Xu, Bangteng

Multidimensional Fourier transforms and nonlinear functions on finite groups. (English)

Zbl 1294.11216
Linear Algebra Appl. 452, 89-105 (2014).

Summary: In this paper we study characterizations of perfect nonlinear functions between arbitrary finite groups. We need to introduce multidimensional Fourier transforms and multidimensional bent functions on arbitrary finite groups, and discuss their properties. Then by using multidimensional bent functions, we obtain a characterization of a perfect nonlinear function between two arbitrary finite groups, and improve the results of *L. Poinsot* [Cryptogr. Commun. 4, No. 1, 1–23 (2012; Zbl 1282.11165)]. Our main result is the characterization of a perfect nonlinear function by the related difference family. As a direct consequence, a perfect nonlinear function determines a partitioned 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.

Cited in **5** Documents

Keywords:

multidimensional Fourier transforms; multidimensional bent functions; perfect nonlinear functions; related difference family

Full Text: DOI

References:

[1] Carlet, C.; Ding, C., Highly nonlinear mappings, J. Complexity, 20, 205-244, (2004) · Zbl 1053.94011

[2] Huppert, B., Character theory of finite groups, (1998), Walter de Gruyter \& Co. Berlin · Zbl 0932.20007

[3] Isaacs, M., Character theory of finite groups, Pure Appl. Math., vol. 69, (1976), Academic Press Inc. New York-London · Zbl 0337.20005

[4] Logachev, O. A.; Salnikov, A. A.; Yashchenko, V. V., Bent functions on a finite abelian group, Discrete Math. Appl., 7, 547-564, (1997) · Zbl 0982.94012

[5] Nagao, H.; Tsushima, Y., Representations of finite groups, (1989), Academic Press, Inc. Boston, MA

[6] Pott, A., Nonlinear functions in abelian groups and relative difference sets, Optimal Discrete Structures and Algorithms, ODSA 2000, Discrete Appl. Math., 138, 177-193, (2004) · Zbl 1035.05023

[7] Poinsot, L., Non-abelian bent functions, Cryptogr. Commun., 4, 1-23, (2012) · Zbl 1282.11165

[8] Poinsot, L., Bent functions on a finite nonabelian group, J. Discrete Math. Sci. Cryptogr., 9, 349-364, (2006) · Zbl 1105.43002

[9] Poinsot, L., Multidimensional bent functions, GESTS Int. Trans. Comput. Sci. Eng., 18, 185-195, (2005)

[10] Poinsot, L.; Pott, A., Non-Boolean almost perfect nonlinear functions on non-abelian groups, Internat. J. Found. Comput. Sci., 22, 1351-1367, (2011) · Zbl 1236.94064

[11] Rothaus, O. S., On bent functions, J. Combin. Theory Ser. A, 20, 300-305, (1976) · Zbl 0336.12012

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

[13] Xu, B., Bentless and nonlinearity of functions on finite groups, Des. Codes Cryptogr., (2014)