Санкт-Петербургский государственный университет

Фундаментальная математика и механика
Теория чисел

Симонов Кирилл Алексеевич

Алгоритмы матричного умножения

Дипломная работа

Научный руководитель:
д. ф.-м. н., профессор Всемирнов М. А.

Рецензент:
к. ф.-м. н. Пастор А. В.

Санкт-Петербург
2017

SAINT-PETERSBURG STATE UNIVERSITY

Fundamental Mathematics and Mechanics
Number theory

Kirill Simonov

Matrix multiplication algorithms

Graduation Thesis

Scientific supervisor:
Doctor of Sciences Maxim Vsemirnov

Reviewer:
Candidate of Sciences Aleksei Pastor

Saint-Petersburg
2017

Оглавление

Введение

Умножение матриц — одна из основных задач вычислительной линейной алгебры. Кроме важности этой операции самой по себе, к ней сводятся все стандартные алгоритмы линейной алгебры, такие, как решение линейной системы, обращение матрицы, вычисление определителя — см. например главу 16 в [2].

Тривиальный алгоритм умножения двух матриц размера $n \times n$ имеет сложность $O(n^3)$. Но в 1969 году Штрассену удалось получить алгоритм, вычисляющий это произведение за $O(n^{2.81})$ операций. С того времени было сделано еще несколько улучшений оценки *экспоненты матричного умножения*, которая определяется как наименьшее вещественное число ω, такое, что умножение двух матриц размера $n \times n$ может быть произведено за $O(n^{\omega+\varepsilon})$ для любого положительного ε. Наилучшая на данный момент оценка $\omega < 2.3728639$ принадлежит Франсуа Ле Галлю [7], и была получена обобщением алгоритма Копперсмита и Винограда [5].

В 2003 году Кон и Уманс предложили новый метод для оценки матричной экспоненты [4], использующий вложение алгебры матриц в некоторую групповую алгебру, подобно тому, как можно умножать многочлены степени n за $O(n \log n)$ операций, вложив их в групповую алгебру циклической группы и совершив быстрое преобразование Фурье. Но если в случае умножения многочленов достаточно циклической группы, и преобразование Фурье переводит $\mathbb{C}[G]$ в $\mathbb{C}^{|G|}$, где умножение производится покомпонентно, то для умножения матриц групповые алгебры абелевых групп не могут дать оценку лучше $\omega \leq 3$ (Лемма 3.1 в [4]). Таким образом, умножение матриц сводится не к покомпонентному умножению, а к умножению нескольких других матриц меньшего размера, и эти размеры являются размерностями неприводимых представлений выбранной группы. В итоге получается рекурсивный алгоритм, эффективность которого зависит от размерностей неприводимых представлений.

Для получения нетривиальных оценок на ω в первую очередь необходимо получать группы, к групповым алгебрам которых можно сводить умножение матриц размера $n \times n$, и размер которых не превосходит n^α, где $\alpha < 3$. В работе [4] были получены семейства групп, обладающих этим свойством с $\alpha = 2 + o(1)$, что является необходимым условием для того, чтобы доказать $\omega = 2$, хотя и не достаточным, поскольку итоговая сложность зависит еще и от размерности представлений.

Впервые доказать с помощью этого метода, что $\omega < 3$, удалось уже в [3]. Конструкции групп в этой работе основываются на комбинаторном объекте под названием *uniquely solvable puzzle* (USP) и некоторых его вариациях. С помощью обобщения этого объекта получается наилучшая оценка в работе [3]: $\omega < 2.376$, что соответствует результату Копперсмита и Винограда [5], но [3] использует для этого исключительно теоретико-групповой подход.

В недавней работе [1] было показано, что невозможно доказать $\omega = 2$ с помощью

конструкций из [3], используя лишь абелевы группы, порождающиеся элементами ограниченного порядка (именно такими были все продуктивные конструкции групп в [3]). Однако, это всё ещё не исключает доказательство $\omega = 2$ с помощью теоретико-группового метода, но для этого понадобится использовать либо семейство абелевых групп, содержащих элементы всё большего порядка, либо неабелевы группы.

В настоящей работе мы в разделе 1 введём конструкции из [4] и [3], позволяющие реализовывать матричное умножение, и в параграфе 1.5 продемонстрируем новый подход к получению оценки $\omega < 2.48$.

В разделе 2 с помощью известных инструментов теории представлений будут явно описаны неприводимые представления групп из [3], реализующих быстрое матричное умножение — необходимый шаг для потенциального практического применения подобных алгоритмов, позволяющий кроме того немного уточнить оценки на ω, получающиеся из групп малого размера.

1. Умножение матриц с помощью групп

В этом разделе мы введём все необходимые понятия и утверждения из [4] и [3], и в параграфе 1.5 получим новый подход к доказательству оценки $\omega < 2.48$.

За $[k]$ будет обозначаться множество $\{1, 2, \ldots, k\}$. Cyc_m обозначает циклическую группу порядка m, для групповой операции будут использоваться аддитивные обозначения. За $\mathrm{Sym}(U)$ обозначаем симметрическую группу на множестве U, и за Sym_n обозначаем $\mathrm{Sym}([n])$.

1.1. Основы теоретико-группового подхода

В этом параграфе мы сформулируем базовые утверждения из [4].

Пусть S — подмножество элементов группы, обозначим $Q(S) = \{s_1 s_2^{-1} : s_1, s_2 \in S\}$.

Определение 1.1 ([4])**.** Группа G реализует $\langle n_1, n_2, n_3\rangle$, если существуют подмножества $S_1, S_2, S_3 \subset G$ такие, что $|S_i| = n_i$ и для любых $q_i \in Q(S_i)$ из $q_1 q_2 q_3 = 1$ следует $q_1 = q_2 = q_3 = 1$. Это условие на S_1, S_2, S_3 мы будем называть *свойством тройного произведения*.

Следующие две леммы показывают, что условие выше ведет себя естественно.

***Лемма* 1.1** ([4])**.** *Если G реализует $\langle n_1, n_2, n_3\rangle$, то она реализует и любую их перестановку.*

***Лемма* 1.2** ([4])**.** *Если $S_1, S_2, S_3 \subset G$ и $S_1', S_2', S_3' \subset G'$ обладают свойством тройного произведения, то и $S_1 \times S_1', S_2 \times S_2', S_3 \times S_3' \subset G \times G'$ им обладают.*

Условие из опеределения 1.1 имеет центральное значение и задает сводимость матричного умножения к умножению элементов групповой алгебры, о чем говорит следующая теорема.

***Теорема* 1.1** ([4])**.** *Пусть R — алгебра над $\mathbb{C}$, не обязательно коммутативная. Если G реализует $\langle n, m, p\rangle$, то количество операций, необходимое для перемножения матриц размера $n \times m$ и $m \times p$ над R, не превосходит числа операций, необходимых для умножения двух элементов $R[G]$.*

Далее приводится теорема, которая позволяет получать оценки на ω через группы, обладающие свойством тройного произведения.

***Теорема* 1.2** ([4])**.** *Пусть G реализует $\langle n, m, p\rangle$, и размерности ее неприводимых представлений равны $\{d_i\}$. Тогда $(nmp)^{\omega/3} \leq \sum_i d_i^\omega$.*

1.2. USP

Здесь мы введем комбинаторный объект, являющийся ключевым для оценок из работы [3].

Определение 1.2 ([3])**.** Uniquely solvable puzzle (USP) ширины k — это подмножество $U \subset \{1,2,3\}^k$, обладающее следующим свойством: для любых перестановок π_1, π_2, π_3 элементов множества U либо $\pi_1 = \pi_2 = \pi_3$, либо существует $u \in U$ и $i \in [k]$ такие, что по крайней мере два равенства из $(\pi_1(u))_i = 1$, $(\pi_2(u))_i = 2$, $(\pi_3(u))_i = 3$ выполнены.

Но важнейшую роль играет следующее усиление этого определения.

Определение 1.3 ([3])**.** Сильное USP ширины k — это подмножество $U \subset \{1,2,3\}^k$, обладающее следующим свойством: для любых перестановок π_1, π_2, π_3 элементов множества U либо $\pi_1 = \pi_2 = \pi_3$, либо существует $u \in U$ и $i \in [k]$ такие, что *ровно* два равенства из $(\pi_1(u))_i = 1$, $(\pi_2(u))_i = 2$, $(\pi_3(u))_i = 3$ выполнены.

Изображать USP удобно в виде таблицы, где строки соответствуют элементам множества U, а столбцы — координатам. Например, следующая таблица задает USP размера 8 и ширины 6.

3	3	3	3	3	3
1	3	3	2	3	3
3	1	3	3	2	3
1	1	3	2	2	3
3	3	1	3	3	2
1	3	1	2	3	2
3	1	1	3	2	2
1	1	1	2	2	2

Следующее предложение показывает, что этот пример — частный случай общей конструкции.

***Предложение* 1.1** ([3])**.** *Для любого $k \geq 1$ существует сильное USP размера 2^k и ширины $2k$.*

Доказательство. Возьмем в качестве U следующее множество

$$\{u \in \{1,3\}^k \times \{2,3\}^k : \forall i \in [k], u_i = 1 \iff u_{i+k} = 2\},$$

$\{1,3\}^k \times \{2,3\}^k$ является подмножеством $\{1,2,3\}^{2k}$.

Пусть $\pi_1, \pi_2, \pi_3 \in \mathrm{Sym}(U)$. Если $\pi_1 \neq \pi_3$, тогда существует $u \in U$ такое, что $(\pi_1(u))_i = 1$, а $(\pi_3(u))_i = 3$ для некоторого $i \in [k]$. При этом, $(\pi_2(u))_i \neq 2$, так как в i-м столбце при $i \in [k]$ двоек нет вообще. Аналогично, если $\pi_2 \neq \pi_3$, то существует

$u \in U$ такое, что $(\pi_2(u))_i = 2$, а $(\pi_3(u))_i = 3$ для некоторого $i \in [2k] \setminus [k]$, и $(\pi_1(u))_i \neq 1$, так как в последних k столбцах встречаются только 2 и 3. В любом случае, условие из определения сильного USP выполнено. □

Определим ёмкость сильных USP как наибольшую константу C такую, что существует сильное USP размера $(C - o(1))^k$ и ширины k для бесконечного числа значений k. Аналогично определяется ёмкость обычных USP.

