$ квадратную подматрицу матрицы коэффициентов $[f] = (h_j(i_1, \dots, i_n))$, соответствующую фиксации первых $n - 1$ индексов значениями $i_1, \dots, i_{k-1} \in \{0, 1, \dots, k - 1\}$:

$$[f] = \begin{pmatrix} [f]_{0, \dots, 0} \\ \dots \\ [f]_{i_1, \dots, i_{n-1}} \\ \dots \\ [f]_{k-1, \dots, k-1} \end{pmatrix}.$$

Элементы матрицы $[f]_{i_1, \dots, i_{n-1}} = (t_{i,j})$ — это коэффициенты $t_{i,j} = h_j(i_1, \dots, i_{n-1}, i)$, $i, j = 0, 1, \dots, k - 1$.

Теорема 18. Если $B^{-1} = (b'_{ai})$, $a \in \Omega$, $i = 0, 1, \dots, k - 1$, то справедливо матричное равенство

$$[f]_{i_1, \dots, i_{n-1}} = B^{-1} \left(\sum_{a_1, \dots, a_{n-1} \in \Omega} b'_{a_1 i_1} \dots b'_{a_{n-1} i_{n-1}} P(\gamma_{a_1, \dots, a_{n-1}}) \right) B,$$

где

$$\gamma_{a_1, \dots, a_{n-1}}(x) = f(a_1, \dots, a_{n-1}, x), \quad a_1, \dots, a_{n-1} \in \Omega.$$

Доказательство. Справедливо равенство

$$[f] = ((B^{-1})^{[n-1]} \otimes E)(E^{[n-1]} \otimes B^{-1})T(f).$$

Поэтому

$$[f]_{i_1, \dots, i_{n-1}} = \sum_{a_1, \dots, a_{n-1} \in \Omega} b'_{a_1 i_1} \dots b'_{a_{n-1} i_{n-1}} B^{-1} T(f)_{a_1, \dots, a_{n-1}},$$

где $T(f)_{a_1, \dots, a_{n-1}}$ — соответствующая квадратная подматрица матрицы $T(f)$. Поскольку согласно лемме 8

$$T(f)_{a_1, \dots, a_{n-1}} = P(\gamma_{a_1, \dots, a_{n-1}})B$$

при всех $a_1, \dots, a_{n-1} \in \Omega$, получаем требуемое равенство.

4.3. Матрицы коэффициентов бесповторной суперпозиции функций

Покажем, что вычисление каждой подматрицы $[f]_{i_1, \dots, i_{n-1}}$ для функции f , допускающей бесповторную декомпозицию, сводится к перемножению матриц коэффициентов, соответствующих функциям — компонентам этой декомпозиции.

Теорема 19. Если при $1 \leq s < n$ выполняется равенство

$$f(x_1, \dots, x_n) = f_1(x_1, \dots, x_s, f_2(x_{s+1}, \dots, x_n)),$$

то при всех $i_1, \dots, i_{n-1} \in \{0, 1, \dots, k - 1\}$ справедливо матричное равенство

$$[f]_{i_1, \dots, i_{n-1}} = [f_2]_{i_{s+1}, \dots, i_{n-1}} [f_1]_{i_1, \dots, i_s}.$$

Доказательство. По теореме 18

$$[f]_{i_1, \dots, i_{n-1}} = B^{-1} \left(\sum_{a_1, \dots, a_{n-1} \in \Omega} b'_{a_1 i_1} \dots b'_{a_{n-1} i_{n-1}} P(\gamma_{a_1, \dots, a_{n-1}}) \right) B.$$

Заметим, что

$$\gamma_{a_1, \dots, a_{n-1}}(x) = \gamma_{a_{s+1}, \dots, a_{n-1}}^{(2)}(\gamma_{a_1, \dots, a_s}^{(1)}(x)),$$

где

$$\begin{aligned} \gamma_{a_1, \dots, a_s}^{(1)}(x) &= f_1(a_1, \dots, a_s, x), \\ \gamma_{a_{s+1}, \dots, a_{n-1}}^{(2)}(x) &= f_2(a_{s+1}, \dots, a_{n-1}, x). \end{aligned}$$

Следовательно,

$$\begin{aligned} [f]_{i_1, \dots, i_{n-1}} &= B^{-1} \left(\sum_{a_{s+1}, \dots, a_{n-1} \in \Omega} b'_{a_{s+1} i_{s+1}} \dots b'_{a_{n-1} i_{n-1}} P(\gamma_{s+1, \dots, n-1}^{(2)}) \right) \\ &\quad \times \left(\sum_{a_1, \dots, a_s \in \Omega} b'_{a_1 i_1} \dots b'_{a_s i_s} P(\gamma_{a_1, \dots, a_s}^{(1)}) \right) B \\ &= [f_2]_{i_{s+1}, \dots, i_{n-1}} [f_1]_{i_1, \dots, i_s}. \end{aligned}$$

В частности, для итеративных функций вычисление подматриц осуществляется наиболее просто.

