Relationships between CCZ and EA equivalence classes and corresponding code invariants

K. J. Horadam and M. Villanueva

[1] RMIT University, Melbourne, VIC 3001, Australia
[2] Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain

Abstract. The purpose of this paper is to provide a brief survey of CCZ and EA equivalence for functions $f : G \to N$ where G and N are finite and N is abelian, and, for the case $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$, to investigate two codes derived from f, inspired by these equivalences. In particular we show the dimension of the kernel of each code determines a new invariant of the corresponding equivalence class. We present computational results for $p = 2$ and small m.

Keywords: EA-equivalence class, CCZ equivalence class, code invariant, APN function, differential cryptanalysis

1 Introduction

The usefulness of any equivalence relation for functions between finite groups depends on the groups, the types of functions and the purpose of the classification. The resulting equivalence classes will have value when each class consists of functions sharing common properties or invariants. If a potentially new function satisfying desirable conditions is found, it is important to be able to show whether or not it is equivalent to a known function.

For functions between finite rings and fields, as functions between the underlying finite abelian groups, such classifications are needed for applications in finite geometry, coding and cryptography. The equivalence classes should preserve properties such as planarity or invariants such as differential uniformity or maximum nonlinearity.

Two quite separate approaches to defining equivalence for functions over $\mathbb{F}_{p^n}$, which preserve important algebraic or combinatorial properties across a wide range of interesting functions, have been used.

The first of these approaches involves pre- and post-composition of a given function $f : G \to G$, $G = (\mathbb{F}_{p^n}, +)$, with other functions having specified characteristics, to define an equivalent function. In 1964, Cavior [11] introduced *weak equivalence* between f and f' as

$$f' = \tau \circ f \circ \sigma \tag{1}$$

for any elements τ, σ of the symmetric group $\mathrm{Sym}(G)$ of G. Mullen [22] restricted τ and σ to (possibly equal) subgroups of $\mathrm{Sym}(G)$, so defining a relative form of weak equivalence. *Linear equivalence* between f and f' is defined by

$$f' = \tau \circ f \circ \sigma + \chi\,, \tag{2}$$

where τ, σ are *linear* permutations and χ is linear, so is a coarsening of weak equivalence relative to linear permutations, by addition of a linear function.

When χ in (2) is extended to include affine functions, it defines *extended affine (EA) equivalence*, introduced in [9] for $p = 2$, and now one of the main classifying equivalences for cryptographic functions.

The second approach involves defining equivalence between functions in terms of an equivalence between their graphs. This approach was originally proposed by Carlet, Charpin and Zinoviev [10, Proposition 3] for $p = 2$ (as cited in [9]), and is called *CCZ equivalence*. More generally, for a function $f : G \to N$ between finite abelian groups G and N, Pott [24] suggests using properties of its graph $\{(x, f(x)),\ x \in G\}$ as a means of measuring combinatorial and spectral properties of f.

Horadam [17] generalises these two types of equivalence to functions $f : G \to N$ between arbitrary finite groups G and N, and both types of equivalence are shown to have a common source in the equivalence relation for splitting semiregular relative difference sets. It is shown to be sufficient to restrict to those functions $f : G \to N$ for which $f(1) = 1$, which form a group $C^1(G, N)$ under the operation of pointwise multiplication of functions, and we will assume this is the case throughout.

We further assume throughout that N is abelian, and is written multiplicatively unless context dictates otherwise. For the non-abelian case see [17, 18].[3]

The affineness in an EA or CCZ equivalence of f is captured by a *shift* $f \cdot r$ of f for some $r \in G$, where

$$f \cdot r(x) = f(r)^{-1} f(rx),\ x \in G\,.$$

Definition 1. *Two functions* $f, f' \in C^1(G, N)$ *are* EA equivalent *if there exist* $r \in G$, $\theta \in Aut(G)$, $\gamma \in Aut(N)$ *and* $\chi \in Hom(G, N)$ *such that*

$$f' = (\gamma \circ (f \cdot r) \circ \theta)\, \chi\,. \tag{3}$$

The graph *of* f *is* $\mathcal{G}_f = \{(x, f(x)) \ :\ x \in G\}$. *Two functions* $f, f' \in C^1(G, N)$ *are* CCZ equivalent *if there exist* $r \in G$ *and* $\alpha \in Aut(G \times N)$ *such that*

$$\alpha(\mathcal{G}_{f \cdot r}) = \mathcal{G}_{f'}\,. \tag{4}$$

If $r = 1$, *we say* f *and* f' *are* EA isomorphic *and* CCZ isomorphic, *respectively.*

In particular, suppose $G = N = (\mathbb{F}_{p^n}, +) \cong \mathbb{Z}_p^n$. Every $f \in C^1(G, G)$ is the evaluation map of some polynomial $f(x) \in \mathbb{F}_{p^n}[x]$ of degree $\leq p^n - 2$ with $f(0) = 0$. The homomorphisms $\mathrm{Hom}(G, G)$ are the linearised polynomials $\sum_{j=0}^{n-1}\ a_j\, x^{p^j},\ a_j \in \mathbb{F}_{p^n}$, and $\mathrm{Aut}(G)$ consists of the linearised permutation polynomials. Weak equivalence (1) relative to $\mathrm{Aut}(G)$ is the case $r = 0,\ \chi \equiv \mathbf{0}$ of (3) and linear equivalence (2) is the case $r = 0$ of (3). In [9], CCZ equivalence uses translation by $e \in G \times G$ on the right, rather than on the left as in (4), but composition with the inner automorphism defined by e shows they give the same CCZ equivalence classes.

The equivalence defined by (3) is known implicitly to finite geometers, because planar functions equivalent by (3) will determine isomorphic planes [12]. Planarity of

[3] In [17, 18], EA equivalence is called bundle equivalence and CCZ equivalence is called graph equivalence.

f is preserved by addition of a linearised polynomial of G or pre- or post-composition with a linearised permutation polynomial, or by linear transformation. For instance, if $r \in G$, then $f \cdot r$ is a linear transformation.

A very large number of cryptographically strong functions over $\mathbb{F}_{2^n}$ have been found in the past decade, and it is important to be able to tell if they are genuinely new. The choice of equivalence relation best suited to classify cryptographic functions has attracted considerable attention in this period. This has been prompted by the observation that if f is invertible, then its compositional inverse $\mathrm{inv}(f)$ has the same cryptographic robustness as f with respect to several measures of nonlinearity, so the inverse of a function is often regarded as being equivalent to it. However, $\mathrm{inv}(f)$ is not always EA equivalent to f.

CCZ equivalence is a coarser equivalence than EA equivalence and includes permutations and their inverses in the same equivalence class. It is currently very difficult to decide, either theoretically or computationally, whether two functions are CCZ equivalent, and if so, whether they are EA-inequivalent.

