EA and CCZ equivalence of functions over GF (2n)

Horadam, Kathryn

https://researchrepository.rmit.edu.au/esploro/outputs/9921861000001341/filesAndLinks?institution=61RMIT_INST&index=null

Horadam, K. (2008). EA and CCZ equivalence of functions over GF (2n). Lecture Notes in Computer Science, 5130, 134–143. https://doi.org/10.1007/978-3-540-69499-1_12
Document Version: Submitted Version

Published Version: https://doi.org/10.1007/978-3-540-69499-1_12

Repository homepage: <https://researchrepository.rmit.edu.au>
Copyright © 2008, Springer Berlin / Heidelberg
Downloaded On 2023/04/26 16:57:55 +1000

EA and CCZ equivalence of functions over $GF(2^n)$

K. J. Horadam

RMIT University, Melbourne, VIC 3001, Australia
kathy.horadam@rmit.edu.au

Abstract. EA-equivalence classes and the more general CCZ-equivalence classes of functions over $GF(2^n)$ each preserve APN and AB properties desirable for S-box functions. We show that they can be related to subsets $\mathbf{c}[T]$ and $\mathbf{g}[T]$ of equivalence classes $[T]$ of transversals, respectively, thus clarifying their relationship and providing a new approach to their study. We derive a formula which characterises when two CCZ-equivalent functions are EA-inequivalent.¹

Keywords: CCZ-equivalence, EA-equivalence, bundle, APN function.

1 Introduction

For functions $\phi : G \rightarrow N$ between groups, the subset $S_\phi = \{(\phi(x), x) : x \in G\}$ of $N \times G$ can be used as the underlying instrument for measuring the nonlinear behaviour of ϕ under several different measures of nonlinearity that are useful in cryptography and coding. Pott in [13] uses S_ϕ to extend the definition of maximal nonlinearity from the case $N = G = \mathbb{Z}_2^n$ to arbitrary finite abelian groups N and G , in terms of values taken by the group characters of $N \times G$ on S_ϕ . For abelian groups N and G for which $|N|$ divides $|G|$, results of Carlet and Ding [5] show the notions of perfect nonlinearity, bentness and Pott's maximal nonlinearity are equivalent. This generalises the corresponding relationships for functions defined on finite fields.

It remains very difficult to find and classify functions over finite fields that satisfy such desirable nonlinearity conditions, or to determine whether, once found, they are essentially new, that is, inequivalent in some sense to any of the functions already found. Several notions of equivalence exist (c.f. [7, Section 9.2.2]), but the most useful for Boolean functions appear to be *Carlet-Charpin-Zinoviev* (CCZ)-equivalence and *extended affine* (EA)-equivalence.

When $N = G = \mathbb{Z}_2^n$, S_ϕ is called the *graph*² of ϕ and is used to define CCZ-equivalence [4, 3], which partitions the set of functions into classes with the same nonlinearity and differential uniformity [4, Proposition 3], [3, Proposition 2], but not necessarily the same algebraic degree. EA-equivalent functions have the same

¹ The published version of this corrected preprint appears in *LNCS* 5130 (2008) 134–143.

² In [2–4], $\{(x, \phi(x)) : x \in G\}$ is called the graph of ϕ but we swap coordinates for consistency with [13, 6, 7], without loss of generality.

nonlinearity, differential uniformity and, for functions of algebraic degree ≥ 2 , the same algebraic degree (see [2] for more details).

It is known [4] that EA-equivalence is a particular case of CCZ-equivalence, and that any permutation is CCZ-equivalent to its inverse. In [2], Budaghyan uses the inverse transformation to derive *almost perfect nonlinear* (APN) functions that are EA-inequivalent to any power function, giving the simplest method to construct such functions. Brinkmann and Leander [1] use backtrack programming to classify all the APN functions in dimensions $n = 4$ and $n = 5$. Over $GF(16)$ there is only one CCZ-equivalence class of APN functions, which consists of 2 EA-equivalence classes. Over $GF(32)$ there are 3 CCZ-equivalence classes of APN functions, containing respectively 3, 3 and 1 (for a total of 7) EA-equivalence classes.

However, no general description of how EA-inequivalent functions might partition a CCZ-class is known. This paper is a contribution to this problem.

As a subset of the group $E = N \times G$, the graph S_ϕ is a transversal of the normal subgroup $N \times \{1\}$; that is, it intersects each coset $N \times \{x\}$ of $N \times \{1\}$ in E in a single element. Therefore CCZ-equivalence classes should be related in some fashion to equivalence classes of transversals. In earlier work [6, 7], the author has related equivalence classes of normalised transversals to equivalence classes of normalised functions $\phi : G \rightarrow N$ (called *bundles* $\mathbf{b}(\phi)$) using the theory of group extensions. When $N = G = \mathbb{Z}_2^n$, the bundle equivalence relation between normalised functions $\phi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ differs slightly from EA-equivalence, but the author's *affine bundle* $\hat{\mathbf{b}}(\phi)$ is identical to the EA-equivalence class of ϕ [10, Lemma 1].