Следствие 9. Если

$$f(x_n, \dots, x_1, x_0) = A_n(\dots A_2(A_1(x_0, x_1), x_2) \dots) x_n),$$

то при всех $i_1, \dots, i_{n-1} \in \{0, 1, \dots, k-1\}$ справедливо матричное равенство

$$\begin{aligned} [f]_{i_n, \dots, i_1} &= [A_1]_{i_1} [A_2]_{i_2} \dots [A_n]_{i_n} \\ &= B^{-1} \Pi_{i_1}(A_1) \Pi_{i_2}(A_2) \dots \Pi_{i_n}(A_n) B, \end{aligned}$$

где

$$[A_i]_j = B^{-1} \Pi_j(A_i) B,$$

а подматрицы $\Pi_j(A_i)$ определяются равенствами

$$\Pi_j(A_i) = \sum_{a \in \Omega} b'_{aj} P(\gamma_a^{(i)}),$$

при $\gamma_a^{(i)}(x) = A_i(a, x)$, $j = 0, 1, \dots, k-1$, $i = 1, \dots, n$, $a, x \in \Omega$.

Утверждение следствия непосредственно вытекает из теоремы 19.

Использование данного представления позволяет вычислять матрицы $[f]_{i_n, \dots, i_1}$ за $O(k^3(n+1))$ арифметических операций в кольце R .

Следствие 10. Если при некотором отображении $\gamma: \Omega \rightarrow \Omega$ и бинарной операции $\circ$ выполняется равенство

$$f(x_n, \dots, x_1, x_0) = \gamma(\dots \gamma(\gamma(x_0) \circ x_1) \circ x_2) \dots) \circ x_n,$$

то при всех $i_1, \dots, i_n \in \{0, 1, \dots, k-1\}$ справедливо матричное равенство

$$\begin{aligned} [f]_{i_n, \dots, i_1} &= [\gamma][\circ]_{i_1} [\gamma][\circ]_{i_2} \dots [\gamma][\circ]_{i_n} \\ &= B^{-1} P(\gamma) \Pi_{i_1} P(\gamma) \Pi_{i_2} \dots P(\gamma) \Pi_{i_n} B, \end{aligned}$$

где матрицы $\Pi_j = \Pi_j(\circ)$ определяются равенствами

$$\Pi_j = \sum_{a \in \Omega} b'_{aj} P(\circ_a),$$

при $\circ_a(x) = a \circ x$, $j = 0, 1, \dots, k-1$, $a, x \in \Omega$.

В заключение приведем еще один пример использования данного подхода для быстрого вычисления параметров вполне приводимой функции.

Следствие 11. Пусть функция f имеет вид

$$f(x_3, x_2, x_1, x_0) = (a_0 \otimes L(\pi(x_0))) \oplus (a_1 \otimes L(\pi(x_1))) \oplus (a_2 \otimes L(\pi(x_2))) \oplus (a_3 \otimes L(\pi(x_3))),$$

где $\otimes, \oplus$ — некоторые бинарные операции, $L, \pi \in S(\Omega)$, $a_1, a_2, a_3 \in \Omega$, и пусть $\otimes_a(x) = a \otimes x$, $a \in \Omega$. Тогда при всех $i_1, i_2, i_3 \in \{0, 1, \dots, k-1\}$ выполнено равенство

$$\begin{aligned} [f]_{i_3, i_2, i_1} &= B^{-1} P(\pi) P(L) P(\otimes_{a_0}) P(\pi) P(L) P(\otimes_{a_1}) \Pi_{i_1} (\oplus) \\ &\quad \times P(\pi) P(L) P(\otimes_{a_2}) \Pi_{i_2} (\oplus) P(\pi) P(L) P(\otimes_{a_3}) \Pi_{i_3} (\oplus) B. \end{aligned} \quad (18)$$

Доказательство. Для удобства введем обозначения

$$\begin{aligned} \gamma(x) &= a_0 \otimes L(\pi(x)), \\ A_j(x_1, x_2) &= x_1 \oplus (a_j \otimes L(\pi(x_2))), \quad j = 1, 2, 3. \end{aligned}$$

