

io-port 01853226**Frandsen, Gudmund Skovbjerg; Hansen, Johan P.; Miltersen, Peter Bro****Lower bounds for dynamic algebraic problems.**

Inf. Comput. 171, No. 2, 333-349 (2001).

Summary: We consider dynamic evaluation of algebraic functions (matrix multiplication, determinant, convolution, Fourier transform, etc.) in the model of Reif and Tate; i.e., if $f(x_1, \dots, x_n) = (y_1, \dots, y_m)$ is an algebraic problem, we consider serving online requests of the form “change input x_i to value v ” or “what is the value of output y_i ?” We present techniques for showing lower bounds on the worst case time complexity per operation for such problems. The first gives lower bounds in a wide range of rather powerful models (for instance, history dependent algebraic computation trees over any infinite subset of a field, the integer RAM, and the generalized real RAM model of Ben-Amram and Galil). Using this technique, we show optimal $\Omega(n)$ bounds for dynamic matrix-vector product, dynamic matrix multiplication, and dynamic discriminant and an $\Omega(\sqrt{n})$ lower bound for dynamic polynomial multiplication (convolution), providing a good match with Reif and Tate’s $O(\sqrt{n \log n})$ upper bound. We also show linear lower bounds for dynamic determinant, matrix adjoint, and matrix inverse and an $\Omega(\sqrt{n})$ lower bound for the elementary symmetric functions. The second technique is the communication complexity technique of Miltersen, Nisan, Safra, and Wigderson which we apply to the setting of dynamic algebraic problems, obtaining similar lower bounds in the word RAM model. The third technique gives lower bounds in the weaker straight line program model. Using this technique, we show an $\Omega((\log n)^2 / \log \log n)$ lower bound for dynamic discrete Fourier transform. Technical ingredients of our techniques are the incompressibility technique of Ben-Amram and Galil and the lower bound for depth-two superconcentrators of Radhakrishnan and Ta-Shma. The incompressibility technique is extended to arithmetic computation in arbitrary fields.

doi:10.1006/inco.2001.3046