ON THE DUBLIN PERMUTATION

VALÉRIE GILLOT, PHILIPPE LANGEVIN, AND ABDOULAYE LO

1. Introduction

At Finite Field conference FQ9 in Dublin, K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe offered to us a very good news : the discovery of an APN permutation in dimension six [3], we will refer to this as "Dublin permutation", or CCZ-class of Dublin. Since this announcement of their "update", numerous attempts have been made to find a new permutation in even dimension, but the very bad news is that nobody found just another one ! Thanks to the paper [5], we now have a list of 14 CCZ-class of 6-bit APN functions with cubic representative of degree less or equal to 3. The numerical classification of cubic functions [7] and the exhaustive search [2] suggest that this list may be exhaustive. However, the lack of theoretical results leaves open the possibility of unknown sporadic classes, hidden within the complexity of the combinatorial of the problem. In order to eventually uncovers a novelty in dimension 6, one must search among functions of degree greater than or equal to 4, probably equal. In this talk, we address the question of the existence of an APN function of degree 4 having a special structure based on observations of the decomposition of the 14 known CCZ-classes [4]. Specifically, 12 out of the 14 of known CCZ-class contain at least one EA-class in which all vectorial functions have components whose fourth-order spectral moments take exactly two distinct values. We present a procedure to classify 6 bits APN quartics sharing this regularity. To achieve this, we introduce a new algorithm to test the existence of an APN extension of a given $(m, m-2)$-function. Our talk will also provide specific results on APN-functions based on the classification of 6-bits Boolean functions. The technical details are developped in the following sections.

2. Boolean and vectorial function

Let $\mathbb{F}_2$ be the finite field of order 2. Let m be a positive integer. We denote $B(m)$ the set of Boolean functions $f\colon \mathbb{F}_2^m \to \mathbb{F}_2$. Every Boolean function has a unique algebraic reduced representation:

$$f(x_1, x_2, \dots, x_m) = f(x) = \sum_{S\subseteq\{1,2,\dots,m\}} a_S X_S, \quad a_S \in \mathbb{F}_2,\ X_S = \prod_{s\in S} x_s. \tag{1}$$

The *degree* of f is the maximal cardinality of S with $a_S = 1$ in the algebraic form. In this paper, we conventionally fix the degree of the null function to zero. To classify Boolean functions, one introduces two definitions of equivalency, for $f, g \in B(m)$, f and g are *affine equivalent* (equivalent) if there exist an affine permutation A of $\mathbb{F}_2^m$ such that $g(x) = (f \circ A)(x)$; f and g are *extended affine equivalent* (EA-equivalent) if there exist an affine permutation A of $\mathbb{F}_2^m$ and an affine Boolean function ℓ such that $g(x) = (f \circ A)(x) + \ell(x)$.The *Walsh coefficient* of $f \in B(m)$ at $a \in \mathbb{F}_2^m$ is

$$\widehat{f}(a) = \sum_{x\in\mathbb{F}_2^m} (-1)^{f(x)+a.x},$$

the set of Walsh coefficients is called the *Walsh spectrum*. Let $q = 2^m$, the Walsh coefficients satisfy Parseval's identity :

$$\sum_{a\in\mathbb{F}_2^m} \widehat{f}(a)^2 = q^2 \tag{2}$$

The *spectral moment of order* r is the integer :

$$\kappa_r(f) = \frac{1}{q^2} \sum_{a\in\mathbb{F}_2^m} \widehat{f}(a)^r. \tag{3}$$

It is an EA-invariant, and we normalize the 4th-order spectral moment :

$$\kappa(f) = \frac{1}{q}\kappa_4(f) = \frac{1}{q^3} \sum_{a\in\mathbb{F}_2^m} \widehat{f}(a)^4 \tag{4}$$

The multiset $\mathfrak{w}(f) := \{\!\{|\widehat{f}(a)| \mid a \in \mathbb{F}_2^m\}\!\}$ of absolute value of Walsh coefficients of f, is an invariant, we used to define our main EA-invariant $\mathfrak{J}$ from the set $\mathcal{Q}$ of quadratic forms of rank 2 : $\mathfrak{J}(f) = \{\!\{\mathfrak{w}(f+g) \mid g \in \mathcal{Q}\}\!\}$. A *bent* function as a Boolean function f whose Walsh transform has constant absolute value. Bent functions exist only for even m, and that for a bent function, we have

$$|\widehat{f}(a)| = \sqrt{q} = 2^{m/2} \iff \kappa(f) = 1 \tag{5}$$

Two complementary notions are defined from the Walsh coefficients of a Boolean function the *linearity* $\mathrm{l}(f)$ and the *non-linearity* $\mathrm{nl}(f)$ with their bound :

$$\mathrm{l}(f) := \max_{a\in\mathbb{F}_2^m} |\widehat{f}(a)| \geq 2^{m/2} \qquad \mathrm{nl}(f) := 2^{m-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^m} |\widehat{f}(a)| \leq 2^{m-1} - 2^{m/2-1}$$

