On constructing bent functions from cyclotomic mappings

Qiang Wang
Carleton University, Canada

30th Applications of Computer Algebra - ACA 2025

A Boolean function f in n variables with $f(0) = 0$ is bent if and only if the Cayley graph defined on $\mathbb{Z}_2^n$ by the support of a Boolean function is a strongly regular with parameters $(2^{2n}, 2^{2n-1} + \varepsilon 2^{n-1}, 2^{2n-2} + \varepsilon 2^{n-1}, 2^{2n-2} + \varepsilon 2^{n-1})$, $\varepsilon = \pm 1$. These bent functions are known as maximally nonlinear, which are as different as possible from the set of all linear and affine functions when measured by Hamming distance between truth tables. In this talk, we discuss some generic construction of Boolean bent functions from cyclotomic mappings. In particular, three generic constructions from this new perspective are obtained by considering Dillon functions, Niho functions and Kasami functions as different branch functions respectively. As a result, several infinite classes of bent functions belonging to the $\mathcal{PS}_{ap}$ class, class $\mathcal{H}$ and the completed $\mathcal{MM}$ class are derived, thereby providing simple representations of known classes of bent functions through cyclotomic mappings. Moreover, computer experiments show that examples of bent functions outside these three well-known classes can also be obtained by selecting other branch functions.