

capabilities over finite field. In this regard, generic software methodology is a powerful tool.

Partly modeled on the STL, LinBox uses the

Minimal polynomial and linear system solution over finite fields. For a matrix $\bar{A} \in \mathbb{F}^{n \times n}$ over a field \mathbb{F} , Lanczo and Krylov subspace methods

Checking $\bar{A}r = b$ make the system solution La Vega. The Lanczo approach allow one to compute r within the iteration for the minimal polynomial, thus the arithmetic and memory cost are only slightly greater than for Basic Lanczo. The main drawback of the Wiedemann approach is that it need to either store or recompute the sequence $\{\bar{A}^i b\}_{0 \leq i \leq d-1}$.

For both minimal polynomial and system of

efficient Monte Carlo rank determination is based on rank computation modulo random prime (see

We have chosen not to focus on this, and the

References

- [1] Z. Bai, J. Demmel, J. Dongarra, A. Ruhe, and H. van der Vorst, editors. *Templates for the solution of Algebraic Eigenvalue*