LeBel, Alain; **Horadam, K. J.**

Direct sums of balanced functions, perfect nonlinear functions, and orthogonal cocycles. (English) Zbl 1136.94006

J. Comb. Des. 16, No. 3, 173-181 (2008).

Summary: Determining if a direct sum of functions inherits nonlinearity properties from its direct summands is a subtle problem. Here, we correct a statement by *K. Nyberg* [Lect. Notes Comput. Sci. 547, 378–386 (1991; Zbl 0766.94012)] on inheritance of balance and we use a connection between balanced derivatives and orthogonal cocycles to generalize Nyberg's result to orthogonal cocycles. We obtain a new search criterion for PN functions and orthogonal cocycles mapping to non-cyclic abelian groups and use it to find all the orthogonal cocycles over $\mathbb{Z}_2^t$, $2 \leq t \leq 4$. We conjecture that any orthogonal cocycle over $\mathbb{Z}_2^t, t \geq 2$, must be multiplicative.

MSC:

94A60 Cryptography
94A55 Shift register sequences and sequences over finite alphabets in information and communication theory
20J06 Cohomology of groups

Keywords:

perfect nonlinear function; balanced function; orthogonal cocycle; relative difference set; generalized Hadamard matrix; exponential sum

Full Text: DOI

References:

[1] Blokhuis, Proc Amer Math Soc 130 pp 1473– (2002)
[2] Bosma, J Symbol Comp 24 pp 235– (1997)
[3] Carlet, J Complexity 20 pp 205– (2004)
[4] Coulter, Codes Cryptogr 10 pp 167– (1997)
[5] Horadam, J Combin Des 8 pp 330– (2000)
[6] Horadam, Proc 2006 ISIT, IEEE pp 1080– (2006)
[7] Shift actions on 2-cocycles, Ph.D. Thesis, RMIT University, Melbourne, Australia, 2005.
[8] Leung, J Algebra 224 pp 427– (2000)
[9] MacDonald, Israel J Math 40 pp 350– (1981)
[10] Perfect nonlinear S-boxes, In: EUROCRYPT-91, LNCS 547, Springer, New York, 1991, pp. 378–385.
[11] Perera, Codes Cryptogr 15 pp 187– (1998)