

# Construction of Bent Functions via Niho Power Functions

Hans Dobbertin<sup>1</sup>, Gregor Leander<sup>1</sup>, Anne Canteaut<sup>2</sup>,  
Claude Carlet<sup>2</sup>, Patrick Felke<sup>1</sup>, Philippe Gaborit<sup>3</sup>

<sup>1</sup>Department of Mathematics, Ruhr-University Bochum, D-44780 Bochum, Germany

<sup>2</sup>INRIA-Project CODES, BP 105, 78153 Le Chesnay Cedex, France

<sup>3</sup>Equipe Arithmétique Codage et Cryptographie, Université de Limoges, France

9th June 2004

## Abstract

A Boolean function with an even number  $n = 2k$  of variables is called bent if it is maximally nonlinear. Bent functions were introduced by Rothaus in 1976. Because of their own sake as interesting combinatorial objects, but also because of their relations to coding theory (Reed-Muller codes) and applications in cryptography (design of stream ciphers), they have attracted a lot of research, specially in the last ten years. We present here a new construction of bent functions. Boolean functions of the form  $f(x) = \text{tr}(\alpha_1 x^{d_1} + \alpha_2 x^{d_2})$ ,  $\alpha_1, \alpha_2, x \in \mathbb{F}_{2^n}$ , are considered, where the exponents  $d_i$  ( $i = 1, 2$ ) are of Niho type, i.e. the restriction of  $x^{d_i}$  on  $\mathbb{F}_{2^k}$  is linear. We prove for  $d_1 = 2^k + 1$  and  $d_2 = 3 \cdot 2^{k-1} - 1$ ,  $d_2 = 2^k + 3$  if  $k$  is odd,  $d_2 = (2^k + 5)/3$  if  $k$  is even, resp., that  $f$  is a bent function if  $\alpha_1 + \overline{\alpha_1} = 1$  and  $\alpha_2 = 1$ .

The starting point of our proofs confirming the bent property is based on a classical theorem of Niho [2] and new methods to handle Walsh transforms of Niho power functions from [1].

## References

- [1] H. Dobbertin, P. Felke, T. Hellesest and P. Rosendahl, *Niho type cross-correlation functions via Dickson polynomials and Kloosterman sums*, IEEE Transactions on Information Theory, submitted.
- [2] Y. Niho, Multivalued cross-correlation functions between two maximal linear recursive sequences, Ph.D. Thesis, University of Southern California (1972).