Bent functions have a maximal non-linearity and achieve the upper bound of non-linearity $2^{m-1} - 2^{m/2-1}$. The *auto-correlation* of a Boolean function f is defined for $t \in \mathbb{F}_2^m$ by :

$$f \times f(t) = \sum_{x+y=t} (-1)^{f(x)+f(y)} = \frac{1}{q} \sum_{a\in\mathbb{F}_2^m} \widehat{f}(a)^2 (-1)^{a.t} \tag{6}$$

A vectorial (m,n)-function is a mapping from $\mathbb{F}_2^m$ into $\mathbb{F}_2^n$, it is defined by n *coordinate Boolean functions* $f_i = e_i.F(x)$ such that $F(x) = \big(f_1(x), f_2(x), \dots, f_n(x)\big)$ with $(e_i)_{1\leq i\leq n}$ is the canonical basis of $\mathbb{F}_2^n$. For any $b \in \mathbb{F}_2^n$, the Boolean function $x \mapsto F_b(x) = b.F(x)$ is a *component* of F, the space $\langle F\rangle$ of the components is generated by the coordinates of F. The degree of a vectorial function is the maximum among the degrees of its Boolean components. Most concepts introduced earlier for Boolean functions can be extended to vectorial functions. We define equivalency of vectorial functions, for F and G two (m,n)-functions, F and G are *affine equivalent* (equivalent) if there exist an affine (m,m)-permutation A, an affine (n,n)-permutation B such that $G(x) = (B \circ F \circ A)(x)$; F and G are *extended affine equivalent* (EA-equivalent) if there exist an affine (m,m)-permutation A, an affine (n,n)-permutation B and an affine (m,n)-function C such that $G(x) = (B \circ F \circ A)(x) + C(x)$; F and G are CCZ-*equivalent* if there exists an affine permutation $\mathcal{A}$ on $\mathbb{F}_2^m \times \mathbb{F}_2^n$ such that $\mathcal{A}(\Gamma(F)) = \Gamma(G)$ where $\Gamma(F) = \{(x, F(x)) \mid x \in \mathbb{F}_2^m\}$ (resp. $\Gamma(G)$) is the graph of F (resp. G).

Lemma 1. *The multiset* $\mathfrak{J}'(F) = \{\!\{\mathfrak{J}(f) \mid f \in \langle F\rangle\}\!\}$ *is an* EA-*invariant.*

The Walsh coefficient of a (m,n)-Function F at $(a,b) \in \mathbb{F}_2^m \times \mathbb{F}_2^n$ is Walsh coefficient of its component F_b :

$$\widehat{F}(a,b) = \widehat{F_b}(a) = \sum_{x\in\mathbb{F}_2^m} (-1)^{F_b(x)+a.x},$$

the linearity and non-linearity of a (m,n)-function F are respectively the maximum of linearity among its components and the minimum non-linearity among its components :

$$\mathrm{l}(F) := \max_{a\in\mathbb{F}_2^m, b\in\mathbb{F}_2^n\setminus\{0\}} |\widehat{F_b}(a)| \qquad \mathrm{nl}(F) := 2^{m-1} - \frac{1}{2}\max_{a\in\mathbb{F}_2^m, b\in\mathbb{F}_2^n\setminus\{0\}} |\widehat{F_b}(a)|$$

A (m,n)-function is *bent* if all its non-zero components are bent. Its exists iff m is even and $n \leq m/2$. For $m = 2k$ and $n > k$, an (m,n)-function F is called (m,n)-MNBC function see [1], if it has the maximum number of bent components $2^n - 2^{n-k}$. We consider the system of two equations and r variables in $\mathbb{F}_2^m$:

$$x_1 + x_2 + \cdots + x_r = 0, \quad \text{and} \quad F(x_1) + F(x_2) + \cdots + F(x_r) = 0. \tag{7}$$

