On the Complexity of the D5 Principle

X. Dahan⋆, M. Moreno Maza†, É. Schost⋆, W. Wu† & Y. Xie†

⋆: LIX, École polytechnique, 91128 Palaiseau, France.

†: ORCCA, University of Western Ontario, London, Canada.

ISSAC, July, 2005.

Introduction

Introductory example. Let $\mathbb{L} = \mathbb{K}[X]/\langle p \rangle$ be an extension of a field $\mathbb{K}$, with p square-free, but not necessarily irreducible: $\mathbb{L}$ is a Direct Product of Fields (DPF).

We want to decide whether some $q \in \mathbb{K}[X]$ is invertible in $\mathbb{L}$. Writing $g = \gcd(p, q)$, then

- q is zero modulo g
- q is invertible modulo p/g.

This is called a quasi-inverse computation. Up to splitting, it allows one to compute in $\mathbb{L}$ as if it were a field.

This idea is known as the D5 Principle. It has been employed in many areas of symbolic computations: linear algebra, polynomial system solving, dynamic evaluation, …

Main Results

Let now $T = T_1(X_1), T_2(X_1, X_2), \ldots, T_n(X_1, X_2, \ldots, X_n)$ be a triangular set, defining a radical ideal. Then

$$\mathbb{L}_n = \mathbb{K}[X_1, X_2, \ldots, X_n]/\langle T_1, T_2, \ldots, T_n \rangle$$

is again a DPF. Let δ be the degree of $\mathbb{K} \to \mathbb{L}$. Then for any $\varepsilon > 0$, we have the following results.

- **Theorem 1** There exists a constant K_1 such that the addition, multiplication, and quasi-inverses in $\mathbb{L}_n$ can be done in $K_1^n \delta^{1+\varepsilon}$ operations in $\mathbb{K}$.
- **Theorem 2** There exists a constant K_2 such that the GCD of two polynomials in $\mathbb{L}_n[X_{n+1}]$ of degree d can be done in $K_2^n \delta^{1+\varepsilon} d^{1+\varepsilon}$ operations in $\mathbb{K}$.

These results extend classical ones known when $\mathbb{L}$ is a field. In view of their dependence in the degree δ, we call such estimates quasi-linear; they are nearly optimal.

Main Difficulties

Using the D5 Principle over $\mathbb{L}_n$ leads to splitting, *i.e.* replacing the triangular set T by a triangular decomposition $\Delta = T^1, \ldots, T^e$. Then, we have to evaluate fast the map

$$\text{SPLIT}: \quad \mathbb{L}_n \quad \to \quad \prod_{1 \le i \le e} \mathbb{K}[X_1, \ldots, X_n]/\langle T^i \rangle$$

Example. Let $a, a', a'' \in \mathbb{K}[X_1]$ be pairwise coprime polynomials and $b, b' \in \mathbb{K}[X_2]$ be coprime polynomials. Then

$$\Delta = \{aa', b\},\ \{a'', b\},\ \{aa'', b'\},\ \{a', b'\}$$

is a triangular decomposition of $T = \{aa'a'', bb'\}$. Evaluating SPLIT implies to compute

$$p \mapsto (p \bmod aa'),\ \ (p \bmod a''),\ \ (p \bmod aa''),\ \ (p \bmod a'),$$

whence some redundancy. We call critical pairs the non-trivial GCD's between the moduli: they prevent us from obtaining a quasi-linear algorithm for SPLIT, so we have to remove them. Here, we need to refine Δ into

$$\Delta' = \{a, b\}, \{a', b\}, \{a'', b\}, \{a, b'\}, \{a', b'\}, \{a'', b'\}.$$

This is done by coprime factorization in $\mathbb{K}[X_1]$.

Key Solutions

We have to extend fast algorithms over fields to DPF:

- Half-GCD for computing gcds and thus quasi-inverses.
- Coprime factorization for removing critical pairs.

Algorithms using only additions and multiplications adapt in a direct manner, and their complexity is preserved. Those with divisions require invertibility tests, splittings and critical pairs removal: preserving their complexity is not obvious. To do so, we propose the following inductive process, explained hereafter. We set $\mathbb{L}_i = \mathbb{K}[X_1, \ldots, X_i]/\langle T_1, \ldots, T_i \rangle$ and δ_i = degree of $\mathbb{K}_i \to \mathbb{L}_i$.

