Quadratic-like permutations over $\mathbb{F}_2^n$

Irene Villa
University of Trento, Italy

30th Applications of Computer Algebra - ACA 2025

Among the so-called (Boolean) (n, m)-functions, $F : \mathbb{F}_2^n \to \mathbb{F}_2^m$, those that are balanced present a particular interest in discrete mathematics. Among balanced functions, those such that $m = n$, that is, (n, n)-permutations, are of a still more specific interest.

In this work, we study the class of permutations whose component functions all admit a derivative equal to constant function 1 (this property itself implies balancedness). We call these functions *quadratic-like permutations*, since all permutation of degree 2 have this property. We study this class of functions, showing that we can have quadratic-like permutations of degree greater than 2 and we can have permutations not quadratic-like. We analyse how the property behaves under some equivalence transformations, and we study the "reversed" property: every derivative in a nonzero direction has a component function equal to constant function 1. We study some known classes of permutations, such as Feistel permutations, crooked permutations and power permutations, and we show that many of them satisfy this property (and also the "reversed" one). We provide also some primary and secondary constructions of quadratic-like permutations.

This is a joint work with Claude Carlet.