УДК 519.7

ОБ ОДНОЙ КОМБИНАТОРНОЙ ПРОБЛЕМЕ, СВЯЗАННОЙ С БЫСТРЫМ УМНОЖЕНИЕМ МАТРИЦ

Ю. В. Кузнецов

Кандидат физико-математических наук, заместитель директора, Научно-исследовательский институт системных исследований РАН, Москва, ykuz@niisi.ras.ru

В рамках теоретико-группового подхода Х. Кона, К. Уманса, Р. Клейнберга, Б. Сегеди к проблеме быстрого умножения матриц возникают специфические комбинаторные объекты, получившие название «однозначно разрешимые матрицы» («uniquely solvable puzzle») или USP-матрицы. В работе обсуждается некоторая числовая характеристика USP-матриц и исследуется связь между USP-матрицами и известной комбинаторной проблемой, в англоязычной литературе носящей название «Cap set problem».

Ключевые слова: быстрое умножение матриц, теоретико-групповой подход, экспонента матричного умножения ω, USP-матрицы, Cap set problem.

Проблема быстрого умножения матриц является одной из наиболее значительных проблем алгебраической теории сложности вычислений. Основные усилия исследователей сосредоточены на получении оценки экспоненты матричного умножения ω. Вплоть до недавнего времени, наилучшей оценкой для ω оставалась оценка Копперсмита (D. Coppersmith) и Винограда (S. Winograd) $\omega < 2.376\ldots$, полученная в 1990 году в работе [1]. В 2012 году в результате чрезвычайно трудоемкого уточнения указанной оценки В. Василевской-Вильямс (V. Vassilevska Williams) в работе [2] была получена оценка $\omega < 2.3727\ldots$ Большинство исследователей в области быстрого умножения матриц считают, что $\omega = 2$.

В 2003–2005 годах в работах [3, 4] Х. Коном (H. Cohn), К. Умансом (C. Umans), Р. Клейнбергом (R. Kleinberg) и Б. Сегеди (B. Szegedy) был предложен принципиально новый подход к проблеме быстрого умножения матриц, носящий теоретико-групповой характер. Один из способов построения групп, пригодных для оценки экспоненты матричного умножения заключается в следующем: искомая группа строится как сплетение некоторой циклической группы и симметрической группы, действующей на некотором множестве U троичных наборов длины n (т. е. $U \subseteq \{1,2,3\}^n$), которые в совокупности обладают специфическими комбинаторными свойствами. Такие множества получили название «однозначно разрешимых матриц» («uniquely solvable puzzle» или сокращенно USP).

Для дальнейшего изложения понадобится серия определений из работы [4] (см. также работы на русском языке [5] и [6]). Для произвольного конечного множества U через $\mathrm{Sym(U)}$ обозначим симметрическую группу, действующую на U.

Определение. *USP-матрицей* ширины n называется множество наборов $U \subseteq \{1,2,3\}^n$, удовлетворяющее следующему свойству.

Для любых трех перестановок π_1, π_2, $\pi_3 \in \mathrm{Sym(U)}$ либо $\pi_1 = \pi_2 = \pi_3$, либо найдется набор $u \in U$ и номер i, $1 \le i \le n$, такие, что выполняются не менее двух равенств из трех: $(\pi_1(u))_i = 1$, $(\pi_2(u))_i = 2$, $(\pi_3(u))_i = 3$.

Для оценки экспоненты матричного умножения ω представляет интерес не весь класс USP-матриц, а некоторый его подкласс — так называемые усиленные USP-матрицы (strong USP) или SUSP-матрицы.

Определение. *SUSP-матрицей* ширины n называется множество наборов $U \subseteq \{1,2,3\}^n$, удовлетворяющее следующему свойству.

Для любых трех перестановок π_1, π_2, $\pi_3 \in \mathrm{Sym(U)}$ либо $\pi_1 = \pi_2 = \pi_3$ либо найдется набор $u \in U$ и номер i, $1 \le i \le n$, такие, что выполняются в точности два равенства из трех: $(\pi_1(u))_i = 1$, $(\pi_2(u))_i = 2$, $(\pi_3(u))_i = 3$.

В свою очередь, важным подклассом SUSP-матриц являются так называемые локальные SUSP-матрицы.

Определение. *Локальной SUSP-матрицей* ширины n называется подмножество $U \subseteq \{1,2,3\}^n$, удовлетворяющее следующему свойству.

