Компьютерные инструменты в образовании, 2021
№ 2: 5–12
УДК: 519.61
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-2-5-12

алгоритмическая математика и математическое моделирование

О НЕКОТОРЫХ АЛГОРИТМАХ КВАЗИПОЛИНОМИАЛЬНОГО ВРЕМЕНИ

Селиверстов А. В.[1], кандидат физико-математических наук, ведущий научный сотрудник,
✉ slvstv@iitp.ru, orcid.org/0000-0003-4746-6396

[1]Институт проблем передачи информации им. А. А. Харкевича Российской академии наук,
Большой Каретный пер., д. 19, стр. 1, 127051, Москва, Россия

Аннотация

С древности алгоритмы неразрывно связаны с математикой. Однако самостоятельное развитие теория алгоритмов получила лишь в первой половине XX века. Начальный период был связан с открытием как неразрешимых, так и очень трудных проблем. Например, в 1927 году Габриэль Судан опубликовал первый пример вычислимой функции, которая доказуемо не служит примитивно рекурсивной. Практическое значение асимптотических оценок вычислительной сложности стало очевидным лишь во второй половине XX века. Мы рассматриваем некоторые хорошо известные задачи принятия решений, которые можно решить за квазиполиномиальное время, то есть задачи, предположительно принадлежащие к промежуточному классу между полиномиальным и экспоненциальным временем. Коллекция включает в себя проверку изоморфности, вычисление исхода игры на чётность и (обоснованную в предположении справедливости обобщенной гипотезы Римана) факторизацию многочленов от одной переменной над конечными полями. Также представлены некоторые технические результаты, которые могут быть использованы для создания новых алгоритмов квазиполиномиального времени.

Ключевые слова: *квазиполиномиальное время, вычислительная сложность, история.*

Цитирование: Селиверстов А. В. О некоторых алгоритмах квазиполиномиального времени // Компьютерные инструменты в образовании. 2021. № 2. С. 5–12. doi: 10.32603/2071-2340-2021-2-5-12

Благодарности: *автор благодарен Семёну Адлаю за замечания.*

1. ВВЕДЕНИЕ

Начиная с глубокой древности, алгоритмы неразрывно связаны с математикой. Однако свободное развитие теория алгоритмов получила лишь в первой половине XX века. Начальный период самостоятельности был связан с исследованиями алгоритмически неразрешимых или очень трудных задач. В 1927 году Габриэль Судан (Gabriel Sudan, 1899–1977) опубликовал первый пример вычислимой функции, для которой было доказано, что она не является примитивно рекурсивной [1, 2]. В 1928 году Вильгельм Аккерман (Wilhelm Friedrich Ackermann, 1896–1962) опубликовал статью [3] с описанием другой такой функции.

Практическая значимость асимптотических оценок вычислительной сложности стала очевидной в 1950-е годы на фоне развития вычислительной техники. Но определение класса задач, вычислимых за полиномиальное время, лишь в 1964 году дал Алан Кобхам (Alan Cobham) [4]. Его поддержал Джек Эдмондс (Jack Edmonds) [5]. Другим важным результатом стала теорема Кука–Левина о существовании NP-полных задач [6, 7]. Известные детерминированные алгоритмы для решения NP-полных задач в естественной постановке, включая задачу распознавания выполнимости 3КНФ, работают экспоненциальное время (в худшем случае). Легко сформулировать NP-полную задачу, разрешимую за время $O(2^{\sqrt{n}})$. Но неизвестно, существует ли NP-полная задача, разрешимая за квазиполиномиальное время, например, за время $O(n^{\log_2 n})$. Это создаёт ложное ощущение пустоты между классами задач, разрешимых за полиномиальное и экспоненциальное время, хотя проблема сокращения перебора обсуждается. В частности, статья С. В. Соловьева [8] рассказывает об истории одного из семинаров в ЛЭТИ, посвящённых этой теме. Мы дадим примеры алгоритмов, имеющих промежуточную вычислительную сложность. При этом рассмотрены асимптотические оценки сложности алгоритмов. Иногда поиск оптимального алгоритма служит трудной задачей [9].

2. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Обозначим через $\omega = \{0, 1, 2, \ldots\}$ множество натуральных чисел, начиная с нуля. Обозначим через n длину входа. Если не оговорено иное, числа отождествляются с их двоичными записями. Если входом служит число $x \in \omega$, то его длина $n = \lceil \log_2(x+1) \rceil$. Здесь $\lceil \cdot \rceil$ обозначает округление до большего целого. Легко создать алгоритм, выходом которого служит достаточно большое число, зависящее от длины входа, а время работы асимптотически растёт как $n^{\lceil \log_2(n+1) \rceil} + O(1)$ и не может быть маленьким из-за большой длины выхода. Более интересны задачи, для которых результатом служит один бит. Можно считать, что вычислительное устройство не записывает выход, но приходит в одно из двух состояний остановки, принимая или отвергая вход.

Класс множеств, распознаваемых за квазиполиномиальное время, содержит все множества, разрешимые за время $O(n^{\log_2^k n})$ для $k > 0$. Начнём с лёгких методов создания таких алгоритмов.

Во-первых, если множество допускается алгоритмом, использующим память $O(\log_2^2 n)$, то время работы этого алгоритма ограничено сверху $O(n^{c \log_2 n})$, где через c обозначена некоторая константа. Это ограничение памяти относится к промежуточным вычислениям; вход не меняется. Такие алгоритмы интересны для реализации на многопроцессорных вычислительных устройствах (суперкомпьютерах), когда ограничена память, доступная одному процессору.

Во-вторых, если некоторое множество чисел $L \subset \omega$ допускается алгоритмом за время $O(2^n)$, то множество упорядоченных пар чисел

$$\left\{ \langle x, y \rangle \in \omega \times \omega \,\middle|\, x \in L, \log_2 \log_2 y = \left\lceil \frac{\log_2(x+1)}{\log_2 \log_2 (x+1)} \right\rceil \right\}$$

распознаётся за время $O(n^{c \log_2 n})$, где через c обозначена константа и через n обозначена сумма длин двоичных записей чисел x и y.

В-третьих, часто в задачах аппроксимации за квазиполиномиальное время можно улучшить качество аппроксимации по сравнению с полиномиальным временем.

В комбинаторных задачах размером входа n обычно служит мощность основного множества, например, порядок группы, число вершин в графе, порядок конечной плоскости.

Проективная плоскость порядка n содержит n^2+n+1 точек и столько же прямых. Каждая прямая инцидентна ровно $n+1$ точкам, каждая точка инцидентна ровно $n+1$ прямым. При этом через любые две точки проходит единственная прямая, любые две прямые пересекаются в одной точке, существуют четыре точки, пары которых соответствуют шести различным прямым. Проективная плоскость порядка два — это плоскость Фано. Аффинная плоскость получается удалением из проективной плоскости одной прямой «на бесконечности» и всех её точек. Аффинная плоскость порядка n содержит n^2 точек и $n(n+1)$ прямых. Подробное описание конечных плоскостей можно найти в работах [10, 11]. Конечные плоскости применяются для создания кодов, исправляющих ошибки. Система Штейнера $S(t,k,n)$ — это n-элементное множество вместе с набором его k-элементных подмножеств, называемых блоками, для которых каждое t-элементное подмножество содержится ровно в одном блоке. Система $S(2,3,n)$ называется системой троек Штейнера. Конечная проективная плоскость порядка q с прямыми в качестве блоков служит системой Штейнера $S(2,q+1,q^2+q+1)$. Конечная аффинная плоскость порядка q с прямыми в качестве блоков служит системой Штейнера $S(2,q,q^2)$.

3. ПРИМЕРЫ ЗАДАЧ

Ниже перечислены некоторые задачи, разрешимые за квазиполиномиальное время, для которых не был найден алгоритм полиномиального времени.

3.1. Проверка изоморфности

Поскольку конечная группа порядка n порождается множеством из самое большее $\log_2 n$ элементов, а изоморфизм достаточно задать на порождающих, проверка изоморфности двух групп, заданных таблицами умножения, выполнима за время $O^*(n^{\log_2 n})$, где символ O^* означает, что опущен полиномиальный множитель $O(n^c)$. Вероятно, это было независимо отмечено несколькими авторами. Более того, согласно пионерской работе Ричарда Липтона и соавторов [12], изоморфность конечных групп проверяется при ограничении на память $O(\log_2^2 n)$. Результат улучшен лишь в частных случаях. Для конечных разрешимых групп, заданных таблицами умножения, оценка времени улучшена, но остаётся квазиполиномиальной [13]. Для конечных групп без нормальных абелевых подгрупп изоморфность проверяется за полиномиальное время [14]. Для конечных абелевых групп изоморфность проверяется за линейное время [15].

