ВЫЧИСЛИТЕЛЬНЫЕ МЕТОДЫ В ДИСКРЕТНОЙ МАТЕМАТИКЕ

УДК 512.54.05+519.712.4

О СЛОЖНОСТИ ЗАДАЧИ ДИСКРЕТНОГО ЛОГАРИФМИРОВАНИЯ В ИНТЕРВАЛЕ В ГРУППЕ С ЭФФЕКТИВНЫМ ИНВЕРТИРОВАНИЕМ

М. В. Николаев

Московский государственный университет им. М. В. Ломоносова, г. Москва, Россия

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы $G = \langle P \rangle$ (с аддитивной записью операции) и заданных $P, Q \in G$, $N < |G| - 1$ такого значения n, что $Q = nP$, $n \in \{-N/2, \ldots, N/2\}$. Одним из наиболее эффективных методов решения данной задачи является алгоритм Годри — Шоста. В 2010 г. С. Гэлбрейт и Р. Руправи представили усовершенствованную версию алгоритма для групп с эффективным инвертированием. Оценка средней трудоёмкости решения задачи составила $(1{,}36 + o(1))\sqrt{N}$ групповых операций в G при $N \to \infty$. В настоящей работе приводится новая модификация алгоритма Годри — Шоста для решения задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием и получена оценка средней трудоёмкости, составляющая $(1 + \varepsilon)\sqrt{\pi N/2}$ групповых операций в G.

Ключевые слова: *задача дискретного логарифмирования в интервале, алгоритм Годри — Шоста.*

DOI 10.17223/20710410/28/10

ON THE COMPLEXITY OF DISCRETE LOGARITHM PROBLEM IN AN INTERVAL IN A FINITE CYCLIC GROUP WITH EFFICIENT INVERSION

M. V. Nikolaev

Lomonosov Moscow State University, Moscow, Russia

E-mail: max.abstract@gmail.com

Discrete logarithm problem in an interval in a finite group $G = \langle P \rangle$ consists in solving the equation $Q = nP$ with respect to $n \in \{-N/2, \ldots, N/2\}$ for the specified $P, Q \in G$ and $0 < N < |G| - 1$. If the group G has an inversion, which may be computed significantly faster than the group operation, then, similarly to the solution of the classical discrete logarithm, we may speed up the algorithm. In 2010, S. Galbraith and R. Ruprai proposed an algorithm solving this problem with the average complexity $(1{,}36 + o(1))\sqrt{N}$ group operations in G where $N \to \infty$. We show that the average complexity of the algorithm for finding the solution of the discrete logarithm problem in interval equals $(1 + \varepsilon)\sqrt{\pi N/2}$ group operations.

Keywords: *discrete logarithm problem in interval, Gaudry — Schost algorithm.*

Приведём постановки задач.

Определение 1. Задача дискретного логарифмирования.
Дано: группа $G = \langle P \rangle$, $Q \in G$.
Найти: $n \in \{0, \ldots, |G| - 1\}$, такое, что $Q = nP$.

Определение 2. Задача дискретного логарифмирования в интервале.
Дано: группа $G = \langle P \rangle$, $Q \in G$, $N \in \mathbb{N}$, $2|N$, $N < |G| - 1$, $Q = nP$ для некоторого (неизвестного) $n \in \{-N/2, \ldots, N/2\}$.
Найти: n.

В настоящее время в общем случае одним из наиболее эффективным алгоритмом решения задачи дискретного логарифмирования в интервале является алгоритм Годри — Шоста [1]. Основная идея алгоритма может быть сформулирована следующим образом. Сначала выбираются так называемые «домашнее» (tame) и «дикое» (wild) множества:

$$T = \{-N/2, \ldots, N/2\}, \quad W = \{-N/2 + n, \ldots, N/2 + n\},$$

затем параллельно вычисляются псевдослучайные последовательности

$$x_i P, \ x_i \in T, \ i = 1, 2, \ldots, \tag{1}$$

$$Q + z_j P, \ (n + z_j) \in W, \ j = 1, 2, \ldots \tag{2}$$

до тех пор, пока в них не найдутся два одинаковых элемента

$$x_k P = Q + z_l P, \tag{3}$$

откуда находим $n = x_k - z_l$.

