Almost-linear time algorithms for operations with triangular sets

Xavier Dahan⋆, Marc Moreno Maza†, Adrien Poteaux†,•, Éric Schost†
⋆: Faculty of Mathematics, Kyûshû University
†: Ontario Research Centre for Computer Algebra, University of Western Ontario, London
•: Institute of Applied Geometry, Johannes Kepler University, Linz

Background

Triangular set: polynomials in $\mathbb{F}[X_1, \ldots, X_n]$ with a triangular structure

$$\mathbf{T} \left| \begin{array}{l} T_n(X_1, \ldots, X_n) \\ \vdots \\ T_1(X_1). \end{array} \right.$$

T_i is monic in X_i and reduced modulo $\langle T_1, \ldots, T_{i-1} \rangle$. Here, $\mathbb{F}$ is a perfect field, and all ideals will be radical.

Triangular decomposition of an ideal I: a family of triangular sets $\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(s)}$ with

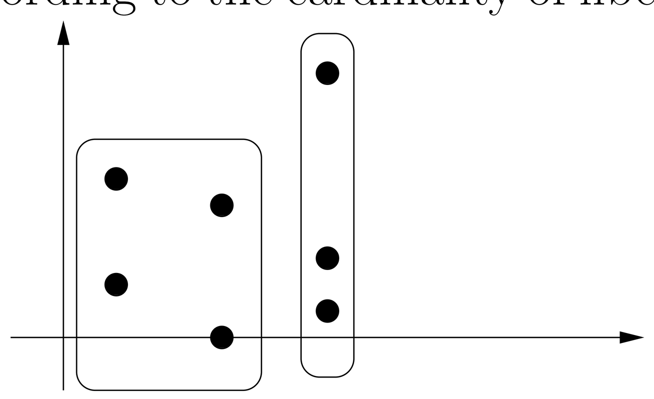
$$I = \langle \mathbf{T}^{(1)} \rangle \cap \cdots \cap \langle \mathbf{T}^{(s)} \rangle$$

and, for all $i \neq j$,

$$\langle \mathbf{T}^{(i)} \rangle + \langle \mathbf{T}^{(j)} \rangle = \langle 1 \rangle.$$

Non unique, in general.

Equiprojectable decomposition: a canonical triangular decomposition. Splits according to the cardinality of fibers of projections.



Complexity measure: δ

- for a single $\mathbf{T}$, $\delta = \deg(T_1, X_1) \cdots \deg(T_n, X_n)$
- for a triangular decomposition, $\delta = \delta(\mathbf{T}^{(1)}) + \cdots + \delta(\mathbf{T}^{(s)})$.

Previous work

- **Triangular sets**:
  - Wu, Kalkbrener, Lazard, Aubry, Moreno Maza, etc.
- **Equiprojectable decomposition**:
  - Aubry, Valibouze (2000)
  - Dahan, Moreno Maza, Schost, Wu, Xie (2005)

Our Problems

Multiplication

- given $\mathbf{T}$ and polynomials A, B reduced modulo $\mathbf{T}$, compute AB modulo $\mathbf{T}$.

Quasi-inverse

- given $\mathbf{T}$ and A reduced modulo $\mathbf{T}$, return:
  - the equiprojectable decomposition $\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(r)}$ of $\langle \mathbf{T}, A \rangle$ (where A vanishes)
  - the equiprojectable decomposition $\mathbf{T}'^{(1)}, \ldots, \mathbf{T}'^{(s)}$ of $\langle \mathbf{T} \rangle : A^\infty$ (where A is invertible), and the inverse of A modulo each $\mathbf{T}'^{(i)}$.

Change of order

- given $\mathbf{T}$ and a target variable order $<'$:
  - return the equiprojectable decomposition $\mathbf{T}'^{(1)}, \ldots, \mathbf{T}'^{(s)}$ of $\langle \mathbf{T} \rangle$ for the order $<'$,
  - for A reduced modulo $\langle \mathbf{T} \rangle$, compute the image of A modulo each $\mathbf{T}'^{(j)}$, and conversely.