В 1978 году Гэри Миллер (Gary L. Miller) предложил несколько алгоритмов квазиполиномиального времени $O^*(n^{\log_2 n})$ для проверки изоморфности конечных квазигрупп, изотопии латинских квадратов, изоморфности систем троек Штейнера, а также для решения других близких задач [16]. Там же дан алгоритм проверки изоморфности конечных аффинных плоскостей порядка n за необычно малое время $O^*(n^{\log_2 \log_2 n})$. И такая же оценка справедлива для проверки изоморфности конечных проективных плоскостей [16].

В 1997 году Сергей Алексеевич Евдокимов и Илья Николаевич Пономаренко предложили алгоритм для следующей задачи [17]. Даны два конечных множества A и B по n точек в d-мерном пространстве $\mathbb{R}^d$. Определить, существует ли изометрия пространства, при которой образом множества A служит множество B. Время работы предложен-

ного алгоритма полиномиальное при $d = O(\sqrt[4]{\log_2 n})$ и квазиполиномиальное при $d = O(\log_2^k n)$.

В 2013 в двух докладах разных авторов предложен алгоритм квазиполиномиального времени $O^*(n^{c\log_2 n})$ для проверки изоморфности систем Штейнера (а не только систем троек Штейнера) [18, 19].

3.2. Выигрышные стратегии

Рассмотрим ориентированный граф с n вершинами, одна из которых выделена, причём из каждой вершины выходит хотя бы одна дуга. Каждой вершине графа приписано натуральное число от 1 до m, называемое его весом, где максимальная величина $m \leqslant n$ — ещё один параметр. Два игрока до начала игры выбирают себе чётность (например первый — нечётный, второй — чётный) и фиксируют стратегии перехода из текущей вершины в следующую по дугам графа. Эти стратегии неадаптивные, то есть очередной ход не зависит от предыдущих ходов. Игра начинается в выделенной вершине графа и продолжается бесконечно долго. Поскольку из каждой вершины выходит какая-то дуга, любой путь можно продолжить. Игроки по очереди делают ход в соответствии со своими стратегиями. Если верхний предел $\limsup$ весов вершин графа, последовательно посещаемых в ходе игры, нечётный, то выигрывает первый игрок, если чётный — выигрывает второй игрок. Поскольку вес вершины ограничен, то верхний предел существует при любых стратегиях игроков. Следовательно, один из игроков выиграет.

Хотя рассматриваемая игра продолжается бесконечно, но стратегия каждого игрока не меняется и имеет конечное описание. Исход этой игры можно предсказать за время $O^*(n^{c\log_2 m})$, где c — некоторая константа [20–22]. При ограничении $m \leqslant n$ это время квазиполиномиальное $O^*(n^{c\log_2 n})$. Ещё в 1998 году было показано, что эта задача принадлежит классу $UP \cap coUP \subseteq NP \cap coNP$, следовательно, не считается NP-трудной [23].

3.3. Факторизация многочленов над конечным полем

В 1994 году Сергей Алексеевич Евдокимов [24] предложил алгоритм разложения на неприводимые множители многочленов от одной переменной над явно заданным конечным полем из $q = p^m$ элементов в предположении справедливости обобщённой гипотезы Римана. В этом случае роль обобщённой гипотезы Римана состоит в обеспечении возможности для извлечения корня над конечным полем за полиномиальное время. Время работы алгоритма $O((n^{\log_2 n} m \log_2 p)^c)$ для некоторой константы c. По сравнению с известным алгоритмом Берлекампа [25, 26], время работы которого $O((nmp)^C)$ для некоторой константы C, новый алгоритм эффективнее в случае больших значений характеристики поля p.

3.4. Простые числа

В 1983 году был предложен алгоритм для проверки простоты натуральных чисел за квазиполиномиальное время $O(n^{c\log\log n})$, где c — некоторая константа [27]. Однако позднее для этой задачи был предложен алгоритм полиномиального времени [28].