***Лемма* 1.3** ([3])**.** *Ёмкость USP не превосходит* $3 \cdot 2^{-2/3}$.

Поскольку любое сильное USP является просто USP, та же оценка верна и для мощности сильных USP.

Кроме того, USP оказываются неявно задействованы в работе Копперсмита и Винограда. Раздел 6 из [5] можно интерпретировать как доказательство точности оценки предыдущей леммы.

***Теорема* 1.3** ([5])**.** *Ёмкость USP равна* $3 \cdot 2^{-2/3}$.

В [3] была выдвинута гипотеза, что и для сильных USP эта оценка сверху оказывается точной, но она была опровергнута в [1]. Однако, существует конструкция, более эффективная, чем в предложении 1.1.

Пусть $U \subset \{1, 2, 3\}^k$ таково, что в каждой координате встречаются только два значения из трех; таким свойством в частности обладает USP из предложения 1.1. В этом случае определения USP и сильного USP совпадают — тройки $\{1, 2, 3\}$ ни в каком столбце встретиться не может. Пусть $\mathrm{Sym}(U)$ действует на U перестановкой строк, и H_1 — подгруппа элементов $\mathrm{Sym}(U)$, которые при действии на U не меняют столбцы, в которых встречаются только 1 и 2, H_2 — подгруппа, не меняющая столбцы , в которых встречаются только 2 и 3, H_3 — подгруппа, не меняющая столбцы, в которых встречаются только 1 и 3.

***Лемма* 1.4** ([3])**.** *Множество U является USP тогда и только тогда, когда* H_1, H_2, H_3 *обладают свойством тройного произведения в* $\mathrm{Sym}(U)$.

Доказательство. Пусть $\pi_1, \pi_2, \pi_3 \in \mathrm{Sym}(U)$. Перестановка $\pi_1\pi_2^{-1}$ не входит в H_1 тогда и только тогда, когда существует $v \in U$ и координата i, что $v_i = 2$, а $((\pi_1\pi_2^{-1})(v))_i = 1$. Если обозначить $\pi_2^{-1}(v)$ за u, то это то же самое, что $(\pi_2(u))_i = 2$, а $(\pi_1(u))_i = 1$. Аналогично,$\pi_2\pi_3^{-1}$ не входит в H_2 тогда и только тогда, когда существует u и i, что$(\pi_2(u))_i = 2$, а $(\pi_3(u))_i = 3$, и $\pi_3\pi_1^{-1}$ не входит в H_3 тогда и только тогда, когда существует u и i, что$(\pi_1(u))_i = 1$, а $(\pi_3(u))_i = 3$.

Таким образом, U является USP тогда и только тогда, когда для любых π_1, π_2, π_3 из того, что $\pi_1\pi_2^{-1} \in H_1$, $\pi_2\pi_3^{-1} \in H_2$, и $\pi_3\pi_1^{-1} \in H_3$, следует $\pi_1 = \pi_2 = \pi_3$, а это равносильно выполнению свойства тройного произведения для H_1, H_2, H_3. □

***Предложение* 1.2** ([3])**.** *Для любого $k \geq 1$ существует сильное USP размера $2^{k-1}(2^k+1)$ и ширины $3k$.*

Доказательство. Рассмотрим множество

$$\Delta_n = \{(a,b,c) \in \mathbb{Z}^3 : a+b+c = n-1, a,b,c \geq 0\},$$

где $n = 2^k$, и пусть H_1, H_2, H_3 — подгруппы $\mathrm{Sym}(\Delta_n)$, сохраняющие первую, вторую и третью координату, соответственно. По теореме 3.3 из [4], эти подгруппы обладают свойством тройного произведения в $\mathrm{Sym}(\Delta_n)$.

Построим теперь сильную USP ширины $3k$. В первых k координатах будут встречаться только 1 и 2, в следующих k только 2 и 3, в последних k только 1 и 3. В каждом из этих трех блоков по k координат может быть 2^k различных значений, пронумеруем их в каждом блоке произвольным образом от 0 до 2^k-1. Элементы U будут соответствовать элементам Δ_n, элемент U, соответствующий тройке $(a,b,c) \in \Delta_n$ будет иметь значение номер a в первом блоке координат, значение номер b во втором, и значение номер c в третьем. По лемме 1.4, U — сильное USP. □

Группа, которая используется для матричного умножения, получается из USP следующим образом: Пусть U — USP, H — абелева группа отображений из $U \times k$ в Cyc_m (операцией является поточечное суммирование). Группа перестановок элементов множества U, $\mathrm{Sym}(U)$, действует на H следующим образом:

$$\pi(h)(u,i) = h(\pi^{-1}(u), i),$$

где $\pi \in \mathrm{Sym}(U)$, $h \in H$, $u \in U$, $i \in [k]$.

В качестве группы G рассмотрим теперь полупрямое произведение $H \rtimes \mathrm{Sym}(U)$, подмножества S_1, S_2, S_3 определим следующим образом: S_i состоит из произведений $h\pi$, $h \in H$, $\pi \in \mathrm{Sym}(U)$, при этом

$$h(u,j) \neq 0 \iff u_j = i$$

для всех $u \in U$ и $j \in [k]$.

***Предложение* 1.3** ([3])**.** *Если U — сильное USP, тогда подмножества S_1, S_2, S_3 группы G обладают свойством тройного произведения.*

Учитывая, что размерности неприводимых представлений G не превосходят $[G : H] = |U|!$ (так как H — абелева), теорема 1.2 дает следующую оценку.

***Следствие* 1.1** ([3])**.** *Пусть U — сильное USP ширины k, $m \geq 3$ — натуральное число, тогда*

$$\omega \leq \frac{3\log m}{\log(m-1)} - \frac{3\log|U|!}{|U|k\log(m-1)},$$

в частности, если ёмкость сильных USP равна C,

$$\omega \leq \frac{3\log m - \log C}{\log(m-1)}. \qquad (1)$$

Из следствия 1.1 и предложения 1.1 получается $\omega < 2.67$, а предложение 1.2 дает $\omega < 2.48$. При этом, если бы гипотеза о том, что ёмкость сильных USP равна ёмкости обычных USP (опровергнутая в [1]), оказалась верна, то было бы $\omega = 2$ из неравенства (1) при $m = 3$.

Мы будем использовать для получения оценок другую разновидность USP, но конструкция группы, определенная выше, демонстрирует общий подход.

1.3. Свойство одновременных тройных произведений

Группа, построенная в предыдущей разделе, представляла из себя полупрямое произведение симметрической группы с абелевой, при этом разделение на три множества, обладающих свойством тройного произведения, происходило внутри абелевой группы. Но это разделение можно было бы представить как сведение нескольких независимых матричных умножений к умножению элементов групповой алгебры. Следующее определение формализует это наблюдение.

Определение 1.4 ([3])**.** n троек подмножеств A_i, B_i, C_i $(1 \leq i \leq n)$ группы G обладают свойством одновременных тройных произведений, если

- для каждого i тройка подмножеств A_i, B_i, C_i обладает свойством тройного произведения, и
- для любых i, j, k из равенства $a_i(a'_j)^{-1}b_j(b'_k)^{-1}c_k(c'_i)^{-1} = 1$, где $a_i \in A_i$, $a'_j \in A_j$, $b_j \in B_j$, $b'_k \in B_k$,$c_k \in C_k$, $c'_i \in C_i$, следует $i = j = k$.

В этом случае мы говорим, что группа G одновременно реализует $\langle|A_1|, |B_1|, |C_1|\rangle$, ...,$\langle|A_n|, |B_n|, |C_n|\rangle$.

Свойство из предыдущего определения как раз позволяет использовать групповую алгебру для вычисления произведения нескольких независимых пар матриц, о чем говорит следующая теорема, являющаяся аналогом теоремы 1.1.

***Теорема* 1.4** ([3])**.** *Пусть R — любая алгебра над $\mathbb{C}$. Если G одновременно реализует $\langle n_1, m_1, p_1\rangle$, ...,$\langle n_k, m_k, p_k\rangle$, то количество операций, необходимое для перемножения k пар матриц размеров $n_1 \times m_1$ и $m_1 \times p_1$, ..., $n_k \times m_k$ и $m_k \times p_k$ над R, не превосходит числа операций, необходимых для умножения двух элементов $R[G]$.*

Ключевой результат для получения оценок на ω — так называемое асимптотическое неравенство суммы Шёнхаге (15.11 в [2]), которое используется и в работах вне теоретико-группового подхода, но в этой модели также работает. Более того, в [3] приведено доказательство этого неравенства, полностью лежащее в рамках теоретико-группового подхода, которое по группе G, обладающей свойством одновременных тройных произведений строит группу, обладающую просто свойством тройного произведения, а именно полупрямое произведение $G^n \rtimes \mathrm{Sym}_n$, где n — количество троек множеств из определения свойства одновременных тройных произведений. То есть, сводит умножение двух матриц к нескольким независимым умножениям матриц меньших размеров.

***Теорема* 1.5** ([3])**.** *Если группа G одновременно реализует $\langle a_1, b_1, c_1\rangle$, ..., $\langle a_n, b_n, c_n\rangle$, и ее неприводимые представления имеют размерности $\{d_k\}$, то*

$$\sum_{i=1}^{n}(a_i b_i c_i)^{\omega/3} \leq \sum_k d_k^{\omega}.$$

В случае абелевой группы G, для любого k имеем k $d_k = 1$, $\sum_k d_k^{\omega} = |G|$, и неравенство принимает вид $\sum_{i=1}^{n}(a_i b_i c_i)^{\omega/3} \leq |G|$.

Для построения групп, обладающих свойством одновременных тройных произведений, хорошо подходит следующее усиление понятия сильного USP.