Для любой упорядоченной тройки наборов $(u,v,w) \in U^3$, среди которых хотя бы два набора различны, найдется координата i, $1 \le i \le n$, такая, что тройка чисел (u_i, v_i, w_i) является одним из элементов множества $\{(1,2,1),\ (1,2,2),\ (1,1,3),\ (1,3,3),\ (2,2,3),\ (3,2,3)\}$.

Иными словами, выполняются в точности два равенства из трех $u_i = 1$, $v_i = 2$, $w_i = 3$.

Аналогичным образом определяются локальные USP-матрицы.

Основной характеристикой USP-мариц является так называемая емкость (capacity).

Определение. *Емкостью* USP-матрицы (SUSP-матрицы) U ширины n назовем величину $C_U = |U|^{1/n}$.

Непосредственно на саму оценку экспоненты матричного умножения ω влияет емкость C_{SUSP} всего класса SUSP-матриц.

Определение. C_{SUSP} — это наибольшее число C, для которого найдется бесконечная последовательность SUSP-матриц $\{U_{n_k}\}$, для которых $C_{U_{n_k}} \to C$ при $k \to \infty$.

Аналогично определяется емкость C_{USP} всего класса USP-матриц и емкость $C_{\text{лок.}SUSP}$ всего класса локальных SUSP-матриц.

В работе [4] было показано, что $C_{USP} = 3/2^{2/3}$, $C_{SUSP} \ge 2^{2/3}$ и $C_{SUSP} = C_{\text{Лок.}SUSP}$. В работе [4] была также выдвинута гипотеза, что $C_{SUSP} = C_{USP}$, т. е. $C_{SUSP} = 3/2^{2/3}$. Из этой гипотезы следует, что $\omega = 2$.

С использованием оценки $C_{SUSP} \ge 2^{2/3}$ удается получить оценку $\omega \le 2.48$. Эта оценка остается на сегодняшний день наилучшей оценкой, которая получается с использованием аппарата USP-матриц.

Таким образом, улучшение оценок для C_{SUSP} является одним из направлений развития теоретико-группового подхода к проблеме быстрого умножения матриц.

SUSP-матрицы оказались новым, интересным и сложным комбинаторно-алгебраическим объектом. В 2011 году Н. Алоном (N. Alon), А. Шпилькой (A. Shpilka) и К. Умансом в работе [7] была обнаружена тесная связь между SUSP-матрицами и глубокой комбинаторной гипотезой П. Эрдёша о «подсолнечнике», известной еще с 1960-х годов.

В настоящей работе изучается связь USP-матриц с другой известной комбинаторной проблемой — о максимальном размере множеств векторов $C \subseteq \mathbb{F}_3^n$, не содержащих «троек», где $\mathbb{F}_3 = \{0,1,2\}$ — поле из трех элементов, «тройка» — три вектора $x,y,z \in \mathbb{F}_3^n$, таких, что $x+y+z=0$. В литературе эта проблема получила название «Cap set problem», при этом само множество векторов C называется «cap», а указанная «тройка» — «set».

Нетрудно заметить, что векторы $x,y,z \in \mathbb{F}_3^n$ образуют «тройку» тогда и только тогда, когда для каждой координаты i, $1 \le i \le n$, либо $x_i = y_i = z_i$, либо x_i, y_i, z_i — попарно различны. С другой стороны, в поле $\mathbb{F}_3$ условие $x+y+z=0$ эквивалентно условию $y-x = z-y$, поэтому о «тройке» иногда говорят как о трехчленной арифметической прогрессии. В вышеуказанной работе [7] в качестве обобщения понятия «тройки» выступал «подсолнечник» в $\mathbb{Z}_D^n$.

Через a_n обозначим максимальную мощность множества $C \subseteq \mathbb{F}_3^n$, не содержащего «троек». Точно вычислены только 6 первых значений этой последовательности: 2, 4, 9, 20, 45, 112 [8].

Основные усилия исследователей направлены на получение оценок для последовательности $\{a_k\}$. На сегодняшний день наилучшая оценка сверху получена Бэйтманом (M. Bateman) и Кацем (N. Katz) в работе [9]:

$$a_n \le C\frac{3^n}{n^{1+\epsilon}},$$

где $\epsilon > 0$ и C — некоторые константы.

Наилучшая оценка снизу получена Эделем (Y. Edel) в работе [10]: $2.2174^n \le a_n$.