Возможно, новые алгоритмы квазиполиномиального времени будут возникать при использовании простых чисел, с которыми связаны асимптотические оценки, содержа-

щие повторный логарифм. Сумма обратных для простых чисел

$$\sum_{p \leqslant x} \frac{1}{p} = \ln\ln x + B + O\left(\frac{1}{\ln x}\right),$$

где при суммировании все p — простые числа, через $B = 0.26149\ldots$ обозначена некоторая константа [29]. Среднее на сегменте $[1, N]$ значение числа простых делителей натурального числа равно

$$\ln\ln N + B + O\left(\frac{1}{\ln x}\right),$$

где $B = 0.26149\ldots$ — та же константа, что в предыдущем равенстве [29].

4. ЗАКЛЮЧЕНИЕ

Показано, что существует много задач с естественной формулировкой, для которых известен разрешающий алгоритм квазиполиномиального времени, но не был найден алгоритм полиномиального времени. Это подтверждает, что рассматриваемый класс вычислительной сложности интересен для изучения. Указанные оценки могут служить для обоснования новых алгоритмов квазиполиномиального времени.

Список литературы

1. *Calude C., Marcus S., Tevy I.* The first example of a recursive function which is not primitive recursive // Historia Mathematica. 1979. Vol. 6, № 4. P. 380–384. doi: 10.1016/0315-0860(79)90024-7
2. *Sudan G.* Sur le nombre transfini ω^{ω} // Bulletin Mathématique de la Société Roumaine des Sciences. 1927. Vol. 30, № 1. P. 11–30. https://www.jstor.org/stable/43769875
3. *Ackermann W.* Zum Hilbertschen Aufbau der reellen Zahlen // Mathematische Annalen. 1928. Vol. 99, № 1. P. 118–133. doi: 10.1007/BF01459088
4. *Cobham A.* The intrinsic computational difficulty of functions. In: Bar-Hillel Y. (ed.) Logic, Methodology and Philosophy of Science. Proc. Intern. Congress 1964. North-Holland, Amsterdam, 1965. P. 24–30. https://www.cs.toronto.edu/~sacook/homepage/cobham_intrinsic.pdf
5. *Edmonds J.* Paths, trees, and flowers // Canadian Journal of Mathematics. 1965. Vol. 17. P. 449–467. doi: 10.4153/CJM-1965-045-4
6. *Cook S. A.* The complexity of theorem-proving procedures. In: Proceedings of Third Annual ACM Symposium on Theory of Computing (Shaker Heights, Ohio, 1971), ACM, N.Y., 1971. P. 151–158.
7. *Левин Л. А.* Универсальные задачи перебора // Проблемы передачи информации. 1973. Т. 9. № 3. С. 115–116. http://mi.mathnet.ru/ppi914
8. *Соловьев С. В.* Судьбы и семинары. О семинаре «Проблемы сокращения перебора» в ЛЭТИ в историко-научном контексте // Компьютерные инструменты в образовании. 2019. № 4. С. 5–14. doi: 10.32603/2071-2340-2019-4-5-14
9. *Коточигов А. М., Сучков А. И.* Метод сокращения перебора в алгоритмах построения минимальных аддитивных цепочек // Компьютерные Инструменты в Образовании. 2020. № 1. С. 5–18. doi: 10.32603/2071-2340-2020-1-5-18
10. *Картеси Ф.* Введение в конечные геометрии. М.: Наука, 1980.
11. *Gogin N. D., Mylläri A. A.* On computer modeling of finite-generated free projective planes // Computer tools in education. 2017. № 4. P. 14–28.
12. *Lipton R. J., Snyder L., Zalcstein Y.* The complexity of word and isomorphism problems for finite groups (Preliminary report). Research Report no. 91. Yale University, 1977. https://archive.org/details/DTIC_ADA053246
13. *Rosenbaum D. J.* Breaking the $n^{\log n}$ barrier for solvable-group isomorphism. In: SODA 2013: Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms. ACM-SIAM, New Orleans Louisiana, 2013. P. 1054–1073. https://dl.acm.org/doi/10.5555/2627817.2627893