Определение 1.5 ([3])**.** Локальное сильное USP ширины k — подмножество $U \subset \{1,2,3\}^k$ такое, что для любой упорядоченной тройки $(u,v,w) \in U^3$, где не все u, v, w равны между собой, существует $i \in [k]$ такое, что упорядоченная тройка (u_i, v_i, w_i) совпадает с одной из

$$(1,2,1), (1,2,2), (1,1,3), (1,3,3), (2,2,3), (3,2,3).$$

"Локальность" заключается в том, что свойство в определении обычной USP должно выполняться для любых трех перестановок и какого-то элемента $u \in U$, а в локальных USP должно выполняться для любых трех элементов U. Любое локальное сильное USP, очевидно, является и просто сильным USP.

Локальные сильные USP полезны тем, что из них сразу получается конструкция группы, обладающей свойством одновременных тройных произведений.

***Теорема* 1.6** ([3])**.** *Пусть U — локальное сильное USP ширины k. Для каждого $u \in U$ определим подмножества $A_u, B_u, C_u \subset \mathrm{Cyc}_l^k$ следующим образом:*

$$A_u = \{x \in \mathrm{Cyc}_l^k : x_j \neq 0 \iff u_j = 1\},$$
$$B_u = \{x \in \mathrm{Cyc}_l^k : x_j \neq 0 \iff u_j = 2\},$$
$$C_u = \{x \in \mathrm{Cyc}_l^k : x_j \neq 0 \iff u_j = 3\}.$$

Тройки множеств A_u, B_u, C_u обладают свойством одновременных тройных произведений.

Доказательство. Пусть $u, v, w \in U$ не все равны между собой, и

$$a_u - a'_v + b_v - b'_w + c_w - c'_u = 0,$$

где $a_u \in A_u$, $a'_v \in A_v$, $b_v \in B_v$, $b'_w \in B_w$, $c_w \in C_w$, $c'_u \in C_u$. По определению локального сильного USP, существует $i \in [k]$ такое, что тройка (w_i, u_i, v_i) совпадает с одной из

$$(1,2,1), (1,2,2), (1,1,3), (1,3,3), (2,2,3), (3,2,3).$$

В каждом случае ровно одно слагаемое должно быть ненулевым, a'_v, b_v, a_u, c'_u, b'_w и c_w соответственно. В любом случае, такая сумма не может равняться 0 — противоречие, следовательно $u = v = w$.

То, что для каждого u тройка подмножеств A_u, B_u, C_u обладает свойством тройного произведения, очевидно, так как в каждой координате ненулевые значения принимаются ровно в одном из этих трех множеств.

□

Хотя определение локальных сильных USP и является усилением определения сильных USP, оказывается, что мощности сильных USP и локальных сильных USP совпадают.

***Предложение* 1.4** ([3])**.** *Ёмкость сильных USP достигается на локальных сильных USP. А именно, по сильному USP ширины k можно построить локальное сильное USP размера $|U|!$ и ширины $|U|k$.*

Доказательство. Пусть U — сильное USP ширины k, зафиксируем некоторый порядок элементов U: u_1, ..., $u_{|U|}$. Для каждой перестановки $\pi \in \mathrm{Sym}(U)$, определим соответствующий ей элемент U_π нового локального сильного USP как конкатенацию $\pi(u_1)$, ..., $\pi(u_{|U|})$. Тогда множество из всех U_π — локальное сильное USP, так как, по определению USP, для любых трех не всех равных между собой перестановок π_1, π_2, π_3, существует $u \in U$ и $i \in [k]$ реализующие свойство из определения сильного USP, и ровно в этой координате, заданной u и i, в построенном множестве будет выполняться свойство из определения локальной сильной USP. □

Таким образом, предложение 1.4 и теорема 1.5 дают следующую оценку на ω:

$$|U|(l-1)^{(k\omega/3)} \leq l^k$$
$$\log|U| + \frac{k\omega}{3}\log(l-1) \leq k\log l$$
$$\omega \leq \frac{3\log l}{\log(l-1)} - \frac{3\log|U|}{k\log(l-1)}$$
$$\omega \leq \frac{3(\log l - \log C)}{\log(l-1)}.$$

При $l = 6$ получаем $\omega < 2.48$.

1.4. Свойство одновременных двойных произведений

Для наших целей понадобится другое свойство из [3], более слабое, чем свойство одновременных тройных произведений, но допускающее более широкий класс конструкций.

Определение 1.6 ([3])**.** Подмножества S_1, S_2 группы G удовлетворяют свойству двойного произведения, если

$$q_1 q_2 = 1 \implies q_1 = q_2 = 1$$

при $q_i \in Q(S_i)$.

Определение 1.7 ([3])**.** n пар подмножеств A_i, B_i $(1 \leq i \leq n)$ группы G обладают свойством одновременных двойных произведений, если

- для каждого i пара подмножества A_i, B_i обладает свойством двойного произведения, и
- для любых i, j, k из $a_i(a'_j)^{-1}b_j(b'_k)^{-1} = 1$, где $a_i \in A_i$, $a'_j \in A_j$, $b_j \in B_j$, $b'_k \in B_k$, следует $i = k$.

Из группы G и n пар ее подмножеств A_i, B_i $(0 \leq i \leq n-1)$, обладающих свойством одновременных двойных произведений, можно построить группу с тройкой подмножеств, обладающую свойством тройного произведения. Пусть

$$\Delta_n = \{(a,b,c) \in \mathbb{Z}^3 : a+b+c = n-1, a,b,c \geq 0\}.$$

Определим тройки подмножеств G^3, проиндексированных $v = (v_1, v_2, v_3) \in \Delta_n$, следующим образом:

$$\widehat{A}_v = A_{v_1} \times \{1\} \times B_{v_3}$$
$$\widehat{B}_v = B_{v_1} \times A_{v_2} \times \{1\}$$
$$\widehat{C}_v = \{1\} \times B_{v_2} \times A_{v_3}$$

***Теорема* 1.7** ([3])**.** *Если n пар подмножеств A_i, B_i группы G обладают свойством одновременных двойных произведений, то следующие подмножества S_1, S_2, S_3 группы $H = (G^3)^{|\Delta_n|} \rtimes \mathrm{Sym}(\Delta_n)$ обладают свойством тройного произведения:*

$$S_1 = \{\widehat{a}\pi : \pi \in \mathrm{Sym}(\Delta_n), \widehat{a}_v \in \widehat{A}_v \text{ для всех } v\}$$
$$S_2 = \{\widehat{b}\pi : \pi \in \mathrm{Sym}(\Delta_n), \widehat{b}_v \in \widehat{B}_v \text{ для всех } v\}$$
$$S_3 = \{\widehat{c}\pi : \pi \in \mathrm{Sym}(\Delta_n), \widehat{c}_v \in \widehat{C}_v \text{ для всех } v\}.$$

***Теорема* 1.8** ([3])**.** *Если G — конечная группа, размерности неприводимых представлений которой равны $\{d_k\}$, и n пар подмножеств $A_i, B_i \subset G$ обладают свойством одновременных двойных произведений, то*

$$\left(\sum_{i=1}^{n}(|A_i||B_i|)^{\omega/2}\right)^{2/3} \leq \sum_k d_k^{\omega}.$$

Для сравнения результатов теоремы 1.8 и теоремы 1.5, представим, что в первом случае равны все $|A_i||B_i|$, а во втором все $|A_i||B_i||C_i|$, тогда неравенства почти совпадают, кроме того, что в первом случае в левой части окажется $n^{2/3}$, а во втором случае в левой части просто n. То есть, при равных размерах групп и равных произведениях размеров подмножеств, для одинаковых оценок на ω, количество пар подмножеств в случае одновременных двойных произведений должно быть в $3/2$ раза больше, чем количество троек в случае тройных. В следующем параграфе мы увидим, что ровно этот случай имеет место для оценки из прошлого параграфа.

1.5. 2-USP

В этом параграфе мы введём новое понятие: упрощение USP, которое позволит нам строить группы с парами подмножеств, обладающими свойством одновременных двойных произведений, похожим образом, как это было с локальными сильными USP.

Определение 1.8. 2-USP ширины k назовем подмножество $U \subset \{1,2\}^k$, такое, что для любой упорядоченной пары $(u,v) \in U^2$ такой, что $u \neq v$, существует $i \in [k]$, что $(u_i, v_i) = (1,2)$.

Иногда удобнее переформулировка: для любых двух $u, v \in U$ таких, что $u \neq v$ существуют $i, j \in [k]$, что $(u_i, v_i) = (1,2)$ и $(u_j, v_j) = (2,1)$.

Определение 2-USP напоминает определение локальной сильной USP, более того, можно рассматривать его как некоторое ослабление: рассмотрим $(u,v,w) \in U^3$, где u, v, w *попарно различны* (а не "не все равны между собой", как в определении локальной USP), тогда, если U является 2-USP, существует $i \in [k]$, что (u_i, v_i, w_i) равно одному из

$(1,2,1),(1,2,2)$, то есть 2-USP подходит под такое ограничение условия на локальное USP, которое запрещает каким-то двум из u,v,w быть равными. На самом деле, быть попарно различными — слишком сильное требование, достаточно $u \neq v$, так как даже если w равно u или v, тройку (u_i,v_i,w_i) это не портит. Сформулируем это в виде предложения.

***Предложение* 1.5.** *Пусть U — 2-USP, $(u,v,w) \in U^3$ — упорядоченная тройка его элементов, причем $u \neq v$, тогда существует $i \in [k]$ такой, что тройка (u_i,v_i,w_i) равна одной из $(1,2,1),(1,2,2)$.*

Аналогично с ёмкостью USP, можно определить и ёмкость 2-USP, однако посчитать ёмкость 2-USP заметно проще.

***Теорема* 1.9.** *Ёмкость 2-USP равна 2, существует 2-USP ширины $2k$ и размера $\binom{2k}{k}$.*

Доказательство. Построим 2-USP ширины $2k$: рассмотрим все подмножества $2k$ координат размера k. Каждому подмножеству сопоставим элемент $u \in \{1,2\}^{2k}$, такой, что $u_i = 2$ тогда и только тогда, когда i входит в выбранное подмножество координат. По построению, $|U| = \binom{2k}{k}$.

