Martin Ziegler

Issued on 2014-04-29
Solutions due: 2014-05-05

# Algebraic Complexity Theory

## SS 2014, Exercise Sheet #3

**EXERCISE 5:**
Devise a straight-line program of length $\mathcal{O}(N \cdot \log N)$ computing the $N$-dimensional discrete Fourier-transform

$$\mathcal{F}_N : \mathbb{C}^N \;\ni\; (x_0, \ldots, x_{N-1}) \;\mapsto\; \big(\sum_{\ell=0}^{N-1} \exp(2\pi i \cdot k \cdot \ell / N) \cdot x_\ell\big)_{k=0,\ldots,N-1} \;\in\; \mathbb{C}^N$$

in case $N = 3^n$.

**EXERCISE 6:**
Fix infinite fields $\mathbb{F} \subseteq \mathbb{E}$.

a) Let $\mathbb{E}[X_1, \ldots, X_n]$ denote the $\mathbb{E}$–algebra of multivariate polynomials and $\deg : \mathbb{E}[X_1, \ldots, X_n] \setminus \{0\} \to \mathbb{N}$ the maximum degree; e.g. $\deg(X^3 \cdot Y^2) = 3$.
Fix $d \in \mathbb{N}$ and some set $\mathcal{X} \subseteq \mathbb{F}$ of $\mathrm{Card}(\mathcal{X}) = d$. Show that every function $f : \mathcal{X}^n \to \mathbb{E}$ can be represented by a unique polynomial $p \in \mathbb{E}[X_1, \ldots, X_n]$ of $\deg(p) < d$.
Moreover the coefficients of said $p$ 'live' in the sub-field $\mathbb{F}(\mathrm{range}\, f)$ of $\mathbb{E}$.

b) Let $a, b, u, v \in \mathbb{R}[X_1, \ldots, X_n]$ denote multivariate polynomials such that both $(a, b)$ and $(u, v)$ are coprime. Suppose the rational functions $a/b$ and $u/v$ are defined and coincide on some non-empty open* subset of $\mathbb{R}^n$. Then there exists $c \in \mathbb{R}$ such that $a = c \cdot u$ and $b = c \cdot v$.

c) Let $a, b \in \mathbb{E}[X_1, \ldots, X_n]$ denote coprime multivariate polynomials where $b$ is *monic* in the sense that some monomial has coefficient 1. Then the coefficients of $a$ and $b$ 'live' in the field extension $\mathbb{F}\big(\{a(\vec{x})/b(\vec{x}) : \vec{x} \in \mathbb{F}^n\}\big) \subseteq \mathbb{E}$.

d) Let $p = \sum_{j=0}^{d} p_j X^j$ and $q = X^d + \sum_{j=0}^{d-1} q_j X^j$ denote polynomials over $\mathbb{E}$.
Devise a straight-line program over $\big(\mathbb{E}, \mathbb{E}, (+, -, \times, \div)\big)$ of length $3d + \mathcal{O}(1)$ computing the rational function $p/q$ (possibly extended to removable singularities).
Hint: Consider the continued fraction representation of $p/q$.

*One may replace $\mathbb{R}$ with $\mathbb{F}$ by understanding open sets with respect to the Zariski Topology