Случайность и сложность в группах матриц

В. ШПИЛЬРАЙН
Городской колледж Нью-Йорка, США
e-mail: shpil@groups.sci.ccny.cuny.edu

УДК 512.52+512.544.6+512.643.8

Ключевые слова: группы матриц, случайность, сложность алгоритмов.

Аннотация

Обсуждаются различные определения сложности матрицы, а также способы порождения обратимых матриц. Также обсуждаются связанные с этим вопросы сложности алгоритмов для матричных групп.

Abstract

V. Shpilrain, Randomness and complexity in matrix groups, Fundamentalnaya i prikladnaya matematika, vol. 22 (2019), no. 4, pp. 253—262.

We reflect on how to define the complexity of a matrix and how to sample a random invertible matrix. We also discuss a related issue of complexity of algorithms in matrix groups.

Памяти Альфреда Львовича Шмелькина,
человека чести и совести

1. Введение

Чтобы определить сложность алгоритма, сначала нужно определить сложность его ввода. В теории групп стандартным является определение сложности элемента g группы G как *длины его записи* в фиксированной системе порождающих группы G. Чтобы такая сложность была определена корректно, нужно говорить о длине *кратчайшей* записи элемента g через порождающие группы G (так называемая *геодезическая длина*), что может быть неудобным, потому что, например, существуют естественные группы, в которых вычисление геодезической длины является NP-сложным (см. [13]). Поэтому в большинстве естественных алгоритмических проблем теории групп вводом являются слова, а не элементы группы. Например, правильной (с точки зрения теории сложности вычислений) формулировкой проблемы сопряжённости является следующая: если даны два слова u и v в порождающих группы G, определить, существует ли другое слово t, такое что слова u и $t^{-1}vt$ определяют один и тот же элемент группы G. Таким образом, вводом алгоритма, решающего эту проблему, является пара слов $\{u, v\}$, и сложностью такого ввода является сумма длин слов u

Фундаментальная и прикладная математика, 2019, том 22, № 4, с. 253—262.

и v. С другой стороны, нужно отметить, что элементы некоторых групп обладают нормальной формой, и в этом случае сложность (в том или ином смысле) этой нормальной формы можно считать сложностью ввода. Примером нормальной формы может служить матрица как элемент, например, группы $\mathrm{SL}_n(\mathbb{Z})$. Будучи элементом группы, такая матрица обладает представлением как слово в фиксированных порождающих этой группы. Такое представление не является единственным (поскольку группа $\mathrm{SL}_n(\mathbb{Z})$ не свободна). С другой стороны, тот же самый элемент обладает однозначным представлением (нормальной формой) как матрица над $\mathbb{Z}$, иными словами, как таблица целых чисел. Что касается конкретно проблемы сопряжённости, можно ещё отметить, что, поскольку проблема равенства является частным случаем проблемы сопряжённости (а именно сопряжённости с единичным элементом), не будет ошибкой сказать, что вводом алгоритма, решающего проблему сопряжённости, являются два элемента группы G, а не два слова в её порождающих. Действительно, проблема сопряжённости в группе G может быть разрешима, только если в этой группе разрешима проблема равенства, и если проблема равенства разрешима, тогда можно считать эти слова элементами группы G.

Теперь мы переходим к вопросу определения сложности матрицы из групп $\mathrm{SL}_n(\mathbb{Z})$ и $\mathrm{SL}_n(\mathbb{Q})$ для фиксированного n. Для данной матрицы $M = (m_{ij})$ существует три основных способа определить её сложность:

1) то, что называется «нормой» матрицы: $\|M\| = \sum |m_{ij}|$. Также норма может быть определена как $\sqrt{\sum m_{ij}^2}$;
2) длина M как группового слова в фиксированной системе порождающих группы, которой M принадлежит. Мы обозначаем эту длину $|M|$, когда понятно, о какой именно системе порождающих идёт речь;
3) колмогоровская сложность. Говоря неформально, это размер кратчайшего описания данной матрицы M. Это наиболее адекватное определение сложности с точки зрения теории сложности вычислений, но одновременно самое неудобное для использования при решении конкретных алгебраических проблем, и поэтому это определение очень редко используется для оценки сложности алгоритмов решения стандартных проблем теории групп, таких как проблемы равенства, проблемы сопряжённости и т. д. Мы обозначаем колмогоровскую сложность матрицы M через $|M|_{\mathrm{Kol}}$.

