Network Coding via Skew Polynomials

Felice Manganiello
Clemson University (USA)

manganm@clemson.edu

Abstract

In 2003 it was proven independently by Kötter and Mérdard, and Li *et al.* that linear network coding over a suitable finite field can be used to achieve the capacity of multicast networks. After this result, networks were connected to matroids. In 2007 Dougherty *et al.* showed how matroids can be deployed to construct matroidal networks. Gadouleau and Goupil in 2011 proved the achievability of the capacity of a multicast network by means of matroids instead of linear spaces. As a consequence of this result together with the fact that matroids can be percieved as a generalization of linear spaces, one can obtain an increase in the size of the codebooks used for communication.

The ring of skew polynomials is a non commutative generalization of the classic univariate polynomial ring. The multiplication of the former obeys a non commutative multiplication rule between the variable and a scalar defined by an automorphism of the underlined field and a derivation map. The ring maintains the structure of a right Euclidean ring without zero divisors. At this point, one obtains a natural evaluation map for skew polynomials as the remainder of the right division by a monomial.

It can be proven that the set of the zero locus of all of the skew polynomials using the aforementioned evaluation map, forms a matroid. Focusing on the case of skew polynomial rings over finite fields with trivial derivation map, it is possible to characterize the flats of this matroid and their sets of generators using minimal skew polynomials. We are going to explore this matroid structure and connect it to multicast communication.

This is a joint work with Siyu Liu and Frank R. Kschischang.

Keywords

Skew polynomial ring, Matroid, Multicast network communication