

Fan, Yun; Xu, Bangteng

Fourier transforms and bent functions on faithful actions of finite abelian groups. (English)

Zbl 1358.43004

Des. Codes Cryptography 82, No. 3, 543-558 (2017).

Let G be a finite abelian group acting faithfully on a finite set X . The authors are concerned with the Fourier analysis on X , as a generalization of the classical Fourier analysis on G . The former is used to study the bentness and perfect nonlinearity of functions on X by their own Fourier transforms on the G -dual set of X . Illustrative examples complete the study.

Reviewer: George Stoica (Saint John)

MSC:

- 43A25 Fourier and Fourier-Stieltjes transforms on locally compact and other abelian groups Cited in 2 Documents
11T71 Algebraic coding theory; cryptography (number-theoretic aspects)
20C99 Representation theory of groups

Keywords:

group actions; G -linear functions; G -dual sets; Fourier transforms on G -sets; bent functions; perfect nonlinear functions

Full Text: DOI

References:

- [1] Alperin J.L., Bell R.B.: Groups and Representations, GTM 162. Springer, New York (1997).
- [2] Carlet C., Ding C.: Highly nonlinear mappings. J. Complex. $\text{\textbf{20}}$, 205-244 (2004). · Zbl 1053.94011
- [3] Dillon J.F.: Elementary Hadamard difference sets, Ph.D. Thesis, University of Maryland (1974). · Zbl 0346.05003
- [4] Logachev O.A., Salnikov A.A., Yashchenko V.V.: Bent functions over a finite abelian group. Discret. Math. Appl. $\text{\textbf{7}}$, 547-564 (1997). · Zbl 0982.94012
- [5] Poinsoot L.: Bent functions on a finite nonabelian group. J. Discret. Math. Sci. Cryptogr. $\text{\textbf{9}}$, 349-364 (2006). · Zbl 1105.43002
- [6] Poinsoot L.: A new characterization of group action-based perfect nonlinearity. Discret. Appl. Math. $\text{\textbf{157}}$, 1848-1857 (2009). · Zbl 1166.94007
- [7] Poinsoot L., Harari S.: Group actions based perfect nonlinearity. GESTS Int. Trans. Comput. Sci. Eng. $\text{\textbf{12}}$, 1-14 (2005).
- [8] Poinsoot L., Pott A.: Non-boolean almost perfect nonlinear functions on non-abelian groups. Int. J. Found. Comput. Sci. $\text{\textbf{22}}$, 1351-1367 (2011). · Zbl 1236.94064
- [9] Pott A.: Nonlinear functions in abelian groups and relative difference sets. In: Optimal Discrete Structures and Algorithms, ODSA 2000. Discret. Appl. Math. $\text{\textbf{138}}$, 177-193 (2004). · Zbl 1035.05023
- [10] Rothaus O.S.: On bent functions. J. Comb. Theory A $\text{\textbf{20}}$, 300-305 (1976). · Zbl 0336.12012
- [11] Serre J.-P.: Representations of Finite Groups. Springer, New York (1984).
- [12] Solodovnikov V.I.: Bent functions from a finite abelian group to a finite abelian group. Diskret. Mat. $\text{\textbf{14}}$, 99-113 (2002). · Zbl 1047.94011
- [13] Xu B.: Multidimensional Fourier transforms and nonlinear functions on finite groups. Linear Algebra Appl. $\text{\textbf{450}}$, 89-105 (2014). · Zbl 1294.11216
- [14] Xu B.: Dual bent functions on finite groups and \mathbb{S} -algebras. J. Pure Appl. Algebra $\text{\textbf{220}}$, 1055-1073 (2016). · Zbl 1327.43004
- [15] Xu B.: Bentness and nonlinearity of functions on finite groups. Des. Codes Cryptogr. $\text{\textbf{76}}$, 409-430 (2015). · Zbl 1359.11092

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.