4. Григорян Э.Р., Климовских Н.В. Управление конкурентоспособностью организации/ Э.Р. Григорян, Н.В. Климовских// Экономика и бизнес: теория и практика. – 2022. – №9 (91) – С. 40 – 42.

5. Ключевые факторы [Электронный ресурс] – режим доступа: https://msu-press.ru/ru/4-62023/upravlenie-konkurentosposobnostyu-v-sovremennykh-usloviyakh-1-1 – Дата доступа: 03.10.2025.

УДК 004.822

В.А. Ворошень
Белорусский государственный технологический университет
Минск, Беларусь

ЭФФЕКТИВНОСТЬ СИНХРОНИЗАЦИИ ДРЕВОВИДНЫХ МАШИН ЧЁТНОСТИ НА ОСНОВЕ СИНТЕЗА АЛГЕБР ДЕЙСТВИТЕЛЬНЫХ И КОМПЛЕКСНЫХ ЧИСЕЛ

Аннотация. *В статье исследуется влияние выбора алгебры на эффективность синхронизации древовидных машин чётности (TPM). Рассматриваются три конфигурации: полностью комплексные TPM, TPM с комплексными весами и действительными входными векторами, а также TPM с действительными весами и комплексными входными векторами.*

V.A. Voroshen
Belarusian State Technological University
Minsk, Belarus

EFFICIENCY OF SYNCHRONIZATION OF TREE-BASED PARITY MACHINES BASED ON THE SYNTHESIS OF ALGEBRAS OF REAL AND COMPLEX NUMBERS

Abstract. *The article examines the effect of algebra selection on the synchronization efficiency of parity tree machines (TPM). Three configurations are considered: fully complex TPM, TPM with complex weights and real input vectors, and TPM with real weights and complex input vectors.*

Введение. Одним из достаточно новых разделов криптографии на сегодняшний день является нейрокриптография, которая изучает применение стохастических алгоритмов, в частности нейронных сетей, для шифрования и криптоанализа [1]. Одной из архитектур нейросетей, используемых исследователями, являются древовидные машины

чётности (tree parity machines, TPM) – многоуровневые нейросети прямого распространения, имеющие один скрытый слой и один нейрон на выходном слое [2]. Две TPM способны синхронизироваться, получая при этом общие веса, благодаря чему можно достичь секретность передачи информации даже по незащищённому каналу.

Традиционно TPM определяются в терминах алгебры действительных чисел, однако их также можно построить на основе алгебр комплексных чисел, кватернионов и октонионов [3]. Каждая из данных алгебр накладывает определённые ограничения на реализацию прямого прохода по сети и обновления её весов при обучении.

Настоящая работа посвящена сравнительному анализу эффективности синхронизации TPM при использовании различных числовых алгебр. Рассматриваются три конфигурации:

TPM, полностью основанная на комплексных числах (cTPM);

TMP, в которой входной вектор представлен действительными числами, а веса – комплексными (rcTPM);

TPM, в которой входной вектор представлен комплексными числами, а веса – действительными (crTPM).

При этом ставится задача определить, какое влияние оказывает на эффективность синхронизации выбор конфигурации.

Основная часть. TPM представляет собой одностороннюю двухуровневую сеть, каждый нейрон которой является персептроном с дискретным вектором весов. Конкретная структура TPM зависит от следующих параметров:

K – количество нейронов скрытого слоя;

N – количество входов каждого нейрона;

L – граница диапазона значений весов (целые числа от $-L$ до L).

Для абстрагирования результатов измерения эффективности от данных параметров, их значения строго фиксируются для каждой конфигурации. При этом $N = 4$, $K = 3$, а $L = 5$.

На выходном слое TPM находится лишь один нейрон, его значение описывается четырёхвалентным комплексным τ, принимающим одно из четырёх значений: (1, 0), (0, 1), (−1, 0), (0, −1). Функция знака вычисляется на основе представленной в работе [3].