Докажем, что U — 2-USP. Рассмотрим $u,v \in U$, $u \neq v$. Каждому из них соответствует некоторое подмножество координат, при этом они одного размера, но не совпадают. Поэтому есть такие индексы i,j, что i лежит в подмножестве, соответствующем v, но не лежит в подмножестве, соответствующем u, а j — наоборот. Но это и значит, что $(u_i,v_i) = (1,2)$, а $(u_j,v_j) = (2,1)$.

Заметим, что $\lim_{n\to\infty} \binom{2k}{k}^{1/2k} = 2$, из чего сразу следует нижняя оценка мощности. Но оценка сверху очевидна, так как $|\{1,2\}^k| = 2^k$. □

Теперь научимся строить по 2-USP группу и пары подмножеств, обладающие свойством одновременных двойных произведений. Конструкция будет аналогична конструкции в теореме 1.6.

***Теорема* 1.10.** *Пусть U — 2-USP ширины k. Для каждого $u \in U$ определим подмножества $A_u, B_u \subset \mathrm{Cyc}_l^k$ следующим образом:*

$$A_u = \{x \in \mathrm{Cyc}_l^k : x_j \neq 0 \iff u_j = 1\},$$
$$B_u = \{x \in \mathrm{Cyc}_l^k : x_j \neq 0 \iff u_j = 2\}.$$

Пары множеств A_u, B_u обладают свойством одновременных двойных произведений.

Доказательство. Утверждение о том, что для каждого u множества A_u и B_u удовлетворяют свойству двойного произведения, очевидно — в каждой координате ненулевые значения принимают элементы ровно одного из этих двух множеств.

Пусть теперь $u, v, w \in U$, и

$$a_u - a'_v + b_v - b'_w = 0,$$

где $a_u \in A_u$, $a'_v \in A_v$, $b_v \in B_v$, $b'_w \in B_w$.

Пусть $u \neq w$, тогда по предложению 1.5 существует $i \in [k]$ такое, что (w_i, u_i, v_i) равно одному из $(1,2,1)$, $(1,2,2)$. В первом случае из четырех слагаемых не равно 0 только a'_v, во втором — только b_v, в каждом случае равенство всей суммы 0 невозможно, противоречие. □

Осталось подставить результат в теорему 1.8:

$$\begin{gathered}
|U|(l-1)^{(k\omega/2)} \leq l^{3k/2} \\
\frac{2}{3}\log|U| + \frac{k\omega}{3}\log(l-1) \leq k\log l \\
\omega \leq \frac{3\log l}{\log(l-1)} - \frac{2\log|U|}{k\log(l-1)} \\
\omega \leq \frac{3(\log l - \frac{2}{3}\log C)}{\log(l-1)}.
\end{gathered}$$

Последнее неравенство получилось тем же, что и неравенство в конце параграфа 1.3, с учетом того, что ёмкость локальных сильных USP оценивается как $2^{2/3}$, а ёмкость 2-USP равна 2. Соответственно, подставив в это неравенство $l = 6$ получаем $\omega < 2.48$.

Заметим, что оценка $\omega < 2.48$ была получена с помощью свойства одновременных двойных произведений и в [3], но без связи с USP и свойством одновременных тройных произведений.

2. Неприводимые представления

В этом разделе мы в параграфах 2.1, 2.2 и 2.4 введём известные результаты из теории представлений. В параграфе 2.5 с их помощью явно опишем неприводимые представления групп вида $A^n \rtimes \mathrm{Sym}_n$, где A — абелева, к которым сводятся все конструкции групп из [3], и на основе этой классификации получим формулу, позволяющую точнее оценивать ω. И в параграфах 2.3 и 2.6 мы в качестве примера построим неприводимые представления групп $(\mathrm{Cyc}_n^3)^2 \rtimes \mathrm{Cyc}_2$ и $(\mathrm{Cyc}_m^3)^3 \rtimes \mathrm{Sym}_3$, соответственно.

2.1. Индуцированные представления

Пусть $\rho : G \to \mathsf{GL}(V)$ — представление G, и ρ_H — его сужение на H. Пусть W — подпространство V, инвариантное относительно всех $\rho(h)$, $h \in H$. Обозначим за $\theta : H \to \mathsf{GL}(W)$ соответствующее представление H. Для $g \in G$, пространство $\rho(g)W$ зависит только от левого класса смежности gH: при $h \in H$, $\rho(gh)W = \rho(g)\rho(h)W = \rho(g)W$, так как $\rho(h)W = W$ для любого $h \in H$. Тогда, для левого класса смежности $\sigma \in G/H$ можно определить пространство $W_\sigma = \rho(g)W$, для любого $g \in \sigma$. Для $g \in G$, $\rho(g)$ переставляет разные W_σ, таким образом $\sum_{\sigma \in G/H} W_\sigma$ задает подпредставление V.

Определение 2.1. Представление ρ группы G над векторным пространством V индуцировано представлением θ группы $H \leq G$ над W, если V — прямая сумма W_σ, по $\sigma \in G/H$.

Определение допускает следующие переформулировки.

- Каждый $x \in V$ можно представить единственным образом в виде $\sum_{\sigma \in G/H} x_\sigma$, $x_\sigma \in W_\sigma$.
- Если R — система представителей G/H, векторное пространство V — прямая сумма $\rho(r)W$ по $r \in R$.

В частности, $\dim V = \sum_{\sigma \in G/H} \dim W_\sigma = [G : H] \cdot \dim W$.

Для заданного представления H всегда существует индуцированное представление G.

***Теорема* 2.1** ([8], глава 3, теорема 11)**.** *Пусть H — подгруппа G. Для любого представления $\theta : H \to \mathsf{GL}(W)$ существует индуцированное представление $\rho : G \to \mathsf{GL}(V)$,оно единственно с точностью до изоморфизма.*

Мы знаем размерность этого представления, это $\dim W \cdot [G : H]$. Более того, мы можем явно описать действие этого представления на V. Пусть R — система представителей G/H, $V = \bigoplus_{r_i \in R} r_i W$, и для любого $g \in G$ и любого $r_i \in R$ существует $h_i \in H$ и $\tilde{r}_i \in R$, что $gr_i = \tilde{r}_i h_i$. Элемент $v \in V$ представляется в виде $v = \sum r_i w_i$, $w_i \in W$, и

$$\rho(g)v = g \cdot v = g \cdot \sum r_i w_i = \sum (gr_i) \cdot w_i = \sum \tilde{r}_i (h_i \cdot w_i) = \sum \tilde{r}_i \theta(h_i) w_i. \qquad (2)$$

2.2. Классификация неприводимых представлений групп вида $A \rtimes H$

Нам понадобится известный подход к вычислению представлений групп вида $G = A \rtimes H$, где A — абелева. Его изложение взято из [8] (раздел 8.2).

Итак, пусть A — абелева группа, $G = A \rtimes H$, и A нормальна в G. Так как A — абелева, все её неприводимые представления одномерны и образуют группу $X = \mathrm{Hom}(A, \mathbb{C}^*)$. Группа G действует на X следующим образом

$$(g\chi)(a) = \chi(g^{-1}ag) \quad \text{при } g \in G, \chi \in X, a \in A.$$

Пусть $(\chi_i)_{i \in X/H}$ — система представителей для орбит при действии H на X, действие элементов из H индуцировано с G. Для каждого $i \in X/H$ обозначим за H_i стабилизатор χ_i — подгруппу H из тех h, для которых $h\chi_i = \chi_i$, и пусть $G_i = A \rtimes H_i$ — соответствующая подгруппа G. Распространим действие χ_i на всё G_i:

$$\chi_i(ah) = \chi_i(a) \quad \text{при } a \in A, h \in H.$$

Так как $h\chi_i = \chi_i$ для любого $h \in H_i$, χ_i — одномерное представление G_i. Пусть теперь ρ — неприводимое представление H_i, композицией с каноническим эпиморфизмом $G_i \to H_i$ из него получается представление $\tilde{\rho}$ группы G_i. Рассмотрим теперь представление $\chi_i \otimes \tilde{\rho}$ группы G_i, и индуцированное с него представление G обозначим за $\theta_{i,\rho}$.

Следующее предложение, доказанное в [8] (предложение 25), показывает, что мы таким образом получили все неизоморфные неприводимые представления G.

***Предложение* 2.1.** *В обозначениях выше верно следующее.*

1. *$\theta_{i,\rho}$ — неприводимое представление G.*
2. *Если $\theta_{i,\rho}$ и $\theta_{i',\rho'}$ изоморфны, то $i = i'$, а ρ изоморфно ρ'.*
3. *Любое неприводимое представление G изоморфно одному из $\theta_{i,\rho}$.*

2.3. Неприводимые представления $(\mathrm{Cyc}_n^3)^2 \rtimes \mathrm{Cyc}_2$

Пусть $B = \mathrm{Cyc}_n^3$ $(n \geq 2)$, $A = B^2$, $H = \mathrm{Cyc}_2$ и действует на A перестановкой компонент. Действуя по схеме из 2.2 вычислим неприводимые представления группы $G = A \rtimes H$ — первого примера группы, дающей нетривиальную оценку на ω из [3].

Пусть $H = \mathrm{Cyc}_2 = <z>$, элементы из G будем обозначать как $g = g_A g_H = g_A z^i$, $g_A \in A$, $g_H \in H$, $i \in \{0, 1\}$, элементы из A как $a = (a_1, a_2)$, $a_1, a_2 \in B$, элементы B как $x = (x_1, x_2, x_3)$, $x_1, x_2, x_3 \in \mathrm{Cyc}_n$, элементы из Cyc_n будем для удобства отождествлять с элементами $\mathbb{Z}/n\mathbb{Z}$.

Опишем, как действует сопряжение элементами из G на элементы из A. Элементы вида $g_A z^0$, $g_A \in A$, очевидно оставляют элементы A на месте — сопряжение происходит внутри абелевой группы A. Для элементов вида $g_A z$,

$$g^{-1}ag = g^{-1}(ag) = (-g_{A2}, -g_{A1})z(a + g_A)z = (a_2, a_1),$$

и A — нормальная подгруппа G.

Таким образом, те элементы A, для которых $a_1 = a_2$, не меняются, а все остальные разбиваются на пары, которые переходят друг в друга под действием сопряжения с любым элементом из G вида $g_A z$.

