Finite Fields and Their Applications 53 (2018) 226–253

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# Componentwise APNness, Walsh uniformity of APN functions, and cyclic-additive difference sets

Claude Carlet [a,b,*]

[a] *LAGA, University of Paris 8, Saint–Denis cedex 02, France*
[b] *University of Bergen, Norway*

ARTICLE INFO

*Article history:*
Received 2 June 2017
Received in revised form 5 April 2018
Accepted 21 June 2018
Available online 9 July 2018
Communicated by Pascale Charpin

*MSC:*
06E30
11T71
94A60

*Keywords:*
Boolean function
Vectorial function
Walsh–Hadamard transform
APN function
Kasami function
Cyclic difference set

ABSTRACT

In [Characterizations of the differential uniformity of vectorial functions by the Walsh transform, IEEE Transactions on Information Theory 2017], the author has characterized differentially $\delta$-uniform functions by equalities satisfied by their Walsh transforms. This generalizes the characterization of APN functions by the fourth moment of the Walsh transform. We study two notions which are related: (1) the componentwise APNness (CAPNness) of $(n,n)$-functions, which is a stronger version of APNness, related to the characterization by the fourth moment, in which the arithmetic mean of $W_F^4(u,v)$ when $u$ ranges over $\mathbb{F}_2^n$ and $v$ is fixed nonzero in $\mathbb{F}_2^n$ equals $2^{2n+1}$ (2) the componentwise Walsh uniformity (CWU) of $(n,m)$-functions ($m=n$, resp. $m=n-1$), which is a stronger version of APNness (resp. of differential 4-uniformity) related to one of the new characterizations, in which the arithmetic mean of $W_F^2(u_1,v_1)W_F^2(u_2,v_2)W_F^2(u_1+u_2,v_1+v_2)$ when $u_1,u_2$ range independently over $\mathbb{F}_2^n$ and $v_1,v_2$ are fixed nonzero and distinct in $\mathbb{F}_2^m$, equals $2^{3n}$. Concerning the first notion, it is known from Berger, Canteaut, Charpin and Laigle-Chapuy that any plateaued function is CAPN if and only if it is AB and that APN power permutations are CAPN. We prove that CAPN functions can exist only if $n$ is odd; this solves an eleven year old open problem by these authors. Concerning the second notion, we show that any crooked function (and in particular any quadratic APN function) is CWU, but we observe also that other APN functions like Kasami

* Correspondence to: LAGA, University of Paris 8, Saint-Denis cedex 02, France.
*E-mail address:* claude.carlet@univ-paris8.fr.

https://doi.org/10.1016/j.ffa.2018.06.007
1071-5797/© 2018 Elsevier Inc. All rights reserved.

functions and the inverse of one of the Gold APN permutations are CWU for $n \leq 11$. We show that the CWUness of APN power permutations is equivalent to a property of $\Delta_F = \{F(x)+F(x+1)+1; x \in \mathbb{F}_{2^n}\}$. This new property, that we call cyclic-additive difference set property, is more complex than the cyclic difference set property (proved in the case of Kasami APN functions by Dillon and Dobbertin). We prove it in the case of the inverse of Gold function. In the case of Kasami functions, we observe that the cyclic-additive property is also true for $n \leq 10$ even and we leave the proof of the CWUness and the cyclic-additive property as open problems.
© 2018 Elsevier Inc. All rights reserved.

## 1. Introduction

Almost perfect nonlinear (APN) functions are those $(n,n)$-functions from the vector space $\mathbb{F}_2^n$ to itself (which can be identified with the field $\mathbb{F}_{2^n}$ since this field is an $n$-dimensional vector space over $\mathbb{F}_2$; this allows to define power functions $F(x) = x^d$), which contribute to an optimal resistance against the differential cryptanalyses of those block ciphers involving them as substitution boxes [19]. The differential uniformity of a vectorial function $F : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is the number $\delta_F = \max_{a\in\mathbb{F}_2^n, b\in\mathbb{F}_2^m, a\neq 0} |\{x \in \mathbb{F}_2^n; F(x) + F(x + a) = b\}|$. Function $F$ is then called a differentially $\delta_F$-uniform function. The best (minimal) value of $\delta_F$ when $m = n$ is 2. The function is then APN. A subclass of APN functions for $n$ odd is that of almost bent (AB) $(n,n)$-functions, whose Walsh transform:

$$W_F(u,v) = \sum_{x\in\mathbb{F}_2^n} (-1)^{v\cdot F(x)+u\cdot x}$$

(some inner product denoted by "$\cdot$" being chosen in $\mathbb{F}_2^n$) takes values 0 and $\pm 2^{\frac{n+1}{2}}$ only. Equivalently, AB functions are those $(n,n)$-functions whose component functions $v \cdot F$, $v \neq 0$, all lie at optimal Hamming distance $2^{n-1} - 2^{\frac{n-1}{2}}$ from the set of affine functions [12]. Any quadratic APN function in odd dimension $n$ is AB (quadratic meaning that the algebraic normal form of the function has degree at most 2, and then here exactly 2). Surveys on APN and AB functions can be found in [2,4,7]. All known infinite classes of APN functions are given by expressions in the field $\mathbb{F}_{2^n}$ (of course, for each $n$, an algebraic normal form, that is, an expression in the vector space $\mathbb{F}_2^n$ can be deduced, but this cannot be done globally for all $n$ or for an infinity of them). The inner product in this field can be taken equal to $u \cdot x = tr_1^n(ux)$, where $tr_1^n$ is the absolute trace function $tr_1^n(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}$.

In [9], the author has characterized differentially $\delta$-uniform $(n,m)$-functions by equalities involving the values of their Walsh transform (defined similarly as above, some inner products, both denoted by "$\cdot$", being chosen in $\mathbb{F}_2^n$ and $\mathbb{F}_2^m$). For $\delta = 2$, this characteriza-

Download English Version:

https://daneshyari.com/en/article/8895607

Download Persian Version:

https://daneshyari.com/article/8895607

Daneshyari.com