Mathematics, Mechanics and Computer Science Faculty

On Analyzing and Implementing 2D-analogue of Berlekamp—Massey Algorithm

Pelenitsyn A.
first-year graduate student
dep. of Algebra and Discrete Mathematics

Tutors: Ph. D. Deundjak V. M.,
Jr. Mem. Mayevsky A. E.

2008

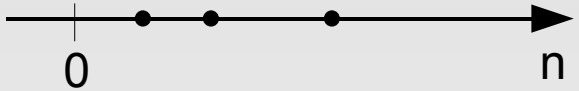
Outline

- Berlekamp—Massey Algorithm
  - 1D version: purpose and applications
  - 2D analogue (Sakata's method): application
- target setting
- algebraic prerequisities
- peculiarities and keynotes of general algorithm
- implementation
- results

1D version: purpose and applications

$$u : \mathbb{N}_0 \to F_q$$

$$u : (0,1,1,0,1,\ldots)$$



algorithm B.—M.

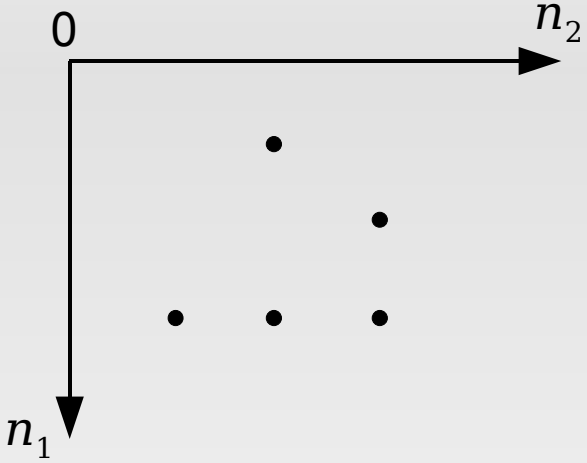
$$f(x) = \sum_{i=0}^{m} f_i \cdot x^i$$

$$\forall n : f[u]_n = \sum_{i=0}^{m} f_i \cdot u_{n+i} = 0$$

- applications:
  - BCH-codes' decoding
  - Testing pseudorandom sequences
  - Solving some classes of algebaic equations sequences
  - Pade approximations

2D analogue (Sakata's method)

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



«Minimal set»:

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

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

- Main known application:
  - Decoding of algebraic-geometric codes of Reed—Solomon type

Target setting

- Analysis of existed method of interpolation an algorithm
- Constructing an implementation
- Studing the ways of application the 2D-analogue

Algebraic prerequisities

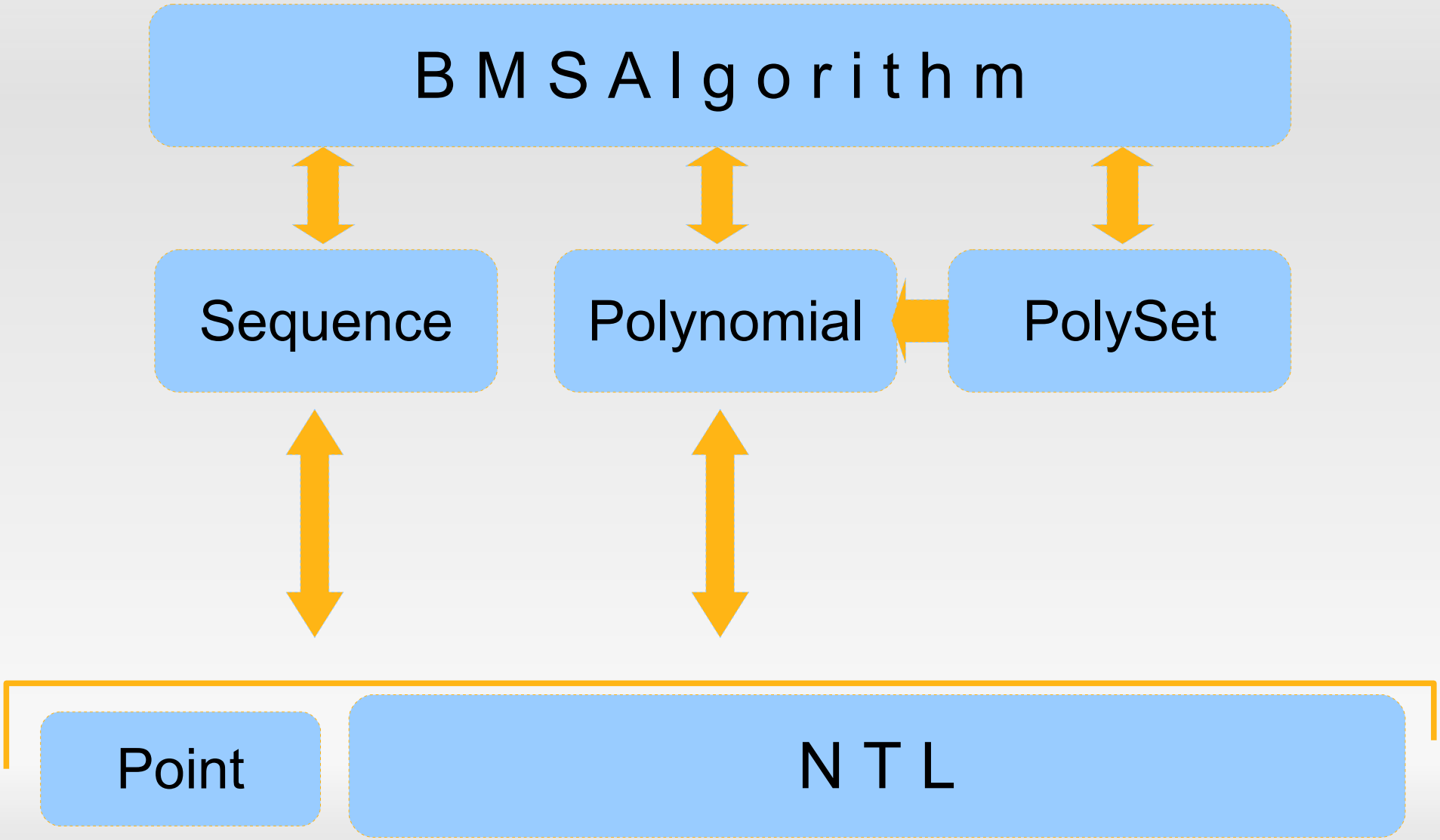
- Noetherian rings and Gilbert's Basis theorem
- Algorithmic approach to constructing bases for ideals in multivariative polynomials' rings. Grobner bases
- Dimension theory in algebraic geometry

Peculiarities and keynotes of general algorithm

1. Nonuniqueness and minimality
2. Polynomial interpretation
3. Iterative nature

...

Implementation



Results

- Generalization of Berlekamp—Massey Algorithm has been studied, general and particular feautures have been distinguished
- Clean and precise description of 2D-analogue has been got
- The framework for implementation of 2D-analogue has been constructed