Проблема получения оценок для $\{a_k\}$ является сложной, глубокой и имеет многочисленные приложения. Филдсовские лауреаты Теренс Тао и Тимоти Гауэрс, а также другой известный математик Гил Калай, неоднократно указывали на важность исследований в этой области.

Пусть $C \subset \mathbb{F}_3^n$. Произведем замены в C: $0 \to 123$, $1 \to 231$, $2 \to 312$.

Полученную матрицу размера $|C| \times 3n$ обозначим через $F(C)$.

В работе [11] показано, что если $C \subset \mathbb{F}_3^n$ — произвольное множество, не содержащее «троек», то $F(C)$ — SUSP-матрица.

На самом деле справедливо более сильное утверждение.

Теорема 1. *Если $C \subset \mathbb{F}_3^n$ — произвольное множество, не содержащее «троек», то $F(C)$ — локальная SUSP-матрица.*

Доказательство. Через C_1 обозначим матрицу, которая получается из матрицы C заменами $0 \to 1$, $1 \to 2$, $2 \to 3$; через C_2 — матрицу, получающуюся из C заменами $0 \to 2$, $1 \to 3$, $2 \to 1$; и, наконец, через C_3 — матрицу, получающуюся из C заменой $0 \to 3$ (т. е. 1 и 2 не заменяются).

Понятно, что $F(C)$ можно получить в результате объединения C_1, C_2, C_3 с соответствующей перестановкой столбцов.

Рассмотрим три набора $(u, v, w) \in F(C)^3$, причем будем считать, что наборы u, v, w попарно различны. Так как матрица C не содержит «троек», то найдется некоторая координата i такая, что среди чисел u_i, v_i, w_i ровно два различных. Пусть для определенности $u_i = \alpha$, $v_i = \beta$, $w_i = \alpha$.

Нетрудно видеть, что в одной из матриц C_1, C_2, C_3 в строке v в соответствующем j-м столбце будет находиться число 2, а в строках u и w — некоторое число α', отличное от 2 . В любом случае мы получаем, что эта координата j — искомая, в которой выполняется ровно два равенства из трех $u_j = 1$, $v_j = 2$, $w_j = 3$.

Аналогично рассматривается случай, когда среди трех наборов $(u, v, w) \in F(C)^3$ ровно два различных. Теорема 1 доказана.

Нетрудно заметить, что если исходная матрица C, не содержащая «троек», имеет емкость σ, то результат $F(C)$ будет иметь емкость $\sigma^{1/3}$. Поэтому даже в самом лучшем случае, если верно, что $a_k = (3 - o(1))^n$ (к чему склоняется Теренс Тао), мы получим оценку для всего класса SUSP-матриц $C_{SUSP} \geq 3^{1/3}$, что хуже, чем $C_{SUSP} \geq 2^{2/3}$. Однако теорема 1 показывает, что конструкция $C \to F(C)$ является избыточной, и поэтому возможно при более экономном переходе $C \to F(C)$ удастся получить оценку лучше, чем $2^{2/3}$.

Пусть $U \subseteq \{1, 2, 3\}^n$. Произведем замены в U: $1 \to 0$, $2 \to 1$, $3 \to 2$.

Полученную матрицу обозначим через $G(U)$.

Теорема 2. *Если U — SUSP-матрица, то $G(U)$ — множество, свободное от «троек».*

Доказательство. Предположим противное, а именно пусть найдутся три попарно различных набора u, v, $w \in G(U)$, образующих «тройку». Обозначим прообразы этих наборов при отображении $U \to G(U)$ через u', v', w' соответственно. Определим три перестановки π_1, π_2, π_3, действующие на U следующим образом:

– перестановка $\pi_1 = E$;

– перестановка π_2 циклически переставляет строки u', v', w', т. е. π_2 осуществляет преобразование $u' \to v'$, $v' \to w'$, $w' \to u'$;

– перестановка π_3 осуществляет преобразование $u' \to w'$, $v' \to u'$, $w' \to v'$.

На остальных строках перестановки π_2 и π_3 действуют тождественно.

Утверждается, что для любой строки $a \in U$ и любой координаты i, $1 \leq i \leq n$, невозможно выполнение в точности двух равенств из трех: $(\pi_1(a))_i = 1$, $(\pi_2(a))_i = 2$, $(\pi_3(a))_i = 3$.

Действительно, если строка a отлична от строк u', v', w', то требуемое утверждение очевидно.

Пусть a совпадает с одной из строк u', v', w'. Для определенности будем считать, что строка a совпадает с u'.

