Bent functions, their properties, and related objects.

Wilfried Meidl, Radon Institute for Computational and Applied Mathematics, OEAW, Linz; Austria

The first part of the talk gives an overview on bent and vectorial bent functions which in the classical case, i.e. the Boolean case, can be seen as the functions with furthest distance to the set of linear and affine functions. Relations to cryptography, coding theory, and objects like almost perfect nonlinear functions (APN functions), difference sets and relative difference sets, projective planes, or semifields will be recalled.

In the second part, regularity of bent functions is discussed. Boolean bent functions are always *regular*, and they always come in pairs since their *duals* are also bent. This also applies to the classical constructions of bent functions in odd characteristic, but is not true in general. In the meantime one knows constructions of infinite classes of not regular bent functions. Lately, the first explicit construction of bent functions for which the dual is not bent (which are necessarily not regular bent functions) has been presented. The results indicate that being not regular and not having a bent dual are not extremal properties for a bent function, but perhaps even the typical behaviour of a bent function in odd characteristic.