Lower Bounds on the Bounded Coefficient Complexity of Bilinear Maps

Peter Bürgisser\textsuperscript{a} and Martin Lotz\textsuperscript{b}

\textsuperscript{a,b}Department of Mathematics and Computer Science, University of Paderborn, D-33095 Paderborn, Germany. Email: \{pbuerg,lotzm\}@math.uni-paderborn.de

We prove lower bounds of order $n \log n$ for both the problems to multiply polynomials of degree $n$, and to divide polynomials with remainder, in the model of bounded coefficient arithmetic circuits over the complex numbers. These lower bounds are optimal up to order of magnitude. The proof uses a recent idea of R. Raz [ECCC Report 12, 2002] proposed for matrix multiplication and reduces the linear problem to multiply a random circulant matrix with a vector to the bilinear problem of cyclic convolution. We treat the arising linear problem by extending J. Morgenstern’s bound [J. ACM 20, pp. 305-306, 1973] in a unitarily invariant way, thus establishing a new lower bound on the bounded coefficient complexity of linear forms in terms of the singular values of the corresponding matrix.