14. *Babai L., Codenotti P., Qiao Y.* Polynomial-time isomorphism test for groups with no abelian normal subgroups. In: Czumaj A., Mehlhorn K., Pitts A., Wattenhofer R. (eds) Automata, Languages, and Programming. ICALP 2012. Lecture Notes in Computer Science, vol 7391. Springer, Berlin, Heidelberg, 2012, pp. 51–62. https://doi.org/10.1007/978-3-642-31594-7_5
15. *Kavitha T.* Linear time algorithms for abelian group isomorphism and related problems // Journal of Computer and System Sciences. 2007. Vol. 73, № 6. P. 986–996.
16. *Miller G. L.* On the $n^{\log n}$ isomorphism technique (A preliminary report). In: STOC 1978: Proceedings of the tenth annual ACM symposium on Theory of computing. ACM, New York, NY, USA, 1978. P. 51–58. doi: 10.1145/800133.804331
17. *Evdokimov S. A., Ponomarenko I. N.* On the geometric graph isomorphism problem // Journal of Pure and Applied Algebra. 1997. Vol. 117–118. P. 253–276. doi: 10.1016/S0022-4049(97)00014-5
18. *Babai L., Wilmes J.* Quasipolynomial-time canonical form for steiner designs. In: STOC 2013: Proceedings of the forty-fifth annual ACM symposium on Theory of Computing. ACM, New York, NY, USA, 2013. P. 261–270. doi: 10.1145/2488608.2488642
19. *Chen X., Sun X., Teng S.-H.* Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems. In: STOC 2013: Proceedings of the forty-fifth annual ACM symposium on Theory of Computing. ACM, New York, NY, USA, 2013. P. 271–280. doi: 10.1145/2488608.2488643
20. *Calude C. S., Jain S., Khoussainov B., Li W., Stephan F.* Deciding parity games in quasipolynomial time. In: STOC 2017: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing. ACM, New York, NY, USA, 2017. P. 252–263. doi: 10.1145/3055399.3055409
21. *Calude C. S., Jain S., Khoussainov B., Li W., Stephan F.* Deciding parity games in quasi-polynomial time // SIAM Journal on Computing. doi: 10.1137/17M1145288
22. *Fearnley J., Jain S., de Keijzer B., Schewe S., Stephan F., Wojtczak D.* An ordered approach to solving parity games in quasi-polynomial time and quasi-linear space // International Journal on Software Tools for Technology Transfer. 2019. Vol. 21. P. 325–349. doi: 10.1007/s10009-019-00509-3
23. *Jurdziński M.* Deciding the winner in parity games is in $UP \cap co-UP$ // Information Processing Letters. 1998. Vol. 68, № 3. P. 119–124. doi: 10.1016/S0020-0190(98)00150-1
24. *Evdokimov S.* Factorization of polynomials over finite fields in subexponential time under GRH. In: Adleman L. M., Huang M.-D. (eds) Algorithmic Number Theory. ANTS 1994. Lecture Notes in Computer Science. 1994. Vol. 877. P. 209–219. doi: 10.1007/3-540-58691-1_58
25. *Berlekamp E. R.* Factoring polynomials over large finite fields // Mathematics of Computation. 1970. Vol. 24, № 111. P. 713–735. doi: 10.2307/2004849
26. *Прасолов В. В.* Многочлены. М.: МЦНМО, 2001.
27. *Adleman L. M., Pomerance C., Rumely R. S.* On distinguishing prime numbers from composite numbers // Annals of Mathematics. 1983. Vol. 117, № 1. P. 173–206.
28. *Agrawal M., Kayal N., Saxena N.* PRIMES is in P // Annals of Mathematics. 2004. Vol. 160, № 2. P. 781–793. doi: 10.4007/annals.2004.160.781
29. *Бухштаб А. А.* Теория чисел. М.: Просвещение, 1966.

Поступила в редакцию 12.04.2021, окончательный вариант — 13.05.2021.

Селиверстов Александр Владиславович, кандидат физико-математических наук, ведущий научный сотрудник Института проблем передачи информации им. А. А. Харкевича Российской академии наук, ✉ **slvstv@iitp.ru**

Computer tools in education, 2021
№ 2: 5–12
http://cte.eltech.ru
doi:10.32603/2071-2340-2021-2-5-12

On Some Quasipolynomial-time Algorithms

Seliverstov A. V.[1], Candidate of Physical and Mathematical Sciences, Leading Researcher,
✉ slvstv@iitp.ru, http://orcid.org/0000-0003-4746-6396

[1]Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), 19, build. 1, Bolshoy Karetny per., 127051, Moscow, Russia

