Gröbner bases of determinantal ideals

Sriram Gopalakrishnan

March 13, 2026

Let $\mathbb{k}$ be a field and $A \in \mathbb{k}[x_1, \ldots, x_n]^{p\times q}$ be a $p \times q$ matrix of polynomials in n variables over $\mathbb{k}$. For $1 \leq r < \min\{p, q\}$, the ideal $\mathcal{I}_r(A)$ of $\mathbb{k}[x_1, \ldots, x_n]$ generated by the minors of A of order r is called a *determinantal ideal*. Such ideals arise naturally in a variety of contexts, including real algebraic geometry, optimization, and cryptography. The vanishing set of the ideal $\mathcal{I}_r(A)$ is precisely the set of points $\{x \in \overline{\mathbb{k}}^n : \mathrm{rank}(A(x)) < r\}$. When $\mathcal{I}_r(A)$ has dimension zero, one can extract the (finite) vanishing set of $\mathcal{I}_r(A)$ from a lexicographic Gröbner basis of $\mathcal{I}_r(A)$. One classical approach to computing such a Gröbner basis requires the computation of a Gröbner basis of $\mathcal{I}_r(A)$ with respect to the DRL order. When using a signature-based Gröbner basis algorithm such as F_5 to compute a DRL Gröbner basis of $\mathcal{I}_r(A)$, reductions to zero are encountered since $\mathcal{I}_r(A)$ cannot, in general, be generated by a regular sequence. We give refined versions of the F_5 Gröbner basis algorithm adapted to specific kinds of determinantal systems. First, when $p = q$, $r = p - 1$, and the entries of A are linear forms, we give an algorithm which generically encounters no reductions to zero, and we provide a complexity analysis in this case, establishing both an upper bound on the arithmetic complexity of our new algorithm and a lower bound on the number of polynomials in the output Gröbner basis. Secondly, when $p < q$ and $r = p$ (the maximal minor case), we provide an adapted algorithm which avoids a significant number of reductions to zero and apply this algorithm to computing the critical points of a polynomial restricted to an algebraic set.

Finally, we report on recent work on bounding the bit sizes of solutions to determinantal polynomial systems defined over $\mathbb{Q}$ using new constructions in arithmetic integral geometry.