В разделе 2 мы постараемся установить связи между различными определениями сложности.

2. Связи между различными определениями сложности

В этом разделе обсуждаются связи между тремя разными определениями сложности, упомянутыми во введении, а также связанный с этим вопрос о том, как выбрать случайную матрицу из того или другого множества матриц.

2.1. Сравнение длины и нормы

Норма $\|M\|$ матрицы обладает хорошими алгебраическими свойствами, в частности, она удовлетворяет неравенству треугольника как для сложения, так и для умножения матриц. Норма матрицы была использована в [6] для изучения сложности некоторых алгоритмов, применимых к матрицам из $\mathrm{SL}_2(\mathbb{Z})$. Но хотя эта сложность интуитивно является подходящей для матриц над $\mathbb{Z}$, она оказывается неподходящей для матриц над $\mathbb{Q}$. Причина этого проста: для рационального числа, например $1/m$ с бо́льши́м m, абсолютная величина может быть очень маленькой, но интуитивно сложность такого числа должна быть столь же велика, как сложность числа m. Таким образом, при определении сложности рационального числа нужно учитывать абсолютное значение как числителя, так и знаменателя, и это должно найти отражение в определении сложности всей матрицы, однако стандартное определение нормы матрицы не позволяет этого сделать.

С другой стороны, для матриц из $\mathrm{SL}_n(\mathbb{Z})$ такой проблемы не возникает, поскольку целое число с бо́льшим абсолютным значением обладает большей сложностью. Теперь рассмотрим интересный вопрос о связи между $\|M\|$ и $|M|$, длиной матрицы M по отношению к естественной системе порождающих группы $\mathrm{SL}_n(\mathbb{Z})$. В дальнейшем мы ограничимся группой $\mathrm{SL}_2(\mathbb{Z})$, чтобы упростить обозначения. У этой группы есть стандартные порождающие, которые мы обозначаем

$$A(1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad B(1) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Группа $\mathrm{SL}_2(\mathbb{Z})$ не является свободной, поэтому имеются соотношения между элементами $A(1)$ и $B(1)$, из чего следует, что для матрицы $M \in \mathrm{SL}_2(\mathbb{Z})$ длина по словам может не совпадать с её геодезической длиной. С другой стороны, подгруппы в $\mathrm{SL}_2(\mathbb{Z})$, порождённые парами матриц

$$A(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad B(k) = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix},$$

являются свободными, если $k \geqslant 2$, и поэтому для этих подгрупп сравнение между длиной по словам и нормой должно было бы быть «более убедительным».

Сначала рассмотрим матрицу

$$L = A(k)^m = \begin{pmatrix} 1 & mk \\ 0 & 1 \end{pmatrix}.$$

Так как $|L| = m$, $\|L\| = mk + 2$, то $|L|$ и $\|L\|$ эквивалентны с точностью до мультипликативной и аддитивной констант.

Напротив, рассмотрим матрицу $C = \big(A(k)B(k)\big)^{m/2}$ (предполагая, что m — чётное число). Тогда $|C| = m$, но $\|C\|$ является экспонентой от m (см. [5]). Таким образом, мы видим, что $\|M\|$ может как быть эквивалентна $|M|$, так и быть экспонентой от $|M|$. В любом случае $|M| = O(\|M\|)$ для матриц из этой подгруппы. Поэтому представляется естественным следующий вопрос.