Here, restriction to *normalised* functions $\phi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ allows us to define a *canonical* transversal T_ϕ and its equivalence class $[T_\phi]$. Inside $[T_\phi]$ is a *canonical* equivalence class $\mathbf{c}[T_\phi]$ of transversals corresponding to the bundle $\mathbf{b}(\phi)$ (Corollary 2). Consideration of the relationship of T_ϕ to its underlying graph S_ϕ leads to the definition of a *graph* class $\mathbf{g}[T_\phi]$ of transversals with $\mathbf{c}[T_\phi] \subseteq \mathbf{g}[T_\phi] \subseteq [T_\phi]$. We introduce the *graph bundle* $\mathcal{B}(\phi)$ of ϕ and show that $\mathbf{b}(\phi) \subseteq \mathcal{B}(\phi)$ (Corollary 2). We relate $\mathcal{B}(\phi)$ to the graph class $\mathbf{g}[T_\phi]$ (Theorem 1), obtaining a version of [3, Proposition 1].

The equivalence relation induced by the $\mathcal{B}(\phi)$ coincides with CCZ-equivalence for normalised functions, and the *affine graph bundle* $\hat{\mathcal{B}}(\phi)$ containing all translates of functions in $\mathcal{B}(\phi)$ is identical to the CCZ-equivalence class containing ϕ (Lemma 2).

Next (Theorem 3 and Lemma 5) we show that $\varphi \in \mathcal{B}(\phi)$ if and only if there exists $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$, $s \in \mathbb{Z}_2^n$, a monomorphism $\iota = (\iota_1, \iota_2) : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ and $\varphi^* \in \mathbf{b}(\phi)$ such that $(\varphi \cdot s) \circ \rho = \iota_1 \circ \varphi^*$ and $\rho = \iota_2 \circ \varphi^*$. In this formula, which characterises how functions in $\mathcal{B}(\phi)$ move away from $\mathbf{b}(\phi)$, the permutation ρ which specifies how a graph underlies a transversal T in $\mathbf{g}[T_\phi]$ seems to be more important than the subgroup $\iota(\mathbb{Z}_2^n)$ of which T is a transversal. In particular, if ρ is an automorphism, $\varphi \in \mathbf{b}(\phi)$ (Theorem 4). If ϕ is itself an automorphism then $\text{inv}(\phi) \in \mathbf{b}(\phi)$ (Example 2).

This gives a new approach to looking for EA-inequivalent APN and other highly nonlinear functions within CCZ equivalence classes as well as for CCZ-inequivalent functions.

The paper is organised as follows. In Section 2 we outline some basic results on graphs and transversals. In Section 3 we show how equivalence of graphs relates to equivalence of transversals and introduce graph classes and graph bundles. In Section 4 we use the theory of group extensions to derive the main results and clarify the relationships between EA and CCZ equivalence classes of normalised functions.

2 Transversals and Graphs

Let G and N be finite abelian groups, written multiplicatively. We denote by $C^1(G, N) = \{f : G \rightarrow N, f(1) = 1\}$ the set of all normalised functions from G to N . Any un-normalised f has a *normalisation* $f \cdot 1 \in C^1(G, N)$ given by $f \cdot 1(x) = f(1)^{-1}f(x)$. If f is normalised, then $f \cdot 1 = f$. For $a \in G$, define the *shift action* $f \cdot a$ of a on f by

$$(f \cdot a)(x) = f(a)^{-1}f(ax), \quad x \in G. \quad (1)$$

For any $a, b \in G$, $(f \cdot a) \cdot b = f \cdot (ab)$.

Denote the subgroup of normalised permutations of a group A by $\text{Sym}_1(A)$, the subgroup of automorphisms by $\text{Aut}(A)$ and the inverse of permutation ρ by $\text{inv}(\rho)$. For $\phi \in C^1(G, N)$, define $\partial\phi : G \times G \rightarrow N$ to be³

$$\partial\phi(x, y) = \phi(x)\phi(y)\phi(xy)^{-1}, \quad x, y \in G \quad (2)$$

which measures how much ϕ differs from a homomorphism.

If $N \xrightarrow{\iota} E \xrightarrow{\pi} G$ is an extension of N by G (that is, ι and π are group homomorphisms with $\ker \pi = \text{im } \iota$) then each section $t : G \rightarrow E$ of π (that is, a mapping such that $\pi(t(x)) = x$, $x \in G$) determines a transversal $T = \{t_x = t(x), x \in G\}$ of the normal subgroup $\iota(N)$ in E (that is, a set of coset representatives) and vice versa. Every element $e \in E$ has a unique representation as $e = \iota(a)t_x$ for $a \in N$ and $x \in G$. The transversal T is *normalised* if it intersects $\iota(N)$ in 1, or equivalently, if $t_1 = 1$.

