Exercises on the chapters "Fast Evaluation and Interpolation" and "Gcd and Resultant"

To prepare for 2021-10-14

In what follows, $\mathbb{K}$ denotes a field of characteristic zero.

Exercise 1. Let f and g be two polynomials in $\mathbb{K}[x, y]$ of degrees at most d_x in x and at most d_y in y.

(a) Show that it is possible to compute the product $h = fg$ using $O(\mathsf{M}(d_x d_y))$ arithmetic operations in $\mathbb{K}$. *Hint*: Use the substitution $x \leftarrow y^{2d_y+1}$ to reduce the problem to the product of univariate polynomials.

(b) Improve this result by proposing an evaluation-interpolation scheme which allows the computation of h in $O(d_x\,\mathsf{M}(d_y) + d_y\,\mathsf{M}(d_x))$ arithmetic operations in $\mathbb{K}$.

Exercise 2. Let $P, Q \in \mathbb{K}[x]$ be two polynomials.

(a) Let $N \in \mathbb{N} \setminus \{0\}$. Show that the unique monic polynomial in $\mathbb{K}[x]$ whose roots are the N-th powers of the roots of P can be obtained by a resultant computation.

(b) If P is the minimal polynomial of an algebraic number α, show that one can determine an annihilating polynomial of $Q(\alpha)$ using a resultant.

Exercise 3. The aim of this exercise is to prove algorithmically the following identity:

$$\sqrt[3]{\sqrt[3]{2} - 1} = \sqrt[3]{\frac{1}{9}} - \sqrt[3]{\frac{2}{9}} + \sqrt[3]{\frac{4}{9}}. \tag{1}$$

Let $a = \sqrt[3]{2}$ and $b = \sqrt[3]{\frac{1}{9}}$.

(a) Determine a polynomial in $\mathbb{Q}[x]$ annihilating $c = 1 - a + a^2$, by using a resultant computation.

(b) Deduce a polynomial in $\mathbb{Q}[x]$ annihilating the right-hand side of (1), by another resultant computation.

(c) Show that the polynomial computed in (b) also annihilates the left-hand side of (1).

(d) Conclude.