Проблема 1. Обозначим через H_k подгруппу в $\mathrm{SL}_2(\mathbb{Z})$, порождённую матрицами $A(k)$ и $B(k)$ при $k \geqslant 2$. Что можно сказать о норме $\|M\|$ для случайной матрицы $M \in H_k$ как о функции от длины по словам $|M|$ относительно образующих $A(k)$ и $B(k)$? Будет ли она экспонентой от $|M|$?

Конечно, определение «случайной» матрицы должно быть как-то формализовано. Это можно сделать разными способами (см. хороший обзор на эту тему в [15]). В контексте проблемы 1 вероятно разумно использовать случайность, вытекающую из *асимптотической плотности* (в духе работы [10]). А именно, рассматривается шар B_N радиуса N в графе Кэли группы H_k, порождённой матрицами $A(k)$ и $B(k)$, и выбирается матрица из B_N равномерно случайным образом. Теперь, полагая, что ответом на тот или иной вопрос (например, проблемы 1) является функция $f(N)$, можно вычислить (верхний) предел для $f(N)$ при N, стремящемся к бесконечности, и этот (верхний) предел, если он существует, и считать ответом на исходный вопрос.

Что касается проблемы 1, то наша гипотеза состоит в том, что $\|M\|$ экспоненциально зависит от $|M|$ для случайных матриц M.

2.2. Норма в сравнении с колмогоровской сложностью

Сначала следует отметить, что колмогоровская сложность целого числа n есть $O(\log n)$, так как для описания n (с помощью бинарной, десятичной или любой другой формы) достаточно использовать $O(\log n)$ цифр. Поэтому для матрицы M над $\mathbb{Z}$ получаем $|M|_{\mathrm{Kol}} = O(\log \|M\|)$.

Для рационального числа p/q колмогоровская сложность есть

$$O(\log p + \log q) = O(\log pq).$$

Поэтому не существует явной формулы, связывающей $|M|_{\mathrm{Kol}}$ и $\|M\|$ для матриц M над $\mathbb{Q}$, и мы пока остановимся на этом.

2.3. Длина слова в сравнении с колмогоровской сложностью

Объединяя наши рассуждения из разделов 2.1 и 2.2, отметим, что для матриц $M \in \mathrm{SL}_2(\mathbb{Z})$ $|M|$ может как экспоненциально зависеть от $|M|_{\mathrm{Kol}}$ (матрица L в разделе 2.1), так и линейно зависеть от $|M|_{\mathrm{Kol}}$ (матрица C в разделе 2.1). Таким образом, естественным представляется вопрос о «промежуточном росте».

Проблема 2. Существует ли такой бесконечный набор матриц в подгруппе H_k, $k \geqslant 2$, группы $\mathrm{SL}_2(\mathbb{Z})$, что для матриц M из этого набора длина $|M|$ суперлинейна, но при этом субэкспоненциальна в $|M|_{\mathrm{Kol}}$? Здесь длина слова $|M|$, как обычно, рассматривается в соответствии со стандартными образующими $A(k)$ и $B(k)$.

3. Случайные матрицы

Случайные матрицы рассматривались многими авторами с различных точек зрения (см., например, недавние монографии [3] и [17]). В контексте данной статьи нас интересует выборка (семплинг) случайных матриц, т. е. процедуры для порождающих матриц, соответствующие некоторым интуитивно разумным вероятностным распределениям.

Определение «случайной» матрицы из пула матриц P может быть основано на том или другом определении сложности следующим образом. Предположим, что $|M|_c$ — одна из разумно определённых сложностей матрицы M. Тогда можно рассмотреть шар B_N радиуса N в нашем пуле матриц P, который мы хотели бы испытывать относительно этой сложности, т. е. $B_N = \{M \in P\colon |M|_c \leqslant N\}$, и выбрать матрицу из B_N равномерно случайно, предполагая, что все B_N конечны. Недостатком этого метода является предпочтение матрицам большей сложности, поскольку сфера радиуса N обычно занимает большую часть шара радиуса N.