Средняя трудоёмкость алгоритма Годри — Шоста и его различных модификаций, измеряемая количеством групповых операций в G, равна по порядку величины среднему значению количества элементов последовательностей, вычисляемых до появления совпадающих элементов, в предположении, что значения n, x_i и z_j выбираются случайно равновероятно и независимо из соответствующих множеств. Это среднее значение может быть получено с использованием следующего результата Гэлбрэйта и Холмса, являющегося обобщением парадокса дней рождения.

Теорема 1 [2, Theorem 1]. Предположим, что выполнены следующие условия.

1) Имеется C различных цветов шаров, $C > 1$. Шар, выбранный под номером k, с вероятностью $r_{k,c}$ имеет цвет c (независимо от предыдущих выбранных шаров); для любого $c = 1, \ldots, C$ существует $p_c = \lim\limits_{n \to \infty} n^{-1} \sum\limits_{k=1}^{n} r_{k,c}$ и $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_C > 0$. Пусть $b_{n,c} = p_c - n^{-1} \sum\limits_{k=1}^{n} r_{k,c}$ и существует константа K, такая, что для любого $c = 1, \ldots, C$, $n > 1$ выполняется неравенство $|b_{n,c}| \leqslant K/n$.
2) Имеется $N' \in \mathbb{N}$ различных урн. Если k-й шар имеет цвет c, то он попадает в урну с номером i с вероятностью $q_{c,i}(N')$ независимо от предыдущих выбранных цветов и размещений шаров. Существует такое $d > 0$, не зависящее от N' и c, что $0 \leqslant q_{c,i} \leqslant d/N'$ для любых $c = 1, \ldots, C$ и $i = 1, \ldots, N'$. Существуют такие константы $\alpha, \mu > 0$, что $|\{i \in \{1, \ldots, N'\} : q_{1,i}, q_{2,i} \geqslant \mu/N'\}| \geqslant \alpha N'$.

Тогда математическое ожидание числа $Z_{N'}$ шаров, размещенных до первого появления двух шаров разных цветов в одной урне, равно

$$\mathbf{M}(Z_{N'}) = \sqrt{\frac{\pi}{2A_{N'}}} + \mathrm{O}(N'^{1/4}),$$

где

$$A_{N'} = \sum_{c=1}^{C} p_c \left(\sum_{c'=1, c \neq c'}^{C} p_{c'} \left(\sum_{i=1}^{N'} q_{c,i} q_{c',i} \right) \right)$$

и константа в O зависит от $C, p_c, d, K, \alpha, \mu$, но не зависит от N' и $q_{c,i}$.

Для оптимизации методов поиска решения задачи дискретного логарифмирования часто используют наличие у исходной группы классов эквивалентности, как это делается, например, в работах [3, 4]. Но в случае задачи дискретного логарифмирования в интервале подойдут только классы эквивалентности, все элементы которых лежат в том же интервале, что и решение задачи. Итак, предположим теперь, что группа G обладает эффективно вычислимой операцией φ взятия обратного элемента, т. е. время, необходимое для вычисления обратного элемента, существенно меньше времени, необходимого для выполнения одной групповой операции. Тогда группа G распадается на непересекающиеся классы эквивалентности (орбиты) относительно действия φ, и подобно тому, как это делается в [4] для классической задачи дискретного логарифмирования, можно ускорить алгоритм, если искать не совпадающие элементы последовательностей (1) и (2), а совпадающие классы эквивалентности этих элементов. Действительно, в этом случае вместо равенства (3) имеем равенство

$$\varphi^s(x_k P) = Q + z_l P$$

для некоторого s, откуда $Q = ((-1)^s x_k - z_l)P$, т. е. $n = (-1)^s x_k - z_l$.