Обучение TPM, включающее в себя обновление весов и исходящее из сравнения τ двух синхронизирующихся машин, осуществляется на основе правила Хебба.

Процесс синхронизации двух машин возможен тогда, когда обе TPM имеют идентичные параметры, о которых стороны, передающие друг другу информацию, должны договориться заранее. В числе данных параметров внутреннее устройство машин (их архитектура),

правило обновления весов и входной вектор.

В контексте прикладных задач входной вектор вычисляется с помощью генератора псевдослучайных чисел. При этом такой генератор должен иметь одинаковое стартовое число на всех синхронизируемых машинах. Это число обеспечивает генерацию вектора, одинакового на обеих машинах.

Сравнение эффективности синхронизации двух TPM на основе различных конфигураций выполнялось экспериментально, для чего с использованием языка программирования Python, а также библиотек numpy, math, os, re и time создавались скрипты, содержащие определения классов `Complex`, `RealComplex` и `ComplexReal`. Данные классы реализуют соответственно конфигурации cTPM, rcTPM и crTPM. В классах имеются методы `forward()` и `update()`, отражающие прямой проход с получением τ и обновление весов.

Для уменьшения влияния случайностей на результаты измерения эффективности, эксперимент по синхронизации машин проводился неоднократно. При этом измерялись следующие показатели:

число итераций, требующееся для синхронизации двух TPM;

время до наступления синхронизации, то есть до полного совпадения весов всех скрытых нейронов.

Время до наступления синхронизации замерялось с момента начала первой итерации и до завершения той, после которой условие наступления синхронизации выполнилось.

Дополнительно вычислялось среднее число итераций:

$$\overline{T} = \frac{1}{m}\sum_{i=1}^{m} T_i ,$$

где m – число синхронизаций, T – число итераций до синхронизации.

Также вычислялось стандартное отклонение:

$$\sigma_T = \sqrt{\frac{1}{m-1}\sum_{i=1}^{m}(T_i - \overline{T})^2} .$$

Аналогично были подсчитаны среднее время до наступления синхронизации $\bar{t}$ и стандартное отклонение σ_t.

Для каждой конфигурации первоначально было выполнено 200 независимых итераций с общими K, N, L и стартовым числом. Учитывалось также то, что машины могут вовсе не достичь состояния синхронизации за определённое число итераций n, принятое в рамках эксперимента равным 50 000. Отношение успешных синхронизаций к их общем числу выражается параметром S.

Результаты показали, что машины при конфигурациях cTPM и crTPM достигли состояния синхронизации в 100% случаев. Однако в

случае rcTPM это число было меньшим: 138 успешных синхронизаций из 200, что составляет 69%. Поскольку судить о средних параметрах синхронизации на различном объёме данных нецелесообразно, было принято решение увеличить количество синхронизаций для rcTPM (всего было выполнено 287, из них 200 успешных). Это, однако, не означает, что 31% неуспешных синхронизаций не учитывается вовсе.

Полученные при этом значения параметров эффективности для всех конфигураций TPM показаны в таблице 1.

Таблица 1- Результаты синхронизации

Конфигурация	$\overline{T}$	σ_T	$\bar{t}$, с	σ_t, с	S
cTPM	2199,98	1997,19	2,06	1,88	1
rcTPM	18722,78	14521,12	22,29	21,22	0,697
crTPM	1396,48	2104,54	1,17	1,75	1

Результаты, отражённые в таблице, говорят об общей неоднозначности эффективности синхронизации при всех конфигурациях. Исходя из средних значений $\overline{T}$ и $\bar{t}$, наилучшим образом показала себя конфигурация crTPM, однако σ_T и σ_t показывают, что она не отличается постоянством своей эффективности, завися, по видимому, от различий входного вектора и начальных значений весов.

В дополнение к рассчитанным параметрам эффективности с использованием библиотеки matplotlib была выполнена визуализация полученных результатов.