Если пул P для испытаний состоит из всех матриц (данного размера) над кольцом R, то проблема семплинга для матриц над R может быть сведена к семплингу элементов кольца R.

С другой стороны, если в качестве пула P для испытаний выбрана, скажем, группа $\mathrm{SL}_n(\mathbb{Z})$, то, выбирая случайную матрицу M из шара B_N, нужно принять во внимание тот факт, что матрица M должна иметь определитель, равный 1. Это сужает выбор сложностей $|M|_c$ для использования в данном контексте до $|M|$, т. е. до длины слова M относительно фиксированной системы образующих группы $\mathrm{SL}_n(\mathbb{Z})$ или её подгруппы (в зависимости от рассматриваемой задачи).

Кроме того, другая идея семплинга матриц из группы $\mathrm{SL}_n(\mathbb{Z})$ обсуждалась в работе [15]. Можно рассмотреть биекцию $\beta\colon \mathrm{SL}_n(\mathbb{Z}) \to S$, где S — множество (возможно, без групповой структуры). Если биекция β эффективно обратима, то можно выбрать случайный элемент из S, затем применить к нему β^{-1} и получить случайный элемент из $\mathrm{SL}_n(\mathbb{Z})$. Идея заключается в том, что биекция β может «искривлять» метрику на $\mathrm{SL}_n(\mathbb{Z})$, что поможет избежать «уклона к длинному элементу». Конкретный пример такой биекции, рассмотренный в [15], был основан на хорошо известном действии группы $\mathrm{SL}_n(\mathbb{R})$ на верхней полуплоскости с гиперболической метрикой. Больше деталей можно найти в [15]. Здесь же мы подчёркиваем точку зрения, что выбор подходящего семплинга часто зависит от конкретной решаемой задачи.

4. Сложность подгрупповой проблемы вхождения

Напомним наши обозначения:

$$A(k) = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \quad B(k) = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$

И. Н. Санов в статье [2] доказал следующие две простые, но замечательные теоремы.

Теорема 1. *Подгруппа группы* $\mathrm{SL}_2(\mathbb{Z})$, *порождённая элементами* $A(2)$ *и* $B(2)$, *свободна.*

Теорема 2. *Подгруппа в группе* $\mathrm{SL}_2(\mathbb{Z})$, *порождённая элементами* $A(2)$ *и* $B(2)$, *состоит из всех матриц вида*

$$\begin{pmatrix} 1+4n_1 & 2n_2 \\ 2n_3 & 1+4n_4 \end{pmatrix}$$

с определителем 1, *где все* n_i *являются произвольными целыми числами.*

Эти две теоремы вместе дают другое доказательство того факта, что группа $\mathrm{SL}_2(\mathbb{Z})$ почти свободна, поскольку группа всех обратимых матриц вида

$$\begin{pmatrix} 1+4n_1 & 2n_2 \\ 2n_3 & 1+4n_4 \end{pmatrix}$$

очевидно имеет конечный индекс в группе $\mathrm{SL}_2(\mathbb{Z})$.

Наше внимание к теореме 2 связано со следующим интересным следствием.

Следствие 1. *Проблема вхождения в подгруппу группы* $\mathrm{SL}_2(\mathbb{Z})$, *порождённую матрицами* $A(2)$ *и* $B(2)$, *разрешима за постоянное время.*

Отметим, что, насколько нам известно, это пока единственный пример естественной (и нетривиальной) алгоритмической проблемы в теории групп, которая разрешима за постоянное время. На самом деле даже проблемы, разрешимые за сублинейное время, крайне редки (см. [16]), и в них обычно получаем либо «да», либо «нет», но не и то и другое. В свете теоремы 2, решающей, будет или нет данная матрица из $\mathrm{SL}_2(\mathbb{Z})$ принадлежать подгруппе, порождённой матрицами $A(2)$ и $B(2)$, вопрос сводится к рассмотрению вычетов по модулю 2 или 4 для целых чисел. Последний же вопрос решается рассмотрением лишь одной или двух последних цифр каждого входа (в предположении, что числа заданы в бинарной или, скажем, десятичной форме). Мы также отметим, что в этом случае не имеет значения, какое определение сложности используется на входе, поскольку константа является константой в любом случае.

