Almost linear time operations with triangular sets

Xavier Dahan (dahan@math.kyushu-u.ac.jp)
Faculty of Mathematics, Kyûshû University, Fukuoka, Japan

Marc Moreno Maza (moreno@csd.uwo.ca), Éric Schost (eschost@uwo.ca)
Computer Science Department, the University of Western Ontario, London, ON

Adrien Poteaux (adrien.poteaux@jku.at)
Institute of Applied Geometry, Johannes Kepler University, Linz, Austria

Let $\mathbb{F}$ be a perfect field, and let $\mathbf{X} = X_1, \ldots, X_n$ be indeterminates over $\mathbb{F}$. A (monic) triangular set $\mathbf{T} = (T_1, \ldots, T_n)$ is a family of polynomials in $\mathbb{F}[\mathbf{X}]$ such that for all i, T_i is in $\mathbb{F}[X_1, \ldots, X_i]$, monic in X_i, and reduced modulo $\langle T_1, \ldots, T_{i-1}\rangle$. The *degree* of $\mathbf{T}$ is the product $\deg(T_1, X_1) \cdots \deg(T_n, X_n)$. These objects allow one to solve a variety of problems for systems of polynomial equations, see [7, 1, 10, 6, 12]. We are interested here in the complexity of operations modulo a given triangular set $\mathbf{T}$.

The first question is modular multiplication: given polynomials A, B reduced modulo $\mathbf{T}$, compute $AB \bmod \mathbf{T}$.

Further operations involve families of triangular sets. The lexicographic Gröbner basis of an ideal I for a given variable order may not be triangular. The workaround is to decompose I as $I = I_1 \cap \cdots \cap I_s$, with pairwise coprime I_j, where each I_j admits a triangular basis. The decomposition is in general not unique, but there exists a canonical choice, the *equiprojectable decomposition* [4].

That said, the most useful notion of "inversion" is *quasi-inverses*: given A reduced modulo $\mathbf{T}$, we decompose the ideal $\langle \mathbf{T} \rangle$ as $I_0 \cap I_1$, where A is zero modulo I_0 and invertible modulo I_1; the output is the equiprojectable decompositions of I_0, I_1, and the inverse of A modulo the triangular sets that define I_1. The next question is *change of order*: starting from $\mathbf{T}$, we output the equiprojectable decomposition of the ideal $\langle \mathbf{T} \rangle$, for a new order on the variables. The last question starts from a family $\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(r)}$ which generate pairwise coprime ideals; our output is the equiprojectable decomposition of the ideal they generate.

The following theorem provides quasi-linear time results for these questions. These results are valid over a finite field, with costs given in a boolean RAM model; the algorithms are Las Vegas. The main idea is to introduce a primitive element and change representation, as most problems above can be solved easily in univariate situations. The change of representation is done using algorithms for *modular composition* [3] and *power projection* [13], but in multivariate setting. In [8], Kedlaya and Umans introduced quasi-linear time algorithms for the univariate versions of these problems; our core technical ingredients are multivariate versions of their algorithms.

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

- *given a triangular set* $\mathbf{T}$ *of degree* δ *in* $\mathbb{F}_q[X_1, \ldots, X_n]$*, testing whether* $\langle \mathbf{T} \rangle$ *is a radical ideal, and, if so, computing products, quasi-inverses, change of order modulo* $\mathbf{T}$*.*
- *given triangular sets* $\mathbf{T}^{(1)}, \ldots, \mathbf{T}^{(r)}$ *in* $\mathbb{F}_q[X_1, \ldots, X_n]$*, with sum of degrees* δ*, testing whether all* $\langle \mathbf{T}^{(i)} \rangle$ *are radical and pairwise coprime ideals, and, if so, computing the equiprojectable decomposition of* $I = \langle \mathbf{T}^{(1)} \rangle \cap \cdots \cap \langle \mathbf{T}^{(r)} \rangle$*.*

In all problems, the input and output bit sizes are essentially $\delta \log(q)$. The best result to date were $4^n \delta \,\mathrm{polylog}(\delta)$ operations in $\mathbb{F}_q$ for modular multiplication [9] and $c^n \delta \,\mathrm{polylog}(\delta)$ for quasi-inverse [5], for some constant c: this is better for fixed n; our result is better when e.g. $\deg(T_i, X_i) = 2$ for all i. For change of order, previous results [2, 11] had super-linear cost, even for $n = 2$. For the equiprojectable decomposition, there was no known complexity result.

References

[1] P. Aubry, D. Lazard, and M. Moreno Maza. On the theories of triangular sets. *J. Symb. Comp.*, 28(1,2):45–124, 1999.

[2] F. Boulier, F. Lemaire, and M. Moreno Maza. Pardi! In *ISSAC'01*, pages 38–47. ACM, 2001.

[3] R. P. Brent and H. T. Kung. Fast algorithms for manipulating formal power series. *Journal of the Association for Computing Machinery*, 25(4):581–595, 1978.

[4] X. Dahan, M. Moreno Maza, É. Schost, W. Wu, and Y. Xie. Lifting techniques for triangular decompositions. In *ISSAC'05*, pages 108–115. ACM, 2005.

[5] X. Dahan, M. Moreno Maza, É. Schost, and Y. Xie. On the complexity of the D5 principle. In *Transgressive Computing*, pages 149–168, 2006.

[6] É. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems. In *SNSC*, volume 2630 of *LNCS*, pages 1–39. Springer, 2003.

[7] M. Kalkbrener. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. *J. Symb. Comp.*, 15:143–167, 1993.

[8] K. S. Kedlaya and C. Umans. Fast polynomial factorization and modular composition. To appear, available at `http://www.cs.caltech.edu/~umans/papers/KU08-final.pdf`.

[9] X. Li, M. Moreno Maza, and É. Schost. Fast arithmetic for triangular sets: from theory to practice. *J. Symb. Comp.*, 44(7):891–907, 2009.

[10] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical Report TR 4/99, NAG Ltd, Oxford, UK, 1999. `http://www.csd.uwo.ca/~moreno/`.

[11] C. Pascal and É. Schost. Change of order for bivariate triangular sets. In *ISSAC'06*, pages 277–284. ACM, 2006.

[12] É. Schost. Complexity results for triangular sets. *J. Symb. Comp.*, 36(3–4):555–594, 2003.

[13] V. Shoup. Fast construction of irreducible polynomials over finite fields. *J. Symb. Comp.*, 17(5):371–391, 1994.