For the extension $N \xrightarrow{\iota} N \times G \xrightarrow{\kappa} G$, with $\iota(a) = (a, 1)$ and $\kappa(a, x) = x$, and for each $\phi \in C^1(G, N)$, we will call

$$T_\phi = \{t_x = (\phi(x), x), x \in G\} \quad (3)$$

the *canonical transversal* of $\iota(N) = N \times \{1\}$ in $N \times G$ determined by ϕ . More generally, we study the set underlying T_ϕ .

³ Note that in [6, 7] the notation $\partial^{-1}\phi$ is used. The technical reasons for this are irrelevant to our purpose and here we write $\partial\phi$ for simplicity.

Definition 1. Let $f : G \rightarrow N$. The graph of f is the set $S_f = \{(f(x), x), x \in G\} \subset N \times G$. It is normalised if $f(1) = 1$.

This definition is consistent with notation in [13, 6, 7] and agrees with that in [3, p. 1143] for the case $G = N = (GF(2^n), +) \cong \mathbb{Z}_2^n$, provided we switch first and second components consistently. This can be done with no loss of generality.

The canonical transversal T_ϕ of $N \times \{1\}$ determined by $\phi \in C^1(G, N)$ in (3) has the graph S_ϕ as underlying set, and conversely, the graph S_ϕ of $\phi \in C^1(G, N)$ becomes the canonical transversal T_ϕ in (3) defined by the section $t : x \mapsto t_x = (\phi(x), x), x \in G$. If we know a set is a normalised transversal in $N \times G$, it is easy to identify when it is a translate of a normalised graph, since the translate has a restricted form and hence the translated graph is itself a graph.

Lemma 1. Suppose $N \xrightarrow{\iota} N \times G \xrightarrow{\pi} G$ is an extension and T is a normalised transversal of $\iota(N)$ in $N \times G$. Set $T = \{t_x = (\lambda(x), \rho(x)), x \in G\}$, where $\pi(t_x) = x$. The following are equivalent:

1. there exists $e \in N \times G$ such that T has the translate eS_ϕ of the graph S_ϕ of $\phi \in C^1(G, N)$ as underlying set;
2. there exists $s \in G$ such that T has the translate $(\phi(s), s)^{-1}S_\phi = S_{\phi \cdot s}$ of the graph S_ϕ of $\phi \in C^1(G, N)$ as underlying set;
3. $\rho \in \text{Sym}_1(G)$ and there exists $s \in G$ such that $\lambda = (\phi \cdot s) \circ \rho$. □

If, as in Lemma 1, T is a normalised transversal of $\iota(N)$ with underlying set $S_{\phi \cdot s}$ for $\phi \in C^1(G, N)$ and $s \in G$, we have $\rho \in \text{Sym}_1(G)$ such that $t_x = ((\phi \cdot s) \circ \rho(x), \rho(x)) = (\phi(s), s)^{-1}(\phi \circ (s\rho)(x), (s\rho)(x))$, for $x \in G$.

We represent T by

$$T_{\phi \cdot s}^\rho = \{t_x = ((\phi \cdot s) \circ \rho(x), \rho(x)), x \in G\}, \quad (4)$$

where $\pi(t_x) = x$, or, for brevity, by $(\iota, T_\varphi^\rho, \pi)$, where $\varphi = \phi \cdot s$. Some basic operations on such transversals $(\iota, T_\varphi^\rho, \pi)$ are listed next.

Corollary 1. Let $\varphi \in C^1(G, N)$, $\rho \in \text{Sym}_1(G)$, and let $(\iota, T_\varphi^\rho, \pi)$ be a transversal as above.

1. If $\sigma \in \text{Aut}(G)$, with inverse $\text{inv}(\sigma)$, then $(\iota, T_\varphi^{\rho \circ \sigma}, \text{inv}(\sigma) \circ \pi)$ is a transversal. In particular, if $\rho \in \text{Aut}(G)$ then $(\iota, T_\varphi^{\text{id}}, \rho \circ \pi)$ is a transversal.
2. If $\gamma \in \text{Aut}(N)$, then $(\iota \circ \gamma, T_\varphi^\rho, \pi)$ is a transversal.

3 Equivalence of Transversals and Graphs

With no loss of generality, we may restrict the study of equivalence of transversals, as defined next, to equivalence of normalised transversals.

Definition 2. Let T, T' be transversals of the isomorphic normal subgroups K, K' , respectively, in a group E . Define T and T' to be equivalent, written $T \sim T'$, if there exist $\alpha \in \text{Aut}(E)$ and $e \in E$ such that $\alpha(K) = K'$ and $eT' = \alpha(T)$, and isomorphic, written $T \cong T'$, if $T' = \alpha(T)$ (ie. $e = 1$). Denote the equivalence class of T by $[T]$.