Подчеркнём всё же, что решение проблемы вхождения за константное время возможно, лишь если известно, что входная матрица принадлежит группе $\mathrm{SL}_2(\mathbb{Z})$; иначе необходимо проверить, что определитель входной матрицы равен 1, что не может быть сделано за константное время, хотя может всё ещё быть сделано за сублинейное время относительно нормы $\|M\|$ входной матрицы M.

Естественное обобщение теоремы 2 Санова на элементы $A(k)$ и $B(k)$, $k \in \mathbb{Z}_+$, не является верным при $k \geqslant 3$; более того, как показано в [6], подгруппа H_k, порождённая элементами $A(k)$ и $B(k)$, имеет бесконечный индекс в группе $\mathrm{SL}_2(\mathbb{Z})$ при $k \geqslant 3$.

В [6] было показано, что существует простой жадный алгоритм для проблемы вхождения в подгруппу H_k, $k \in \mathbb{Z}$, $k \geqslant 2$. По ходу дела отметим, что

в общем случае проблема вхождения в подгруппу для $\mathrm{SL}_2(\mathbb{Q})$ открыта, в то время как для группы $\mathrm{SL}_2(\mathbb{Z})$ разрешима, поскольку группа $\mathrm{SL}_2(\mathbb{Z})$ почти свободна. Общее решение, основанное на автоматном строении группы $\mathrm{SL}_2(\mathbb{Z})$ (см. [7]), не столь прозрачно и имеет квадратичную временную сложность (относительно длины слов входа). Для конкретного случая подгрупп H_k мы имеем следующее утверждение.

Предложение 1 (см. [6]). *Пусть $k \in \mathbb{Z}$, $k \geqslant 2$, и пусть сложность $\|M\|$ матрицы*

$$M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$$

равна сумме всех $|m_{ij}|$. Тогда существует (жадный) алгоритм, решающий, будет ли заданная матрица $M \in \mathrm{SL}_2(\mathbb{Z})$ принадлежать подгруппе H_k группы $\mathrm{SL}_2(\mathbb{Z})$, порождённой матрицами $A(k)$ и $B(k)$ (и если это имеет место, то находится представление матрицы M в виде группового слова от матриц $A(k)$ и $B(k)$) за время $O(n \cdot \log n)$, где $n = \|M\|$).

Подчеркнём, что результат работы [7] о сложности связан с длиной по словам от входной матрицы, в то время как результат предложения 1 о временной сложности $O(n \cdot \log n)$ связан с нормой $n = \|M\|$ входной матрицы. Связь между длиной по словам $|M|$ и нормой $\|M\|$ обсуждается в разделе 2.1, но итог этого следующий:

$$|M| = O(\|M\|) \quad \text{для} \quad M \in H_k.$$

Однако если вход задан как матрица, то для применения алгоритма из [7] следовало бы сначала представить нашу матрицу как некоторое слово от образующих, а эта процедура возвращает нас к алгоритму, отражённому в предложении 1.

Наконец, отметим, что утверждение, подобное предложению 1, имеет место также для моноида, порождённого матрицами $A(k)$ и $B(k)$ для любого $k \in \mathbb{Z}$, $k > 0$.

4.1. Генерическая сложность

Сложность наихудшего случая для алгоритма, приведённого в предложении 1, равна $O(n \cdot \log n)$. Было бы интересно прояснить, какова генерическая сложность (в смысле [10]) для этого алгоритма.