На рис. 1 слева показано, сколько итераций было проведено в рамках одной синхронизации, а справа – сколько времени затрачено на одну синхронизацию в рамках конфигурации cTPM.

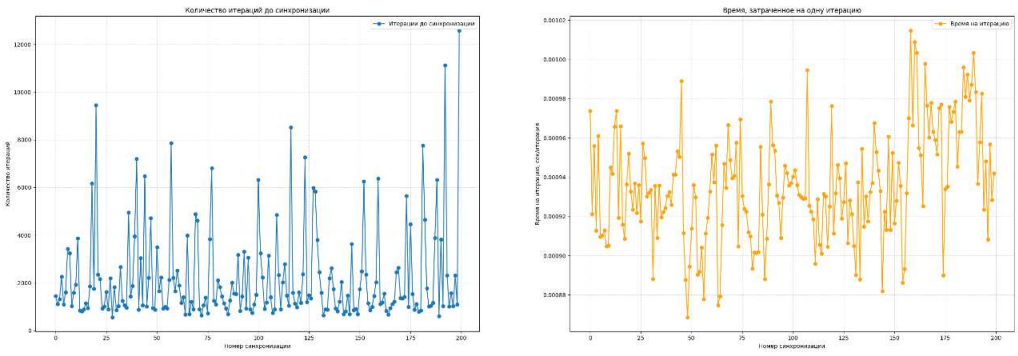

Рис. 1- Количество итераций до синхронизации для cTPM

На рисунке 2 показана аналогичная информация для конфигурации rcTPM.

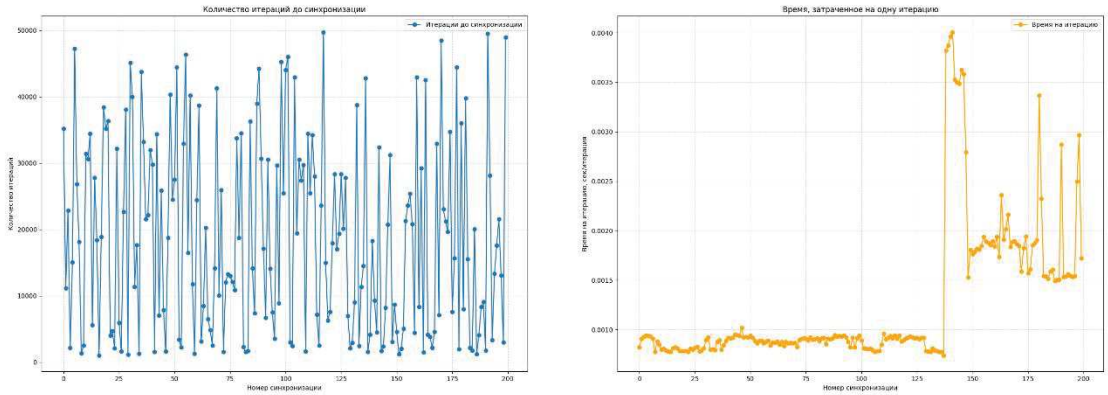

Рис. 2 - Количество итераций до синхронизации для rcTPM

На рис. 3 показана аналогичная информация для конфигурации crTPM.

