On the complexity of the D5 principle

X. Dahan, É. Schost[a], M. Moreno Maza, W. Wu, Y. Xie[b]

[a]LIX, École polytechnique, 91128 Palaiseau, France {dahan, schost}@lix.polytechnique.fr

[b]ORCCA, University of Western Ontario, London, Ontario, Canada {moreno, wwu25, yxie}@orcca.on.ca

The standard approach for computing with an algebraic number using its irreducible minimal polynomial over some base field k. However, many algebraic numbers may appear when solving a polynomial system; applying them this approach requires possibly costly factorization algorithms. Della Dora, Dicrescenzo and Duval introduced "dynamic evaluation" techniques (also termed "D5 principle") [2] as a means to compute with algebraic numbers, avoiding factorization. This approach leads one to compute over *direct products of field extensions of* k, instead of only field extensions.

We address complexity issues for such computations. Let $\mathbf{T} = T_1(X_1),\ T_2(X_1, X_2),\ \ldots$ $T_n(X_1, \ldots, X_n)$ be polynomials such that $k \to K = k[X_1, \ldots, X_n]/\mathbf{T}$ is a direct product of fields. We write δ for the dimension of K over k. Using fast polynomial arithmetic, it is a folklore result that for any $\varepsilon > 0$, the operations $(+, \times)$ in K can be performed in $c_\varepsilon^n \delta^{1+\varepsilon}$ operations in k, for some constant c_ε. Using fast Euclidean algorithm, a similar result carries over to inversion, *in the special case when* K *is a field*.

Our main results are similar estimates for the general case. Following the D5 philosophy, meeting zero-divisors in the computation will lead to *splitting* $\mathbf{T}$ into a family thereof, defining the same extension. Inversion is then replaced by *quasi-inversion*: a quasi-inverse [4] of $\alpha \in K$ is a splitting of $\mathbf{T}$, such that α is either zero or invertible in each component, together with the corresponding inverses. We obtain similar result for gcd computation with coefficients in K. Again, the notion of a gcd has to be adapted: a gcd of two polynomials F and G in $K[y]$ consists of a splitting of $\mathbf{T}$, together with *monic* polynomials that form gcd's of F and G over each factor.

Theorem. *Let* $\varepsilon > 0$. *There exists* $C_\varepsilon > 0$ *such that addition, multiplication and quasi-inversion in* K *can be done in* $C_\varepsilon^n\, \delta^{1+\varepsilon}$ *operations in* k. *There exists* $C' > 0$ *such that one can compute a gcd of degree* d *polynomials in* $K[y]$ *using* $C'\, C_\varepsilon^n\, d^{1+\varepsilon}\, \delta^{1+\varepsilon}$ *operations in* k.

In both cases, the main difficulty comes from handling splittings: if $\mathbf{T}$ has been split into a family $\mathbf{T}_1, \ldots, \mathbf{T}_s$, this corresponds to making effective the map $k[X_1, \ldots, X_n]/\mathbf{T} \to \prod_{i=1}^{s} k[X_1, \ldots, X_n]/\mathbf{T}_i$. This operation has a quasi-linear complexity when $n = 1$; $n > 1$, a similar result lacks. However, it is possible to extend the result from the univariate case when $\mathbf{T}_1, \ldots, \mathbf{T}_s$ satisfy a regularity condition, the absence of *critical pairs*. To reduce to this case, we have to remove critical pairs. This is done by introducing a new algorithm for *coprime factorization* of univariate polynomials [1] (this tool that was already used in [3] for parallel complexity estimates in a similar context).

References

[1] D. J. Bernstein. Factoring into coprimes in essentially linear time. *J. Algorithms*, 54(1):1–30, 2005.

[2] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *Eurocal '85 Vol. 2*, volume 204 of *Lecture Notes in Computer Science*, pages 289–290, 1985.

[3] T. Gautier and J.-L. Roch. $\mathcal{NC}^2$ computation of gcd-free basis and application to parallel algebraic numbers computation. In *PASCO'97*, pages 31–37. ACM Press, 1997.

[4] M. Moreno Maza and R. Rioboo. Polynomial gcd computations over towers of algebraic extensions. In *Proc. AAECC-11*, pages 365–382. Springer, 1995.