Основы теории генерической сложности были развиты в [10] и [9]. Оказывается, что во многих интересных случаях традиционные теоретико-групповые проблемы разрешимости, такие, как проблемы слов, сопряжённости, вхождения в подгруппу, вероятно, имеют очень низкую генерическую сложность, даже когда сложность наихудшего случая очень высока или проблема неразрешима. Более того, в [9] было доказано, что сложность в среднем часто также низка. Это верно даже тогда, когда решение проблемы слов для некоторых специфических слов может забирать намного больше, чем линейное время в наихудшем случае. Фактически, не требуется даже вообще никакого алгоритма

решения проблемы слов для всех слов. Подобного сорта результаты следуют и для других теоретико-групповых проблем с привлечением индивидуальных групповых элементов (см. [10, 12]), а также подгрупп (см. [4]). В каждом из случаев решение проблемы, которое могло бы быть довольно сложным в наихудшем случае, как было показано, может быть лёгким для «большинства» входов, т. е. для входов из так называемого генерического множества. Точное определение генерического множества зависит от рассматриваемой задачи, при этом предполагается, что оно является естественным в каждом конкретном случае. Для изучения генерической сложности алгоритмов на конкретной группе G следовало бы как-то определить меру на G; тогда множества, имеющие ту же меру, что и вся группа G, будут генерическими. Оказывается, что для естественности такого определения следует принимать во внимание не только природу рассматриваемой проблемы, но также природу группы G. Например, в [11] было показано, что для подмножества S свободной абелевой группы $\mathbf{Z}^k$ и его полного прообраза $\hat{S}$ в свободной группе F_k того же ранга мера (чаще называемая плотностью) для S в $\mathbf{Z}^k$ в «классическом» смысле (давно используемом в теории чисел) равна мере для $\hat{S}$ в F_k, определённой естественным, но достаточно тонким способом («кольцевая плотность»). Другие возможные определения плотности обсуждаются в недавнем обзоре [8].

В любом случае генерическая сложность указывает на сложность решения той или иной проблемы на генерическом множестве входов, или, интуитивно, на «случайных» входах.

Теперь мы попытаемся объяснить причину того, почему, по нашему мнению, проблема вхождения в подгруппу группы $\mathrm{SL}_2(\mathbb{Z})$, порождённую матрицами $A(k)$ и $B(k)$, имеет низкую (скорее всего сублинейную) сложность. Исходной точкой является следующее наблюдение: элементы матриц, являющиеся произведениями длины n положительных степеней матриц $A(k)$ и $B(k)$, показывают самый быстрый рост (как функции от n), если $A(k)$ и $B(k)$ чередуются в произведении: $A(k)B(k)A(k)B(k)\ldots$. Приведём более формальную формулировку.

Предложение 2 (см. [5]). *Пусть $w_n(a,b)$ — произвольное положительное слово чётной длины n, и пусть $W_n = w_n\big(A(k), B(k)\big)$, $k \geqslant 2$. Пусть $C_n = \big(A(k)\cdot B(k)\big)^{n/2}$. Тогда*

а) *сумма элементов в любой строке матрицы C_n по крайней мере так же велика, как сумма элементов в любой строке матрицы W_n;*

б) *наибольший элемент матрицы C_n по крайней мере так же велик, как наибольший элемент матрицы W_n.*

Элементы матрицы C_n могут быть явно найдены из системы рекуррентных соотношений. Эти рекуррентные соотношения линейные с постоянными коэффициентами, поэтому их решения — суммы экспоненциальных функций от n. Из этого следует, что сложность (жадного) алгоритма, упомянутого в предложении 1, является логарифмом сложности (= нормы) входа, если алгоритм применяется к матрице C_n. С другой стороны, если этот алгоритм применяется к степени матрицы $A(k)$ или $B(k)$, то его сложность линейна от размера

входа. Интуитивно, случайное произведение матриц $A(k)^{\pm 1}$ и $B(k)^{\pm 1}$ «ближе» к C_n для некоторого n, чем к некоторой степени матриц $A(k)$ или $B(k)$, поскольку ожидаемое число множителей $A(k)^{\pm 1}$ в таком произведении такое же, как ожидаемое число множителей $B(k)^{\pm 1}$. Вот почему мы считаем, что генерическая сложность алгоритма, упомянутого в предложении 1, сублинейно (фактически логарифмически) зависит от нормы входной матрицы, что было бы действительно интересным результатом, и поэтому мы ставим следующий вопрос.

