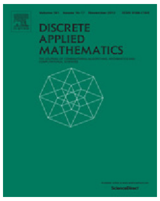
Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam



Infinite classes of vectorial plateaued functions, permutations and complete permutations

E. Pasalic [a,b,*], N. Cepak [a], Y. Wei [c,d]

[a] *University of Primorska, FAMNIT, Koper, Slovenia*
[b] *University of Primorska, IAM, Koper, Slovenia*
[c] *Guangxi Key Laboratory of Cryptography and Information Security, Guilin University of Electronic Technology, Guilin, P.R. China*
[d] *Guangxi Cooperative Innovation Center of Cloud Computing and Big Data, Guilin University of Electronic Technology, P.R. China*

ARTICLE INFO

Article history:
Received 5 February 2016
Received in revised form 22 June 2016
Accepted 24 June 2016
Available online xxxx

Keywords:
Maiorana–McFarland class
Boolean functions
Plateaued functions
Permutations
Complete mappings

ABSTRACT

We use the well-known Maiorana–McFarland class to construct several important combinatorial structures. In the first place, we easily identify infinite classes of vectorial plateaued functions $\{F\} : \mathbb{F}_2^n \to \mathbb{F}_2^n$ such that all non-zero linear combinations of its component functions are also plateaued. More importantly, by setting certain restrictions on the component functions, the same approach also yields many infinite classes of permutations for any $n \geq 6$. Finally, we deduce some infinite classes of complete permutations, as a subclass of these permutations. Most notably, all these classes are of variable and controllable degree, the property being intrinsic to the construction method. The construction method is highly tweakable giving rise to many variations that again provide us with infinite classes of these structures.

1. Introduction

Boolean plateaued functions and vectorial functions with plateaued components have a significant impact in many applications such as cryptography, sequences for communications, and related combinatorics and designs. Boolean plateaued functions were introduced in [11] as a class of functions characterized by the property of having at most three values in its Walsh spectra. In particular, when n is odd the functions whose spectra belong to $\{0, \pm 2^{\frac{n+1}{2}}\}$ are known as semi-bent functions and they play a significant role in certain cryptographic primitives and additionally these functions constitute the component functions of certain mappings such as almost perfect nonlinear (APN) mappings with Gold exponent. Nevertheless, while there are a few known generic constructions of Boolean plateaued functions (a nice survey can be found in [2]) little is known about vectorial plateaued functions. In [2], several characterizations of those vectorial functions whose components are all plateaued (with possibly different amplitudes) were derived. In particular, it was shown that an extension of the Maiorana–McFarland class gives rise to a vectorial plateaued functions $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$. Namely, using a permutation π over $\mathbb{F}_{2^m}$ and two arbitrary functions $\phi, \psi : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ it could be shown that $F : \mathbb{F}_{2^m} \times \mathbb{F}_{2^m}$ defined by $F(x, y) = (x\pi(y) + \phi(y), x\pi^{2^i}(y) + \psi(y))$ is plateaued.

Even though the above approach gives an infinite class of vectorial plateaued functions the component functions of F are bent and therefore they are not balanced. As a consequence this approach can never give rise to permutations due to the

[*] Corresponding author. Fax: +386 5 611 75 71.
E-mail addresses: enes.pasalic6@gmail.com (E. Pasalic), nastja.cepak@gmail.com (N. Cepak), walker_wei@msn.com (Y. Wei).

http://dx.doi.org/10.1016/j.dam.2016.06.022
0166-218X/© 2016 Published by Elsevier B.V.

Please cite this article in press as: E. Pasalic, et al., Infinite classes of vectorial plateaued functions, permutations and complete permutations, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.06.022

property of permutations that all linear combinations of its component functions are balanced Boolean functions. Therefore, we consider an alternative design method of vectorial plateaued functions which specifies the component functions of F in such a way so that all linear combinations of them are balanced Boolean functions, thus implying that F is a permutation. This way two infinite classes of non-quadratic permutations are proposed but there are many variations of the proposed method which may give many more infinite classes. The framework is also extendible in terms of getting varying degree of these permutations since it is based on a suitable separation of the variable space. More precisely, the component functions can be seen as a concatenation of linear functions from some fixed variable space whose size can be adjusted to accommodate the design of permutations of even higher degree. The polynomial form, as a univariate representation over the corresponding finite field, appears to be complicated and it is retrieved using Lagrange interpolation. On the other hand, the algebraic normal form (ANF) description of the component functions is usually simple.

Complete mappings are a particular class of permutations characterized by the property that both $F(x)$ and $F(x)+x$ are permutation polynomials over some finite field $\mathbb{F}_{2^n}$. Complete mappings have got attention in several works [8,6,10,5] and it appears to be a topic of current research interest as well, see [1,9] and the references therein. In particular, for the well-known Even–Mansour block cipher that uses a public n-bit permutation $F(x)$ and two n-bit secret keys k_1, k_2, and encrypts an n-bit plaintext x by computing $F(x+k_1)+k_2$, it was demonstrated that this cipher usually suffered from the attacks that rely on the non-uniform behavior of $F(x)+x$. In order to resist these attacks, the distribution of $F(x)+x$ should be uniform, i.e., $F(x)+x$ should also be a permutation (see the work of [5]).