The paper is organised as follows. In Section 2 we survey briefly the main results known about CCZ and EA equivalence and their interrelationships. We will need the *coboundary* function $\partial f : G \times G \to N$ defined for $f : G \to N$ by

$$\partial f(x,y) = f(x)^{-1}\, f(y)^{-1}\, f(xy),\ x, y \in G\,, \tag{5}$$

which measures how much f differs from a homomorphism. Section 3 discusses two codes inspired by these equivalences for functions over $\mathbb{Z}_p^m$: the graph code $\mathcal{G}_f$ and the coboundary code $\mathcal{D}_f = \operatorname{im} \partial f$. We survey known results and show that the dimension of the kernel of each code determines a new invariant of the corresponding class. In Section 4 new computational results about the codes and their invariants, and some open problems, are presented.

2 Equivalence of functions between groups

Let G be a finite group and N a finite abelian group, written multiplicatively. If $\alpha \in Aut(G \times N)$, it has a unique factorisation $\alpha = \eta \times \imath$, where its action on the first component $G \times \{1\}$ determines a monomorphism $\eta = (\eta_2, \eta_1) : G \rightarrowtail G \times N$ and its action on the second component $\{1\} \times N$ determines a monomorphism $\imath = (\imath_2, \imath_1) : N \rightarrowtail G \times N$ which commutes with (η_2, η_1), with

$$\alpha(x,a) = (\eta \times \imath)(x,a) = (\imath_2(a)\, \eta_2(x),\ \imath_1(a)\, \eta_1(x)). \tag{6}$$

CCZ equivalence has the following functional form, which is a mix of weak equivalence (1) and EA equivalence (3).

Proposition 1. [17] *Two functions $f, f' \in C^1(G,N)$ are CCZ equivalent if and only if there exist $\alpha = \eta \times \imath \in Aut(G \times N)$ and $r \in G$ such that:*
the function $\rho := (\imath_2 \circ (f \cdot r))\, \eta_2$ that they define with f is a permutation of G; and

$$f' = (\imath_1 \circ (f \cdot r) \circ \sigma)\, (\eta_1 \circ \sigma)\,, \tag{7}$$

where $\sigma = inv(\rho)$.

Corollary 1. [17] *For functions in $C^1(G,N)$, EA equivalence implies CCZ equivalence.*

Proof. If (3) holds, define α in Proposition 1 by setting $\imath = (1,\gamma)$ and $\eta = (\mathrm{inv}(\theta), \chi \circ \mathrm{inv}(\theta))$. □

If $\alpha = \eta \times \imath \in Aut(G \times N)$ in Proposition 1 fixes the subgroup $\{1\} \times N$ then $\imath_2 = 1$ so $\eta_2 \in Aut(G)$ and (3) holds. This correspondence, proved in [9] for $p = 2$, can be used as an alternative definition of EA equivalence.

Corollary 2. [17] *Two functions $f, f' \in C^1(G,N)$ are EA equivalent if and only if there exist $r \in G$ and $\alpha \in Aut(G \times N)$ such that*

1. *$\alpha(\mathcal{G}_{f\cdot r}) = \mathcal{G}_{f'}$ and*
2. *$\alpha(\{1\} \times N) = \{1\} \times N$.* □

In a few cases (as well as those in Lemma 1 below) it is known that the converse of Corollary 1 holds.

Corollary 3. *The CCZ class of $f \in C^1(G,N)$ is its EA class in the following cases:*

1. *if $f \in Hom(G,N)$;*
2. *if $\gcd(|G|,|N|) = 1$.*

Proof. Case 1 follows by definition. Case 2 follows from Corollary 2 because any automorphism of $G \times N$ must fix $\{1\} \times N$ (and $G \times \{1\}$ by symmetry). The argument is due to Pott and Zhou [25] for G abelian but holds in general, and in particular, includes the case $G \cong \mathbb{Z}_p^n$, $N \cong \mathbb{Z}_q^m$, p, q different primes. □

The restricted set of automorphisms used to redefine EA equivalence in Corollary 2 are not the only automorphisms preserving the graphs of EA equivalent functions. It is possible to say exactly when a CCZ equivalence in (7) can be rewritten as an EA equivalence in (3). Note that for any $r \in G$, f and $f \cdot r$ are trivially EA equivalent by (3), and thus CCZ equivalent by Corollary 1, so here we we give the case for $r = 1$ and EA and CCZ isomorphism. The results extend straightforwardly to the general case.

Theorem 1. [18] *Set $r = 1$ in (7) and (3). The CCZ isomorphism between f and f' determined by α in (7) can be rewritten as an EA isomorphism (3) if and only if*

1. *$\rho \in Aut(G)$ and*
2. *there exists $\delta \in Aut(N)$ such that the permutation $\hat{\delta}$ of $G \times N$ defined by*

$$\hat{\delta} \circ \alpha((x,\, f(x)a)) \;=\; \alpha((x,\, f(x)))\,(1,\, \delta(a)),\; x \in G,\; a \in N\,, \tag{8}$$

is an automorphism of $G \times N$.

In this case, the rewriting as an EA isomorphism is

$$f' = (\delta \circ f \circ \sigma)\,(\chi_\delta \circ \sigma)\,,$$

where $\chi_\delta := (\delta \circ f)^{-1}(f' \circ \rho)$. □

2.1 The case $N \cong \mathbb{Z}_p^m$

Whent N is elementary abelian, Condition 2 in Theorem 1 always holds. If we find an automorphism of $G \times \mathbb{Z}_p^m$ which proves two functions are CCZ equivalent, this gives us more flexibility than Corollary 2 does to determine if they are EA equivalent. A direct proof is given for convenience.

Theorem 2. *Let $N = \mathbb{Z}_p^m$. Suppose f and f' are CCZ isomorphic. For $\alpha \in Aut(G \times N)$ as in Proposition 1 (with $r = 1$), write $f' = f^\alpha$.*

Then f and f' are EA isomorphic

1. $\Leftrightarrow$ **there exists** α *with $f' = f^\alpha$ for which $\alpha(\{1\} \times N) = \{1\} \times N$*
2. $\Leftrightarrow$ **there exists** α *with $f' = f^\alpha$ for which $\rho \in Aut(G)$.*

Proof. $1 \Rightarrow 2$. Suppose $\alpha(\{1\} \times N) = \{1\} \times N$. Then in (6), for all $x \in G$, $\imath_2(x) = 1$ so $\rho = \eta_2$ and is an automorphism of G.
$2 \Rightarrow 1$. Suppose $\rho \in Aut(G)$. Let $\iota : N \to \{1\} \times N$ be given by $\iota(a) = (1, a),\ a \in N$. Set $J = \alpha(\iota(N)) \cap \iota(N),\ M = \mathrm{inv}(\alpha \circ \iota)(J) \leq N$ and $M' = \mathrm{inv}(\iota)(J) \leq N$, and let $\breve{\alpha} : M \to M'$ be the isomorphism induced by α, ie.