Проблема 3. Является ли генерическая сложность алгоритма, заявленного в предложении 1, сублинейной от $\|M\|$?

Отметим, что, в отличие от алгоритмов с низкой генерической сложностью, рассмотренных в [10], этот алгоритм имеет хороший шанс иметь низкую генерическую сложность как в случае ответа «да», так и в случае ответа«нет».

Исследование автора было частично поддержано грантом CNS-1117675 Национального научного фонда США и грантом N000141512164 Управления военно-морских исследований США.

Литература

[1] Линдон Р., Шупп П. Комбинаторная теория групп. — М.: Мир, 1980.

[2] Санов И. Н. Свойство одного представления свободной группы // ДАН СССР. — 1947. — Т. 57, № 7. — С. 657—659.

[3] Akemann G., Baik J., Di Francesco P. The Oxford Handbook of Random Matrix Theory. — Oxford: Oxford Univ. Press, 2015.

[4] Bassino F., Nicaud C., Weil P. Generic properties of subgroups of free groups and finite presentations // Contemp. Math. — 2016. — Vol. 677. — P. 1—44.

[5] Bromberg L., Shpilrain V., Vdovina A. , Navigating in the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$ and applications to hashing // Semigroup Forum. — 2017. — Vol. 94, no. 2. — P. 314—324.

[6] Chorna A., Geller K., Shpilrain V. On two-generator subgroups of $\mathrm{SL}_2(\mathbb{Z})$, $\mathrm{SL}_2(\mathbb{Q})$ and $\mathrm{SL}_2(\mathbb{R})$ // J. Algebra. — 2017. — Vol. 478. — P. 367—381.

[7] Epstein D. B. A., Cannon J., Holt D. F., Levy S. V. F., Paterson, Thurston M. S. W. P. Word Processing in Groups. — Boston: Jones and Bartlett, 1992.

[8] Kapovich I. Musings on generic-case complexity: preprint. — `arXiv:1505.03218`.

[9] Kapovich I., Myasnikov A. G., Schupp P., Shpilrain V. Average-case complexity and decision problems in group theory // Adv. Math. — 2005. — Vol. 190. — P. 343—359.

[10] Kapovich I., Myasnikov A. G., Schupp P., Shpilrain V. Generic-case complexity, decision problems in group theory and random walks // J. Algebra. — 2003. — Vol. 264. — P. 665—694.

[11] Kapovich I., Rivin I., Schupp P., Shpilrain V. Densities in free groups and $\mathbb{Z}^k$, visible points and test elements // Math. Res. Lett. — 2007. — Vol. 14. — P. 263—284.

[12] Kapovich I., Rivin I., Schupp P., Shpilrain V. Generic properties of Whitehead's algorithm and isomorphism rigidity of random one-relator groups // Pacific J. Math. — 2006. — Vol. 223. — P. 113—140.

[13] Myasnikov A., Roman'kov V., Ushakov A., Vershik A. The word and geodesic problems in free solvable groups // Trans. Amer. Math. Soc. — 2010. — Vol. 362. — P. 4655—4682.

[14] Myasnikov A. G., Shpilrain V., Ushakov A. Non-Commutative Cryptography and Complexity of Group-Theoretic Problems. — Providence: Amer. Math. Soc., 2011. — (Math. Surveys Monographs; Vol. 177).

[15] Rivin I. How to pick a random integer matrix? (and other questions) // Math. Comput. — 2016. — Vol. 85. — P. 783—797.

[16] Shpilrain V. Sublinear time algorithms in the theory of groups and semigroups // Illinois J. Math. — 2011. — Vol. 54. — P. 187—197.

[17] Tao T. Topics in Random Matrix Theory. — Providence: Amer. Math. Soc., 2012. — (Grad. Stud. Math.; Vol. 132).