

О реализации декодера одного класса алгебро-геометрических кодов на проективных кривых с использованием алгоритма Сакаты

Пеленицын А. М.
магистрант 1-го года каф. АДМ

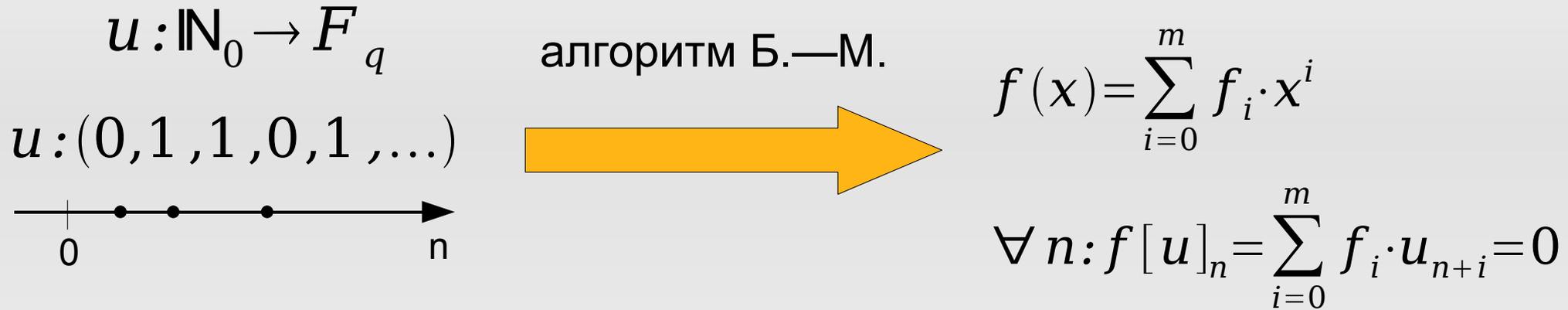
Научный руководитель: доцент, к.ф.-м.н.
Деундяк В. М., асс. Маевский А. Э.

Конференция в рамках «Недели науки» ЮФУ
2008

Обзор

- алгоритм Берлекэмп—Месси
 - одномерный алгоритм: задача и применение
 - двумерный аналог (метод Сакаты): применение
- постановка задачи
- алгебраические сведения
- особенности и ключевые идеи общего алгоритма
- реализация
- полученные результаты

Одномерный алгоритм: задача и применение

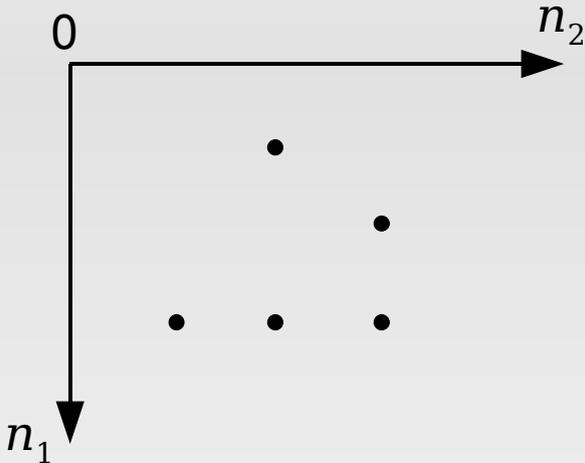


- применения:

- декодирование БЧХ-кодов
- тестирование псевдослучайных последовательностей
- решение САУ с ганкелевыми и теплицевыми матрицами
- аппроксимации Паде

Двумерный аналог (метод Сакаты)

$$u : \mathbb{N}_0^2 \rightarrow F_q$$



«Минимальное множество»:

$$\{f^{(1)}(x), \dots, f^{(l)}(x)\}, x = x_1 \cdot x_2$$

$$\forall k, n : f^{(k)}[u]_n = \sum_i f_i^{(k)} \cdot u_{n+i} = 0$$

- основное известное применение:
 - декодирование АГ-кодов типа Рида—Соломона

Постановка задачи

- анализ имеющегося метода распространения алгоритма на двумерный случай
- получение программной реализации
- изучение возможностей применения двумерного аналога