$$\breve{\alpha}(a) = \mathrm{inv}(\iota) \circ \alpha \circ \iota(a),\ a \in M.$$

Calculation using (5) shows $\mathrm{im}\, \partial f \subseteq M$ and $\breve{\alpha}(\partial f) = \partial(f' \circ \rho)$. Then $\breve{\alpha}$ can be extended, by extension of a minimal generating set for M to one for N, to at least one $\delta \in Aut(N)$. Thus $\partial(f' \circ \rho) = \breve{\alpha}(\partial f) = \delta(\partial f) = \partial(\delta \circ f)$, so $\partial((\delta \circ f)^{-1}(f' \circ \rho)) = \mathbf{1}$. Consequently, $\chi_\delta = (\delta \circ f)^{-1}(f' \circ \rho) \in \mathrm{Hom}(G, N)$. Calculation using (8) shows $\hat{\delta} \circ \alpha((x, a)) = (\rho(x),\ \delta(a)\chi_\delta(x))$, so that $\hat{\delta} \circ \alpha((1, a)) = (1,\ \delta(a))$ and $f' = f^{\hat{\delta} \circ \alpha}$. □

It is worth noting that two functions that are CCZ equivalent as in Proposition 1 may still be EA equivalent without the automorphism α satisfying $\rho \in Aut(G)$. The following example is due to Hou [20]. A particular instance is $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ defined by $f(\pm 1) = \mp 1$ and $f(x) = x$ for all $x \in \mathbb{Z}_5 \setminus \{\pm 1\}$; that is, $f(x) = -x^3$.

Example 1. Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ be such that $f = \mathrm{inv}(f)$ but f is not linear. Let $\alpha \in Aut(\mathbb{Z}_p^m \times \mathbb{Z}_p^m)$ be defined by $\alpha(x, a) = (a, x)$ for all $(x, a) \in \mathbb{Z}_p^m \times \mathbb{Z}_p^m$. Then $\alpha(x, f(x)) = (f(x), x)\ \forall x \in \mathbb{Z}_p^m$, so $\alpha(\mathcal{G}_f) = \mathcal{G}_{\mathrm{inv}(f)}$. Here f is necessarily EA equivalent to itself (= $\mathrm{inv}(f)$), but ρ is not linear. □

2.2 The case $G = \mathbb{Z}_p^n$ and $N = \mathbb{Z}_p^m$

From now on, we write G and N additively. It is known [7] that CCZ equivalence implies EA equivalence for functions $\mathbb{Z}_2^n \to \mathbb{Z}_2$. This is not always true for functions $\mathbb{Z}_2^m \to \mathbb{Z}_2^m$, however, as a permutation and its inverse under composition lie in the same CCZ class, but permutations over $\mathbb{Z}_2^m$ exist which are EA-inequivalent to their inverses.

Recall that if $n \geq m$, a function $f : \mathbb{Z}_p^n \to \mathbb{Z}_p^m$ is PN (perfect nonlinear) if for each $a \neq \mathbf{0} \in \mathbb{Z}_p^n$ the function $\partial(f)(a, x)$ takes each value of $\mathbb{Z}_p^m$ exactly p^{n-m} times. A function $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ is APN (almost perfect nonlinear) if for each $a \neq \mathbf{0},\ b \in \mathbb{Z}_2^m$ the equation $\partial(f)(a, x) = b$ has no more than two solutions x in $\mathbb{Z}_2^m$. In some important instances of PN and APN functions, CCZ equivalence does imply EA equivalence.

Lemma 1. *Over $\mathbb{Z}_p^m$, CCZ equivalence implies EA equivalence in the following cases.*

1. [19] *If $p = 2$ and $m \leq 3$.*
2. [21] *If p is odd, two PN functions are CCZ equivalent if and only if they are EA equivalent.*
3. [4, 29] *If $p = 2$ and $m \geq 2$, two quadratic APN functions are CCZ equivalent if and only if they are EA equivalent.* □

More generally, for $G = \mathbb{Z}_p^n$ with n large enough and $N = \mathbb{Z}_p^m$ with $m > 1$, CCZ equivalence does not imply EA equivalence.

Theorem 3. (Budaghyan, Carlet, Helleseth [7, 8]) *Let p be an odd (even) prime, $n \geq 3$ ($n \geq 5$) and $k > 1$ the smallest divisor of n. Then for any $m \geq k$, CCZ equivalence of functions from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p^m$ is strictly more general than EA equivalence.* □

Even though the two equivalences can be compared directly using either the functional or the graphical approach, it is more computationally difficult to check functions for CCZ equivalence than for EA equivalence, and more computationally difficult to generate CCZ equivalence classes than EA equivalence classes.

One advantage of determining either equivalence lies in the properties shared by equivalent functions, and the chance it provides of replacing a complex function by a simpler equivalent function to improve efficiency in applications.

A recent illustration of this appears in [27] for $G = \mathbb{Z}_2^m \times \mathbb{Z}_2^m$. It is shown, after mapping each element of $\mathbb{Z}_{2^m}$ to the coefficient vector of its binary representation, that addition modulo 2^m is CCZ equivalent to a very simple quadratic vectorial Boolean function. This is applied to simplify attacks on cryptosystems which employ addition modulo 2^m.

Conversely, finding more complex functions which are EA-inequivalent to known simple functions but which nonetheless possess similar desirable properties can improve cryptographic security or enlarge the known set of sequences with optimal correlation properties.

A recent illustration of this appears in [15] where it is shown that for $p \geq 5$ and m an integer that does not divide $p^m + 1$, then the function $f(x) = x^{p^m+2}$ over $\mathbb{Z}_p^m$ is an Alltop function (that is, its differential functions are PN) which is EA-inequivalent to the Alltop function $f'(x) = x^3$, even though ∂f and $\partial f'$ are EA equivalent PN functions.

2.3 The case $G = N = \mathbb{Z}_2^m$

EA equivalence partitions the set of (non-affine) functions over $\mathbb{Z}_2^m$ into classes with the same nonlinearity, differential uniformity and algebraic degree [9]. CCZ equivalence partitions the set of functions over $\mathbb{Z}_2^m$ into classes with the same Walsh spectrum, differential uniformity and resistance to algebraic cryptanalysis [10, 9] but not necessarily the same algebraic degree.

It remains very difficult to tell when CCZ equivalent functions are EA-inequivalent. Some results for APN functions in small orders are known. Computation has shown [5] that there is 1 CCZ class of APN functions over $\mathbb{Z}_2^4$, containing 2 EA classes; and 3 CCZ classes of APN functions over $\mathbb{Z}_2^5$, containing 1, 3 and 3 EA classes, respectively. There are at least 14 CCZ classes of APN functions over $\mathbb{Z}_2^6$ [5], at least 302 over $\mathbb{Z}_2^7$ and at least 33 over $\mathbb{Z}_2^8$ [28], and at least 11 over $\mathbb{Z}_2^9$ [14]. Edel [13] has computed the partition of many of them into EA classes. He shows, for example, that, for $n = 5, 6, 7, 8$ and 9 the CCZ class of the Gold quadratic APN function $f(x) = x^3$ contains $3, 3, 3, 2$ and 5 EA classes, respectively. Summaries appear in [6, 21].

