Fan, Yun; **Xu, Bangteng**

Fourier transforms and bent functions on finite groups. (English) Zbl 1393.43003

Des. Codes Cryptography 86, No. 9, 2091-2113 (2018).

The authors introduce a dual basis on a finite nonabelian group, determined by its unitary irreducible representations. Furthermore they define the Fourier transform on such a basis, and obtain characterizations of bent, dual and perfect nonlinear functions by their Fourier transforms.

Reviewer: George Stoica (Saint John)

MSC:

43A30 Fourier and Fourier-Stieltjes transforms on nonabelian groups and on semigroups, etc.
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
20C15 Ordinary representations and characters

Keywords:

Fourier transforms; bent functions; perfect nonlinear functions; dual basis; dual functions

Full Text: DOI

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. Inform. 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. Inform. Theory, 35, 206-209, (1989) · Zbl 0677.05015

[6] Dillon J.F.: Elementary Hadamard Difference Sets. Ph.D. Thesis, University of Maryland (1974). · Zbl 0346.05003

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

[8] Fan, Y; Xu, B, Fourier transforms and bent functions on faithful actions of finite abelian groups, Des. Codes Cryptogr., 82, 543-558, (2017) · Zbl 1358.43004

[9] Fan, Y; Xu, B, Nonlinear functions and difference sets on group actions, Des. Codes Cryptogr., 85, 319-341, (2017) · Zbl 1371.05036

[10] Galati, JC; LeBel, AC, Relative difference sets in semidirect products with an amalgamated subgroup, J. Comb. Des., 13, 211-221, (2005) · Zbl 1067.05013

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

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

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

[14] 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 (1991). · Zbl 0764.94017

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

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

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

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

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

[20] 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

[21] Pott, A, Nonlinear functions in abelian groups and relative difference sets, in: optimal discrete structures and algorithms,

ODSA 2000, Discret. Appl. Math., 138, 177-193, (2004) · Zbl 1035.05023

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

[23] 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

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

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

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

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

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