Vectorial bent functions in odd characteristic and their components

Ayça Çeşmelioğlu^{*}, Wilfried Meidl^{**}, and Alexander Pott^{***}

^{*}İstanbul Bilgi University, Hacıahmet Mahallesi Pir Hüsamettin Sokak No:20, Beyoğlu, 34440 İstanbul, Turkey

**Johann Radon Institute for Computational and Applied Mathematics, Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria

***Otto von Guericke University, Faculty of Mathematics, 39106 Magdeburg, Germany

Let p be an odd prime and \mathbb{V}_n an n-dimensional vector space over \mathbb{F}_p . By a result of Kumar, Scholtz and Welsh 1986, for a bent function $f : \mathbb{V}_n \to \mathbb{F}_p$ the Walsh coefficient $\widehat{f}(b)$ at $b \in \mathbb{V}_n$ of f always satisfies

$$\widehat{f}(b) = \begin{cases} \pm \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 1 \mod 4; \\ \pm i \epsilon_p^{f^*(b)} p^{n/2} & : \quad p^n \equiv 3 \mod 4, \end{cases}$$
(1)

where f^* is a function from \mathbb{V}_n to \mathbb{F}_p , called the dual of f. A bent function $f : \mathbb{V}_n \to \mathbb{F}_p$ is called weakly regular if, for all $b \in \mathbb{V}_n$, we have $\widehat{f}(b) = \zeta \epsilon_p^{f^*(b)} p^{n/2}$ for some $\zeta \in \{\pm 1, \pm i\}$, cf. Equation (1). If $\zeta = 1$ we call f regular. If (the sign of) ζ changes with $b \in \mathbb{V}_n$, then f is called non-weakly regular bent. Weakly regular bent functions f belong to the class of dual-bent functions, for which the dual f^* is bent as well. A non-weakly regular bent function can be either dual-bent or non-dual-bent.

The classical examples of bent functions are all weakly regular. In particular all known infinite classes of bent monomials and binomials are weakly regular, the components of the vectorial Maiorana-McFarland and the vectorial spread bent functions are regular, and the components of all known planar functions are weakly regular (all of which besides from the Coulter-Matthews function are quadratic hence necessarily weakly regular). The first construction of non-weakly regular though dual bent functions is given in [1], recently the first construction of non-dual bent functions was presented in [2].

We first show that many infinite classes of p-ary bent monomials and binomials in the literature are actually vectorial constructions. In the second part we give a positive answer to the question if non-weakly regular bent functions can be components of a vectorial bent function. We present the first construction of vectorial bent functions of which the components are non-weakly regular but dual-bent, and the first construction of vectorial bent functions with non-dual bent components.

References

- A. Çeşmelioğlu, G. McGuire, W. Meidl, A construction of weakly and non-weakly regular bent functions, J. Comb. Theory, Series A 119 (2012), 420–429.
- [2] A. Çeşmelioğlu, W. Meidl, A. Pott, There are infinitely many bent functions for which the dual is not bent. IEEE Trans. Inform. Theory 62 (2016), 5204–5208.