Martin Ziegler

Issued on 2014-04-22
Solutions due: 2014-04-28

Algebraic Complexity Theory

SS 2014, Exercise Sheet #2

$$\begin{pmatrix} p_0\cdot q_0 \\ p_1\cdot q_0+p_0\cdot q_1 \\ p_2\cdot q_0+p_1\cdot q_1+p_0\cdot q_2 \\ p_2\cdot q_1+p_1\cdot q_2 \\ p_2\cdot q_2 \end{pmatrix} \overset{(*)}{=} \begin{pmatrix} 1 & x_0 & x_0^2 & x_0^3 & x_0^4 \\ 1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 \\ 1 & x_3 & x_3^2 & x_3^3 & x_3^4 \\ 1 & x_4 & x_4^2 & x_4^3 & x_4^4 \end{pmatrix}^{-1} \cdot \begin{pmatrix} (p_0+p_1\cdot x_0+p_2\cdot x_0^2)\cdot(q_0+q_1\cdot x_0+q_2\cdot x_0^2) \\ (p_0+p_1\cdot x_1+p_2\cdot x_1^2)\cdot(q_0+q_1\cdot x_1+q_2\cdot x_1^2) \\ (p_0+p_1\cdot x_2+p_2\cdot x_2^2)\cdot(q_0+q_1\cdot x_2+q_2\cdot x_2^2) \\ (p_0+p_1\cdot x_3+p_2\cdot x_3^2)\cdot(q_0+q_1\cdot x_3+q_2\cdot x_3^2) \\ (p_0+p_1\cdot x_4+p_2\cdot x_4^2)\cdot(q_0+q_1\cdot x_4+q_2\cdot x_4^2) \end{pmatrix}$$

EXERCISE 3:
Recall Karatsuba's Algorithm for polynomial multiplication using $\mathcal{O}(n^{\log_2 3}) \subseteq \mathcal{O}(n^{1.585})$ arithmetic operations. Now fix an algebra $\mathcal{A}$ over the infinite field $\mathbb{F}$.

a) Verify the above identity (*) for any pairwise distinct $x_0, x_1, \ldots, x_d \in \mathbb{F}$ and arbitary $p_0 + p_1 \cdot X + p_2 \cdot X^2, q_0 + q_1 \cdot X + q_2 \cdot X^2 \in \mathcal{A}[X]$.

b) Choose $x_j = j$, say, and conclude that two quadratic polynomials over $\mathcal{A}$ can me multiplied using 5 — instead of 9 — multiplications in $\mathcal{A}$ (and arbitrary many additions in $\mathcal{A}$ as well as multiplications by constants from $\mathbb{F}$).

c) Derive an algorithm for multiplying two polynomials over $\mathcal{A}$ of degree n using $\mathcal{O}(n^{\log_3 5}) \subseteq \mathcal{O}(n^{1.465})$ arithmetic operations and constants from $\mathbb{F}$.

d) Generalize a) and b) in order to obtain an algorithm multiplying $p \in \mathcal{A}[X]$ of $\deg(p) \leq k$ and $q \in \mathcal{A}[X]$ of $\deg(q) \leq \ell$ using $k + \ell + 1$ multiplications in $\mathcal{A}$ (and arbitrary many additions in $\mathcal{A}$ as well as multiplications by constants from $\mathbb{F}$).
Can you identify Karatsuba as a special case?

e) Derive, for any fixed $\varepsilon > 0$, an algorithm multiplying two polynomials over $\mathcal{A}$ of degree at most n using $\mathcal{O}(n^{1+\varepsilon})$ arithmetic operations and constants from $\mathbb{F}$.

EXERCISE 4:
Formalize the following algorithms as straight-line programs and analyze their costs:

a) Compute the determinant of a given 3×3–matrix using Sarrus' Rule.

b) Compute the determinant of a given $n \times n$–matrix using Laplace's Expansion.

c) Compute the determinant of a given $n \times n$–matrix using Leibnitz' Formula.

d) Compute the determinant of a given 3×3–matrix via its LU–decomposition/Gaussian Elimination.