WAYNE EBERLY, Department of Computer Science, University of Calgary

On the Reliability of Block Wiedemann and Lanczos Algorithms—Another Piece of the Puzzle

Block Wiedemann and Lanczos algorithms are now available as part of the Linbox package. These have been proved to be reliable in limited cases, or more generally if matrix preconditioners are used to avoid pathological inputs. On the other hand, considerably simpler heuristics (based on the same ideas) have been used with considerable success for various number-theoretic computation. This motivates work to generalize the proofs of reliability that we now have by weakening or eliminating assumptions about the input upon which these proofs currently depend.

Various claims about the reliability of such algorithms depend on bounds for the expected nullity of various "block Hankel" matrices. These are matrices that are generated using a matrix $A \in \mathsf{F}^{N \times N}$ with entries in a field F — generally part of the input for the given problem — as well as blocks of vectors $u, v \in \mathsf{F}^{N \times k}$ that are randomly generated. Given A, u, and v, the (i,j)-th block of the matrix that is of interest is the $k \times k$ matrix $u^T A^{i+j} v$.

Bounds on the nullity of such matrices are now available in a reasonably general case, namely, that the number of nontrivial invariant factors of the matrix A is less than the "blocking factor" k. In this talk I will sketch a proof that this assumption about invariant factors is not, in fact, necessary: Useful bounds on the nullity of the above block Hankel matrices can be obtained for arbitrary matrices $A \in \mathsf{F}^{N \times N}$.