Due to the additional requirement that $F(x)+x$ is a permutation as well, the design of component functions of F is certainly more complicated. However, we demonstrate that even complete permutations can be generated using the same framework as in the case of ordinary permutations. We exhibit one infinite class of complete permutations but nevertheless the same method may give many more (affinely non-equivalent) classes, though we do not pursue this issue further. The polynomial form of this class of permutations is again retrieved through Lagrange interpolation and it is very complex though the ANF of the component functions is somewhat simple.

The rest of this article is organized as follows. Section 2 provides some basic definitions and notions used throughout this manuscript. The design methods of constructing permutations whose component functions (and their linear combinations) are plateaued is given in Section 3. In Section 4, a generic method for constructing complete mappings is presented. The differential properties and the existence of linear functions (for some linear combinations of the component functions) are addressed in Section 5. Some concluding remarks are found in Section 6.

2. Preliminaries

The Galois field of order 2^n will be denoted by $\mathbb{F}_{2^n}$ and the corresponding vector space by $\mathbb{F}_2^n$. An n-variable Boolean function $f(x_1,\ldots,x_n)$ can be considered to be a multivariate polynomial over $\mathbb{F}_2$. This polynomial can be expressed as a sum of distinct kth order products $(0\le k\le n)$ of the variables. More precisely, $f(x_1,\ldots,x_n)$ can be written as

$$f(x_1,\ldots,x_n)=\bigoplus_{u\in\mathbb{F}_2^n}\lambda_u\left(\prod_{i=1}^{n}x_i^{u_i}\right), \tag{1}$$

for $\lambda_u\in\mathbb{F}_2$, $u=(u_1,\ldots,u_n)$.

This representation of f is called the *algebraic normal form* (ANF) of f. The *algebraic degree* of f, denoted by $\deg(f)$, is the maximal value of the Hamming weight of u such that $\lambda_u\neq 0$. There is a one-to-one correspondence between the truth table and the ANF via so called inversion formulae. The set of all Boolean functions in n variables is denoted by $\mathcal{B}_n$. A function $f\in\mathcal{B}_n$ is said to be *balanced* if $\#\{x\in\mathbb{F}_2^n: f(x)=0\}=\#\{x\in\mathbb{F}_2^n: f(x)=1\}=2^{n-1}$, which implies that $\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)}=0$. The *Walsh transform* of $f\in\mathcal{B}_n$ at point $\omega\in\mathbb{F}_2^n$ is a real valued function defined by,

$$W_f(\omega)=\sum_{x\in\mathbb{F}_2^n}(-1)^{f(x)\oplus x\cdot\omega}, \tag{2}$$

where "$\cdot$" denotes the standard dot (inner) product of two vectors. We say that f is a *plateaued* function if its Walsh spectra $\{W_f(\omega):\omega\in\mathbb{F}_2^n\}\subseteq\{0,\pm 2^r\}$ for some $1\le r\le n$.

There is a basis $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ of $\mathbb{F}_{2^n}$ considered as a vector space over $\mathbb{F}_2$. The isomorphism between the vector space $\mathbb{F}_2^n$ and the finite field $\mathbb{F}_{2^n}$ through the fixed basis $\{\alpha_1,\ldots,\alpha_n\}$ allows the following representation of $x,y\in\mathbb{F}_{2^n}$,

$$\begin{aligned} x&=x_1\alpha_1+x_2\alpha_2+\cdots+x_n\alpha_n,\\ y&=y_1\alpha_1+y_2\alpha_2+\cdots+y_n\alpha_n, \end{aligned} \tag{3}$$

where $x_i,y_j\in\mathbb{F}_2$.

Using the vector space representation any function $F:\mathbb{F}_2^n\to\mathbb{F}_2^n$ can be represented as $F(x)=(f_1(x),\ldots,f_n(x))$, where $f_i:\mathbb{F}_2^n\to\mathbb{F}_2$ are called the component (Boolean) functions of F, for $i=1,\ldots,n$. Through the isomorphism of $\mathbb{F}_2^n$ and $\mathbb{F}_{2^n}$ the function $F:\mathbb{F}_2^n\to\mathbb{F}_2^n$ can also be represented in the polynomial form so that $F(x)=\sum_{i=0}^{2^n-1}a_ix^i$, where $a_i\in\mathbb{F}_{2^n}$, and thus $F\in\mathbb{F}_{2^n}[x]$. Its *polynomial degree* equals to the largest exponent i for which $a_i\neq 0$. Its *algebraic degree* is defined to be the largest Hamming weight of the exponents i for which $a_i\neq 0$.