Неприводимые представления χ_α группы Cyc_n устроены просто — порождающий элемент должен отправиться в комплексный корень из 1 n-й степени. Если считать порождающим элементом класс единицы в отождествлении с $\mathbb{Z}/n\mathbb{Z}$, то $\chi_\alpha(1) = \exp(2\pi i\alpha/n) = \varepsilon^\alpha$, где α — целое число от 0 до $n-1$, и для удобства $\exp(2\pi i/n)$ обозначено за ε. И для произвольного элемента $a \in \mathrm{Cyc}_n$, $\chi_\alpha(a) = \varepsilon^{\alpha a}$, если отождествить a с остатком по модулю n и умножение α на a производить в $\mathbb{Z}$.

Так как A является произведением шести копий Cyc_n, неприводимые представления A это всевозможные тензорные произведения неприводимых представлений сомножителей. Таким образом, их можно параметризовать вектором из шести целых чисел от 0 до $n-1$ вида $(\alpha_{11}, \alpha_{12}, \alpha_{13}, \alpha_{21}, \alpha_{22}, \alpha_{23})$, и

$$\chi_\alpha(a) = \prod_{\substack{i\in\{1,2\}\\ j\in\{1,2,3\}}} \chi_{\alpha_{ij}}(a_{ij}) = \varepsilon^{\sum \alpha_{ij}a_{ij}} = \varepsilon^{\alpha\cdot a},$$

где элемент $a \in A$ также отождествляется с элементом $(\mathbb{Z}/n\mathbb{Z})^6$, и $\alpha \cdot a$ понимается как скалярное произведение.

Теперь посмотрим, как действуют элементы G на множестве $X = \{\chi_\alpha\}_{\alpha\in(\mathbb{Z}/n\mathbb{Z})^6}$ неприводимых представлений A.

$$(g\cdot\chi_\alpha)(a) = \chi_\alpha(g^{-1}ag) = \begin{cases} \varepsilon^{\alpha_1\cdot a_1+\alpha_2\cdot a_2} = \chi_\alpha(a), & \text{если } g = g_A z^0 \\ \varepsilon^{\alpha_1\cdot a_2+\alpha_2\cdot a_1} = \chi_{(\alpha_2,\alpha_1)}(a), & \text{если } g = g_A z \end{cases}$$

Таким образом, орбиты X под действием G следующие: для α с $\alpha_1 = \alpha_2$, $\{\chi_\alpha\}$ — одноэлементная орбита, а все остальные элементы X разбиваются на двухэлементные орбиты вида $\{(\alpha_1, \alpha_2), (\alpha_2, \alpha_1)\}$, $\alpha_1 \neq \alpha_2$. Первых будет n^3, а вторых $(n^6 - n^3)/2$. В качестве представителей из двухэлементных орбит выберем элемент с лексикографически меньшей первой компонентой.

Вычислим для i-го элемента из системы представителей подгруппу H_i группы $H = \mathrm{Cyc}_2$, оставляющую на месте этот элемент. Для представлений χ_α с $\alpha_1 = \alpha_2$ это будет вся группа H, поскольку они не меняются под действием вообще любого элемента G. Представления же из двухэлементных орбит заменяются на свою пару

под действием и элемента $z \in H$, поэтому для них $H_i = \{e_H\}$.

Неприводимых представлений у H два: $\rho_0 \equiv 1$ и $\rho_1 : \rho_1(z) = -1$. Поэтому каждое представление A вида χ_α, где $\alpha_1 = \alpha_2$ (для которой, как мы уже знаем, соответствующая $H_i = H$), даёт два неприводимых представления $G_i = A \rtimes H_i = A \rtimes H = G$: $\theta_{\alpha 0} = \chi_\alpha \otimes \rho_0$ и $\theta_{\alpha 1} = \chi_\alpha \otimes \rho_1$, которые определяются следующим образом:

$$\begin{aligned}
\theta_{\alpha 0} = (\chi_\alpha \otimes \rho_0)(g) = \chi_\alpha(g_A)\rho_0(g_H) &= \varepsilon^{\alpha_1 \cdot g_{A1} + \alpha_1 \cdot g_{A2}} \\
\theta_{\alpha 1} = (\chi_\alpha \otimes \rho_1)(g) = \chi_\alpha(g_A)\rho_1(g_H) &= \varepsilon^{\alpha_1 \cdot g_{A1} + \alpha_1 \cdot g_{A2}}(-1)^i, \text{где } g_H = z^i
\end{aligned}$$

Всего таким способом получается $2n^3$ одномерных представлений G, так как α_1 пробегает $(\mathbb{Z}/n\mathbb{Z})^3$.

Представления A вида χ_α, где $\alpha_1 \neq \alpha_2$, дают $H_i = \{e_H\}$, и соответственно одно представление для $G_i = A \rtimes H_i = A$: $\tilde{\theta}_\alpha = \chi_\alpha \otimes \rho_0 = \chi_\alpha$. Индекс $[G : A] = 2$, поэтому индуцированное на G представление θ_α будет двумерным, представим пространство, на котором оно действует, в виде $e_H\mathbb{C} \bigoplus z\mathbb{C}$. При этом, для $g = g_A e_H$, $ge_H = e_H g_A$ и $gz = z(g_{A2}, g_{A1})$, а для $g = g_A z$, $ge_H = g_A z e_H = z(g_{A2}, g_{A1})$ и $gz = g_A zz = g_A$. Таким образом, из формулы действия индуцированного представления (2) получаем:

$$\begin{aligned}
\theta_\alpha(g_A e_H)e_H &= e_H \varepsilon^{\alpha \cdot g_A} \\
\theta_\alpha(g_A e_H)z &= z\varepsilon^{\alpha_1 \cdot g_{A2} + \alpha_2 \cdot g_{A1}} \\
\theta_\alpha(g_A z)e_H &= z\varepsilon^{\alpha_1 \cdot g_{A2} + \alpha_2 \cdot g_{A1}} \\
\theta_\alpha(g_A z)z &= e_H \varepsilon^{\alpha \cdot g_A}.
\end{aligned}$$

Таким образом, в этом базисе

$$\begin{aligned}
\theta_\alpha(g_A e_H) &= \begin{pmatrix} \varepsilon^{\alpha \cdot g_A} & 0 \\ 0 & \varepsilon^{\alpha_1 \cdot g_{A2} + \alpha_2 \cdot g_{A1}} \end{pmatrix}, \\
\theta_\alpha(g_A z) &= \begin{pmatrix} 0 & \varepsilon^{\alpha \cdot g_A} \\ \varepsilon^{\alpha_1 \cdot g_{A2} + \alpha_2 \cdot g_{A1}} & 0 \end{pmatrix}.
\end{aligned}$$

Всего таких двумерных представлений будет $(n^6 - n^3)/2$, они параметризуются множеством $\{\alpha \in (\mathbb{Z}/n\mathbb{Z})^6 : \alpha_1 \text{ лексикографически меньше } \alpha_2\}$.

Зная все неприводимые представления, можно уточнить оценку на ω. Как было показано в [3], в группе G свойством тройного произведения обладают множества $|S_1|$, $|S_2|$, $|S_3|$, каждое размера $2n(n-1)$. По теореме 1.2,

$$\begin{aligned}
(2n(n-1))^\omega &\leq 2n^3 1^\omega + \frac{n^6 - n^3}{2} 2^\omega \\
-(2n(n-1))^\omega + 2n^3 + \frac{n^6 - n^3}{2} 2^\omega &\geq 0.
\end{aligned}$$

Рассмотрим левую часть как функцию от ω при фиксированном n, и вычислим её производную:

$$\left(-(2n(n-1))^{\omega} + 2n^3 + \frac{n^6 - n^3}{2}2^{\omega}\right)' =$$
$$-\log(2n(n-1))(2n(n-1))^{\omega} + (\log 2)\frac{n^6 - n^3}{2}2^{\omega} =$$
$$2^{\omega}(\alpha - \beta\gamma^{\omega}),$$

где α, β, γ — положительные константы, и $\gamma > 1$. Отсюда видно, что знак производной может измениться не более одного раза, и при достаточно больших значениях ω функция убывает. Таким образом, если для некоторого значения ω из той области, где функция убывает, значение функции отрицательно, то и для всех больших ω оно отрицательно, и значит они не подходят. В нуле функция заведомо положительна ($n \geq 2$), поэтому значения ω из $[2, 3]$ точно относятся к убывающей части.

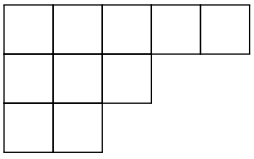
Таким образом, при $n = 17$ мы получаем оценку $\omega < 2.908776$, так как при значении из правой части функция отрицательна. При использовании же как в [3] более грубого неравенства $(2n(n-1))^{\omega} \leq 2^{\omega-2}2n^6$, также при $n = 17$, получается наилучшая оценка $\omega < 2.908795$, что несколько хуже.

2.4. Неприводимые представления симметрической группы Sym_n

Для классификации представлений групп вида $A^n \rtimes \mathrm{Sym}_n$, с помощью которых в [3] получаются алгоритмы быстрого матричного умножения, нужно в первую очередь знать неприводимые представления группы Sym_n. Эта тема хорошо изучена, и ниже мы изложим необходимые для нашего случая факты, подробно рассмотренные и доказанные в [6].

Как и в случае любой группы, неизоморфных неприводимых представлений Sym_n столько же, сколько классов сопряженности. В случае Sym_n, класс сопряженности задаётся цикловым типом перестановки, то есть разбиением числа n на слагаемые $\lambda = \{\lambda_i\}_{i=1}^k$, $\sum_{i=1}^k \lambda_i = n$, $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k > 0$. Разбиению на слагаемые λ соответствует диаграмма Юнга — таблица из ячеек, состоящая из k выровненных по левому краю рядов, такая что в i-м ряду λ_i ячеек.

Например, разбиению на слагаемые числа $10 = 5 + 3 + 2$ соответствует класс сопряженности перестановок с одним циклом длины 5, одним циклом длины 3 и одним циклом длины 2, и следующая диаграмма Юнга:



Для Sym_n, в отличие от произвольных групп, каждому классу сопряженности,

или разбиению, можно явно поставить в соответствие неприводимое представление — некоторую проекцию регулярного представления Sym_n, задав таким образом их все.