From now on, we assume $G = N = \mathbb{Z}_2^n \cong (GF(2^n), +)$, written additively, and $E = \mathbb{Z}_2^n \times \mathbb{Z}_2^n = \mathbb{Z}_2^{2n}$.

We will focus on equivalence classes $[T_\phi]$ for $\phi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. However, $[T_\phi]$ will usually contain normalised transversals which are not graphs as well as those, such as T_ϕ itself, which are. Consequently, we isolate a subset of $[T_\phi]$ consisting of normalised transversals with (translates of) normalised graphs as underlying set, as well as a special subset containing the canonical transversals.

Definition 3. Let $\phi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. Define $\mathbf{c}[T_\phi] \subseteq \mathbf{g}[T_\phi] \subseteq [T_\phi]$ as follows.

The graph class $\mathbf{g}[T_\phi]$ of T_ϕ is the set of normalised transversals in $[T_\phi]$ which have a translate of a normalised graph as underlying set; that is, by Lemma 1,

$$\mathbf{g}[T_\phi] = \{T_{\varphi \cdot s}^\rho : T_{\varphi \cdot s}^\rho \sim T_\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n), s \in \mathbb{Z}_2^n, \rho \in \text{Sym}_1(\mathbb{Z}_2^n)\}.$$

The canonical class $\mathbf{c}[T_\phi]$ of T_ϕ is the set of canonical transversals in $[T_\phi]$; that is,

$$\mathbf{c}[T_\phi] = \{T_\varphi : T_\varphi \sim T_\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)\}.$$

By Corollary 1 it is possible that the graph class $\mathbf{g}[T_\phi]$ may contain transversals $(\iota, T_\phi^{\text{id}}, \pi)$ with exactly the same elements as the canonical transversal (ι, T_ϕ, κ) , that is, defined by the same section, which are transversal to some normal subgroup $\iota(N)$ different from $\iota(N) = \mathbb{Z}_2^n \times \{0\}$. An example to show that this does occur is given in [8].

We now introduce an equivalence relation on normalised functions which coincides with CCZ-equivalence by affine permutations. This permits us to relate CCZ and EA equivalence very naturally using transversals. Because this equivalence relation is defined for functions between arbitrary groups in [8], we use a different name.

Definition 4. Two functions $\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ are graph equivalent if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(S_\phi) = e + S_\varphi$. They are graph isomorphic if $\alpha(S_\phi) = S_\varphi$, ie. $e = 0$. Denote the graph equivalence class of ϕ by $\mathcal{B}(\phi)$ and term it the graph bundle of ϕ .

Two functions $f, f' : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ are affine graph equivalent if their normalisations $f \cdot 0, f' \cdot 0 \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ are graph equivalent; that is, if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(S_{f \cdot 0}) = e + S_{f' \cdot 0}$. Denote the affine graph equivalence class of f by $\widehat{\mathcal{B}}(f)$ and term it the affine graph bundle of f .

Because $S_f = (f(0), 0) + S_{f \cdot 0}$ we see that

$$f \in \widehat{\mathcal{B}}(f') \Leftrightarrow f \cdot 0 \in \mathcal{B}(f' \cdot 0), \quad (5)$$

so again, we may restrict to normalised functions with no loss of generality.

We now show that affine graph equivalence equals CCZ-equivalence (using the *affine* permutation definition of CCZ-equivalence in [3, Definition 1]). The *linear* permutation case of CCZ-equivalence corresponds to a particular case of affine graph equivalence, which for normalised functions is graph *isomorphism*.

Lemma 2. *Let $f, f' : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$. Then f is CCZ-equivalent to f' if and only if $\widehat{\mathcal{B}}(f) = \widehat{\mathcal{B}}(f')$.*

Proof. By (5), $f \in \widehat{\mathcal{B}}(f')$ if and only if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(S_f) = \alpha((f(0), 0)) + e - (f'(0), 0) + S_{f'}$ if and only if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e' \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(S_f) = e' + S_{f'}$ if and only if f is CCZ-equivalent to f' . Note $e' = 0$ if and only if $e = (f'(0), 0) - \alpha((f(0), 0))$. $\square$

Since a graph is always representable as a canonical transversal, we may describe graph equivalence in terms of graphs and transversals. The affine version of Theorem 1.1 is the extension of the characterisation [3, Proposition 1] of CCZ-equivalence from the linear permutation case to the affine permutation case.