3 Code invariants of EA and CCZ classes of functions over $\mathbb{Z}_p^m$

For cryptographic applications, the focus is to find functions over $\mathbb{Z}_2^m$ which have simultaneously low differential uniformity (APN or 4-uniform), high nonlinearity and algebraic degree ≥ 4 and which are, preferably, permutations. This aim can be aided by working with specific codes they generate. The graph code for APN functions was introduced in [6] and the coboundary code was introduced in [19].

Definition 2. *Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ satisfy $f(\mathbf{0}) = \mathbf{0}$.*
Define the graph code *of f to be the p-ary code $\mathcal{G}_f = \{(x, f(x)) \ : \ x \in \mathbb{Z}_p^m\} \subseteq \mathbb{Z}_p^{2m}$.*
Define the coboundary code *of f to be the p-ary code $\mathcal{D}_f = \{\partial f(x, y) \ : \ x,\ y \in \mathbb{Z}_p^m\}$ $\subseteq \mathbb{Z}_p^m$.*

The linear codes they generate are denoted $\langle \mathcal{G}_f \rangle$ and $\langle \mathcal{D}_f \rangle$, respectively.
Let $n(f) = \mathrm{rank}_p\ \mathcal{D}_f = \dim_p \langle \mathcal{D}_f \rangle$ and $s(f) = \mathrm{rank}_p\ \mathcal{G}_f = \dim_p \langle \mathcal{G}_f \rangle$; that is $|\langle \mathcal{D}_f \rangle| = p^{n(f)}$ and $|\langle \mathcal{G}_f \rangle| = p^{s(f)}$.

For the remainder of this Section we will investigate the properties of, and relationships between, these codes. The following simple properties of their dimensions appear in [19, Theorem 4].

Theorem 4. *1. $0 \leq n(f) \leq m$ and $m \leq s(f) \leq 2m$;*
2. $n(f) = 0 \Leftrightarrow f$ is linear $\Leftrightarrow \mathcal{G}_f = \langle \mathcal{G}_f \rangle \Leftrightarrow s(f) = m$;
3. $\{0\} \times \langle \mathcal{D}_f \rangle < \langle \mathcal{G}_f \rangle$ and $n(f) < s(f)$;
4. if $n(f) = m$ then $s(f) = 2m$; i.e. if $\mathcal{D}_f$ generates $\mathbb{Z}_p^m$ then $\mathcal{G}_f$ generates $\mathbb{Z}_p^{2m}$. □

Both these dimensions are related to the differential uniformity $\Delta(f)$, which is defined to be the maximum over $a \neq \mathbf{0} \in \mathbb{Z}_p^m$ of the number of solutions of

$$-f(x) + f(x + a) = b;\ \ b \in \mathbb{Z}_p^m\,. \tag{9}$$

Lemma 2. [19] *For each f, $n(f) \geq m - \lfloor \log_p \Delta(f) \rfloor$. In particular,*

if p is odd and $1 \leq \Delta(f) < p$, $n(f) = m$;
if $p = 2$ and $\Delta(f) = 2$, $n(f) = m$ or $n(f) = m - 1$;
if $p = 2$ and $\Delta(f) = 4$, $n(f) = m$ or $n(f) = m - 1$ or $n(f) = m - 2$. □

A further parameter of each of the codes $\mathcal{D}_f$ and $\mathcal{G}_f$ is the dimension of its kernel. Recall that the *p-kernel* of a code C over $\mathbb{Z}_p$ of length n is defined [23] as

$$K(C) = \{x \in \mathbb{Z}_p^n \ : \ x + C = C\}\,.$$

If $\mathbf{0} \in C$, then $K(C)$ is a linear subspace of C and C can be written as the union of cosets of $K(C)$. If so, $K(C)$ is the largest such linear code for which this is true. For $p = 2$, the kernel was introduced in [2].

Definition 3. *Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ satisfy $f(\mathbf{0}) = \mathbf{0}$, so $K(\mathcal{G}_f)$ is a linear subcode of $\mathcal{G}_f$ and $K(\mathcal{D}_f)$ is a linear subcode of $\mathcal{D}_f$. Set $K(f) = \dim_p K(\mathcal{G}_f)$.*
Set $k(f) = \dim_p K(\mathcal{D}_f)$ and let $M(f)$ be the multiset $\{\{k(f \cdot r),\ r \in \mathbb{Z}_p^m\}\}$, denoted $M(f) = \{0^\wedge a_0, 1^\wedge a_1, \ldots, m^\wedge a_m\}$, for some $a_0, \ldots, a_m$ with $\sum_{i=0}^m a_i = p^m$.

It is known that differential uniformity $\Delta(f)$ is a combinatorial invariant of the EA equivalence class of f [16, Corollary 9.52.1]. In fact this is a consequence of it being a combinatorial invariant of the CCZ equivalence class of f.

Lemma 3. *If f and f' are CCZ equivalent, then $\Delta(f) = \Delta(f')$.*

Proof. Differential uniformity is a combinatorial invariant of CCZ isomorphism [18, Lemma 5], so if $\alpha(\mathcal{G}_{f \cdot r}) = \mathcal{G}_{f'}$ as in (4) then $\Delta(f \cdot r) = \Delta(f')$. It remains only to show that $\Delta(f \cdot r) = \Delta(f)$. Suppose $a \neq \mathbf{0} \in \mathbb{Z}_p^m$. Then for each $b \in \mathbb{Z}_p^m$, $\{x \in \mathbb{Z}_p^m\ :\ -(f \cdot r)(x) + (f \cdot r)(x+a) = b\} = \{x \in \mathbb{Z}_p^m\ :\ -f(r+x) + f(r+x+a) = b\}$ $= \{y \in \mathbb{Z}_p^m\ :\ -f(y) + f(y+a) = b\}$ and the set sizes are identical. □

We show that the dimensions $n(f)$ and $s(f)$ are algebraic invariants of the EA and CCZ equivalence classes of f, respectively.