А именно, для заданного разбиения λ рассмотрим соответствующую ей каноническую таблицу Юнга — диграмму Юнга, заполненную числами от 1 до n по рядам сверху вниз. Например, каноническая таблица для разбиения $10 = 5 + 3 + 2$:

1	2	3	4	5
6	7	8		
9	10			

В общем случае таблица Юнга — любая нумерация ячеек диаграммы Юнга числами от 1 до n, но здесь смена нумерации лишь заменит представление на изоморфное.

Теперь любая перестановка из Sym_n действует на таблице Юнга для разбиения λ переставлением ячеек. Выделим две связанные с этим действием подгруппы Sym_n:

$$P_\lambda = \{\pi \in \mathrm{Sym}_n : \pi \text{ оставляет на месте все строки таблицы } \lambda\},$$
$$Q_\lambda = \{\pi \in \mathrm{Sym}_n : \pi \text{ оставляет на месте все столбцы таблицы } \lambda\}.$$

В частности, $P_\lambda \cong \mathrm{Sym}_{\lambda_1} \times \mathrm{Sym}_{\lambda_2} \times \cdots \times \mathrm{Sym}_{\lambda_k}$.

Рассмотрим соответствующие этим группам элементы групповой алгебры $\mathbb{C}\mathrm{Sym}_n$

$$a_\lambda = \sum_{g \in P_\lambda} e_g \text{ и } b_\lambda = \sum_{g \in Q_\lambda} \mathrm{sgn}(g) e_g,$$

и рассмотрим элемент $\mathbb{C}\mathrm{Sym}_n$

$$c_\lambda = a_\lambda b_\lambda = \sum_{\substack{g \in P_\lambda \\ h \in Q_\lambda}} \mathrm{sgn}(h) e_{gh}.$$

Элемент c_λ называется симметризатором Юнга для данной таблицы, и задаёт неприводимое представление $\mathbb{C}\mathrm{Sym}_n \cdot c_\lambda$.

***Теорема* 2.2** ([6])**.** *Представления $\mathbb{C}\mathrm{Sym}_n \cdot c_\lambda$ группы Sym_n неприводимы и неизоморфны для разных разбиений λ.*

При этом в качестве базиса для этого представления можно взять стандартные таблицы Юнга, то есть те таблицы, в которых ячейки возрастают в каждой строке и столбце, рассматривая таблицы как перестановки ячеек и соответственно элементы Sym_n. Число стандартных таблиц Юнга для данного разбиения λ задаётся формулой крюков

$$\frac{n!}{\prod_x \mathrm{hook}(x)},$$

где произведение берётся по всем ячейкам диаграммы, а $\mathrm{hook}(x)$ — число ячеек, лежащих правее в той же строке, что и x, и ниже в том же столбце, считая саму ячейку x. Соответственно, таким будет и размерность представления ρ_λ, заданного разбиением λ.

Чтобы явно задать образ элемента $\pi \in \mathrm{Sym}_n$ под действием ρ_λ в базисе из стандартных таблиц Юнга, нужно для каждого i вычислить разложение элемента $\pi s_i c_\lambda$ в базисе $\{s_i c_\lambda\}$ пространства $\mathbb{C}\mathrm{Sym}_n \cdot c_\lambda$, где $\{s_i\}$ — стандартные таблицы Юнга для разбиения λ.

Для разбиения $\lambda = \{n\}$ в диаграмме Юнга одна строка, $P_\lambda = \mathrm{Sym}_n$, $Q_\lambda = \{e\}$, $c_\lambda = \sum_{g \in \mathrm{Sym}_n} e_g$. Существует единственная стандартная таблица Юнга, совпадающая с канонической, поэтому представление $\mathbb{C}\mathrm{Sym}_n \cdot c_\lambda$ одномерно. Хотя для этого достаточно и того, что для любого $\pi \in \mathrm{Sym}_n$, $\pi \cdot c_\lambda = c_\lambda$, так как умножение на фиксированный элемент лишь переставляет элементы группы. Из последнего наблюдения следует, что $\rho_\lambda(\pi) \equiv 1$, то есть соответствующее представление — тривиальное.

Если взять $\lambda = \{1, 1, \ldots, 1\}$, то, наоборот, $P_\lambda = \{e\}$, $Q_\lambda = \mathrm{Sym}_n$ и $c_\lambda = \sum_{g \in \mathrm{Sym}_n} \mathrm{sgn}(g) e_g$. При умножении чётной перестановки на c_λ получится c_λ, а при умножении нечётной каждое слагаемое поменяет знак, и получится $-c_\lambda$. Таким образом, мы получили представление $\rho_\lambda(\pi) = \mathrm{sgn}(\pi)$.

Определим с помощью общего метода все неприводимые представления Sym_3. Есть три разбиения: $\{3\}$, $\{2, 1\}$ и $\{1, 1, 1\}$. Первое соответствует тривиальному представлению, а третье — знаку перестановки, осталось определить представление для $\lambda = \{2, 1\}$.

Существует две стандартные таблицы Юнга для этого разбиения.

1	2
3	

1	3
2	

Соответственно, представление будет двумерным. $P_\lambda = \{123, 213\}$, $Q_\lambda = \{123, 312\}$, $c_\lambda = e_{123} + e_{213} - e_{321} - e_{312}$. Базисом будет

$$v_1 = c_\lambda = e_{123} + e_{213} - e_{321} - e_{312}$$
$$v_2 = 132 \cdot c_\lambda = e_{132} + e_{231} - e_{312} - e_{321},$$

действие элементов Sym_3 на них:

$$
\begin{aligned}
&123 \cdot v_1 = v_1\\
&123 \cdot v_2 = v_2\\
&132 \cdot v_1 = v_2\\
&132 \cdot v_2 = v_1\\
&213 \cdot v_1 = e_{213} + e_{123} - e_{231} - e_{132} = v_1 - v_2\\
&213 \cdot v_2 = e_{312} + e_{321} - e_{231} - e_{132} = -v_2\\
&321 \cdot v_1 = e_{321} + e_{312} - e_{123} - e_{213} = -v_1\\
&321 \cdot v_2 = e_{231} + e_{132} - e_{123} - e_{213} = -v_1 + v_2\\
&231 \cdot v_1 = e_{231} + e_{132} - e_{213} - e_{123} = -v_1 + v_2\\
&231 \cdot v_2 = e_{321} + e_{312} - e_{213} - e_{123} = -v_1\\
&312 \cdot v_1 = e_{312} + e_{321} - e_{132} - e_{231} = -v_2\\
&312 \cdot v_2 = e_{213} + e_{123} - e_{132} - e_{231} = v_1 - v_2,
\end{aligned}
$$

или в матричном виде:

$$
\begin{aligned}
\rho(123) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\\
\rho(132) &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\\
\rho(213) &= \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}\\
\rho(321) &= \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}\\
\rho(231) &= \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}\\
\rho(312) &= \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.
\end{aligned}
$$

2.5. Неприводимые представления групп вида $A^n \rtimes \mathrm{Sym}_n$

Пусть A — абелева группа, Sym_n действует на A^n перестановкой компонент. Опишем неприводимые представления группы $G = A^n \rtimes \mathrm{Sym}_n$.

Элемент $g \in G$ будем обозначать как $g_A g_S$, где $g_A \in A^n$, $g_S \in \mathrm{Sym}_n$, для элемента $a \in A^n$ за $a_1, a_2, \ldots, a_n$ обозначим его компоненты, каждая из которых лежит в A.

Рассмотрим сопряжение элемента $a \in A$ элементом $g \in G$:

$$g^{-1}ag = (g_S^{-1} \cdot (-g_A))g_S^{-1}(a + g_A)g_S = g_S^{-1} \cdot a,$$

в частности A^n — нормальная подгруппа G.

Неприводимые представления группы A естественно нумеруются элементами A, а представления A^n — вектором из n элементов A, то есть собственно элементом A_n, и

$$\chi_\alpha(a) = \prod_{i=1}^{n} \chi_{\alpha_i}(a_i),$$

где $a, \alpha \in A^n$, χ_α — соответствующее неприводимое представление A^n, а χ_{α_i} — соответствующее элементу $\alpha_i \in A$ неприводимое представления A.

Нужно определить, как устроены орбиты при действии элементов из G на множестве неприводимых представлений $X = \{\chi_\alpha\}_{\alpha \in A^n}$ группы A^n. Действие определено как

$$(g \cdot \chi_\alpha)(a) = \chi_\alpha(g^{-1}ag) = \chi_\alpha(g_S^{-1} \cdot a) = \prod_{i=1}^{n} \chi_{\alpha_i}(a_{g_S^{-1}(i)}) = \prod_{i=1}^{n} \chi_{\alpha_{g_S(i)}}(a_i) = \chi_{g_S \cdot \alpha}(a),$$

где $g \in G$, $a, \alpha \in A^n$.

Таким образом, орбита представления χ_α при некотором фиксированном $\alpha \in A^n$ это представления вида $\chi_{\pi \cdot \alpha}$ по всем $\pi \in \mathrm{Sym}_n$, то есть представления, заданные всевозможными перестановками компонент α.

Определим по α разбиение числа n на слагаемые: пусть $\mu_a = |\{i \in [n] : \alpha_i = a\}|$, $a \in A$, а $\lambda = \{\lambda_i\}_{i=1}^{k}$, $k \leq n$ — упорядочивание $\{\mu_a\}_{a \in A}$ по убыванию величины, без нулевых элементов (ясно, что ненулевых не более n). Размер орбиты χ_α определяется только λ: он равен

$$\frac{n!}{\lambda_1! \dots \lambda_k!} = \binom{n}{\lambda},$$

так как можно получить любую перестановку тех же самых элементов, то есть λ_1 элементов a_1, λ_2 элементов a_2, ..., λ_k элементов a_k, $a_i \in A$, и все они различны.