Theorem 1. *Let $\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. Let S_ϕ, S_φ , be their respective graphs and let T_ϕ be the canonical transversal (3) determined by ϕ .*

1. $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$, $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ and $s \in \mathbb{Z}_2^n$ such that

$$\alpha(T_\phi) = T_{\varphi \cdot s}^\rho;$$

2. $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $s \in \mathbb{Z}_2^n$ and $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ such that $T_{\varphi \cdot s}^\rho \in \mathbf{g}[T_\phi]$.

Proof. 1. By definition, $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that the normalised transversal $\alpha(T_\phi)$ of $\alpha(\mathbb{Z}_2^n \times \{0\})$ (with underlying set $\alpha(S_\phi)$) has the translate $e + S_\varphi$ as underlying set. Then Lemma 1 applies.

2. By Part 1 and Lemma 1, if $\varphi \in \mathcal{B}(\phi)$ there exist $s \in \mathbb{Z}_2^n$ and $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ such that $T_{\varphi \cdot s}^\rho \cong T_\phi$, so $T_{\varphi \cdot s}^\rho \in \mathbf{g}[T_\phi]$. Conversely if there exist $s \in \mathbb{Z}_2^n$ and $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ such that $T_{\varphi \cdot s}^\rho \sim T_\phi$, then there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(T_\phi) = e + T_{\varphi \cdot s}^\rho$, so $\alpha(S_\phi) = e - (\varphi(s), s) + S_\varphi$ and $\varphi \in \mathcal{B}(\phi)$. $\square$

In the next section, we use the theory of group extensions to relate graph bundles $\mathcal{B}(\phi)$ to bundles $\mathbf{b}(\phi)$.

4 Transversals and Bundles

Transversals T are used in the theory of group extensions to define cocycles ψ_T according to the following standard construction. See [7] for further details.

Lemma 3. Suppose that $\mathbb{Z}_2^n \xrightarrow{\iota} \mathbb{Z}_2^n \times \mathbb{Z}_2^n \xrightarrow{\pi} \mathbb{Z}_2^n$ is an extension of $\mathbb{Z}_2^n$ by $\mathbb{Z}_2^n$ and let $T = \{t_x, x \in \mathbb{Z}_2^n : \pi(t_x) = x\}$ be a normalised transversal of $\iota(\mathbb{Z}_2^n)$ in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$. Then ψ_T defined by

$$\psi_T(x, y) = \iota^{-1}(t_x + t_y - t_{xy}), \quad (6)$$

for all $x, y \in \mathbb{Z}_2^n$, is a cocycle, and must be of the form $\partial\phi$ for some $\phi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. $\square$

The mapping from transversal to cocycle given in Lemma 3 is surjective. We illustrate this for the case at hand.

Lemma 4. Let $\phi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. Let T_ϕ in (3) be the canonical transversal. Then $\psi_{T_\phi} = \partial\phi$. $\square$

Equivalence of transversals determines a corresponding equivalence of cocycles.

Theorem 2. [7, Theorem 8.5] Let T and T' be normalised transversals in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n = E$ of the normal subgroups K and K' isomorphic to $\mathbb{Z}_2^n$, respectively, for which $E/K \cong E/K' \cong \mathbb{Z}_2^n$. Let $\psi_T = \partial\phi$, $\psi_{T'} = \partial\varphi$ be the corresponding cocycles of Lemma 3, respectively. The following are equivalent:

1. $T \sim T'$;
2. there exist $\gamma, \theta \in \text{Aut}(\mathbb{Z}_2^n)$ and $a \in \mathbb{Z}_2^n$ such that

$$\partial\varphi = \partial(\gamma \circ (\phi \cdot a) \circ \theta); \quad (7)$$

3. there exist $\gamma, \theta \in \text{Aut}(\mathbb{Z}_2^n)$, $a \in \mathbb{Z}_2^n$ and $\chi \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ such that

$$\varphi = (\gamma \circ (\phi \cdot a) \circ \theta) \chi. \quad \square$$

Equivalence classes of normalised functions $\phi : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ are defined using Theorem 2.3. These equivalence classes are termed bundles; that is, the **bundle** $\mathbf{b}(\phi)$ of ϕ is

$$\{(\gamma \circ (\phi \cdot a) \circ \theta) \chi : (\gamma, a, \theta, \chi) \in (\text{Aut}(\mathbb{Z}_2^n), \mathbb{Z}_2^n, \text{Aut}(\mathbb{Z}_2^n), \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n))\} \quad (8)$$

Bundles exactly characterise the canonical classes of transversals.

Corollary 2. Let $\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$.