Theorem 5. *If f and f' are EA equivalent, then $n(f) = n(f')$. If f and f' are CCZ equivalent, then $s(f) = s(f')$.*

Proof. The dimensions $n(f)$ and $s(f)$ are algebraic invariants of EA and CCZ isomorphism, respectively [19, Theorem 5], so that we only need to consider $f' = f \cdot r,\ r \neq \mathbf{0}$ and note $(f \cdot r) \cdot (-r) = f$. Then $\partial(f \cdot r)(x, y) = \partial f(r + x, y) - \partial f(r, y) \in \langle \mathcal{D}_f \rangle$ so by symmetry $\langle \mathcal{D}_{f \cdot r} \rangle = \langle \mathcal{D}_f \rangle$. Also $\mathcal{G}_{f \cdot r} = \mathcal{G}_f - (r, f(r))$ so $\langle \mathcal{G}_{f \cdot r} \rangle = \langle \mathcal{G}_f \rangle$. □

Now we show that $M(f)$ and $K(f)$ are algebraic invariants of the EA and CCZ equivalence classes of f, respectively.

Theorem 6. *If f and f' are EA equivalent, then $M(f) = M(f')$. If f and f' are CCZ equivalent, then $K(f) = K(f')$.*

Proof. If f and f' are EA equivalent, suppose $\theta,\ \gamma \in \mathrm{Aut}(\mathbb{Z}_p^m)$, $\chi \in \mathrm{Hom}(\mathbb{Z}_p^m, \mathbb{Z}_p^m)$ and $r \in \mathbb{Z}_p^m$ are such that $f' = \gamma \circ (f \cdot r) \circ \theta\ +\ \chi$, so that $\partial f'(\vartheta(x), \vartheta(y)) = \gamma(\partial(f \cdot r)(x, y))$ for all $x,\ y \in \mathbb{Z}_p^m$, where $\vartheta = \mathrm{inv}(\theta)$. Suppose $c \in K(\mathcal{D}_{f \cdot r})$, so that $c = \partial(f \cdot r)(a,\ b)$ for some $a,\ b \in \mathbb{Z}_p^m$ and $c + \partial(f \cdot r)(x,\ y) = \partial(f \cdot r)(x',\ y')$. Then $\gamma(c) + \gamma(\partial(f \cdot r)(x,\ y)) = \gamma(\partial(f \cdot r)(x',\ y'))$ so $\gamma(c) \in K(\mathcal{D}_{f'})$. Thus γ is an isomorphism between $K(\mathcal{D}_{f \cdot r})$ and $K(\mathcal{D}_{f'})$, so that $k(f') = k(f \cdot r) \in M(f)$. By symmetry, $k(f) \in M(f')$ and $M(f) = M(f')$.

If f and f' are CCZ isomorphic, $\alpha \in \mathrm{Aut}(\mathbb{Z}_p^{2m})$ and $\alpha(\mathcal{G}_f) = \mathcal{G}_{f'}$, suppose $c \in K(\mathcal{G}_f)$. Then $c = (a, f(a))$ for some $a \in \mathbb{Z}_p^m$ and if $c + (x,\ f(x)) = (x', f(x'))$ then $\alpha(c) + \alpha((x,\ f(x))) = \alpha((x', f(x')))$ and $\alpha(c) \in K(\mathcal{G}_{f'})$. Thus α is an isomorphism between $K(\mathcal{G}_f)$ and $K(\mathcal{G}_{f'})$. Finally, $K(\mathcal{G}_f) = K(\mathcal{G}_{f \cdot r})$ for all r. □

When $p = 2$, we are interested in additional properties of the codes $\mathcal{G}_f$ and $\mathcal{D}_f$.

Definition 4. *Let $f : \mathbb{Z}_2^m \to \mathbb{Z}_2^m$ satisfy $f(\mathbf{0}) = \mathbf{0}$. Let H be an $m \times (2^m - 1)$ parity check matrix of the Hamming code $\mathcal{H}^m$, that is, its columns are the transposes $x^\top$ of the non-zero row vectors $x \in \mathbb{Z}_2^m$. Define*

$$H_f = \begin{pmatrix} H \\ H^{(f)} \end{pmatrix} = \begin{pmatrix} \cdots & x^\top & \cdots \\ \cdots & f(x)^\top & \cdots \end{pmatrix}.$$

Let $\mathcal{C}_f$ be the linear code of length $2^m - 1$ admitting H_f as a parity check matrix.

Note that $\mathcal{C}_f$ is a subcode of $\mathcal{H}^m$. Since $\mathcal{G}_f = H_f^\top \cup \{(\mathbf{0}, \mathbf{0})\}$, $\langle H_f^\top \rangle = \langle \mathcal{G}_f \rangle$, and $\langle H_f \rangle$ is the dual of $\mathcal{C}_f$. The dimension of $\mathcal{C}_f$, or equivalently the dimension of the extended code $\mathcal{C}_f^*$, is $2^m - 1 - s(f)$. Therefore, the rank of $\mathcal{G}_f$ can also be computed using the dimension of $\mathcal{C}_f^*$.

Proposition 2. [6] *Let f and f' be maps from $\mathbb{Z}_2^m$ to $\mathbb{Z}_2^m$ with $\dim_2\langle H_f \rangle = \dim_2\langle H_{f'} \rangle = 2m$. Then, f and f' are CCZ equivalent if and only if their extended codes $\mathcal{C}_f^*$ and $\mathcal{C}_{f'}^*$ are equivalent.* □

If f is APN, the dimension $s(f)$ is already known to be maximal, ie. $s(f) = 2m$, by [6]. It has also been proved that $s(f) = 2m$ for another class of functions, the AF permutations [26], but the AF property itself is not an invariant of CCZ equivalent permutations.

Consideration of Theorem 4 raises the possibility that $s(f)$ and $n(f)$ are not independent invariants, which we formulate as a conjecture in the next Section. However we demonstrate computationally that $K(f)$ and $M(f)$ are independent.

4 Examples for $p = 2$ with low dimensions

In this Section, we concentrate on computations for $p = 2$ and functions which are either monomial power functions or have differential uniformity 4. Let S_n be the symmetric group of permutations of length n, where $n = 2^m - 1$.

4.1 Monomial power functions

Table 1 shows the classification of all monomial power functions into CCZ equivalence classes for all $3 \leq m \leq 7$. Additional properties have been computed, and included in the table. These are: whether they are APN; the pair (rank, kernel dimension) = $(s(f), K(f))$ for the binary code $\mathcal{G}_f$; and the possibilities for the number of solutions of (9) for $p = 2$.

For $m = 5$, it is known that the three CCZ classes of APN functions in Table 1 contain $3, 3$ and 1 EA classes respectively [5]. Two of the EA classes in the CCZ equivalence class of x^3 contain the monomials x^3 and x^{11}, respectively, and two of the EA classes in the CCZ equivalence class of x^5 contain the monomials x^5 and x^7, respectively. Non-monomial representatives of each other EA class are given in [5].