Назовем такие орбиты орбитами типа λ. Количество орбит такого типа — это число способов выбрать элемент из A для каждого из a_i, они должны быть различны, и если в разбиении есть одинаковые слагаемые, то порядок на них не важен:

$$o_\lambda = \frac{(|A|)_k}{\prod_{i=1}^{n} \tilde{\lambda}_i!},$$

где $(|A|)_k = |A| \cdot (|A| - 1) \cdot \dots \cdot (|A| - k + 1)$ — убывающий факториал, а $\tilde{\lambda}_i = |\{j \in [k] : \lambda_j = i\}|$ — число слагаемых разбиения, равных i.

В качестве представителя орбиты выберем элемент χ_α, для которого в первых λ_1 компонентах стоит a_1, в следующих λ_2 a_2, и так далее. При равных λ_i считаем,

что раньше идут меньшие a_i по некоторому фиксированному отношению порядка на элементах A.

Подгруппа H_α элементов $H = \mathrm{Sym}_n$, оставляющих на месте представителя орбиты χ_α, будет состоять из тех перестановок, что оставляют на месте группы равных элементов α, возможно, меняя их порядок. Поскольку в представителе сначала идут λ_1 элементов a_1, затем λ_2 элементов a_2, и так далее, то элементы H_α оставляют на месте первые λ_1 элементов, следующие λ_2, и так далее, то есть оставляют на месте строки канонической таблицы Юнга для λ. То есть, $H_\alpha = P_\lambda$ в обозначениях 2.4, и благодаря выбору представителей зависит только от λ.

Поскольку $P_\lambda \cong S_{\lambda_1} \times S_{\lambda_2} \times \cdots \times S_{\lambda_k}$, мы знаем и неприводимые представления P_λ — это всевозможные произведения $\rho = \bigotimes_{i=1}^k \rho_i$, где ρ_i — неприводимое представление S_{λ_i}. При фиксированном представлении ρ, нам нужно построить представление $\theta_{\alpha,\rho}$, которое задаётся как индуцированное с $A^n \rtimes P_\lambda$ на $A^n \rtimes \mathrm{Sym}_n$ представление $\chi_\alpha \otimes \rho$.

В качестве системы представителей R левых классов смежности $\mathrm{Sym}_n / P_\lambda$ возьмём перестановки, соответствующие таблицам Юнга для λ, в которых числа в ячейках одной строки упорядочены по возрастанию, очевидно что в каждом классе ровно один такой элемент. То есть, для заданного элемента $g_S \in \mathrm{Sym}_n$ и для любого $r_i \in R$ существует $\tilde{r}_i \in R$ и $h_i \in P_\lambda$, что $g_S r_i = \tilde{r}_i h_i$. В терминах таблиц Юнга, $g_S r_i$ — некоторая таблица, $\tilde{r}_i$ — она же, только каждая строка упорядочена по возрастанию, а h_i — обратная перестановка к этому упорядочиванию по строкам.

Эта же система будет и системой представителей для $A^n \rtimes \mathrm{Sym}_n / A^n \rtimes P_\lambda$, если отождествить элемент из Sym_n с образом его канонического вложения. Действие будет следующим:

$$g r_i = (g_A g_S) r_i = g_A \tilde{r}_i h_i = \tilde{r}_i g_A^{\tilde{r}_i^{-1}} h_i,$$

где $g_A \in A^n$, $g_A^{\tilde{r}_i^{-1}}$ получен из g_A перестановкой компонент в соответствии с $\tilde{r}_i \in \mathrm{Sym}_n$, и $g_A^{\tilde{r}_i^{-1}} h_i \in A^n \rtimes P_\lambda$.

Индуцированное представление будем считать действующим на $V = \bigoplus_{r_i \in R} r_i W$, где $\rho : P_\lambda \to \mathsf{GL}(W)$, и по (2) образ элемента $g \in G$ действует на элементах этого пространства как

$$\theta(g) v = (g_A g_S) \cdot \left(\sum r_i w_i \right) = \sum \tilde{r}_i \chi_\alpha(g_A^{\tilde{r}_i^{-1}}) \rho(h_i) w.$$

Таким образом мы перечислили все представления. Для каждого разбиения λ числа n на слагаемые, есть

$$o_\lambda = \frac{(|A|)_k}{\prod_{i=1}^n \tilde{\lambda}_i!}$$

орбит представлений A такого типа, и каждая из них вместе с неприводимым представлением ρ группы $P_\lambda \cong \prod_{i=1}^k S_{\lambda_i}$ даёт индуцированное представление группы G размерности $\binom{n}{\lambda} \cdot \dim \rho$.

Чтобы получать оценки на ω по теореме 1.2, нужно подставить в правую часть неравенства, которая задаётся как

$$\sum_{\theta}(\dim\theta)^{\omega}$$

размерности всех неприводимых представлений группы, в нашем случае получится

$$\sum_{\lambda}\frac{(|A|)_k}{\prod_{i=1}^{n}\tilde{\lambda}_i!}\sum_{\{\rho_j\}_{j=1}^{k}}\left(\binom{n}{\lambda}\prod_{j=1}^{k}\dim\rho_j\right)^{\omega},$$

или

$$\sum_{\lambda}\frac{(|A|)_k}{\prod_{i=1}^{n}\tilde{\lambda}_i!}\binom{n}{\lambda}^{\omega}\prod_{j=1}^{k}\sum_{\rho_j}(\dim\rho_j)^{\omega}, \tag{3}$$

где каждое ρ_j — неприводимое представление S_{λ_j}, соответствующее неприводимому представлению ρ группы P_λ.

Применим полученное к конструкциям групп из [3]. Одна из продуктивных конструкций, описанная в части 1.2, по сильному USP размера n и ширины k получает подходящие для матричного умножения подмножества S_1, S_2, S_3 в группе $(\mathrm{Cyc}_m^l)^n \rtimes \mathrm{Sym}_n$ (предложение 1.3).

Подмножества S_1, S_2, S_3 таковы, что $|S_1||S_2||S_3| = n!^3(m-1)^{nl}$. Из теоремы 1.2 и формулы (3) следует неравенство

$$(n!^3(m-1)^{nl})^{\omega/3} \le \sum_{\lambda}\frac{(m^l)_k}{\prod_{i=1}^{n}\tilde{\lambda}_i!}\binom{n}{\lambda}^{\omega}\prod_{j=1}^{k}\sum_{\rho_j}(\dim\rho_j)^{\omega}, \tag{4}$$

из которого можно извлечь оценку на ω. В [3] используется более грубое неравенство

$$(n!^3(m-1)^{nl})^{\omega/3} \le d^{\omega-2}|G| = n!^{\omega-1}m^{nl}, \tag{5}$$

где d — максимальная размерность представления, равная $n!$.

В [3] рассматривается две конструкции сильных USP: размера 2^l и ширины l (предложение 1.1), и размера $2^{l-1}(2^l+1)$ и ширины $3l$ (предложение 1.2). Оценки на ω, получающиеся из небольших USP видов с использованием неравенств (4) и (5), приведены в таблицах 1 и 2 для первой и второй конструкции, соответственно. Оценки получены численно, код программы находится в Приложении А. Выбор m минимизирует каждую из оценок. Для заданных m и ω, вычисление производится по формуле 3 за квадратичное от количества разбиений числа n время, где n — размер соответствующей USP. Выбор USP, для которых вычислена оценка, обусловлен экспоненциальным ростом их размеров, и экспоненциальным ростом числа разбиений. Например, следующая по размеру USP из предложения 1.2 будет иметь ширину 9 и размер 36, и различных разбиений будет 17977, что приводит к значительному времени работы и

большим промежуточным величинам в вычислениях.

Размер	Ширина	m	Неравенство (4)	Неравенство (5)
2	2	24	2.8747	2.8749
4	4	20	2.849884	2.849885
8	6	17	2.82654699	2.82654701
16	8	15	2.8060318351	2.8060318353

Таблица 1: Оценки на ω для USP из предложения 1.1.

Размер	Ширина	m	Неравенство (4)	Неравенство (5)
3	3	20	2.84940	2.84942
10	6	14	2.7922388	2.7922389

Таблица 2: Оценки на ω для USP из предложения 1.2.

По таблице 1 видно, что с ростом размеров выигрыш от использования более точной оценки уменьшается, соответственно есть основания полагать, что асимптотически разница между (4) и (5) несущественна.

2.6. Неприводимые представления $(\mathrm{Cyc}_m^3)^3 \rtimes \mathrm{Sym}_3$

Применим теперь технику из параграфа 2.5 чтобы описать неприводимые представления группы $G = (\mathrm{Cyc}_m^3)^3 \rtimes \mathrm{Sym}_3$, которая соответствует USP ширины 3 и размера 3.

Рассмотрим отдельно все три возможные разбиения λ числа 3 на слагаемые. Если $\lambda = \{3\}$, это соответствует неприводимому представлению χ_α группы $(\mathrm{Cyc}_m^3)^3$ такому что $\alpha_1 = \alpha_2 = \alpha_3$. Таких представлений столько, сколько различных неприводимых представлений есть у Cyc_m^3, то есть m^3.

Орбита χ_α в таком случае состоит из одного элемента, поэтому подгруппа H_i элементов Sym_3, оставляющих это представление на месте, совпадает со всем Sym_3. Тогда для каждого из неприводимых представлений ρ группы Sym_3, которых три: два одномерных и одно двумерное (как мы знаем из параграфа 2.4), мы получаем неприводимое представление группы G как

$$\theta_{\alpha,\rho}(g) = \varepsilon^{(g_{A1}+g_{A2}+g_{A3})\cdot\alpha_1}\rho(g_S),$$

где $g = g_A g_S \in G$, $g_A \in A = \mathrm{Cyc}_m^3$, $g_S \in \mathrm{Sym}_3$, $\varepsilon = \exp(2\pi i/m)$. Всего таким образом мы получим $2m^3$ одномерных представлений, и m^3 двумерных.

Рассмотрим разбиение $\lambda = \{2, 1\}$. Это соответствует представлению χ_α с двумя равными компонентами из трёх. Орбитой будут всевозможные перестановки компонент, и в качестве представителя мы выбираем такой χ_α, что $\alpha_1 = \alpha_2 \neq \alpha_3$. Всего

таких орбит будет $m^3(m^3-1)$ — нужно выбрать элемент Cyc_m^3 для $\alpha_1=\alpha_2$, и другой элемент для α_3.

