Almost-linear time algorithms for operations with triangular sets

Xavier Dahan*, Marc Moreno Maza†, Adrien Poteaux§, Éric Schost†

* Faculty of Mathematics, Kyushu 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 \( F[X_1, \ldots, X_n] \) with a triangular structure

\[
T = \left\{ \frac{f_i}{f_j} \right\}_{f_i, f_j \in \mathcal{F}(X_1, \ldots, X_n)}
\]

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

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

\[ I = \langle T^{(1)} \rangle \cap \cdots \cap \langle T^{(s)} \rangle \]

and, for all \( i \neq j \),

\[ (T^{(i)}) + (T^{(j)}) = \langle 1 \rangle. \]

Non unique, in general.

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

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

Our Problems

**Multiplication**
- given \( T \) and polynomials \( A, B \) reduced modulo \( T \), compute \( AB \) modulo \( T \).

**Quasi-inverse**
- given \( T \) and \( A \) reduced modulo \( T \), return:
  - the equiprojectable decomposition \( T^{(1)}, \ldots, T^{(s)} \) of \( \langle T, A \rangle \) (where \( A \) vanishes)
  - the equiprojectable decomposition \( T^{(1)}, \ldots, T^{(s)} \) of \( \langle T \rangle : A^\infty \) (where \( A \) is invertible), and the inverse of \( A \) modulo each \( T^{(i)} \).

**Change of order**
- given \( T \) and a target variable order \( \prec' \),
  - return the equiprojectable decomposition \( T^{(1)}, \ldots, T^{(s)} \) of \( \langle T \rangle \) for the order \( \prec' \).
  - for \( A \) reduced modulo \( T \), compute the image of \( A \) modulo each \( T^{(i)} \), and conversely.

### Previous work

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

- **Classical algorithms (subquadratic time)**
  - Modular composition: Brent, Kung (1978)

- **Almost linear time**
  - any finite field: Kedlaya-Umans (2008)

Main results

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

**Remarks:**
- cost are in a boolean RAM model
- Las Vegas algorithm

**Discussion:**
- input and output size are \( \delta \log(q) \)
- multiplication (previous: \( 4^n \delta \log(q) \)) and quasi-inverse (previous: \( K^n \delta \log(q) \)).
  - 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