Рассмотрим произвольную координату i, $1 \leq i \leq n$. Возможно два варианта.

1. Выполняются равенства $u'_i = v'_i = w'_i$. В этом случае опять требуемое утверждение очевидно.

2. Все числа u'_i, v'_i, w'_i попарно различны. Но тогда:

$$(\pi_1(u'))_i = u'_i, \qquad (\pi_2(u'_i))_i = v'_i, \qquad (\pi_3(u'_i))_i = w'_i$$

и может выполняться только либо три равенства, либо одно, либо ни одного. Получили противоречие. Аналогично рассматриваются случаи, когда строка a совпадает с v' или w'. Теорема 2 доказана.

Как показывает следующий пример, существуют USP-матрицы U такие, что $G(U)$ содержит «тройки». Тем самым утверждение теоремы 2 справедливо не для всех USP-матриц.

Пример. *Матрица*

1	*2*	*3*
2	*1*	*2*
3	*3*	*1*

является USP-матрицей.

Доказательство этого факта можно провести методом, изложенным в работе [11].

Таким образом теорема 2 позволяет в некотором смысле выделить класс SUSP-матриц в классе всех USP-матриц и косвенно объясняет трудности, возникающие при исследовании SUSP-матриц.

Работа выполнена при финансовой поддержке РФФИ (проекты 12-01-00190-а и 13-01-12402 оф_м2).

Библиографический список

1. *Coppersmith D., Winograd S.* Matrix multiplication via arithmetic progressions // J. Symbolic Comput. 1990. Vol. 9, № 3. P. 251–280.

2. *Vassilevska Williams V.* Multiplying Matrices Faster than Coppersmith–Winograd // Proceedings of the 44-th Symposium on Theory of Computing, STOC'12. 2012. URL: www.cs.berkeley.edu/ virgi/matrixmult.pdf (дата обращения 30.09.2013).

3. *Cohn H., Umans C.* A group theoretic approach to fast matrix multiplication // Proceedings of the 44-th Annual IEEE Symposium on Foundations of Computer Science. 2003. P. 438–449. DOI: 10.1109/SFCS.2003.1238217.

4. *Cohn H., Kleinberg R., Szegedy B., Umans C.* Group-theoretic algorithms for matrix multiplication // Proceedings of the 46-th Annual IEEE Symposium on Foundations of Computer Science. 2005. P. 379–388. DOI: 10.1109/SFCS.2005.39.

5. *Платонов В. П., Кузнецов Ю. В., Петрунин М. М.* О теоретико-групповом подходе к проблеме быстрого умножения матриц. Математическое и компьютерное моделирование систем : теоретические и прикладные аспекты // Сб. науч. тр. НИИСИ РАН. М., 2009. С. 4–15.

6. *Кузнецов Ю. В.* Некоторые комбинаторные аспекты теоретико-группового подхода к проблеме быстрого умножения матриц // Чебышевский сб. 2012. Т. 13, № 1. С. 102–109.

7. *Alon N., Shpilka A., Umans C.* On sunflowers and matrix multiplication // Electronic Colloquium on Computational Complexity. 2011. Report № 67. P. 1–16.

8. *Davis B. L., Maclagan D.* The card game SET // Mathematical Intelligencer. 2003. Vol. 25, № 3. P. 33–40.

9. *Bateman M., Katz N.* New bounds on caps sets // J. American Math. Soc. 2012. Vol. 25, № 2. P. 585–613.

10. *Edel Y.* Extensions of generalized product caps // Designs, Codes and Cryptography. 2004. Vol. 31. P. 5–14.

11. *Mebane P.* Uniquely Solvable Puzzles and Fast Matrix Multiplication. HMC Senior Theses, 2012. 37 p.

On Combinatorial Problem, Related with Fast Matrix Multiplication

Yu. V. Kuznetsov

Scientific Research Institute for System Studies of RAS, Russia, 117218, Moscow, Nakhimovskii pr., k. 1, 36, ykuz@niisi.ras.ru

The group-theoretical approach to fast matrix multiplication generates specific combinatorial objects, named Uniquely Solvable Puzzles (briefly USP). In the paper some numerical characteristic of the USP was discussed and the relation of USPs to famous combinatorial problem named «Cap set problem» was investigated.

Key words: fast matrix multiplication, group-theoretical approach to fast matrix multiplication, USP, Cap set problem.

References

1. Coppersmith D., Winograd S. Matrix multiplication via arithmetic progressions. *J. Symbolic Comput.*, 1990. Vol. 9, no. 3, pp. 251–280.