1. [7, Theorem 9.22] $\mathbf{b}(\phi) = \mathbf{b}(\varphi) \Leftrightarrow \mathbf{c}[T_\phi] = \mathbf{c}[T_\varphi]$. Hence $\mathbf{c}[T_\phi] =$

$$\{T_{(\gamma \circ (\phi \cdot a) \circ \theta) \chi} : (\gamma, a, \theta, \chi) \in (\text{Aut}(\mathbb{Z}_2^n), \mathbb{Z}_2^n, \text{Aut}(\mathbb{Z}_2^n), \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n))\}. \quad (9)$$

2. $\mathbf{b}(\phi) \subseteq \mathcal{B}(\phi)$ so if $\mathbf{b}(\varphi) = \mathbf{b}(\phi)$ then $\mathcal{B}(\varphi) = \mathcal{B}(\phi)$ and $\mathbf{c}[T_\phi] = \mathbf{c}[T_\varphi] \subset \mathbf{g}[T_\varphi] \cap \mathbf{g}[T_\phi]$.

Proof. 1. By definition, $\mathbf{c}[T_\phi] = \mathbf{c}[T_\varphi] \Leftrightarrow T_\phi \sim T_\varphi$ which, by Lemma 4, Theorem 2 and (8), holds $\Leftrightarrow \mathbf{b}(\phi) = \mathbf{b}(\varphi)$.

2. By Part 1, if $\varphi \in \mathbf{b}(\phi)$, $T_\phi \sim T_\varphi$ and by Definition 2 there exist $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ and $e \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ such that $\alpha(\mathbb{Z}_2^n \times \{0\}) = \mathbb{Z}_2^n \times \{0\}$ and $\alpha(T_\phi) = e + T_\varphi$, so $\alpha(S_\phi) = e + S_\varphi$. By Definition 4, $\varphi \in \mathcal{B}(\phi)$. The rest follows by symmetry. $\square$

The affine bundle $\widehat{\mathbf{b}}(f)$ of $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ is

$$\widehat{\mathbf{b}}(f) = \{f' : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n, f' \cdot 0 \in \mathbf{b}(f \cdot 0)\}. \quad (10)$$

Example 1. [10, Lemma 1] The affine bundle $\widehat{\mathbf{b}}(f)$ of $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ equals the EA-equivalence class of f .

In general, the surjective mapping of Lemma 4 is not injective: more than one transversal will define the same cocycle. All transversals determining the same cocycle $\partial\phi$ as T_ϕ may be characterised, using Lemma 3.

Lemma 5. Let $\mathbb{Z}_2^n \xrightarrow{\iota} \mathbb{Z}_2^n \times \mathbb{Z}_2^n \xrightarrow{\pi} \mathbb{Z}_2^n$ be an extension of $\mathbb{Z}_2^n$ by $\mathbb{Z}_2^n$. Let $T = \{t_x, x \in \mathbb{Z}_2^n\}$ with $\pi(t_x) = x$ be a normalised transversal in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ of the normal subgroup $K = \iota(\mathbb{Z}_2^n)$, with corresponding cocycle ψ_T . Set $\iota(n) = (\iota_1(n), \iota_2(n))$, $n \in \mathbb{Z}_2^n$, for $\iota_1, \iota_2 \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$, and $t_x = (\lambda(x), \rho(x))$, $x \in \mathbb{Z}_2^n$ for $\lambda, \rho \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. Let $\phi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$.

Then $\psi_T = \partial\phi$ if and only if there exists $\chi = (\chi_1, \chi_2) \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ such that

$$\lambda = \iota_1 \circ \phi + \chi_1, \quad \rho = \iota_2 \circ \phi + \chi_2. \quad (11)$$

In particular, if $\varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$, $s \in \mathbb{Z}_2^n$ and $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$, $\psi_{T_{\varphi \cdot s}} = \partial\phi$ if and only if there exists $\chi = (\chi_1, \chi_2) \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ such that

$$(\varphi \cdot s) \circ \rho = \iota_1 \circ \phi + \chi_1, \quad \rho = \iota_2 \circ \phi + \chi_2. \quad (12)$$

Proof. Note $\iota_1(\mathbb{Z}_2^n)$, $\iota_2(\mathbb{Z}_2^n)$ are subgroups of $\mathbb{Z}_2^n$. Application of Lemma 3 is straightforward:

$$\begin{aligned} \iota(\psi_T(x, y)) &= t_x + t_y - t_{xy} \\ &= (\lambda(x) + \lambda(y) - \lambda(xy), \rho(x) + \rho(y) - \rho(xy)) \\ &= (\partial\lambda(x, y), \partial\rho(x, y)) \end{aligned}$$

by (2), so $\psi_T = \partial\phi \Leftrightarrow \iota \circ \psi_T = \iota \circ \partial\phi \Leftrightarrow (\partial\lambda, \partial\rho) = (\iota_1 \circ \partial\phi, \iota_2 \circ \partial\phi) \Leftrightarrow (\partial\lambda, \partial\rho) = (\partial(\iota_1 \circ \phi), \partial(\iota_2 \circ \phi))$, because ι_1 and ι_2 are homomorphisms. $\square$

Next we relate bundles and graph bundles. If S_φ is a transversal T in $[T_\phi]$ this DOES NOT necessarily imply $\varphi \in \mathbf{b}(\phi)$ (though this can be true). Nor does it imply that $\psi_T = \partial\varphi$, though again, this may be true. To combine Theorem 2 with Theorem 1 we need the case $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ of Lemma 5.