Abstract

Since ancient times, algorithms are inextricably linked with mathematics. However, the theory of algorithms received independent development only in the first half of the 20th century. The initial period was associated with discovery of unsolvable as well as very difficult problems. So, in 1927 Gabriel Sudan published the first example of a computable function that is provably not primitive recursive. The practical significance of asymptotic estimates of computational complexity became apparent only in the second half of the 20th century. We consider some well-known decision problems solvable in quasipolynomial time, that is, problems presumably belonging to the intermediate class between polynomial time and exponential time. The collection comprises isomorphism testing, solution to the parity game, and (validated under the generalized Riemann hypothesis) factorization of univariate polynomials over finite fields. We also present some technical results, which can be used to create new quasipolynomial-time algorithms.

Keywords: *quasipolynomial time, computational complexity, history.*

Citation: A. V. Seliverstov, "On Some Quasipolynomial-time Algorithms," *Computer tools in education*, no. 2, pp. 5–12, 2021; doi: 10.32603/2071-2340-2021-2-5-12

Acknowledgements: *The author is grateful to Semjon Adlaj for comments.*

References

1. C. Calude, S. Marcus, and I. Tevy, "The first example of a recursive function which is not primitive recursive," *Historia Mathematica*, vol. 6, no. 4, pp. 380–384, 1979; doi: 10.1016/0315-0860(79)90024-7
2. G. Sudan, "Sur le nombre transfini ω^{ω}," *Bulletin Mathématique de la Société Roumaine des Sciences*, vol. 30, no. 1, pp. 11–30, 1927. [Online]. Available: https://www.jstor.org/stable/43769875
3. W. Ackermann, "Zum Hilbertschen Aufbau der reellen Zahlen," *Mathematische Annalen*, vol. 99, no. 1, pp. 118–133, 1928; doi: 10.1007/BF01459088
4. A. Cobham, "The intrinsic computational difficulty of functions," Y. Bar-Hillel ed., in *Logic, Methodology and Philosophy of Science. Proc. Intern. Congress 1964. North-Holland, Amsterdam*, 1965, pp. 24–30. [Online]. Available: https://www.cs.toronto.edu/~sacook/homepage/cobham_intrinsic.pdf
5. J. Edmonds, "Paths, trees, and flowers," *Canadian Journal of Mathematics*, vol. 17, pp. 449–467, 1965; doi: 0.4153/CJM-1965-045-4
6. S. A. Cook, "The complexity of theorem-proving procedures," in *Proc. of Third Annual ACM Symposium on Theory of Computing (Shaker Heights, Ohio, 1971), ACM, N. Y.*, 1971, pp. 151–158.
7. L. A. Levin, "Universal sequential search problems," *Problems of Information Transmission*, vol. 9, no. 3, pp. 265–266, 1973.
8. S. V. Soloviev, "Destinies and Seminars (On the Seminar 'Problems of Reducing the Exhaustive Search' at LETI in a Historical and Scientific Context)," *Computer tools in education*, no. 4, pp. 5–14, 2019 (in Russian); doi: 10.32603/2071-2340-2019-4-5-14

