МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра веб-технологий и компьютерного моделирования

ФАДЕЕВ
Владислав Андреевич

Аннотация к дипломной работе:

ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Научный руководитель:
кандидат физ.-мат. наук,
доцент Тихонов С.В.

Минск, 2023

РЕФЕРАТ

Дипломная работа: 33 страницы, 3 использованных источника, 20 рисунков и одна таблица.

Ключевые слова: АЛГОРИТМ БЕРЛЕКЭМПА, АЛГОРИТМ ЦАССЕНХАУЗА, КОНЕЧНЫЕ ПОЛЯ, ФАКТОРИЗАЦИЯ МНОГОЧЛЕНОВ, РЕЗУЛЬТАНТ, ЛИНЕЙНАЯ КОМБИНАЦИЯ, МЕТОД ГАУССА, НУЛЬ-ПРОСТРАНСТВО МАТРИЦЫ.

Объект исследования: усовершенствование алгоритма Берлекэмпа алгоритмом Цассенхауза с результантом и с линейной комбинацией.

Цель работы: рассмотрение и реализация усовершенствованного алгоритма Берлекэмпа, сравнение эффективности способов усовершенствования алгоритма. Задачи необходимые для достижения цели:

1. Изучение теоретических материалов
2. Реализация усовершенствованного алгоритма Берлекэмпа
3. Проведение вычислительных экспериментов
4. Анализ результатов

Реализованные алгоритмы: алгоритм Цассенхауза с результантом и с линейной комбинацией, усовершенствованный алгоритм Берлекэмпа. Реализованные алгоритмы работают только для полей вида $\mathbb{Z}_p$. Для больших полей сложность представляет описание элементов данных полей и нахождение обратных элементов.

Результат работы: сравнение сложности различных усовершенствований и сравнение времени выполнения алгоритмов. Сделан вывод об эффективности метода с линейной комбинацией, по сравнению с методом основанным на использовании результанта. Данный вывод подтверждается проведенными вычислительными экспериментами.

Дипломная работа является завершенной, поставленные задачи решены в полной мере, присутствует возможность дальнейшего развития исследований.

Дипломная работа выполнена автором самостоятельно.

ABSTRACT

Scope of the diploma work: 33 pages, 3 references, 20 pictures and one table.

Key words: BERLECAMP ALGORITHM, ZASSENHAUS ALGORITHM, FINITE FIELDS, POLYNOMIAL FACTORIZATION, RESULTANT, LINEAR COMBINATION, GAUSSIAN ELIMINATION, NULL-SPACE OF MATRIX.

Object of the research: an improvement of the Berlekamp algorithm with the Zassenhaus's algorithm with a resultant and a linear combination.

Purpose of the research: consideration and implementation of the improved Berlekamp algorithm, comparison of efficiency of methods of improvement of the algorithm. The tasks necessary to achieve the goals:

1. Study of theoretical materials
2. Implementation of the improved Bredekamp's algorithm.
3. Carry out computational experiments
4. Analysis of the results

Implemented algorithms: Zassenhaus algorithm with resultant and linear combination, advanced Bredekamp algorithm. The implemented algorithms work only for fields of type $\mathbb{Z}_p$. For large fields it is difficult to describe the elements of the given fields and to find the inverse elements.

Results of the work: a comparison of the complexity of the different refinements and a comparison of the execution times of the algorithms. It is concluded that the effectiveness of the method with the linear combination, compared with the method based on the use of the resultant. This conclusion is confirmed by computational experiments.

The diploma work is complete, the set tasks are solved completely, there is a possibility of further research development.

The thesis was completed by the author independently.