We propose to denote by $N_r(F)$ the number of solutions, and $T_r(F)$ the number of solutions where $x_1, x_2, \ldots, x_r$ are not all distincts. Let us denote

$$Q_r(F) := \frac{1}{r!}(N_r(F) - T_r(F)) \tag{8}$$

It is well known that the number of solutions $N_r(F)$ of the above system reads in term of moments of order r by of the components of F :

$$N_r(F) = \sum_{f \in \langle F \rangle} \kappa_r(f). \tag{9}$$

When we observe the Boolean components space $\langle F \rangle$ of a vectorial function F, we are interested on the one hand in the set of their EA-classes $C_F := \{\text{EA-classes}(f) \mid \forall f \in \langle F \rangle\}$ and on the other hand in the set of all normalised 4th-order spectral moments $K_F := \{\kappa(f) \mid \forall f \in \langle F \rangle\}$. For these two sets, we also study their cardinality and their distribution of values. Note that $\sharp K_F \leq \sharp C_F$. We are particularly interested in vectorial functions such that $\kappa(f)$ take few values. A vectorial function F has k levels of spectral moments if the cardinality of K_F is k.

Example 1. *If m is odd then all the non zero components of the power function x^3 in $\mathbb{F}_{2^m}$ are* EA*-equivalents, $\sharp C_F = 1$, and thus $\sharp K_F = 1$.*

3. APN AND COUNTING FUNCTION

Let F a (m,n)-function. For $u \neq 0$, $v \in \mathbb{F}_2^m$, we denote $N_F(u,v)$ the number of solutions in $\mathbb{F}_2^m$ of the equation $F(x+u) + F(x) = v$. Note that if x is a solution then $x+u$ is also a solution. Thus, $N_F(u,v)$ is even.

$$N_F(u,v) = \frac{1}{2^{m+n}} \sum_{a \in \mathbb{F}_2^m, b \in \mathbb{F}_2^n} \widehat{F_b}(a)^2 (-1)^{a.u}(-1)^{b.v} = \frac{1}{2^n} \sum_{b \in \mathbb{F}_2^n} F_b \times F_b(u)(-1)^{b.v}. \tag{10}$$

The *differential uniformity* of a (m,n)-function F is $\Delta_F := \max_{u \in \mathbb{F}_2^m \setminus \{0\}, v \in \mathbb{F}_2^n} N_F(u,v)$. A (m,m)-function F is *almost perfect non linear* (APN) iff it satisfies one of the following properties :

(i) The differential uniformity of F is $\Delta_F = 2$.
(ii) For all 2-flat $\{x,y,z,t\} \subseteq \mathbb{F}_2^m$, $F(x) + F(y) + F(z) + F(t) \neq 0$.
(iii) $N_4(F) = T_4(F) = 3q^2 - 2q$. (iv) $\sum_{0 \neq f \in \langle F \rangle} \kappa(f) = 2(q-1)$

Lemma 2. *If F is* APN *in even dimension then $K_F \geq 2$.*

Proof. If f is non zero component of F with $\sharp K_F = 1$, and (iv) implies $\kappa(f) = 2$. Parseval and little Fermat's Theorem give $\kappa(f) \equiv 1 \mod 3$, implying m odd. ☐

Lemma 3. *If F is* APN *in dimension m the number of trivial solutions are*

$$T_4(F) = 3q^2 - 2q, \quad T_6(F) = q + 15q(q-1) + 15q(q-1)(q-2).$$

The above Lemma can be used to give information on automorphism order. There are 2-spectral levels APN functions. The CCZ-class of Π is divided into 13 EA-classes [4], 3 of which have 2 spectral levels, see line 1 and 2. This table also gives the distribution of the degrees and spectral levels of the components, specifying the number of EA-classes. For example, the line 2 there is 2 EA-classes which one that contains the Dillon's permutation, 7 components are cubics and 56 are quartics.

#	degree			4th-spectral moment			
	2	3	4	1	1.75	2.5	4.0
1	63			42[1]			21[1]
2		7	56		56[1]		7[1]
5	1	62		30[2]		24[2]	9[3]
2		31	32	12[2]	32[3]	12[2]	7[2]
1		31	32	12[1]	32[2]	12[2]	7[2]
2		31	32	12[2]	32[2]	12[2]	7[2]

Moreover, 56 components with spectral moment 1.75 are in [1] EA-class, 7 components with spectral moment 4.0 are in [1] EA-class and form a vector space of dimension 3. For an APN vectorial function F, we introduce the *counting function* n_u for a given $u \in \mathbb{F}_2^m$ defined for $v \in \mathbb{F}_2^m$ by

$$n_u(v) = \begin{cases} 1, & \text{if } N_F(u,v) = 2; \\ 0, & \text{if } N_F(u,v) = 0. \end{cases}$$

This counting function is defined for each $u \in \mathbb{F}_2^m$ and verify for $b \in \mathbb{F}_2^m$:

$$\forall b \in \mathbb{F}_2^m \setminus \{0\}, \widehat{n_u}(b) = -F_b \times F_b(u) \quad \text{and} \quad \widehat{n_u}(0) = 0. \tag{11}$$

If all counting functions n_u are Boolean function of degree at most 1, the vectorial function F is called *crooked*. We apply the relation 11 to obtain the following observations that are mainly consequences of known classification of 6-bits Boolean functions.