Theorem 3. Let $\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$. Then $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$, $s \in \mathbb{Z}_2^n$, $\theta, \gamma \in \text{Aut}(\mathbb{Z}_2^n)$ and $\chi \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ such that

$$\psi_{T_{\varphi \cdot s}^\rho} = \partial\varphi^* \quad (13)$$

for

$$\varphi^* = (\gamma \circ \phi \circ \theta) + \chi.$$

Proof. By Theorem 2, $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ and $s \in \mathbb{Z}_2^n$ such that $T_{\varphi \cdot s}^\rho \cong T_\phi$, if and only if (by Lemma 4 and Theorem 2 with $e = 0$) there exist $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$, $s \in \mathbb{Z}_2^n$, $\theta \in \text{Aut}(\mathbb{Z}_2^n)$, $\gamma \in \text{Aut}(\mathbb{Z}_2^n)$ and $\chi \in \text{Hom}(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ such that $\psi_{T_{\varphi \cdot s}^\rho} = \partial\varphi^*$ where $\varphi^* = (\gamma \circ \phi \circ \theta) + \chi$. $\square$

From Theorem 3 and Lemma 5 we see that $\varphi \in \mathcal{B}(\phi)$ if and only if there exist $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$, $s \in \mathbb{Z}_2^n$, homomorphisms $\iota = (\iota_1, \iota_2), \chi = (\chi_1, \chi_2) : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ with ι a monomorphism and $\varphi^* \in \mathbf{b}(\phi)$ such that $(\varphi \cdot s) \circ \rho = \iota_1 \circ \varphi^* + \chi_1$ and $\rho = \iota_2 \circ \varphi^* + \chi_2$.

An important example is the case $\rho \in \text{Aut}(\mathbb{Z}_2^n)$.

Theorem 4. Let $\phi, \varphi \in C^1(\mathbb{Z}_2^n, \mathbb{Z}_2^n)$ and $\varphi \in \mathcal{B}(\phi)$. If there exist $\rho \in \text{Aut}(\mathbb{Z}_2^n)$ and $s \in \mathbb{Z}_2^n$ such that $T_{\varphi \cdot s}^\rho \cong T_\phi$ then $\varphi \in \mathbf{b}(\phi)$.

Proof. If $T_{\varphi \cdot s}^\rho \cong T_\phi$, there exists $\alpha \in \text{Aut}(\mathbb{Z}_2^n \times \mathbb{Z}_2^n)$ such that $T_{\varphi \cdot s}^\rho = \alpha(T_\phi)$ is a normalised transversal of $\alpha \circ \iota(\mathbb{Z}_2^n)$, where $\alpha(t_x) = ((\varphi \cdot s) \circ \rho(x), \rho(x))$ for $t_x \in T_\phi$. By Lemma 3, $\alpha \circ \iota(\psi_{T_{\varphi \cdot s}^\rho}(x, y)) = \alpha \circ \iota(\partial\phi(x, y))$; that is, $\psi_{T_{\varphi \cdot s}^\rho} = \partial\phi$. Let $J = (\mathbb{Z}_2^n \times \{0\}) \cap \alpha(\mathbb{Z}_2^n \times \{0\})$, so α restricted to J is an automorphism which extends to an automorphism of $\mathbb{Z}_2^n \times \{0\}$. Thus there is a $\gamma \in \text{Aut}(\mathbb{Z}_2^n)$ such that $\alpha \circ \iota = \iota \circ \gamma$ on J . Because ρ is a homomorphism, $\alpha \circ \iota(\psi_{T_{\varphi \cdot s}^\rho}(x, y)) = (\partial((\varphi \cdot s) \circ \rho)(x, y), 0) = \iota(\partial((\varphi \cdot s) \circ \rho)(x, y)) = \iota \circ \gamma(\partial\phi(x, y))$. Therefore $\partial((\varphi \cdot s) \circ \rho) = \partial(\gamma \circ \phi)$. By Theorem 2, $\varphi \in \mathbf{b}(\phi)$. $\square$

In [7, Corollary 9.23], the author claimed incorrectly that a normalised permutation and its inverse lie in the same bundle. For instance, a Gold power function $\phi(x) = x^{2^t+1}, (i, n) = 1$, over $G = (GF(2^n), +)$, n odd, has algebraic degree 2, so is not itself affine, and thus all functions in its bundle have algebraic degree 2 [3, p. 1142]. However its inverse has algebraic degree $(n+1)/2$ [11]. Instead, a normalised permutation and its inverse lie in the same graph bundle.