Для такого выбора представителей, χ_α оставляется на месте подгруппой $H_i=\{e_S,(12)\}$. У этой группы есть два неприводимых представления — тривиальное и задающее знак перестановки, оба одномерны. Представление $\theta_{\alpha,\rho}$ группы G индуцируется с представления $\chi_\alpha\otimes\rho$ группы $A^3\rtimes H_i$, и будет иметь размерность 3, так как таков индекс подгруппы H_i в Sym_3. Стандартным образом введём систему представителей левых классов смежности Sym_n/H_i как таблицы Юнга, строки в которых упорядочены. В данном случае это будут 123, 132 и 312. Выпишем матрицы для образов элементов G, для которых g_S — транспозиция, из-за мультипликативности достаточно знать образы только таких элементов:

$$\theta_{\alpha,\rho}(g_A(12))=\begin{pmatrix}\varepsilon^{(g_{A1}+g_{A2})\cdot\alpha_1+g_{A3}\cdot\alpha_3}\rho(12) & 0 & 0\\ 0 & 0 & \varepsilon^{(g_{A1}+g_{A3})\cdot\alpha_1+g_{A2}\cdot\alpha_3}\quad 0\\ 0 & \varepsilon^{(g_{A2}+g_{A3})\cdot\alpha_1+g_{A1}\cdot\alpha_3} & 0\end{pmatrix},$$

так как

$$213\cdot 123=123\cdot 213$$
$$213\cdot 132=312\cdot 123$$
$$213\cdot 312=132\cdot 123,$$

$$\theta_{\alpha,\rho}(g_A(12))=\begin{pmatrix}0 & 0 & \varepsilon^{(g_{A1}+g_{A2})\cdot\alpha_1+g_{A3}\cdot\alpha_3}\rho(12)\\ 0 & \varepsilon^{(g_{A1}+g_{A3})\cdot\alpha_1+g_{A2}\cdot\alpha_3}\rho(12) & 0\\ \varepsilon^{(g_{A2}+g_{A3})\cdot\alpha_1+g_{A1}\cdot\alpha_3}\rho(12) & 0 & 0\end{pmatrix},$$

так как

$$321\cdot 123=312\cdot 213$$
$$321\cdot 132=132\cdot 213$$
$$321\cdot 312=123\cdot 213,$$

$\theta_{\alpha,\rho}(g_A(12)) =$

$$\begin{pmatrix} 0 & \varepsilon^{(g_{A1}+g_{A2})\cdot\alpha_1+g_{A3}\cdot\alpha_3} & 0 \\ \varepsilon^{(g_{A1}+g_{A3})\cdot\alpha_1+g_{A2}\cdot\alpha_3} & 0 & 0 \\ 0 & 0 & \varepsilon^{(g_{A2}+g_{A3})\cdot\alpha_1+g_{A1}\cdot\alpha_3}\rho(12) \end{pmatrix},$$

так как

$$132 \cdot 123 = 132 \cdot 123$$
$$132 \cdot 132 = 123 \cdot 123$$
$$132 \cdot 312 = 312 \cdot 213.$$

Всего так получается $2m^3(m^3-1)$ трёхмерных представлений.

В случае разбиения $\lambda = \{1,1,1\}$, элементы α состоят из трёх различных компонент. Орбита состоит из всевозможных перестановок, то есть имеет размер 6, а всего таких орбит $\binom{m^3}{3}$. Группа H_i здесь будет тривиальной, её представление тоже бывает только тривиальное, а размерности индуцированных представлений будут равны 6 — представителями левых классов смежности G/A^3 будут все перестановки из Sym_3.

Для элемента $g = g_A g_S \in G$, $\theta_\alpha(g) \cdot e_\pi = e_{g_S\cdot\pi}\chi_\alpha(g_A^{(g_S\cdot\pi)^{-1}})$, таким образом матрица получится как в регулярном представлении, только на месте единицы в строке π будет стоять $\chi_\alpha(g_A^{\pi^{-1}})$. Например, для $g_S = (12)$, матрица будет такой

$\theta_\alpha(g_A(12)) =$

$$\begin{pmatrix} 0 & (g_A) & 0 & 0 & 0 & 0 \\ (g_{A2}, g_{A1}, g_{A3}) & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & (g_{A3}, g_{A2}, g_{A1}) & 0 \\ 0 & 0 & 0 & 0 & 0 & (g_{A1}, g_{A3}, g_{A2}) \\ 0 & 0 & (g_{A3}, g_{A1}, g_{A2}) & 0 & 0 & 0 \\ 0 & 0 & 0 & (g_{A2}, g_{A3}, g_{A1}) & 0 & 0 \end{pmatrix},$$

где к каждому элементу из A^3 нужно применить χ_α. Считаем, что элементы базиса упорядочены как $e_{123}, e_{213}, e_{321}, e_{132}, e_{231}, e_{312}$.

Всего таким образом получается $\binom{m^3}{3}$ шестимерных представлений.

Заключение

В рамках настоящей работы получены следующие результаты.

- Продемонстрирован новый подход к получению оценки на экспоненту матричного умножения $\omega < 2.48$.
- Сформулирована техника для вычисления неприводимых представлений семейства групп из [3], дающих эффективные алгоритмы матричного умножения, что необходимо для потенциальной реализации подобных алгоритмов.
- Из явной классификации неприводимых представлений получена более точная чем в [3] формула для оценки ω. С её помощью уточнена временная сложность для алгоритмов из [3], основанных на группах малого размера. Эмпирически показано, что с ростом размера групп выигрыш от более точной оценки падает.

A. Вычисление оценок на ω

```
from collections import Counter

def get_partitions(n, maxl, cur, res):
    if n == 0:
        res.append(cur[:])
        return
    for i in range(maxl, 0, -1):
        cur.append(i)
        get_partitions(n - i, min(n - i, i), cur, res)
        cur.pop()
def get_hook(n, p):
    res = fact[n]
    for i in range(len(p)):
        for j in range(p[i]):
            d = p[i] - j
            g = i + 1
            while (g < len(p) and p[g] > j):
                g += 1
            d += g - i - 1
            res //= d
    return res
def get_den(p):
    cur = 0
    prev = 0
    res = 1
    for l in p:
        if l != prev:
            res *= fact[cur]
            cur = 0
        cur += 1
        prev = l
    return res * fact[cur]
def get_reps_bound(n, asize, omega):
    res = 0
    for p in partitions[n]:
        ak = 1
        for i in range(len(p)):
```

```
            ak *= (asize - i)
        cur = ak // get_den(p)
        binom = fact[n]
        for l in p:
            binom //= fact[l]
        binom = binom ** omega
        cur *= binom
        for l in p:
            sum = 0
            for k, v in sym_reps[l].items():
                sum += v * k**omega
            cur *= sum
        res += cur
    return res


N = 22
fact = [1] * (N + 1)
partitions = [[] for _ in range(N + 1)]
sym_reps = [Counter() for _ in range(N + 1)]
for n in range(1, N + 1):
    fact[n] = fact[n - 1] * n
    get_partitions(n, n, [], partitions[n])
    for p in partitions[n]:
        sym_reps[n][get_hook(n, p)] += 1

def bound_coarse(n, k, m, omega):
    return (fact[n]**(omega - 1) * m **(n * k)
        - fact[n]**omega * (m - 1) ** (n * k * omega / 3))
def bound_fine(n, k, m, omega):
    return (get_reps_bound(n, m**k, omega)
        - fact[n]**omega * (m - 1) ** (n * k * omega / 3))

STEP_FRAC = 0.01
def get_omega(n, k, m, bound):
    omega = 3
    step = STEP_FRAC
    for it in range(6):
        while omega > 2:
```

```
            if bound(n, k, m, omega) < 0:
                omega -= step
            else:
                break
        omega += step
        step *= STEP_FRAC
    return omega

for i in (1, 2):
    n = 2**(i - 1) * (2**i + 1)
    k = 3 * i
    print(n, k)
    print(min([(get_omega(n, k, m, bound_coarse), m)
        for m in range(3, 30)]))
    print(min([(get_omega(n, k, m, bound_fine), m)
        for m in range(3, 30)]))
for i in range(1, 5):
    n = 2**i
    k = 2 * i
    print(n, k)
    print(min([(get_omega(n, k, m, bound_coarse), m)
        for m in range(3, 30)]))
    print(min([(get_omega(n, k, m, bound_fine), m)
        for m in range(3, 30)]))
```

Список литературы

[1] J. Blasiak, T. Church, H. Cohn, J. A. Grochow, E. Naslund, W. F. Sawin, and C. Umans. On cap sets and the group-theoretic approach to matrix multiplication. *Discrete Analysis*, 2017(3):27pp, 2017.

[2] P. Bürgrisser, M. Clausen, and M. A. Shokrollahi. *Algebraic Complexity Theory*, volume 315 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, 1997.

[3] H. Cohn, R. Kleinberg, B. Szegedy, and C. Umans. Group-theoretic algorithms for matrix multiplication. In *Proceedings of the 46th Annual Symposium on Foundations of Computer Science*, pages 379–388, Pittsburgh, PA, 23–25 October 2005. IEEE Computer Society. arXiv:math.GR/0511460.

[4] H. Cohn and C. Umans. A group-theoretic approach to fast matrix multiplication. In *Proceedings of the 44th Annual Symposium on Foundations of Computer Science*, pages 438–449, Cambridge, MA, 11–14 October 2003. IEEE Computer Society. arXiv:math.GR/0307321.

[5] D. Coppersmith and S. Winograd. Matrix multiplication via arithmetic progressions. *J. Symbolic Computation*, 9:251–280, 1990.

[6] W. Fulton and J. Harris. *Representation theory : a first course*. Graduate texts in mathematics, 129.; Graduate texts in mathematics., Readings in mathematics. Springer-Verlag, 1991.

[7] F. L. Gall. Powers of tensors and fast matrix multiplication. In *Proceedings of the 39th International Symposium on Symbolic and Algebraic Computation*, 2014. arXiv:1401.7714.

[8] J.-P. Serre and L. L. Scott. *Linear representations of finite groups*. Graduate texts in mathematics 42. Springer, 1996.