Примером такой группы *с эффективным инвертированием* является группа точек эллиптической кривой $y^2 = x^3 + Ax + B$ над конечным простым полем из $p > 3$ элементов. Действительно, $\varphi(x, y) = (x, -y)$, т. е. $\varphi(aP) = -aP$, и класс эквивалентности точки aP относительно действия группы $\langle\varphi\rangle$ состоит из aP и $\varphi(aP)$. Каждому такому классу эквивалентности соответствует множество $C(a) = \{a, -a\}$.

В [5] для этого случая предложена соответствующая модификация алгоритма Годри — Шоста, имеющая при $N \to \infty$ трудоёмкость $(1{,}36 + \mathrm{o}(1))\sqrt{N}$ групповых операций. Для получения этого результата использовались «домашнее» множество

$$T = \{C(a) : -N/2 \leqslant a \leqslant N/2\},$$

а также «дикое» множество

$$W = \{C(n + a) : -N/4 \leqslant a \leqslant N/4\}.$$

Используя описанный автоморфизм φ, получим, что множество «представителей» для каждого класса $C(a) \in T$ равно $\widetilde{T} = \{a : 0 \leqslant a \leqslant N/2\}$.

На рис. 1 изображены «дикое» множество, множество T_0 — объединение классов из множества T, а также пересечение $U = \widetilde{W} \cap \widetilde{T}$, где $\widetilde{W} = \{(n + a) : -N/4 \leqslant a \leqslant N/4\}$.

Следующая теорема конструктивно доказывает возможность дальнейшего улучшения оценки средней трудоёмкости решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием.

Теорема 2. Пусть G — циклическая группа с эффективным инвертированием, пусть также $2|N$. Тогда для любого $\varepsilon > 0$ существует такой алгоритм решения задачи дискретного логарифмирования в интервале в группе G, что при случайном равновероятном выборе n его средняя трудоёмкость не превосходит $(1 + \varepsilon)\sqrt{\pi N/2} + \mathrm{O}_\varepsilon(N^{1/4})$ групповых операций, где $N \to \infty$. (Здесь запись O_ε означает, что константа под символом O зависит от ε.)

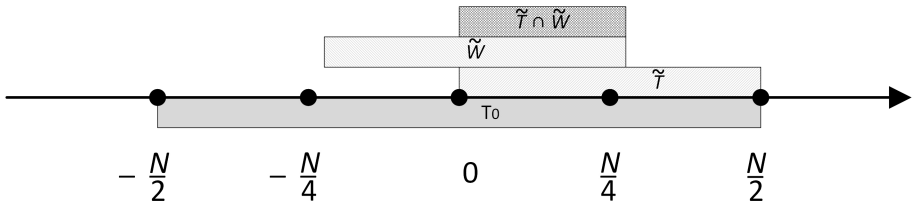

Рис. 1

Доказательство. Определим «домашнее» множество T и множество $\widetilde{T}$ представителей классов T

$$T = \{C(a) : -N/2 \leqslant a \leqslant N/2\}, \quad \widetilde{T} = \{0, \ldots, N/2\}$$

(в работах [5, 6] такое множество называется фундаментальной областью «домашнего» множества). Обозначим T_0 объединение классов из множества T. Для регулирования размера «дикого» множества W введём параметр τ:

$$W_\tau = \{C(n + a) : -\tau N/4 \leqslant a \leqslant \tau N/4\},$$

тогда $\widetilde{W}_\tau = \{a : -\tau N/4 + n \leqslant a \leqslant \tau N/4 + n\}$ и $|\widetilde{W}_\tau| = 2\lfloor \tau N/4 \rfloor + 1$.

Как и в алгоритме Годри — Шоста, будем параллельно вычислять последовательности точек

$$x_i P, \ x_i \in \widetilde{T}, \ i = 1, 2, \ldots, \tag{4}$$

$$Q + z_j P, \ z_j \in \widetilde{W}_\tau, \ j = 1, 2, \ldots \tag{5}$$

до тех пор, пока в них не найдутся две точки из одного класса эквивалентности, после чего находим решение задачи, как показано ранее. При этом предполагается, что значения x_i и z_j выбираются случайно равновероятно и независимо из соответствующих множеств.

