PASCAL GIORGI, Laboratoire LIP, ENSL, Lyon, France, and Waterloo
On the use of polynomial matrix approximant in the block Wiedemann algorithm

The resolution of a linear system is one of the most studied problems in linear algebra. It is well known that by using Gaussian elimination one can solve a linear system with a cubic time complexity. However, when the matrix is sparse (only a few elements are non-zero) or structured (Toeplitz, ...) the use of iterative methods such as Krylov/Lanczos allows better time and space complexity. Nevertheless, these methods are probabilistic and the chances of success rely on randomness properties of the computation domain. In order to achieve better probability of success one can use blocking technique. One of the main concern in the Wiedemann algorithm is to compute the minimal generating polynomial of matrix. When we switch to the block Wiedemann algorithm the main concern becomes the computation of a matrix minimal generating polynomial. The use of the block Wiedemann algorithm leads us to deal with matrix polynomial operations instead of scalar polynomial operations.

In order to provide fast computation in the block Wiedemann algorithm, we use some recent reduction to matrix multiplication in polynomial matrix computation. In particular, we rely on polynomial matrix approximant (Pade Approximant) through minimal basis computation in order to obtain the block minimal polynomial of a matrix. In practice, the minimal basis allows us to use matrix multiplication and so to benefit from implementation based on hybrid numerical/symbolic computation. We present our work on the reduction of minimal basis computation to matrix multiplication and we present an adaptation of our algorithm to handle the computation of block minimal polynomial. We also shows some performances obtained within the Linbox library (`http://www.linalg.org`) for the block Wiedemann algorithm using minimal basis computation.