2. Vassilevska Williams V. Multiplying Matrices Faster than Coppersmith–Winograd. *Proceedings of the 44-th Symposium on Theory of Computing, STOC'12*. 2012. URL: www.cs.berkeley.edu/ virgi/matrixmult.pdf (Accsessed 30, September, 2013).

3. Cohn H., Umans C. A group theoretic approach to fast matrix multiplication. *Proceedings of the 44-th Annual IEEE Symposium on Foundations of Computer Science*. 2003, pp. 438–449. DOI: 10.1109/SFCS.2003.1238217.

4. Cohn H., Kleinberg R., Szegedy B., Umans C. Group-theoretic algorithms for matrix multiplication. *Proceedings of the 46-th Annual IEEE Symposium on Foundations of Computer Science*. 2005, pp. 379–388. DOI: 10.1109/SFCS.2005.39.

5. Platonov V. P., Kuznetsov Iu. V., Petrunin M. M. O teoretiko-gruppovom podkhode k probleme bystrogo umnozheniia matrits. Matematicheskoe i komp'iuternoe modelirovanie sistem: teoreticheskie i prikladnye aspekty [A group-theoretical approach to the problem of fast matrix multiplication. Mathematical and computer modeling of systems: theoretical and applied aspects]. *Sbornik nauchnuh trudov NIISI RAN* [Collection of scientific papers NIISI RAS]. Moscow, 2009, pp. 4–15 (in Russian).

6. Kuznetsov Yu. V. Nekotorye kombinatornye aspekty teoretiko-gruppovogo podkhoda k probleme bystrogo umnozheniia matrits [Some combinatorial aspects of the group-theoretic approach to fast matrix multiplication]. *Chebyshevskii sbornik.*, 2012, vol. 13, no. 1, pp. 102–109 (in Russian).

7. Alon N., Shpilka A., Umans C. On sunflowers and matrix multiplication. *Electronic Colloquium on Computational Complexity*, 2011, Report no. 67, pp. 1–16.

8. Davis B. L., Maclagan D. The card game SET. *Mathematical Intelligencer*, 2003, vol. 25, no. 3, pp. 33–40.

9. Bateman M., Katz N. New bounds on caps sets. *J. American Math. Soc.*, 2012. vol. 25, no. 2, pp. 585–613.

10. Edel Y. Extensions of generalized product caps. *Designs, Codes and Cryptography*, 2004, vol. 31, pp. 5–14.

11. Mebane P. *Uniquely Solvable Puzzles and Fast Matrix Multiplication*. HMC Senior Theses, 2012, 37 p.

УДК 511.3

ОБ УНИВЕРСАЛЬНОСТИ НЕКОТОРЫХ ДЗЕТА-ФУНКЦИЙ

А. Лауринчикас[1], Р. Мацайтене[2], Д. Мохов[3], Д. Шяучюнас[4]

[1]Академик АН Литвы, доктор физико-математических наук, профессор, заведующий кафедрой теории вероятностей и теории чисел, Вильнюсский университет (Литва), antanas.laurincikas@mif.vu.lt

[2]Доктор математических наук, профессор кафедры математики, Шяуляйский университет (Литва), renata.macaitiene@mi.su.lt

[3]Магистрант факультета математики и информатики, Вильнюсский университет (Литва), dmitrij.mochov@mif.vu.lt

[4]Доктор математических наук, профессор кафедры математики, Шяуляйский университет (Литва), siauciunas@fm.su.lt

Хорошо известно, что обобщение дзета функции Гурвица — периодическая дзета функция Гурвица — с трансцендентным параметром универсальна в том смысле, что её сдвигами приближается всякая аналитическая функция. В статье условие трансцендентности параметра заменяется более слабым условием о линейной независимости некоторого множества.

Ключевые слова: периодическая дзета функция Гурвица, пространство аналитических функций, слабая сходимость, универсальность.

1. INTRODUCTION

Let $s = \sigma + it$ be a complex variable, and α, $0 < \alpha \leq 1$, be a fixed parameter. The Hurwitz zeta-function $\zeta(s, \alpha)$ is defined, for $\sigma > 1$, by the Dirichlet series

$$\zeta(s, \alpha) = \sum_{m=0}^{\infty} \frac{1}{(m + \alpha)^s},$$

and continues analytically to the whole complex plane, except for a simple pole at $s = 1$ with residue 1.