Output-sensitive Modular Algorithms for Row Reduction of Matrices of Ore Polynomials

Howard Cheng[1] and George Labahn[2]

Abstract

We consider the problem of row reduction of a matrix of Ore polynomials with coefficients in $Z[t]$, computing both the transformation matrix and the transformed matrix. Such computations are useful for finding the rank and left nullspace of such matrices, computing GCRD and LCLM of Ore polynomials to name just a few applications.

As in any process that involves elimination operations there is a significant problem with intermediate expression swell with such computations. In our case we propose a new modular algorithm which is output sensitive, that is, the number of homomorphic images required depends on the size of the output. Furthermore, this output sensitivity does not come at the expense of any costly verification step using trial division or multiplication.

1: Department of Mathematics and Computer Science University of Lethbridge Lethbridge, Canada

2: Symbolic Computation Group School of Computer Science University of Waterloo Waterloo, Canada