$$z_{11} = x_{11} + y_{11} + x_5y_3 + 2x_6y_2 + x_7y_1 + x_2x_3y_1 + x_2y_1y_3 + 2x_3y_1y_2,$$
$$z_{12} = x_{12} + y_{12} + x_5y_4 + 2x_8y_2 + x_9y_1 + x_2x_4y_1 + x_2y_1y_4 + 2x_4y_1y_2,$$
$$z_{13} = x_{13} + y_{13} + x_{10}y_1 + x_6y_4 + 2x_8y_3 + x_3x_4y_1 + x_3y_1y_4 + 2x_4y_1y_3,$$
$$z_{14} = x_{14} + y_{14} + x_{10}y_2 + x_7y_4 + 2x_9y_3 + x_3x_4y_2 + x_3y_2y_4 + 2x_4y_2y_3.$$

ЛИТЕРАТУРА

1. *Levi F. and van der Waerden B.* Uber eine besondere Klasse von Gruppen // Abh. Math. Sem. Univ. Hamburg. 1933. No. 9. S. 154–158.
2. *Sims C.* Computation with Finitely Presented Groups. Cambridge: Cambridge University Press, 1994. 628 p.
3. *Holt D., Eick B., and O'Brien E.* Handbook of computational group theory. Boca Raton: Chapman & Hall/CRC Press, 2005. 514 p.
4. *Hall P.* Nilpotent groups, Notes of lectures given at the Canadian Mathematical Congress 1957 Summer Seminar, in The collected works of Philip Hall. Oxford: Clarendon Press, 1988. P. 415–462.
5. *Кузнецов А. А., Кузнецова А. С.* Быстрое умножение элементов в конечных двупорождённых группах периода пять // Прикладная дискретная математика. 2013. №1. С. 110–116.
6. *Кузнецов А. А. Сафонов К. В.* Hall's polynomials of finite two-generator groups of exponent seven // Журнал СФУ. Сер. математика и физика. 2014. №2. С. 186–190.

УДК 512.54.05+519.712.4 DOI 10.17223/2226308X/8/58

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

М. В. Николаев

Задача дискретного логарифмирования в интервале заключается в поиске для заданной конечной группы G (с аддитивной записью операции), заданных $P, Q \in G$, $N < |G| - 1$ такого значения n, что $Q = nP$, $0 \leqslant n \leqslant N$. Одним из наиболее эффективных методов решения данной задачи является алгоритм Годри — Шоста. В 2010 г. С. Гэлбрейт и К. 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.*

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 его идея 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

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

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

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 результата [2], являющегося обобщением парадокса дней рождения.

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 работе [3] 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 $\{a, -a\}$.

В [4] для этого случая предложена соответствующая модификация алгоритма Годри — Шоста, имеющая при $N \to \infty$ трудоёмкость $(1{,}36 + \mathrm{o}(1))\sqrt{N}$ групповых операций.

В настоящей работе конструктивно доказывается возможность дальнейшего улучшения оценки средней трудоёмкости решения задачи дискретного логарифмирования в интервале для группы с эффективным инвертированием. Основной результат может быть сформулирован в виде следующей теоремы.

Теорема 1. 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. Подробное изложение представленных результатов можно найти в [5].

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. *Wiener M. J. and Zuccherato R. J.* Faster attacks on elliptic curve cryptosystems // LNCS. 1999. V. 1556. P. 190–200.
4. *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`.
5. *Николаев М. Н.* О сложности задачи дискретного логарифмирования в интервале в группе с эффективным инвертированием // Прикладная дискретная математика. 2015. № 2(28). С. 97–102.

УДК 621.396:621.372 DOI 10.17223/2226308X/8/59

РЕАЛИЗАЦИЯ НЕЙРОННОЙ WTA-СЕТИ НА МЕМРИСТОРНОМ КРОССБАРЕ

М. С. Тарков

Предложен алгоритм отображения матрицы весовых коэффициентов нейронной WTA-сети на мемристорный кроссбар. Выполнено моделирование нейронной WTA-сети, построенной на основе мемристорного кроссбара, с использованием программы LTSPICE. Полученные результаты могут быть использованы как при математическом моделировании, так и при физической реализации нейронных сетей с межнейронными связями на мемристорах.

Ключевые слова: *мемристор, сопротивление мемристора, кроссбар, нейронная сеть, матрица весовых коэффициентов, WTA.*

Искусственная нейронная сеть обычно использует матрицу весовых коэффициентов для представления множества синапсов слоя нейронов. Соответственно вычисление активации слоя нейронов можно рассматривать как умножение этой матрицы весов на вектор входных сигналов слоя. Аппаратная реализация нейронной сети требует много памяти для хранения матрицы весов слоя нейронов и является дорогостоящей.

Решение этой проблемы упрощается при использовании в качестве ячейки памяти устройства, называемого мемристором. Мемристор был предсказан теоретически в 1971 г. Леоном Чуа [1]. Первую физическую реализацию мемристора продемонстрировала в 2008 г. лаборатория фирмы «Hewlett Packard» в виде тонкоплёночной структуры TiO_2 [2]. В России первый мемристор на основе TiO_2 получен в 2012 г. в Тюменском государственном университете.