Тогда

$$f(x_3, x_2, x_1, x_0) = A_3(A_2(A_1(\gamma(x_0), x_1), x_2), x_3)$$

и при всех $i_1, i_2, i_3 \in \{0, 1, \dots, k-1\}$ выполнено равенство

$$[f]_{i_3, i_2, i_1} = [\gamma][A_1]_{i_1} [A_2]_{i_2} [A_3]_{i_3},$$

где

$$\begin{aligned} [\gamma] &= B^{-1} P(\pi) P(L) P(\otimes_{a_0}) B, \\ [A_j]_i &= B^{-1} P(\pi) P(L) P(\otimes_{a_j}) \Pi_i (\oplus) B, \quad j = 1, 2, 3, \quad i \in \{0, 1, \dots, k-1\}. \end{aligned}$$

Заметим, что в произведении (18) необходимо вычислять только произведения на матрицы B и $\Pi_i(\otimes)$. Остальные матрицы являются подстановочными, поэтому результат умножения на подстановочную матрицу можно вычислять путем перестановки столбцов в соответствии с текущей подстановкой, которую можно вычислить заранее.

Список литературы

1. Шеннон К., Синтез двухполюсных переключательных схем. В кн.: *Работы по теории информации и кибернетике*. ИЛ, Москва, 1963, с. 59–105.
2. Кузнецов А. В., О неповторных контактных схемах и неповторных суперпозициях функций алгебры логики. *Труды МИАН СССР* (1958) **51**, 186–225.
3. Ashenurst R. L., The decomposition of switching functions. *Ann. Comput. Labor. Harvard Univ.* (1959) **29**, 74–116.
4. Закревский А. Д., Алгоритм разделения булевых функций. *Труды Сиб. физ.-техн. ин-та* (1964) **3**, №44, 5–16.
5. Tase A., A fast algorithm for the proper decomposition of boolean functions. *Philips Res. Repts* (1972) **27**, 140–150.
6. Вщенко В. П., Метод синтеза одного класса схем на основе функциональной разделимости. *Кибернетика* (1969), №1, 32–40.
7. Шурупов А. Н., О функциональной разделимости булевых пороговых функций. *Дискретная математика* (1997) **9**, №2, 59–73.
8. Яблонский С. В., Об алгоритмических трудностях синтеза минимальных контактных схем. *Проблемы кибернетики* (1959) **2**, 75–121.
9. Перязев Н. А., Реализация булевых функций неповторными формулами. *Дискретная математика* (1995) **7**, №3, 61–68.
10. Винокуров С. Ф., Перязев Н. А., *Избранные вопросы теории булевых функций*. Физматлит, Москва, 2001.
11. Белоусов В. Д., Уравновешенные тождества в квазигруппах. *Матем. сб.* (1966) **70** (112), №1, 55–97.
12. Белоусов В. Д., Лившиц Э. С., Уравновешенные функциональные уравнения на квазигруппах любой ариности. *Матем. исследования. Квазигруппы и комбинаторика* (1966) **43**, 9–29.
13. Горбатов А. В., *Характеризационная теория синтеза функциональных декомпозиций в k -значных логиках*. Физматлит, Москва, 2000.
14. Белоусов В. Д., n -арные квазигруппы. Штинца, Кишинев, 1972.
15. Черемушкин А. В., Каноническая декомпозиция n -арных квазигрупп. *Матем. исследования. Исследование операций и квазигрупп* (1988) **102**, 97–105.
16. Сохацкий Ф. Н., Обобщение двух теорем Белоусова для сильно зависимых функций k -значной логики. В кн.: *Исследования по теории квазигрупп и луп*. Штинца, Кишинев, 1985, с. 105–115.
17. Белоусов В. Д., *Основы теории квазигрупп и луп*. Наука, Москва, 1967.
18. Курош А. Г., *Общая алгебра*. Наука, Москва, 1974.
19. Черемушкин А. В., Группы автострофий разделимых сильно зависимых функций. *Матем. исследования. Квазигруппы и их системы* (1990) **113**, 119–123.
20. Колбин С. Л. О некоторых свойствах взаимно-обратных систем функций. *Дискретная математика* (1994) **6**, №2, 145–149.
21. Davio M., Deschamps J. P., Thayse A., *Discrete and switching functions*. Academiai Kiado, Budapest, 1974.
22. Moraga C., Complex spectral logic. In: *Proc. 8th Int. Symp. Multiple-Valued Logic*. New York, 1978, pp. 149–156.

Статья поступила 24.06.2003.

Переработанный вариант поступил 22.06.2004.