For $m = 7$, it is only necessary to check the cases x^7 and x^{21} computationally, since the other CCZ classes of non-APN monomials can be distinguished by the number of solutions of (9).

m	f	APN	j, for all x^j CCZ equivalent	$(s(f), K(f))$	Number of solutions of (9)
3	x^1	no	1,2,4	(3,3)	$\{0^\wedge 49, 8^\wedge 7\}$
3	x^3	yes	3,5,6	(6,0)	$\{0^\wedge 28, 2^\wedge 28\}$
4	x^1	no	1,2,4,8	(4,4)	$\{0^\wedge 225, 16^\wedge 15\}$
4	x^3	yes	3,6,9,12	(8,0)	$\{0^\wedge 120, 2^\wedge 120\}$
4	x^5	no	5,10	(6,0)	$\{0^\wedge 180, 4^\wedge 60\}$
4	x^7	no	7,11,13,14	(8,0)	$\{0^\wedge 135, 2^\wedge 90, 4^\wedge 15\}$
5	x^1	no	1,2,4,8,16	(5,5)	$\{0^\wedge 961, 32^\wedge 31\}$
5	x^3	yes	3,6,11,12,13,17,21,22,24,26	(10,0)	$\{0^\wedge 496, 2^\wedge 496\}$
5	x^5	yes	5,7,9,10,14,18,19,20,25,28	(10,0)	$\{0^\wedge 496, 2^\wedge 496\}$
5	x^{15}	yes	15,23,27,29,30	(10,0)	$\{0^\wedge 496, 2^\wedge 496\}$
6	x^1	no	1,2,4,8,16,32	(6,6)	$\{0^\wedge 3969, 64^\wedge 63\}$
6	x^3	yes	3,6,12,24,33,48	(12,0)	$\{0^\wedge 2016, 2^\wedge 2016\}$
6	x^5	no	5,10,13,17,19,20,26,34,38,40,41,52	(12,0)	$\{0^\wedge 3024, 4^\wedge 1008\}$
6	x^7	no	7,14,28,35,49,56	(12,0)	$\{0^\wedge 2205, 2^\wedge 1701, 4^\wedge 63, 6^\wedge 63\}$
6	x^9	no	9,18,36	(9,0)	$\{0^\wedge 3528, 8^\wedge 504\}$
6	x^{11}	no	11,22,23,25,29,37,43,44,46,50,53,58	(12,0)	$\{0^\wedge 2520, 2^\wedge 1323, 6^\wedge 126, 10^\wedge 63\}$
6	x^{15}	no	15,30,39,51,57,60	(12,0)	$\{0^\wedge 2205, 2^\wedge 1764, 8^\wedge 63\}$
6	x^{21}	no	21,42	(8,0)	$\{0^\wedge 3780, 12^\wedge 126, 20^\wedge 126\}$
6	x^{27}	no	27,45,54	(9,0)	$\{0^\wedge 3528, 2^\wedge 63, 6^\wedge 189, 8^\wedge 63, 12^\wedge 189\}$
6	x^{31}	no	31,47,55,59,61,62	(12,0)	$\{0^\wedge 2079, 2^\wedge 1890, 4^\wedge 63\}$
7	x^1	no	1,2,4,8,16,32,64	(7,7)	$\{0^\wedge 16129, 128^\wedge 127\}$
7	x^3	yes	3,6,12,24,43,45,48,53,65,85,86,90,96,106	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$
7	x^5	yes	5,10,20,27,33,40,51,54,66,77,80,89,102,108	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$
7	x^7	no	7,14,28,55,56,59,67,91,93,97,109,110,112,118	(14,0)	$\{0^\wedge 9906, 2^\wedge 5461, 6^\wedge 889\}$
7	x^9	yes	9,15,17,18,30,34,36,60,68,71,72,99,113,120	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$
7	x^{11}	yes	11,13,22,26,35,44,49,52,69,70,81,88,98,104	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$
7	x^{19}	no	19,25,38,47,50,61,73,76,87,94,100,107,117,122	(14,0)	$\{0^\wedge 10795, 2^\wedge 2794, 4^\wedge 2667\}$
7	x^{21}	no	21,31,37,41,42,62,74,79,82,84,103,115,121,124	(14,0)	$\{0^\wedge 9906, 2^\wedge 5461, 6^\wedge 889\}$
7	x^{23}	yes	23,29,39,46,57,58,75,78,83,92,101,105,114,116	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$
7	x^{63}	yes	63,95,111,119,123,125,126	(14,0)	$\{0^\wedge 8128, 2^\wedge 8128\}$

Table 1. Classification of all monomial power functions $f(x) = x^i$ for $3 \leq m \leq 7$ into CCZ equivalence classes, and some properties of these classes.

For $m = 8$, a classification of monomial power functions by cyclotomic coset, differential uniformity and nonlinearity is given in [1, Table 3]. After combining cyclotomic cosets containing f with those containing inv(f) (recall that f and inv(f) are CCZ equivalent [10]) and comparing the number of solutions of (9) for representative power functions, the only power functions which still need distinguishing are x^{15} and x^{45}. The graph codes corresponding to these two functions have $s(f) = 2m = 16$, and as the two extended codes are inequivalent, the functions are CCZ inequivalent by Proposition 2. The classification in [1, Table 3] reduces to a list of 28 CCZ classes of monomial power functions. These are given in Table 2, together with their differential uniformity $\varDelta(f)$ and the values $(s(f), K(f))$.

We have computed the invariant multiset $M(f)$ for every $f(x) = x^i$ in Tables 1 and 2. The results appear in Table 3. In these cases we have very simple and uniform results in terms of the cyclotomic coset C_i of i mod $2^m - 1$. For instance, for $m = 4$, $M(x^5) = \{2^\wedge 16\}$ and for $m = 6$, $M(x^9) = \{3^\wedge 64\}$.

Thus $M(f)$ can distinguish between some, but not all, representatives of distinct CCZ classes for these special cases. Furthermore, for each CCZ class in these Tables which consists of APN functions but contains more than one EA class, we computed

i	$\Delta(f)$	$(s(f),K(f))$	i	$\Delta(f)$	$(s(f),K(f))$	i	$\Delta(f)$	$(s(f),K(f))$	i	$\Delta(f)$	$(s(f),K(f))$
1	256	(8,8)	15	14	(16,0)	31	16	(16,0)	63	6	(16,0)
3	2	(16,0)	17	16	(12,0)	39	2	(16,0)	85	84	(10,0)
5	4	(16,0)	19	16	(16,0)	43	30	(16,0)	87	30	(16,0)
7	6	(16,0)	21	4	(16,0)	45	14	(16,0)	95	4	(16,0)
9	2	(16,0)	23	16	(16,0)	51	50	(12,0)	111	4	(16,0)
11	10	(16,0)	25	6	(16,0)	53	16	(16,0)	119	22	(12,0)
13	12	(16,0)	27	26	(16,0)	55	12	(16,0)	127	4	(16,0)

Table 2. Classification of representative functions $f(x) = x^i$ for $m = 8$ into CCZ equivalence classes, and some invariants of these classes. Classes with $\Delta(f) = 2$ are the APN functions.

