Algorithms for computing with multivariate polynomials over rings

Ihsen Yengui

November 28, 2017

Abstract

In the first part of my talk, I will present an efficient algorithm for completing unimodular matrices over $\mathbb{C}[X_1^{\pm}, \ldots, X_k^{\pm}]$). Contrary to the existing algorithms, this algorithm does not convert the given Laurent polynomial vector to a "regular" polynomial vector, it eliminates all the variables at one time (contrary to the polynomial case), and does not use maximal ideals nor Noetherianity. Note that in concrete applications in systems theory (e.g., in signal processing and control theory), most of the arising polynomial matrices are actually multivariate Laurent polynomial matrices (partly due to the time-delay). For example, various signal processing problems can be understood in terms of multi-input multi-output MIMO systems which are characterized by their transfer matrices whose entries are in $\mathbb{C}[X_1^{\pm}, \ldots, X_k^{\pm}]$.

In the second part of my talk, I will focus on the computation of Gröbner bases on some (finite) rings with zero-divisors. Recently Gröbner bases techniques in multivariate polynomial rings over $\mathbb{Z}/m\mathbb{Z}$ and $(\mathbb{Z}/p^{\alpha}\mathbb{Z}) \times (\mathbb{Z}/p^{\alpha}\mathbb{Z})$ (in particular $\mathbb{Z}/2^{\alpha}\mathbb{Z}$ and $(\mathbb{Z}/2^{\alpha}\mathbb{Z}) \times (\mathbb{Z}/2^{\alpha}\mathbb{Z})$) have attracted some attention due to their potential applications in formal verification of data paths, and coding theory. We will give a new approach for the construction of Gröbner bases over valuation rings (i.e., rings, possibly with zero-divisors, in which every two elements are comparable under division). We will dynamically extend this Gröbner bases construction to arithmetical rings (rings which are locally valuation rings). We will illustrate our approach with some dynamical Gröbner bases compuations over $\mathbb{Z}/p^{\alpha}\mathbb{Z}$, $\mathbb{Z}/m\mathbb{Z}$, and $(\mathbb{Z}/p^{\alpha}\mathbb{Z}) \times (\mathbb{Z}/p^{\alpha}\mathbb{Z})$. Moreover, we will show that dynamical Gröbner bases over $\mathbb{F}_2[a, b]/\langle a^2 - a, b^2 - b\rangle$ (as a typical example of a Boolean ring) can be a satisfactory solution to an open problem pointed by Cai and Kapur.