Example 2. Let $\phi \in \text{Sym}_1(\mathbb{Z}_2^n)$ have inverse $\text{inv}(\phi)$. Then

1. $\mathcal{B}(\text{inv}(\phi)) = \mathcal{B}(\phi)$;
2. if $\phi \in \text{Aut}(\mathbb{Z}_2^n)$, $\mathbf{b}(\phi) = \mathbf{b}(\text{inv}(\phi))$.

Proof. 1. Consider the extension $\mathbb{Z}_2^n \xrightarrow{\iota} \mathbb{Z}_2^n \times \mathbb{Z}_2^n \xrightarrow{\pi} \mathbb{Z}_2^n$, with $\iota(y) = (0, y)$ and $\pi((x, y)) = x$. The transversal $T = \{t_x^\phi = (x, \phi(x)), x \in \mathbb{Z}_2^n\}$ with $\pi(t_x^\phi) = x$ of $\{0\} \times \mathbb{Z}_2^n$ in $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ is $T_{\text{inv}(\phi)}^\phi$ by (4), and $\psi_T = \partial\phi$, by Lemma 3. Since $\phi \in \mathbf{b}(\phi)$ the result follows from Theorem 3 on setting $\varphi^* = \rho = \phi$ and $\varphi = \text{inv}(\phi)$.

2. If $\phi \in \text{Aut}(\mathbb{Z}_2^n)$, $\text{inv}(\phi) = \text{inv}(\phi) \circ \phi \circ \text{inv}(\phi)$ satisfies (8). $\square$

In order to identify the way in which $\mathcal{B}(\phi)$ partitions into bundles (see Corollary 2) we must first isolate the $\rho \in \text{Sym}_1(\mathbb{Z}_2^n)$ and $\varphi \in \mathcal{B}(\phi)$ such that $\varphi \in \mathbf{b}(\phi)$. By Theorem 4 the set of such ρ includes $\text{Aut}(\mathbb{Z}_2^n)$. We conclude that it is the set of permutations ρ for which there is a transversal $T_{\varphi \cdot s}^\rho$ which is the key to these problems, rather than the way in which automorphisms of $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ act on the subgroup $\mathbb{Z}_2^n \times \{0\}$.

Acknowledgements

The author is very grateful to Claude Carlet, Lilya Budaghyan and Alex Pott for numerous conversations and insightful comments which helped clarify her understanding of EA and CCZ equivalence, and correct errors in earlier publications [6, 7, 9]. She is also grateful to Pascale Charpin and the hospitality of INRIA, where this work was initiated. Finally she is grateful to the three anonymous referees whose comments much improved the clarity and motivation of the exposition.

References

1. M. Brinkmann and G. Leander, On the classification of APN functions up to dimension 5, in *Proc. International Workshop on Coding and Cryptography*, eds. D. Augot, N. Sendrier and J.-P. Tillich, Versailles, France, 2007, 39–58.
2. L. Budaghyan, The simplest method for constructing APN polynomials EA-inequivalent to power functions, *Proc. WAIFI 2007*, LNCS 4547, Springer, Berlin 2007, 177–188.
3. 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.
4. C. Carlet, P. Charpin and V. Zinoviev, Codes, bent functions and permutations suitable for DES-like cryptosystems, *Des. Codes Cryptogr.* 15 (1998) 125–156.
5. C. Carlet and C. Ding, Highly nonlinear mappings, *J. Complexity* 20 (2004) 205–244.
6. K. J. Horadam, A theory of highly nonlinear functions, *AAECC-16*, M. Fossorier et al., eds., LNCS 3857, Springer, Berlin, 2006, 87–100.
7. K. J. Horadam, *Hadamard Matrices and Their Applications*, Princeton University Press, Princeton, NJ 2007.
8. K. J. Horadam, Transversals, graphs and bundles of functions, in preparation.
9. K. J. Horadam and D. G. Farmer, Bundles, presemifields and nonlinear functions, extended abstract in *Proc. International Workshop on Coding and Cryptography*, eds. D. Augot, N. Sendrier and J.-P. Tillich, Versailles, France, 2007, 197–206.
10. K. J. Horadam and D. G. Farmer, Bundles, presemifields and nonlinear functions, *Des., Codes Cryptogr.*, 2008, to appear, DOI 10.1007/s10623-008-9172-z.
11. K. Nyberg, Differentially uniform mappings for cryptography, *EUROCRYPT-93*, LNCS 765, Springer, New York, 1994, 55–64.
12. A. Pott, A survey on relative difference sets, *Groups, Difference Sets and the Monster*, de Gruyter, New York, 1996, 195–232.
13. A. Pott, Nonlinear functions in abelian groups and relative difference sets, *Discr. Appl. Math.* 138 (2004) 177–193.