Scolie 1. *In dimension 6, an* APN *crooked function is quadratic.*

Scolie 2. *All the counting functions of* APN *function of degree 6 are quintic.*

Scolie 3. *In dimension 6, if F is a* MNBC *function then it is not* APN .

4. Function with 2-spectral levels

We observe the existence of two spectral level function in each of the 14 known CCZ-classes in dimension 6, and we decided to search for other examples by extension process. A vectorial APN function F is with *2-spectral levels* if the normalized 4th-order spectral moments of its components take 2 values α and β. In this case,

$$\alpha A + \beta B = 2(q-1), \quad A + B = q - 1; \tag{12}$$

where A (resp. B) is the number of components f of F such that $\kappa(f) = \alpha$ (resp. $\kappa(f) = \beta$). We suppose that $\alpha < \beta$ and we say F is a function of type (α, β). Using the classification of Boolean functions, among 293 values of κ, we found 62 possible pairs satisfying 12 , involving function of degree less or equal to 4 :

α	A	deg	♯	β	B	deg	♯
1.0	42	23.	4	4.0	21	234	86
1.0	60	23.	4	22.0	3	.3.	1
1.0	56	23.	4	10.0	7	.3.	1
1.0	49	23.	4	5.50	14	.34	29
1.0	21	23.	4	2.50	42	.34	216
1.0	57	23.	4	11.50	6	.34	5
1.0	35	23.	4	3.250	28	.34	191
1.0	15	23.	4	2.3125	48	.34	214
1.0	51	23.	4	6.250	12	..4	13
1.0	47	23.	4	4.9375	16	..4	37
1.0	39	23.	4	3.6250	24	..4	67
1.0	7	23.	4	2.1250	56	..4	49
1.0	55	23.	4	8.8750	8	..4	2

α	A	deg	♯	β	B	deg	♯
1.750	56	..4	8	4.0	7	234	86
1.750	42	..4	8	2.50	21	.34	216
1.750	60	..4	8	7.0	3	.34	3
1.750	51	..4	8	3.0625	12	.34	321
1.750	35	..4	8	2.3125	28	.34	214
1.750	59	..4	8	5.6875	4	..4	25
1.750	21	..4	8	2.1250	42	..4	49
1.750	49	..4	8	2.8750	14	..4	119
1.750	57	..4	8	4.3750	6	..4	34
1.9375	56	..4	54	2.50	7	.34	216
1.9375	60	..4	54	3.250	3	.34	191
1.9375	42	..4	54	2.1250	21	..4	49
1.9375	62	..4	54	5.8750	1	..4	19

If we restrict our attention to the case where the set of components such that $\kappa(f) = \alpha$ or $\kappa(f) = \beta$ forms a vector space, thus A or B is a power of 2 minus 1, we obtain 6 possible pairs listed in the Table 1. The Table describes the structure of a potential vectorial function of type (α, β). For example, the 4-th line corresponds to the pair $(1.75, 4)$, for which we have $A = 56$ and $B = 7$. The components corresponding to $\alpha = 1.75$ (resp. $\beta = 4.0$) must be chosen from 8 (resp. 86) classes of Boolean functions of degree 4 (resp. 2, 3 and 4). We remark that the permutation obtained in [3] is of type (1.75,4) and corresponds to this line. The pair $(1, 10)$ corresponding to the first line of the table,

TABLE 1. All the possible pairs.

α	A	degree	classe	β	B	degree	classe
1.0000	(56)	23...	4	10.0000	(7)	.3...	1
1.0000	(15)	23...	4	2.3125	(48)	.34..	214
1.0000	(7)	23...	4	2.1250	(56)	..4..	49
1.7500	(56)	..4..	8	4.0000	(7)	234..	86
1.9375	(56)	..4..	54	2.5000	(7)	.34..	216
1.9375	(62)	..4..	54	5.8750	(1)	..4..	19

describes an APN and MNBC vectorial function of degree less than 3. It follows from the [1] it does not exists. The second line describes a vector function with a bent-space of dimension 4, that is impossible. Our objective is to found new vectorial functions of type (α, β) in the Table 1. The Table covers the case of the Dublin permutation, and potentially new CCZ-APN classes because of the large number of possibility in term of classes. We decided to restrict the area of exploration assuming degree 4 for the α-components and degree 3 for the β-components.