Equiprojectable decomposition

- given a triangular decomposition $\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(r)}$ of an ideal I
  - return its equiprojectable decomposition $\mathbf{T}'^{(1)}, \ldots, \mathbf{T}'^{(s)}$
  - for $A = (A_1, \ldots, A_r)$, with A_i reduced modulo $\langle \mathbf{T}^{(i)} \rangle$, compute the image of A modulo each $\mathbf{T}'^{(j)}$, and conversely.

Previous work

Multiplication:

- Li, Moreno Maza, Schost (2009)

Quasi-inverse:

- Dahan, Moreno Maza, Schost, Xie (2006)

Change of order:

- Boulier, Lemaire, Moreno Maza (2001)
- Pascal, Schost (2006)

Main results

Theorem. *For any $\varepsilon > 0$, there exists a constant c_ε such that over $\mathbb{F}_q$, all previous problems can be solved using an expected $c_\varepsilon\, \delta^{1+\varepsilon} \log(q) \log\log(q)^5$ bit operations.*

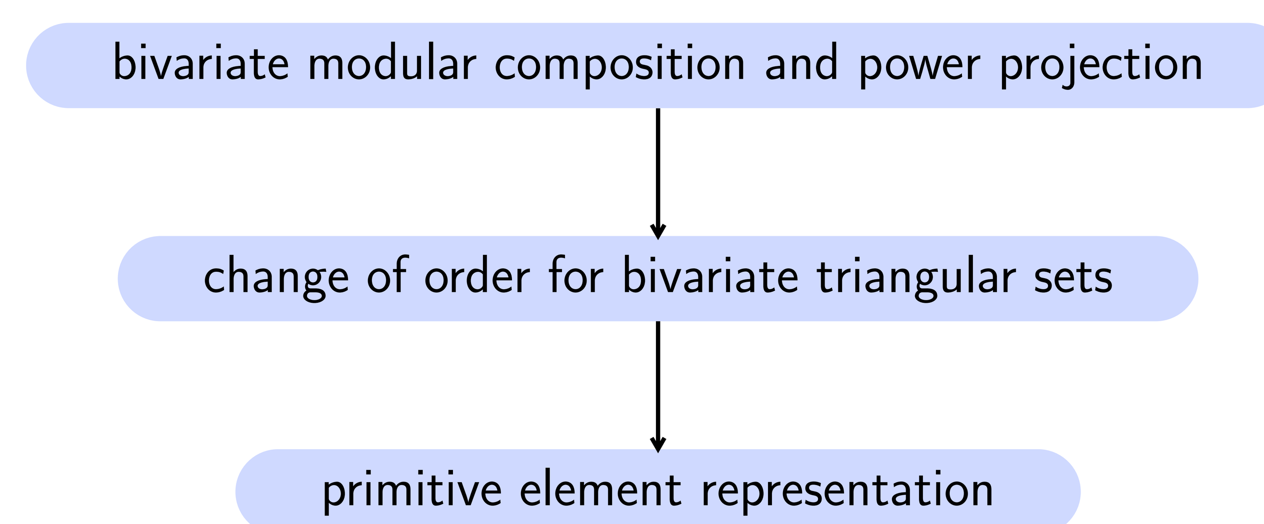
Remarks:

- cost are in a boolean RAM model
- Las Vegas algorithm

Discussion:

- input and output size are $\delta \log(q)$
- multiplication (previous: $4^n \delta\, \mathrm{polylog}(\delta)$) and quasi-inverse (previous: $K^n \delta\, \mathrm{polylog}(\delta)$),
  - not an improvement w.r.t. previous work if n is fixed
  - better if each $\deg(T_i, X_i)$ fixed
- change of order, equiprojectable decomposition:
  - first quasi-linear time result

Main ideas: introduce a primitive element, change representation, and solve the problem for univariate polynomials



Previous work

Classical algorithms (subquadratic time)

- Modular composition: Brent, Kung (1978)
- Power projection: Shoup (1994), Kaltofen (2000)

Almost linear time

- In small characteristic: Umans (2008)
- Any finite field: Kedlaya-Umans (2008)