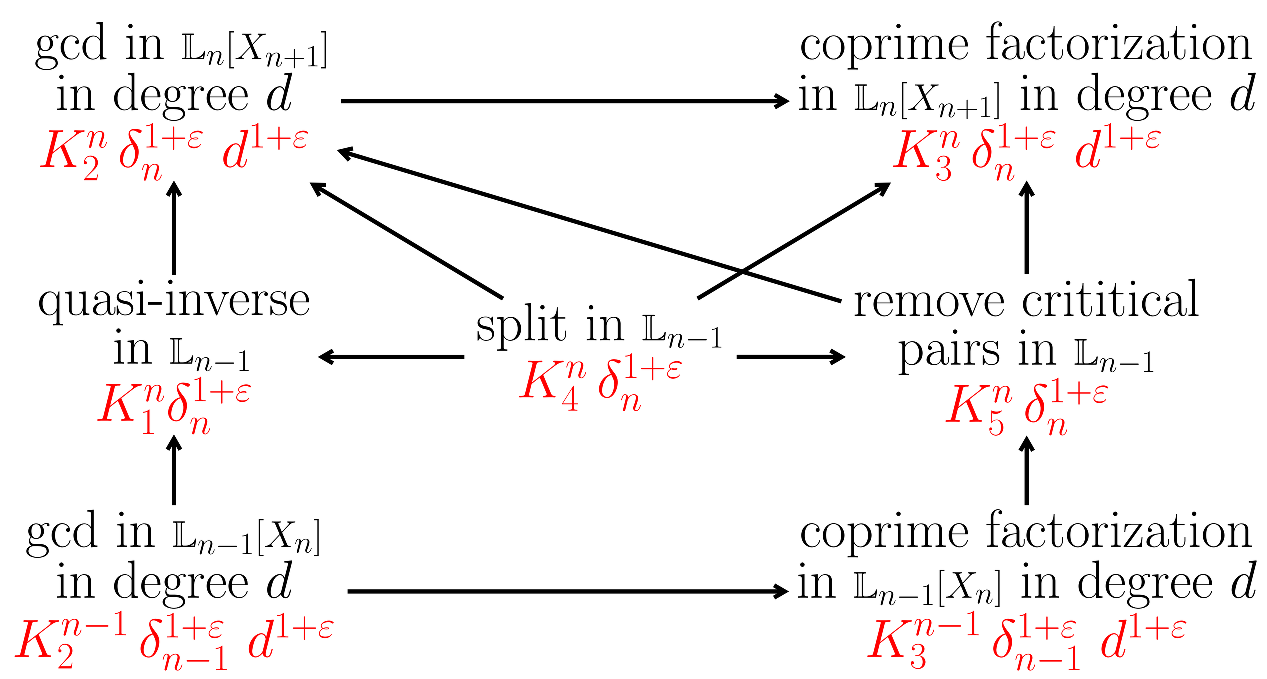

Figure: A View of the Inductive Process

- Assuming that GCDs can be computed fast in $\mathbb{L}_{n-1}[X_n]$, we obtain fast coprime factorization in $\mathbb{L}_{n-1}[X_n]$.
- Then we obtain fast removal of critical pairs and thus fast evaluation of the split map.
- We can then adapt the Half-GCD and preserve its complexity.

Conclusions and Future Work

- We have proposed nearly optimal algorithms for computing quasi-inverses and GCDs over direct products of fields presented by triangular sets.
- An implementation of these techniques is in progress.
- This should lead to faster algorithms for computing triangular decompositions, in particular, for computing the equiprojectable decomposition of a variety and thus in developing modular methods for triangular decompositions.
- More generally, our work provides tools for analyzing the complexity of algorithms based on the D5 Principle.

References

Our algorithms use Subproduct-tree techniques, which were introduced in the **1970's** (Fiduccia, Borodin-Moenck, Strassen).

The D5 principle appears in Della-Dora, Dicreszenzo, Duval (**1985**) and is detailed in Duval's **1987** thesis. No complexity estimate.

Complexity results for GCD's over products of fields are used by Langemyr (**1991**), but with no proof.

Coprime factorization is also known as gcd-free basis computation. Bernstein (**2005**) gives a first quasi-linear time algorithm.

The equiprojectable decomposition of 0-dimensional varieties is introduced in (Dahan et al., **2005**).