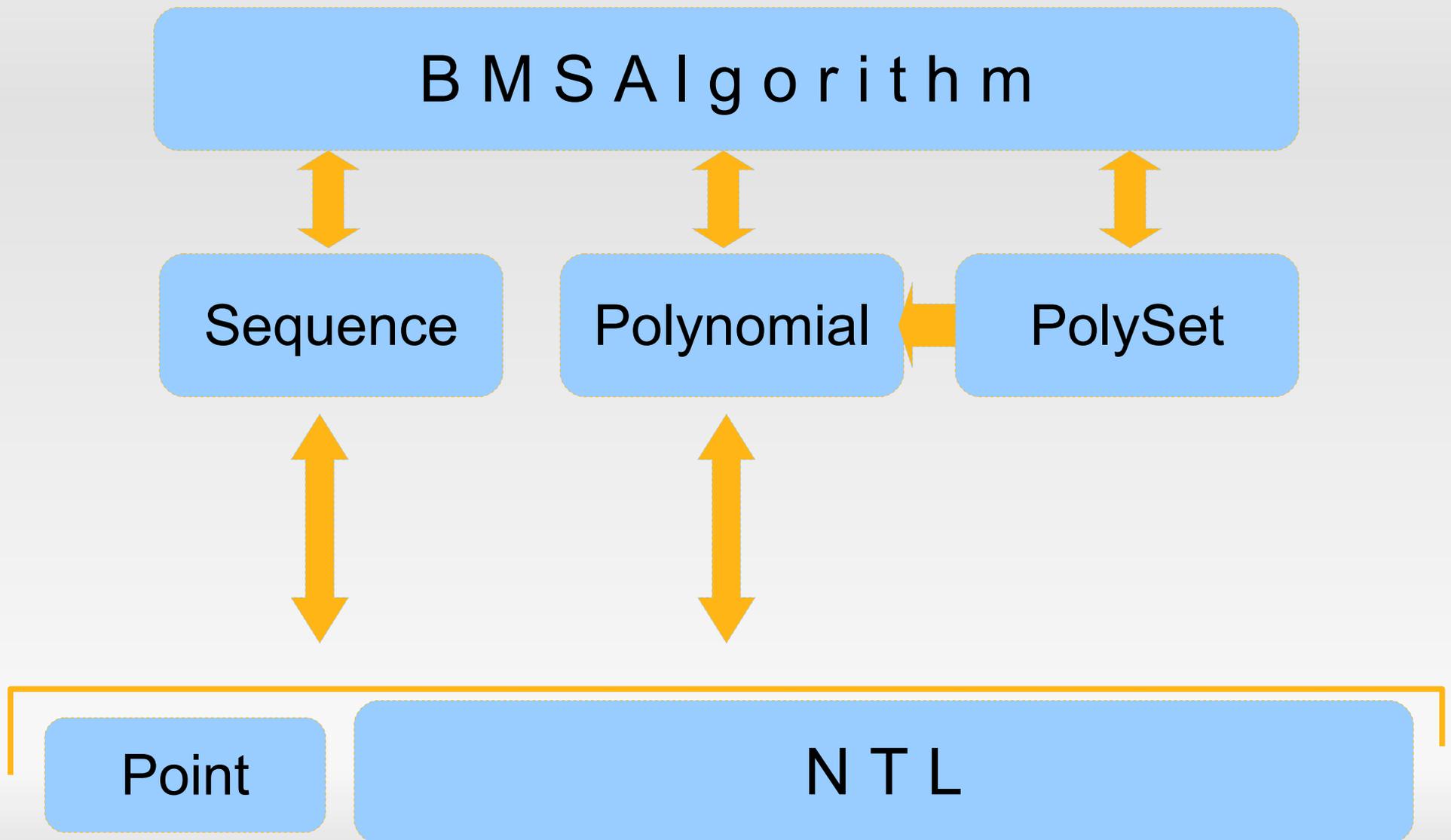
Алгебраические сведения

- нётеровы кольца и теорема Гильберта о базисе
- алгоритмический подход к построению базиса идеала в кольце полиномов многих переменных. Базисы Грёбнера
- теория размерности в алгебраической геометрии

Особенности и ключевые идеи общего алгоритма

1. Неединственность и минимальность
 2. Полиномиальная интерпретация
 3. Итеративный характер
-
4. Нижняя оценка для степени полинома, «лучшего» чем данный
 5. Процедура Берлекэмп:
$$h = VP(f, g); h \succ f \succ g;$$
для f и h достигается нижняя граница из п.4
 6. Случаи увеличения и сохранения степени существенно различны

Реализация



Полученные результаты

- изучено обобщение алгоритма Берлекэмпа—Месси, выделены общие и частные моменты
- получено четкое, замкнутое в себе описание двумерного аналога Берлекэмпа—Месси
- построен каркас программной реализации двумерного аналога Берлекэмпа—Месси