Xu, Bangteng

Bentness and nonlinearity of functions on finite groups. (English) Zbl 1359.11092

Des. Codes Cryptography 76, No. 3, 409-430 (2015).

Summary: Perfect nonlinear functions between two finite abelian groups were studied by *C. Carlet* and *C. Ding* [J. Complexity 20, No. 2–3, 205–244 (2004; Zbl 1053.94011)] and *A. Pott* [Discrete Appl. Math. 138, No. 1–2, 177–193 (2004; Zbl 1035.05023)], which can be regarded as a generalization of bent functions on finite abelian groups studied by *O. A. Logachev* et al. [Discrete Math. Appl. 7, 547–564 (1997; Zbl 0982.94012)]. *L. Poinsot* [Multidimensional bent functions. GESTS Int. Trans. Comput. Sci. Eng. 18, No. 1, 185–195 (2005); J. Discrete Math. Sci. Cryptography 9, No. 2, 349–364 (2006; Zbl 1105.43002), Cryptogr. Commun. 4, No. 1, 1–23 (2012; Zbl 1282.11165)] extended this research to arbitrary finite groups, and characterized bent functions on finite nonabelian groups as well as perfect nonlinear functions between two arbitrary finite groups by the Fourier transforms of the related functions at irreducible unitary representations. The purpose of this paper is to study the characterizations of the bentness (perfect nonlinearity) of functions on arbitrary finite groups by the Fourier transforms of the related functions at irreducible characters. We will also give a characterization of a perfect nonlinear function by the relative pseudo-difference family.

MSC:

11T71	Algebraic coding theory; cryptography (number-theoretic aspects)
20C99	Representation theory of groups
43A30	Fourier and Fourier-Stieltjes transforms on nonabelian groups and on semigroups, etc.
94A55	Shift register sequences and sequences over finite alphabets in information and communication theory

Keywords:

bent functions; perfect nonlinear functions; Fourier transforms; class functions; representations; characters

Full Text: DOI

References:

[1] Carlet C., Ding C.: Highly nonlinear mappings. J. Complex. \textbf{20}, 205-244 (2004). · Zbl 1053.94011

[2] Diaconis P., Rockmore D.: Efficient computation of the Fourier transform on finite groups. J. Am. Math. Soc. \textbf{3}, 297-332 (1990). · Zbl 0709.65125

[3] Huppert B.: Character Theory of Finite Groups. Walter de Gruyter \& Co., Berlin (1998). · Zbl 0932.20007

[4] Isaacs M.: Character Theory of Finite Groups. Pure and Applied Mathematics, vol. 69. Academic Press, New York (1976). · Zbl 0337.20005

[5] Logachev O.A., Salnikov A.A., Yashchenko V.V.: Bent functions on a finite abelian group. Discret. Math. Appl. \textbf{7}, 547-564 (1997). · Zbl 0982.94012

[6] Nagao H., Tsushima Y.: Representations of Finite Groups. Academic Press, Boston (1989). · Zbl 0673.20002

[7] Pott A.: Nonlinear functions in abelian groups and relative difference sets. Optimal discrete structures and algorithms (ODSA 2000). Discret. Appl. Math. \textbf{138}, 177-193 (2004). · Zbl 1035.05023

[8] Poinsot L.: Multidimensional bent functions. GESTS Int. Trans. Comput. Sci. Eng. \textbf{18}, 185-195 (2005).

[9] Poinsot L.: Bent functions on a finite nonabelian group. J. Discret. Math. Sci. Cryptogr. \textbf{9}, 349-364 (2006). · Zbl 1105.43002

[10] Poinsot L.: Non abelian bent functions. Cryptogr. Commun. \textbf{4}, 1-23 (2012). · Zbl 1282.11165

[11] Poinsot L., Pott A.: Non-Boolean almost perfect nonlinear functions on non-abelian groups. Int. J. Found. Comput. Sci. \textbf{22}, 1351-1367 (2011). · Zbl 1236.94064

[12] Rothaus O.S.: On bent functions. J. Comb. Theory Ser. A \textbf{20}, 300-305 (1976). · Zbl 0336.12012

[13] Tokareva N.: Generalizations of bent functions: a survey of publications. J. Appl. Ind. Math. \textbf{5}, 110-129 (2011).

[14] Xu B.: Multidimensional Fourier transforms and nonlinear functions on finite groups. Linear Algebra Appl. \textbf{452}, 89-105 (2014). · Zbl 1294.11216