$M(f)$ for a representative function from each EA class, and obtained exactly the same $M(f)$ for each EA class. In other words, in all these cases, $k(f)$ itself is an invariant of EA class. It is determined by the size of a corresponding cyclotomic coset, and does not distinguish between different EA classes in the same CCZ class of APN functions.

However, this does not hold in general, as we shall see in the following Subsection.

i	$M(f(x) = x^i)$
$i \in C_1$	{0^2^m}
$i \notin C_1$	{$\lvert C_i \rvert$^2^m}

Table 3. Invariant multiset $M(f)$ for the monomial power functions $f(x) = x^i$ for all $3 \leq m \leq 8$ in Tables 1 and 2, where C_i is the cyclotomic coset of i mod $2^m - 1$.

4.2 Differentially 4-uniform permutations

For $m = 4$, in general (not only considering monomial power permutations), it is well known that there are no APN permutations.

According to [19] there are 5 EA equivalent classes of differentially 4-uniform permutations, and as they all have different extended Walsh spectra, they each form a single CCZ equivalence class. On the other hand, using MAGMA [3] and checking all differentially 4-uniform permutations in S_{15}, there are exactly 10 CCZ equivalence classes, given by the following permutations:

$$\begin{aligned}
\sigma_1 &= (5,6,7,8)(10,12,11,15,13,14) \ \ (= f_3 \text{ in } [19]),\\
\sigma_2 &= (5,6,7,8)(10,12,14,13)(11,15) \ \ (= f_4 \text{ in } [19]),\\
\sigma_3 &= (5,6,8)(7,10,12)(9,11,15,14,13) \ \ (= f_5 \text{ in } [19]),\\
\sigma_4 &= (5,6,8)(7,10,12)(9,11,15,14) \ \ (= f_6 \text{ in } [19]),\\
\sigma_5 &= (5,6,8)(7,11,14,10,12,13),\\
\sigma_6 &= (5,6,8)(7,11,14)(10,12,13) \ \ (= f_7 \text{ in } [19]),\\
\sigma_7 &= (5,6,8)(7,11,13,15)(9,12,10),\\
\sigma_8 &= (5,6,8)(7,11,13)(9,12,14,10),\\
\sigma_9 &= (5,6,8)(7,11,13,10,9,12,14),\\
\sigma_{10} &= (5,6,8)(7,11)(9,12,10,13,15,14)\,.
\end{aligned}$$

Table 4 corrects [19, Table 2], where the CCZ classes of $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_6$ were claimed to exhaust the differentially 4-uniform classes of permutations fixing **0** over $\mathbb{Z}_2^4$. For every f in Table 4, the dimension $K(f)$ of the kernel of the binary code $\mathcal{G}_f$ is the minimum value 0 and the rank $s(f)$ is the maximum value $2m = 8$, so Proposition 2 applies. Computation of $n(f)$ confirms that $n(f) = 4 = m$ in all cases. Table 4 lists invariants of the 10 CCZ equivalence classes: the order of the automorphism group of $\mathcal{C}_f^*$; the minimum distance and covering radius of $\mathcal{C}_f^*$ as a pair (d, ρ); the weight distribution of the dual of $\mathcal{C}_f^*$; and the possibilities for the number of solutions of (9).

f	$\lvert Aut(\mathcal{C}_f^*)\rvert$	(d,ρ)	Weight distribution of the dual of C_f^*	Number of solutions of (9)
σ_1	4	$(4,5)$	$1+x^2+28x^4+119x^6+214x^8+119x^{10}+28x^{12}+x^{14}+x^{16}$	$\{0\^{}141, 2\^{}78, 4\^{}21\}$
σ_2	96	$(4,5)$	$1+x^2+30x^4+111x^6+226x^8+111x^{10}+30x^{12}+x^{14}+x^{16}$	$\{0\^{}144, 2\^{}72, 4\^{}24\}$
σ_3	1152	$(4,4)$	$1+36x^4+96x^6+246x^8+96x^{10}+36x^{12}+x^{16}$	$\{0\^{}144, 2\^{}72, 4\^{}24\}$
σ_4	16	$(4,5)$	$1+32x^4+112x^6+222x^8+112x^{10}+32x^{12}+x^{16}$	$\{0\^{}138, 2\^{}84, 4\^{}18\}$
σ_5	12	$(4,5)$	$1+32x^4+112x^6+222x^8+112x^{10}+32x^{12}+x^{16}$	$\{0\^{}138, 2\^{}84, 4\^{}18\}$
σ_6	4	$(4,5)$	$1+30x^4+120x^6+210x^8+120x^{10}+30x^{12}+x^{16}$	$\{0\^{}135, 2\^{}90, 4\^{}15\}$
σ_7	28	$(4,5)$	$1+x^2+28x^4+119x^6+214x^8+119x^{10}+28x^{12}+x^{14}+x^{16}$	$\{0\^{}141, 2\^{}78, 4\^{}21\}$
σ_8	20	$(4,5)$	$1+30x^4+120x^6+210x^8+120x^{10}+30x^{12}+x^{16}$	$\{0\^{}135, 2\^{}90, 4\^{}15\}$
σ_9	16	$(4,5)$	$1+30x^4+120x^6+210x^8+120x^{10}+30x^{12}+x^{16}$	$\{0\^{}135, 2\^{}90, 4\^{}15\}$
σ_{10}	720	$(4,4)$	$1+30x^4+120x^6+210x^8+120x^{10}+30x^{12}+x^{16}$	$\{0\^{}135, 2\^{}90, 4\^{}15\}$

Table 4. Classification of all differentially 4-uniform permutations of order 15 into CCZ equivalence classes, and some invariants of these classes.

All these functions have $n(f) = 4 = m$ so that Theorem 4.4 applies, and we observe that $n(f) = s(f) - 4$. A computational check of the 7 CCZ classes of functions over $\mathbb{Z}_2^3$ ([19, Table 1]) shows that even though only f_2 and f_4 have $n(f) = 3$, it remains true that $n(f) = s(f) - 3$. We conjecture that this holds in general.

Conjecture 1. Let $f : \mathbb{Z}_p^m \to \mathbb{Z}_p^m$ satisfy $f(\mathbf{0}) = \mathbf{0}$. Then $n(f) = s(f) - m$.

However, it is not the case that all parameters of the codes $\mathcal{D}_f$ and $\mathcal{G}_f$ must be related. For instance $K(f) = 0$ for every f in Table 4, but $M(f)$ varies.

