Refined F_5 algorithms for ideals of minors of square matrices

Sriram Gopalakrishnan

February 24, 2023

Let $\Bbbk$ be a field with algebraic closure $\overline{\Bbbk}$, M be an $n \times n$ matrix of linear forms in the polynomial ring $\Bbbk[x_1, \ldots, x_k]$ and $r \leq n-1$ be a fixed integer. The MinRank problem asks to compute the set of points $a \in \overline{\Bbbk}^k$ such that the evaluation of M at a has rank at most r. This set is defined as the vanishing set in $\overline{\Bbbk}^k$ of all polynomials in the ideal $I_r(M)$ generated by the $(r+1)$-minors of M. The MinRank problem arises in areas related to computational algebra such as effective real algebraic geometry and more recently in cryptography in pursuit of quantum-safe cryptography schemes. The set of $(r+1)$-minors of M is not a regular sequence and the ideal $I_r(M)$ which it generates cannot be generated by a regular sequence. Thus, reductions to zero are encountered when running the F_5 algorithm to compute a grevlex Gröbner basis of $I_r(M)$, regardless of the generators chosen for $I_r(M)$. We consider the case when $I_r(M)$ has dimension zero.

We use known results about the first syzygy module of $I_r(M)$ to introduce a new F_5 criterion which predicts reductions to zero when computing a Gröbner basis for $I_r(M)$. In practice this criterion allows us to remove a significant number of reductions to zero, and in so doing speeds up the grevlex Gröbner basis computation. The sizes of the matrices generated in this altered F_5 algorithm indicate an improvement on the best-known complexity bound for Gröbner basis solutions to the MinRank problem.

In the case $r = n-2$, we exploit a known free resolution of $I_r(M)$ described by Gulliksen and Negård in order to obtain a Gröbner basis for the first syzygy module of $I_r(M)$. Subsequently, we refine our F_5 criterion using this knowledge to avoid all reductions to zero when computing a grevlex Gröbner basis for $I_{n-2}(M)$. We analyze the complexity of our new algorithm, and show that it indeed improves on current best-known complexity bounds for Gröbner basis solutions to the MinRank problem.

This is joint work with Vincent Neiger and Mohab Safey El Din.