Очевидно, что средняя трудоёмкость, выраженная в количестве групповых операций, не превосходит математического ожидания суммарного числа $Z_{N'}$ значений x_i и $(n+z_j)$, выбираемых до появления значений x_k и $(n+z_l)$, таких, что $C(x_k) = C(n_1+z_l)$.

Условное математическое ожидание $\mathbf{M}(Z_{N'}|(n))$ случайной величины $Z_{N'}$ при фиксированном n найдём с помощью теоремы 1, как это делается в [7]. Тогда в обозначениях теоремы $C = 2$; шары цвета 1 — элементы множества $\widetilde{T}$, а шары цвета 2 — элементы множества $\widetilde{W}_\tau$. Вычисление последовательностей (4) и (5) происходит параллельно, поэтому можно считать, что $r_{k,1} = r_{k,2} = 1/2$ для всех $k = 1, 2, \ldots$, откуда $p_1 = p_2 = 1/2$. Множество урн в нашем случае — это $T \cup W_\tau$, и шар a попадает в урну $C(a)$. Ясно, что $N' = \mathrm{O}(N)$. В целях упрощения записи далее величины $\mathrm{o}(N)$ при $N \to \infty$ опускаются. Тогда имеем

$$q_{1,i} = \begin{cases} 2/N, & \text{если } i \in T, \\ 0 & \text{в противном случае.} \end{cases}$$

С учётом последнего равенства и утверждения теоремы 1 нас интересуют значения $q_{2,i}$ только для $i \in T \cap W_\tau$. Поскольку каждый класс $C(a)$ содержит не более двух элементов, $T \cap W_\tau$ разбивается на два непересекающихся подмножества U_j, $j = 1, 2$, таких, что в каждый класс из U_j попадает ровно j элементов из $\widetilde{W}_\tau$, т. е. $q_{2,i} = j/|\widetilde{W}_\tau|$, $i \in U_j$.

Из двух последних равенств получаем

$$A_{N'} = 2 \cdot \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{2}{N} \cdot \frac{1}{|\widetilde{W}_\tau|} \sum_{j=1}^{2} j|U_j| = \frac{|U|}{N|\widetilde{W}_\tau|},$$

где $U = \widetilde{W}_\tau \cap T_0$, и по теореме 1 $\mathbf{M}(Z_{N'}|(n)) = \sqrt{\dfrac{\pi N|\widetilde{W}_\tau|}{2|U|}}$.

Следуя работам [5, 6], положим $n = xN/2$, $|x| \leqslant 1$. Оценим мощность множества U в зависимости от значения x.

1) $n \in B_1 = \{(xN) : |x| \leqslant 1 - \tau/2\}$ (рис. 2). Вероятность события $n \in B_1$ равна $(1 - \tau/2)$. В этом случае множество $\widetilde{W}_\tau$ полностью содержится в T_0, т. е. $|\widetilde{W}_\tau|/|U| = 1$.

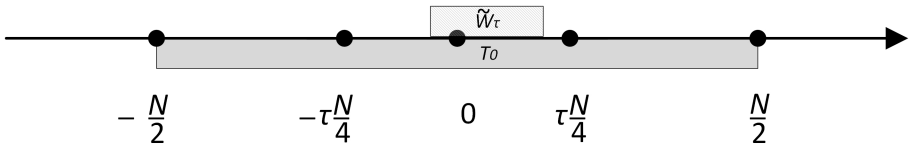

Рис. 2

2) $n \in B_2 = \{(xN) : |x| > 1 - \tau/2\}$ (рис. 3). Вероятность события $n \in B_2$ равна $\tau/2$. В этом случае можно сделать оценку $|\widetilde{W}_\tau|/|U| \leqslant 2$.