We have calculated
$M(\sigma_1) = \{0\^{}8, 1\^{}4, 4\^{}4\}$,
$M(\sigma_2) = \{1\^{}6, 4\^{}10\}$,
$M(\sigma_3) = \{4\^{}16\}$,
$M(\sigma_4) = \{0\^{}4, 4\^{}12\}$,
$M(\sigma_5) = \{0\^{}6, 4\^{}10\}$,
$M(\sigma_6) = \{0\^{}4, 4\^{}12\}$,
$M(\sigma_7) = \{0\^{}15, 4\}$,
$M(\sigma_8) = \{0\^{}10, 4\^{}6\}$,
$M(\sigma_9) = \{0\^{}8, 4\^{}8\}$,
$M(\sigma_{10}) = \{4\^{}16\}$.

So the two invariants $K(f)$ and $M(f)$ are independent in general. Furthermore, in these examples, the dimension $k(f \cdot r)$ of the kernel of the code $\mathcal{D}_{f \cdot r}$ does vary with the affine term r within an EA equivalence class.

4.3 Open questions

It seems to us that $\mathcal{D}_f$ provides a new code-based technique for investigating EA equivalence classes, while $\mathcal{G}_f$ can be used for investigating CCZ classes and, in some cases, EA classes [6, 4]. For future work, we expect that further study of the relationship between the invariants $n(f)$ and $s(f)$, and $M(f)$ and $K(f)$, will clarify how CCZ classes partition into EA classes, particularly for functions with low differential uniformity. It will be valuable if $n(f)$ or $M(f)$ can distinguish between two CCZ equivalent functions which are EA-inequivalent, especially for APN functions. The cases $n(f) = m,\ m-1$ and $m-2$ (for both odd and even p) are the most interesting. Do APN functions f exist for which $n(f) = m - 1$? Of course, if the answer to Conjecture 1 is "yes" then the answer to this question is "no". We can ask if, for the EA equivalence class of a power function f, the constant value of $k(f \cdot r),\ r \in \mathbb{Z}_2^m$ and its dependence on a cyclotomic coset that we have observed in low dimensions, can be proved to hold in general. We can also ask if there is a relationship between $n(f)$ or $M(f)$ and the algebraic degree of f, since they are all invariants of EA equivalence class.

Acknowledgements. We thank the anonymous referee for helpful comments which improved the content and clarity of the paper. The second author has been partially supported by the Spanish MICINN under Grants TIN2010-17358 and TIN2013-40524-P, and by the Catalan AGAUR under Grant 2014SGR-691. She thanks RMIT School of Mathematical and Geospatial Sciences for hosting her while this research was undertaken.

References

1. B. Aslan, M. T. Sakalli and E. Bulus, Classifying 8-Bit to 8-Bit S-Boxes based on power mappings from the point of DDT and LAT distributions, *Proc. WAIFI 2008* LNCS 5130 (2008) 123–133.
2. H. Bauer, B. Ganter and F. Hergert, Algebraic techniques for nonlinear codes, *Combinatorica* 3 (1983) 21–33.
3. W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: the user language, *J. Symbol. Comp.* 24 (1997) 235–265.
4. C. Bracken, E. Byrne, G. McGuire and G. Nebe, On the equivalence of quadratic APN functions, *Des. Codes Cryptogr.* 61 (2011) 261–272.
5. M. Brinkmann and G. Leander, On the classification of APN functions up to dimension 5, *Des. Codes Cryptogr.* 49 (2008) 273–288.
6. K. A. Browning, J. F. Dillon, R. E. Kibler and M. T. McQuistan, APN polynomials and related codes, *J. Comb. Inf. Syst. Sci.* **34** (2009) 135–159. Special issue honoring the 75th birthday of Prof. D.K. Ray-Chaudhuri.
7. L. Budaghyan and C. Carlet, CCZ-equivalence of single and multi-output Boolean functions, Post-proceedings of the 9^{th} International Conference on Finite Fields and Their Applications Fq'09, *Contemporary Math.* 518 (2010) 43–54.
8. L. Budaghyan and T. Helleseth, Planar functions and commutative semifields, *Tatra. Mt. Math. Publ.* 45 (2010) 15–45.
9. L. Budaghyan, C. Carlet and A. Pott, New classes of almost bent and almost perfect nonlinear polynomials, *IEEE Trans. Inform. Theory* 52 (2006) 1141–1152.
10. C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* 15 (1998) 125–156.

11. S. R. Cavior, Equivalence classes of functions over a finite field, *Acta Arith.* 10 (1964) 119–136.
12. R. S. Coulter and R. W. Matthews, Planar functions and planes of Lenz-Barlotti Class II, *Des. Codes Cryptogr.* 10 (1997) 167–184.
13. Y. Edel, personal correspondence, March 2010.
14. Y. Edel and A. Pott, A new almost perfect nonlinear function which is not quadratic, *Advances Math. Comp.* 3 (2009) 59–81.
15. J. Hall, A. Rao and S. M. Gagola III, A family of Alltop functions that are EA-inequivalent to the cubic function, *IEEE Trans. Commun.* 61(11) (2013) 4722–4727.
16. K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, 2007.
17. K. J. Horadam, Relative difference sets, graphs and inequivalence of functions between groups, *J. Combin. Des.* 18 (2010) 260–273.
18. K. J. Horadam, Equivalence classes of functions between finite groups, *J. Algebr. Combin.* 35 (2012) 477–496.
19. K. J. Horadam and R. East, Partitioning CCZ classes into EA classes, *Advances Math. Comm.* 6 (2012) 95–106.
20. X.-D. Hou, personal correspondence, May 2013.
21. G. M. Kyureghyan and A. Pott, *Some theorems on planar mappings*, Proc. WAIFI 2008, J. von zur Gathen et al (eds), LNCS 5130, Springer, Berlin (2008) 117–122.
22. G. L. Mullen, Weak equivalence of functions over a finite field, *Acta Arith.* 35 (1979) 259–272.
23. K. T. Phelps, J. Rifà and M. Villanueva, Kernels and p-kernels of p^r-ary 1-perfect codes, *Des., Codes Cryptogr.*, 37 (2001) 243–261.
24. A. Pott, Nonlinear functions in abelian groups and relative difference sets, *Discr. Appl. Math.* 138 (2004) 177–193.
25. A. Pott and Y. Zhou, CCZ and EA equivalence between mappings over finite Abelian groups, *Des. Codes Cryptogr.* 66(1-3) (2013) 99–109.
26. J. Rifà, F. I. Solov'eva and M. Villanueva, Intersection of Hamming codes avoiding Hamming subcodes, *Des. Codes Cryptogr.* 62 (2012) 209–223.
27. E. Schulte-Geers, On CCZ-equivalence of addition mod 2^n, *Des. Codes Cryptogr.* 66(1-3) (2013) 111–127.
28. G. Weng, Y. Tan and G. Gong, On quadratic almost perfect nonlinear functions and their related algebraic object, CACR Tech. Report 18 (2013),
cacr.uwaterloo.ca/techreports/2013/cacr2013-18.pdf .
29. S. Yoshiara, Equivalences of quadratic APN functions, *J. Algebraic Combin.* 35 (2012) 461–475.