подобная группе экспоненцирования $S_2 \uparrow S_n$. Стабилизатор $G_{\mathbf{0}}$ каждой не 2-транзитивной примитивной группы G, $A\tilde{S}_n \leqslant G \leqslant AGL_n$, сохраняет некоторое нетривиальное разбиение множества $V_n^\times$, блоками которого являются орбиты стабилизатора $G_{\mathbf{0}}$ на $V_n^\times$. Все такие разбиения описаны в [2], а классификация соответствующих групп — в [3, 4]. С применением теоремы 1, утверждения 1 и классификации надгрупп группы $A\tilde{S}_n$ описаны классы нелинейных $\oplus_{\mathbf{W},\mathrm{ch}}$-марковских преобразований для разбиений $\mathbf{W}$ пространства V_n, отличных от рассмотренных в теореме 1.

Очевидно, что $AGL_n = (AGL_n)_{\mathbf{W}}$ для $\mathbf{W} \in \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\alpha : \alpha \in V_n\}\right\}$.

Утверждение 2. Если 2-транзитивная группа $G < AGL_n$ такова, что $G_{\mathbf{0}}$ примитивна на $V_n^\times$, то $G \neq (AGL_n)_{\mathbf{W}}$ для каждого разбиения $\mathbf{W} \notin \left\{\{\Delta_0^{(n)}, V_n^\times\}, \{\{\alpha\} : \alpha \in V_n\}\right\}$.

В общем случае из $\oplus_{\mathbf{W},\mathrm{ch}}$-марковости преобразований $b_1, b_2 \in S(V_n)$ для некоторого разбиения $\mathbf{W}$ пространства V_n не следует $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$. Приведены условия на преобразования b_1, b_2, из которых вытекает $\oplus_{\mathbf{W},\mathrm{ch}}$-марковость преобразования $b_1 b_2$, а также условия того, что раундовая функция, задаваемая этими преобразованиями, является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской.

Пусть раундовая функция $g : V_n^2 \to V_n$ задана условием $g : (x, k) \mapsto (x \oplus k)^{sh}$, где $s = (s_{d-1}, \ldots, s_0) \in S(V_m)^d$, $h \in GL_n$. Приведены условия на h, при которых раундовая функция $g : (x, k) \mapsto (x \oplus k)^{sh}$ является $\oplus_{\mathbf{W},\mathrm{ch}}$-марковской для некоторого разбиения $\mathbf{W}$ пространства V_n.

ЛИТЕРАТУРА

1. *Погорелов Б. А., Пудовкина М. А.* $\otimes_{\mathbf{W},\mathrm{ch}}$-марковские преобразования // Прикладная дискретная математика. Приложение. 2015. № 8. С. 17–20.
2. *Музычук М. Е.* Подсхемы схемы Хемминга // Исследования по алгебраической теории комбинаторных объектов. ВНИИ системных исследований. Труды семинара. 1985. С. 49–76.
3. *Погорелов Б. А.* Подметрики метрики Хемминга и теорема А.А. Маркова // Труды по дискретной математике. 2006. № 9. С. 190–219.
4. *Погорелов Б. А., Пудовкина М. А.* Подметрики метрики Хемминга и преобразования, распространяющие искажения в заданное число раз // Труды по дискретной математике. 2007. № 10. С. 202–238.

УДК 510.52 DOI 10.17223/2226308X/8/26

О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ПРОБЛЕМЫ РАСПОЗНАВАНИЯ КВАДРАТИЧНЫХ ВЫЧЕТОВ[1]

А. Н. Рыбалов

Генерический подход к алгоритмическим проблемам предложен А. Мясниковым, И. Каповичем, П. Шуппом и В. Шпильрайном в 2003 г. В рамках этого подхода рассматривается поведение алгоритмов на множествах почти всех входов. В данной работе изучается генерическая сложность проблемы распознавания квадратичных вычетов в группах вычетов. Доказывается, что её естественная подпроблема генерически трудноразрешима (то есть трудна для почти всех входов) при условии, что проблема распознавания квадратичных вычетов трудноразрешима в классическом смысле.

[1]Работа поддержана грантом РФФИ № 15-41-04312.

Ключевые слова: *генерическая сложность, квадратичный вычет, вероятностный алгоритм.*

В работе [1] развита теория генерической сложности вычислений. В рамках этого подхода алгоритмическая проблема рассматривается не на всем множестве входов, а на некотором подмножестве «почти всех» входов. Такие входы образуют так называемое генерическое множество. Понятие «почти все» формализуется введением естественной меры на множестве входных данных. С точки зрения практики алгоритмы, решающие быстро проблему на генерическом множестве, так же хороши, как и быстрые алгоритмы для всех входов.

С точки зрения современной криптографии интересны такие алгоритмические проблемы, которые, являясь (гипотетически) трудными в классическом смысле, остаются трудными и в генерическом смысле, т. е. для почти всех входов. Это объясняется тем, что при случайной генерации ключей в криптографическом алгоритме происходит генерация входа некоторой трудной алгоритмической проблемы, лежащей в основе алгоритма. Если проблема является генерически легко разрешимой, то для почти всех таких входов её можно быстро решить, и ключи почти всегда будут нестойкими. Поэтому проблема должна быть генерически трудной. Например, для проблемы дискретного логарифма такие результаты получены в работе [2].

