Handling vectorial functions by means of their graph indicators

Claude Carlet,
University of Bergen, Norway; University of Paris 8, France.

E-mail: claude.carlet@gmail.com

The graphs of functions play an important role in coding theory: a code, linear or not, is called systematic if, up to a reordering of the codeword coordinates, it has the form of the graph $\mathcal{G}_F = \{(x, F(x));\ x \in \mathbb{F}_q^k\}$ of a function F from $\mathbb{F}_q^k$ to $\mathbb{F}_q^{n-k}$ for some k (equal to the dimension when the code is linear). All linear codes are systematic and most important nonlinear codes such as the Kerdock, Preparata and Delsarte-Goethals codes are systematic.

Graphs also play a significant role in symmetric cryptography, in the diffusion layers and substitution boxes of block ciphers. This role is essentially hidden in the latter case, but it is actual. For instance, the Walsh transform of a vectorial function F, which plays a central role in the determination of its nonlinearity, equals by definition the Fourier-Hadamard transform of the indicator (i.e. characteristic function) of its graph (that we call the graph indicator of the function). The CCZ equivalence of vectorial functions is also defined by means of their graphs. A notion of algebraic immunity of vectorial functions is directly related to graph indicators as well. The important notion of almost perfect nonlinearity is naturally defined by means of the graphs of functions. And graph indicators play roles in recent advances of cryptography, such as counter-measures against side channel attacks.

Moreover, looking at these graphs helps simplifying some studies on vectorial functions. For instance, the graph of a permutation and the graph of its compositional inverse are equal, up to variable swap; the indicators are then the same function up to this swap, while computing the expression of the compositional inverse of a permutation from that of the function is complex (there are only few known classes of permutation polynomials whose compositional inverses are also known).

We shall characterize the ANF and the univariate representation of any vectorial function as parts of the ANF and bivariate representation of the Boolean function equal to its graph indicator.

We shall show how this provides, when F is bijective, the expression of F^{-1} and/or allows deriving properties of F^{-1}. We shall illustrate this with an example and with a tight upper bound on the algebraic degree of F^{-1} by means

of that of F.

We shall characterize by the Fourier-Hadamard transform, by the ANF, and by the bivariate representation, that a given Boolean function is the graph indicator of a vectorial function.

We shall express the graph indicators of the sum, product, composition and concatenation of vectorial functions by means of the graph indicators of the functions.

We shall deduce from these results a characterization of the bijectivity of any (n, n)-function by the fact that some Boolean function, which appears as a part of the ANF (resp. the bivariate representation) of its graph indicator, is equal to constant function 1.

We have other results on this subject, but we will be able only to briefly mention them in a conclusion, for lack of time.