9. A. M. Kotochigov and A. I. Suchkov, “A method for reducing iteration in algorithms for building minimal additive chains,” *Computer Tools in Education*, no. 1, pp. 5–18, 2020 (in Russian); doi: 10.32603/2071-2340-2020-1-5-18
10. F. Kárteszi, *Introduction to finite geometries*, Budapest: Akadémiai Kiadó, 1976.
11. N. D. Gogin and A. A. Mylläri, “On computer modeling of finite-generated free projective planes,” *Computer tools in education*, no. 4, pp. 14–28, 2017.
12. R. J. Lipton, L. Snyder and Y. Zalcstein, *The complexity of word and isomorphism problems for finite groups (Preliminary report)*, [Research Report], no. 91, Yale University, 1977. [Online]. Available: https://archive.org/details/DTIC_ADA053246
13. D. J. Rosenbaum, “Breaking the $n^{\log n}$ barrier for solvable-group isomorphism,” in *SODA 2013: Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms. ACM-SIAM, New Orleans Louisiana*, 2013, pp. 1054–1073; doi: 10.5555/2627817.2627893
14. L. Babai, P. Codenotti, and Y. Qiao, “Polynomial-time isomorphism test for groups with no abelian normal subgroups,” A. Czumaj, K. Mehlhorn, A. Pitts, and R. Wattenhofer, eds. in *Automata, Languages, and Programming. ICALP 2012. Lecture Notes in Computer Science*, vol 7391, Berlin, Heidelberg: Springer, 2012, pp. 51–62; doi: 10.1007/978-3-642-31594-7_5
15. T. Kavitha, “Linear time algorithms for abelian group isomorphism and related problems,” *Journal of Computer and System Sciences*, vol. 73, no. 6, pp. 986–996, 2007.
16. G. L. Miller, “On the $n^{\log n}$ isomorphism technique (A preliminary report),” in *STOC 1978: Proceedings of the tenth annual ACM symposium on Theory of computing. ACM, New York, NY, USA*, 1978, pp. 51–58; doi: 10.1145/800133.804331
17. S. A. Evdokimov and I. N. Ponomarenko, “On the geometric graph isomorphism problem,” *Journal of Pure and Applied Algebra*, vol. 117-118, pp. 253–276, 1997; doi: 10.1016/S0022-4049(97)00014-5
18. L. Babai and J. Wilmes, “Quasipolynomial-time canonical form for steiner designs,” in *STOC 2013: Proceedings of the forty-fifth annual ACM symposium on Theory of Computing. ACM, New York, NY, USA*, 2013, pp. 261–270; doi: 10.1145/2488608.2488642
19. X. Chen, X. Sun, and S.-H. Teng, “Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems,” in *STOC 2013: Proceedings of the forty-fifth annual ACM symposium on Theory of Computing. ACM, New York, NY, USA*, 2013, pp. 271–280; doi: 10.1145/2488608.2488643
20. C. S. Calude, S. Jain, B. Khoussainov, and W. Li, F. Stephan, “Deciding parity games in quasipolynomial time,” in *STOC 2017: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing. ACM, New York, NY, USA*, 2017, pp. 252–263; doi: 10.1145/3055399.3055409
21. C. S. Calude, S. Jain, B. Khoussainov, and W. Li, F. Stephan, “Deciding parity games in quasi-polynomial time,” *SIAM Journal on Computing*, pp. STOC17-152-STOC17-188, 2020; doi: 10.1137/17M1145288
22. J. Fearnley, S. Jain, B. de Keijzer, S. Schewe, F. Stephan, and D. Wojtczak, “An ordered approach to solving parity games in quasi-polynomial time and quasi-linear space,” *International Journal on Software Tools for Technology Transfer*, vol. 21, pp. 325–349, 2019; doi: 10.1007/s10009-019-00509-3
23. M. Jurdziński, “Deciding the winner in parity games is in $UP \cap co-UP$,” *Information Processing Letters*, vol. 68, no. 3, pp. 119–124, 1998; doi: 10.1016/S0020-0190(98)00150-1
24. S. Evdokimov, “Factorization of polynomials over finite fields in subexponential time under GRH,” L. M. Adleman and M.-D. Huang, eds, in *Algorithmic Number Theory. ANTS 1994. Lecture Notes in Computer Science*, vol. 877, 1994, pp. 209–219; doi: 10.1007/3-540-58691-1_58
25. E. R. Berlekamp, “Factoring polynomials over large finite fields,” *Mathematics of Computation*, vol. 24, no. 111, pp. 713–735, 1970; doi: 10.2307/2004849
26. V. V. Prasolov, *Polynomials*, Berlin: Springer, 2004; doi: 10.1007/978-3-642-03980-5
27. L. M. Adleman, C. Pomerance, and R. S. Rumely, “On distinguishing prime numbers from composite numbers,” *Annals of Mathematics*, vol. 117, no. 1, pp. 173–206, 1983.
28. M. Agrawal, N. Kayal, and N. Saxena, “PRIMES is in P,” *Annals of Mathematics*, vol. 160, no. 2, pp. 781–793, 2004; doi: 10.4007/annals.2004.160.781
29. A.A. Buchstab, *The number theory*, Moscow: Prosveshchenie publ., 1966 (in Russian).

Received 12-04-2021, the final version — 13-05-2021.

Seliverstov Alexandr Vladislavovich, Candidate of Physical and Mathematical Sciences, Leading Researcher, Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute), ✉ **slvstv@iitp.ru**