Данная работа посвящена изучению генерической сложности классической проблемы распознавания квадратичных вычетов в группах вычетов. До сих пор не известно полиномиальных алгоритмов её решения. Более того, на предположении о её трудноразрешимости основаны некоторые криптографические алгоритмы [3].

Пусть I — некоторое множество входов. На множестве I определена функция размера $\mathrm{size} : I \to \mathbb{N}$, сопоставляющая каждому элементу $a \in I$ его размер $\mathrm{size}(a)$. Допустим, что для любого n множество I_n элементов из I размера n конечно. Для любого подмножества $S \subseteq I$ определим следующую последовательность:

$$\rho_n(S) = \frac{|S \cap I_n|}{|I_n|},\ n = 1, 2, 3, \ldots$$

Величина $\rho_n(S)$ — это вероятность получить вход из множества S при случайной и равномерной генерации элементов из I_n. *Асимптотической плотностью* S назовём следующий предел (если он существует):

$$\rho(S) = \lim_{n\to\infty} \rho_n(S).$$

Множество S называется *генерическим*, если $\rho(S)=1$, и *пренебрежимым*, если $\rho(S)=0$. Очевидно, что S генерическое тогда и только тогда, когда его дополнение $I \setminus S$ пренебрежимо. Понятие генерического множества является некоторой формализацией интуитивного понятия множества «почти всех» элементов множества I в том смысле, что при увеличении размера элемента вероятность попасть в генерическое множество при случайной и равновероятной генерации элементов стремится к 1.

Алгоритмическая проблема распознования множества $S \subseteq I$ *генерически полиномиально разрешима*, если существует множество $G \subseteq I$, такое, что

1) G — генерическое;
2) G — разрешимое за полиномиальное время;
3) $G \cap S$ — разрешимое за полиномиальное время.

Генерический алгоритм, решающий проблему S, работает на входе $x \in I$ следующим образом. Сначала определяет, принадлежит ли x генерическому множеству G.

Если да, то проверяет принадлежность входа S. Если нет, то отвечает НЕ ЗНАЮ. Такой алгоритм правильно решает проблему S на почти всех входах.

Пусть $\mathbb{Z}/(m)$ — мультипликативная группа вычетов по модулю $m \in \mathbb{N}$. Напомним, что квадратичным вычетом в группе $\mathbb{Z}/(m)$ называется любой элемент x, для которого существует $y \in \mathbb{Z}/(m)$, такой, что $x = y^2$. В противном случае элемент x называется квадратичным невычетом. Под проблемой распознавания квадратичных вычетов понимается проблема распознавания следующего множества:

$$QR = \{(m, x) \in \mathbb{N}^2 : m = pq, \text{ где } p, q \text{ — простые числа,}$$
$$x - \text{ квадратичный вычет в } \mathbb{Z}/(m)\}.$$

В настоящее время неизвестно полиномиальных алгоритмов (в том числе и вероятностных), решающих проблему распознавания квадратичных вычетов для всех таких модулей m.

Для изучения генерической сложности этой проблемы необходимо провести некоторую стратификацию на множестве входов. Рассмотрим любую бесконечную последовательность натуральных чисел $\mu = \{m_1, m_2, \ldots\}$, удовлетворяющую следующим условиям:

1) $2^n < m_n < 2^{n+1}$ для любого n;
2) m_n — произведение двух различных простых чисел для любого $n > 1$.

Будем называть такую последовательность *экспоненциальной*. Из знаменитого постулата Бертрана, доказанного П. Л. Чебышевым, следует, что экспоненциальные последовательности существуют. Определим алгоритмическую проблему $QR(\mu)$ как ограничение проблемы распознавания квадратичных вычетов QR на следующее множество входных данных:

$$I = \{(m, x) : m \in \mu, x \in \mathbb{Z}/(m)\}.$$

Под размером входа (m, x) понимается количество бит в двоичной записи числа m минус 1. Заметим, что множество I_n входов проблемы $QR(\mu)$ размера n состоит из всех пар (m, x), где m — единственное число $m \in \mu$, удовлетворяющее условию $2^n < m < 2^{n+1}$, а x — любой элемент из $\mathbb{Z}/(m)$.

Теорема 1. Если проблема $QR(\mu)$ генерически полиномиально разрешима, то существует полиномиальный вероятностный алгоритм, решающий $QR(\mu)$ для всех входов.

Теорема 2. Если для проблемы QR не существует полиномиального вероятностного алгоритма, то существует экспоненциальная последовательность μ, такая, что проблема $QR(\mu)$ не является генерически полиномиально разрешимой.

Более подробно полученные результаты представлены в [4].

ЛИТЕРАТУРА

1. *Kapovich I., Miasnikov A., Schupp P., and Shpilrain V.* Generic-case complexity, decision problems in group theory and random walks // J. Algebra. 2003. V. 264. No. 2. P. 665–694.
2. *Blum M. and Micali S.* How to generate cryptographically strong sequences of pseudorandom bits // SIAM J. Computing. 1984. V. 13. No. 4. P. 850–864.
3. *Мао В.* Современная криптография: теория и практика. М.: Вильямс, 2005. 768 с.
4. *Рыбалов А. Н.* О генерической сложности проблемы распознавания квадратичных вычетов // Прикладная дискретная математика. 2015. № 2. С. 54–58.