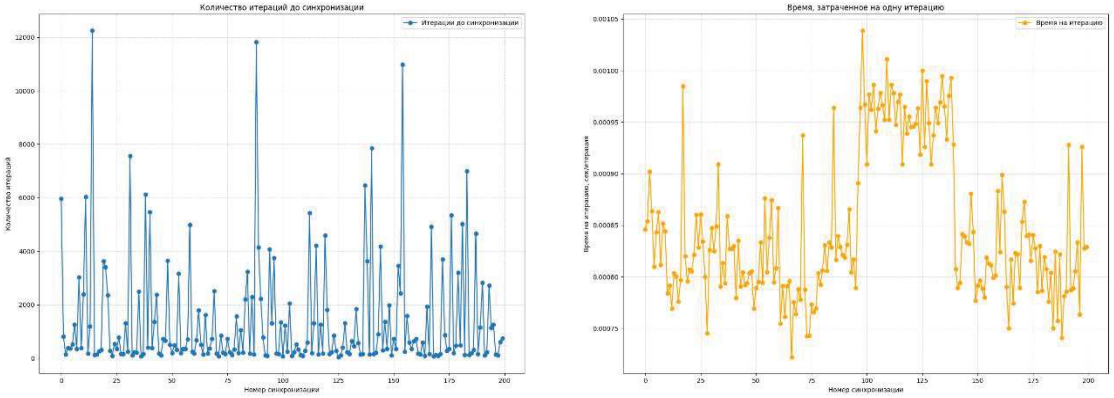

Рис. 3 - Количество итераций до синхронизации для crTPM

Из рисунков видно, что наиболее удачными с точки зрения предложенных метрик эффективности являются конфигурации cTPM и crTPM. Именно их можно использовать в дальнейшем для изучения криптографической ценности TPM на основе алгебр действительных и комплексных чисел.

Заключение. Проведённые серии экспериментов позволили провести сравнительную оценку трёх методов синхронизации TPM: cTPM, crTPM и rcTPM.

Исходя из полученных значений среднего числа итераций и времени, самый быстрый и наиболее эффективный ($\overline{T} \approx 1396$, $\bar{t} \approx 1{,}2$), но менее стабильный ($\sigma_T \approx 2105$, $\sigma_t \approx 1{,}8$) процесс синхронизации показала crTPM. Конфигурация cTPM, являющаяся стандартной реализацией TPM, имеющей в основе алгебру комплексных чисел, была несколько менее эффективна ($\overline{T} \approx 2200$, $\bar{t} \approx 2$), но немного более стабильна по итерациям ($\sigma_T \approx 1997$), но менее – по времени ($\sigma_t \approx 1{,}9$).

Самые слабые и плохо применимые на практике результаты показала конфигурация rcTPM ($\overline{T} \approx 18723$, $\bar{t} \approx 22{,}3$, $\sigma_T \approx 14521$, $\sigma_t \approx 21{,}2$).

Список использованных источников

1. Урбанович, П.П. Сравнительный анализ методов взаимообучения нейронных сетей в задачах обмена конфиденциальной информацией / П.П. Урбанович, К.В. Чуриков // Труды БГТУ. №6. Физико-математические науки и информатика. – 2010. – С. 163–166.

2. Kanter, I. Secure exchange of information by synchronization of neural networks / I. Kanter, W. Kinzel, E. Kanter // EPL (Europhysics Letters), V. 57. – 2002. – P. 141–147.

Урбанович, П. П. Нейросетевые технологии в криптографических приложениях : [монография] / П. П. Урбанович, М. Д. Плонковски, М. Долецки. – Мин

УДК 007.5

Н.А. Жиляк, М.В. Высоцкий
БГУИР
Минск, Беларусь

МОДЕРНИЗАЦИЯ СКОРИНГОВОЙ МОДЕЛИ ОЦЕНКИ КРЕДИТНОГО РИСКА НА ОСНОВЕ ГРАДИЕНТНОГО БУСТИНГА

Аннотация. *В работе рассматривается модернизация скоринговой модели оценки кредитного риска с использованием ансамблевых методов. Цель – повышение точности прогнозирования и сохранение интерпретируемости решений в банковских системах.*

N.A. Zhilyak, M.V. Vysotski
BSUIR
Minsk, Belarus

MODERNIZATION OF THE SCORING MODEL FOR ASSESSING CREDIT RISK BASED ON GRADIENT BOOSTING

Abstract. *The paper discusses the modernization of the scoring model for assessing credit risk using ensemble methods. The goal is to improve forecasting accuracy and maintain interpretability of decisions in banking systems.*