5. Numerical investigation

An extension G of F is obtained by adding a some coordinate functions, in that case $\langle F\rangle$ becomes a subspace of components space of G.

Lemma 4. *If a (m, n)-function F has an* APN *extension then $\Delta_F \leq 2^{m-n+1}$.*

The vectorial $(m, m-2)$-function F has an APN extension , if and only if, for all $(x, y, z, t) \in Q_F$ the system quadratic equations :

$$g(x)+g(y)+g(z)+g(t) \neq 0 \Leftrightarrow \big(g(x)+g(y)+g(z)+g(t)\big)^3 = 1. \tag{13}$$

is solvable in $\mathbb{F}_2^4$. We remark that $\big(g(x)+g(y)+g(z)+g(t)\big)^3$ equal to :

$$x^3+y^3+z^3+t^3+xy(x+y)+xz(x+z)+xt(x+t)+yz(y+z)+yt(y+t)+zt(z+t).$$

so we can transform system (13) in an affine system S_F N equations in $q(q+1)/2$ variables, by introducing the q Boolean variables x^3, and the $q(q-1)/2$ variables $xy(x+y)$.

Lemma 5. *If the affine system S_F has no solution then F has no* APN *extension.*

We say that an $(m, m-2)$-vectorial function passes the extension test if it satisfies conditions of Lemma 4 and Lemma 5. Even it is an hard task, it is possible to use the following procedure to "classify" all APN functions of type (α, β) that are quartic extensions of a $(6, 3)$-vectorial cubic. Let $\mathcal{E}$ be a set of (m, n)-functions. We define $\mathrm{Ext}(\mathcal{E})$ as the set of extensions (F, f) having (α, β) type that satisfy Lemma 4 and "filtered" by invariant $\mathfrak{J}'$. Starting from $\mathcal{E}_0 := \{h\}$ where $\deg(h) = 4$ and $\kappa(f) = \alpha$, we contruct $\mathcal{E}_1 = \mathrm{Ext}(\mathcal{E}_0)$, $\mathcal{E}_2 = \mathrm{Ext}(\mathcal{E}_1)$, and $\mathcal{E}_3 = \mathrm{Ext}(\mathcal{E}_2)$. We keep the $(6, 4)$-function passing the extension test, and we terminate by a backtracking algorithm to identify APN extension, and then 2-level APN functions.

Applying the procedure using the invariant of Lemma 1 for the pair (1.75,4), we remark that only 4 of the 8 possible quartic representatives provide APN extensions. Moreover, the APN functions obtained after the backtracking phase are not necessarily at 2 spectral levels, but all those of type (1.75,4) are finally CCZ-equivalent to Dublin permutation !

References

[1] Amar Bapić, Enes Pasalic, Alexandr Polujan, and Alexander Pott. Vectorial Boolean functions with the maximum number of bent components beyond the Nyberg's bound. *Des. Codes Cryptography*, 92(3):531–552, 2024. 2, 5

[2] Christof Beierle, Marcus Brinkmann, and Gregor Leander. Linearly self-equivalent APN permutations in small dimension. *IEEE Trans. Inform. Theory*, 67(7):4863–4875, 2021. 1

[3] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe. An APN permutation in dimension six. In *Finite fields: theory and applications*, volume 518 of *Contemp. Math.*, pages 33–42. Amer. Math. Soc., Providence, RI, 2010. 1, 4

[4] Marco Calderini. On the EA-classes of known APN functions in small dimensions. *Cryptogr. Commun.*, 12(5):821–840, 2020. 1, 3

[5] Yves Edel and Alexander Pott. A new almost perfect nonlinear function which is not quadratic. *Adv. Math. Commun.*, 3(1):59–81, 2009. 1

[6] Valérie Gillot and Philippe Langevin. Classification of $B(s, t, m)$, 2022. http://langevin.univ-tln.fr/data/bst/.

[7] Philippe Langevin, Zülfükar Saygi, and Efim Saygi. Classification of apn cubics in dimension 6 over gf(2), 2011. http://langevin.univ-tln.fr/project/apn-6/apn-6.html. 1