Fan, Yun; **Xu, Bangteng**

Nonlinear functions and difference sets on group actions. (English) Zbl 1371.05036

Des. Codes Cryptography 85, No. 2, 319-341 (2017).

Summary: There are many generalizations of the classical Boolean bent functions. Let G, H be finite groups and let X be a finite G-set. G-perfect nonlinear functions from X to H have been studied in several papers. They are generalizations of perfect nonlinear functions from G itself to H. By introducing the concept of a (G, H)-related difference family of X, we obtain a characterization of G-perfect nonlinear functions on X in terms of a (G, H)-related difference family. When G is abelian, we prove that there is a normalized G-dual set $\widehat{X}$ of X, and characterize a G-difference set of X by the Fourier transform on a normalized G-dual set $\widehat{X}$. We will also investigate the existence and constructions of G-perfect nonlinear functions and G-bent functions. Several known results are direct consequences of our results.

MSC:

05B10 Combinatorial aspects of difference sets (number-theoretic, group-theoretic, etc.)
05E18 Group actions on combinatorial structures
65T50 Numerical methods for discrete and fast Fourier transforms

Cited in **1** Document

Keywords:

G-perfect nonlinear functions; G-difference sets; (G, H)-related difference families; normalized G-dual sets; Fourier transforms

Full Text: DOI arXiv

References:

[1] Alperin J.L., Bell R.B.: Groups and Representations, GTM 162. Springer, New York (1997).

[2] Arasu, KT; Ding, C; Helleseth, T; Kumar, PV; Martinsen, H, Almost difference sets and their sequences with optimal autocorrelations, IEEE Trans. Inf. Theory, 47, 2934-2943, (2001) · Zbl 1008.05027

[3] Beth T., Jungnickel D., Lenz H.: Design Theory, 2nd edn. Cambridge University Press, Cambridge (1999). · Zbl 0945.05005

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

[5] Chung, H; Kumar, PV, A new general construction of generalized bent functions, IEEE Trans. Inf. Theory, 35, 206-209, (1989) · Zbl 0677.05015

[6] Davis, JA; Poinsot, L, G-perfect nonlinear functions, Des. Codes Cryptogr., 46, 83-96, (2008) · Zbl 1179.94060

[7] Dillon J.F.: Elementary Hadamard difference sets. Ph.D. thesis, University of Maryland, College Park (1974). · Zbl 0346.05003

[8] Fan Y., Xu B.: Fourier transforms and bent functions on faithful actions of finite abelian groups. Des. Codes Cryptogr. (2016). doi:10.1007/s10623-016-0177-8. · Zbl 1358.43004

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

[10] Kumar, PV; Scholtz, RA; Welch, LR, Generalized bent functions and their properties, J. Comb. Theory Ser. A, 40, 90-107, (1985) · Zbl 0585.94016

[11] Lai X., Massey J.L.: A proposal for a new block encryption standard. In: Advances in Cryptology-Eurocrypt'90. Lecture Notes in Computer Science, vol. 473, pp. 389-404. Springer, New York (1991). · Zbl 0764.94017

[12] Logachev, OA; Salnikov, AA; Yashchenko, VV, Bent functions over a finite abelian group, Discret. Math. Appl., 7, 547-564, (1997) · Zbl 0982.94012

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

[14] Poinsot, L, A new characterization of group action-based perfect nonlinearity, Discret. Appl. Math., 157, 1848-1857, (2009) · Zbl 1166.94007

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

[16] Poinsot, L; Harari, S, Group actions based perfect nonlinearity, GESTS Int. Trans. Comput. Sci. Eng., 12, 1-14, (2005)

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

[18] Pott, A, Nonlinear functions in abelian groups and relative diference sets. optimal discrete structures and algorithms, ODSA 2000, Discret. Appl. Math., 138, 177-193, (2004) · Zbl 1035.05023

[19] Rothaus, OS, On bent functions, J. Comb. Theory Ser. A, 20, 300-305, (1976) · Zbl 0336.12012

[20] Serre J.-P.: Representations of Finite Groups, GTM. Springer, New York (1984).

[21] Shorin V.V., Jelezniakov V.V., Gabidulin E.M.: Linear and differential cryptanalysis of Russian GOST. In: Augot D., Carlet C. (eds.) Workshop on Coding and Cryptography, pp. 467-476 (2001). · Zbl 0985.94035

[22] Solodovnikov, VI, Bent functions from a finite abelian group to a finite abelian group, Diskret. Mat., 14, 99-113, (2002) · Zbl 1047.94011

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

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

[25] Xu, B, Bentness and nonlinearity of functions on finite groups, Des. Codes Cryptogr., 76, 409-430, (2015) · Zbl 1359.11092

[26] Xu, B, Dual bent functions on finite groups and C-algebras, J. Pure Appl. Algebra, 220, 1055-1073, (2016) · Zbl 1327.43004