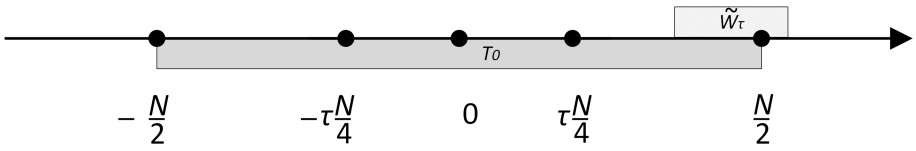

Рис. 3

Теперь можем оценить математическое ожидание:

$$\mathbf{M}(Z_{N'}) = \left(1 - \frac{\tau}{2}\right) \mathbf{M}(Z_{N'}|n \in B_1) + \frac{\tau}{2}\mathbf{M}(Z_{N'}|n \in B_2) \leqslant \left(1 - \frac{\tau}{2}\right)\sqrt{\pi N/2} + \frac{\tau}{2}\sqrt{\pi N} =$$
$$= \left(1 + \frac{(\sqrt{2} - 1)\tau}{2}\right)\sqrt{\pi N/2}.$$

Тогда при $\tau \to 0$ получаем утверждение теоремы. ■

ЛИТЕРАТУРА

1. *Gaudry P. and Schost E.* A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm // LNCS. 2004. V. 3076. P. 208–222.
2. *Galbraith S. D. and Holmes M.* A non-uniform birthday problem with applications to discrete logarithms // Discr. Appl. Math. 2012. V. 160. No. 10–11. P. 1547–1560. `eprint.iacr.org/2010/616`
3. *Gallant R., Lambert R., and Vanstone S.* Faster point multiplication on elliptic curves with efficient endomorphisms // CRYPTO'2001. LNCS. 2001. V. 2139. P. 190–200.

4. *Wiener M. J. and Zuccherato R. J.* Faster attacks on elliptic curve cryptosystems // LNCS. 1999. V. 1556. P. 190–200.
5. *Galbraith S. D. and Ruprai R. S.* Using equivalence classes to accelerate solving the Discrete Logarithm Problem in a short interval // LNCS. 2010. V. 6056. P. 368–383. eprint.iacr.org/2010/615
6. *Liu W.* Improved algorithms for the 2-dimensional discrete logarithm problem with equivalence classes. MSc Thesis, University of Auckland, 2010. http://www.math.auckland.ac.nz/~sgal018/Wei-Liu-MSc.pdf
7. *Николаев М. В., Матюхин Д. В.* О сложности двумерной задачи дискретного логарифмирования в конечной циклической группе с эффективным автоморфизмом порядка 6 // Дискретная математика. 2013. Т. 25. № 4. С. 54–65.

REFERENCES

1. *Gaudry P. and Schost E.* A low-memory parallel version of Matsuo, Chao and Tsujii's algorithm. LNCS, 2004, vol. 3076, pp. 208–222.
2. *Galbraith S. D. and Holmes M.* A non-uniform birthday problem with applications to discrete logarithms. Discr. Appl. Math., 2012, vol. 160, no. 10–11, pp. 1547–1560. eprint.iacr.org/2010/616
3. *Gallant R., Lambert R., and Vanstone S.* Faster point multiplication on elliptic curves with efficient endomorphisms. CRYPTO'2001. LNCS, 2001, vol. 2139, pp. 190–200.
4. *Wiener M. J. and Zuccherato R. J.* Faster attacks on elliptic curve cryptosystems. LNCS, 1999, vol. 1556, pp. 190–200.
5. *Galbraith S. D. and Ruprai R. S.* Using equivalence classes to accelerate solving the Discrete Logarithm Problem in a short interval. LNCS, 2010, vol. 6056, pp. 368–383. eprint.iacr.org/2010/615
6. *Liu W.* Improved algorithms for the 2-dimensional discrete logarithm problem with equivalence classes. MSc Thesis, University of Auckland, 2010. http://www.math.auckland.ac.nz/~sgal018/Wei-Liu-MSc.pdf
7. *Nikolaev M. V. and Matyukhin D. V.* On the complexity of two-dimensional discrete logarithm problem in a finite cyclic group with effective automorphism of order 6. Discr. Math. Appl., 2013, vol. 23, iss. 3–4, pp. 313–326.