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 $c[T]$ and $g[T]$ 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.

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 $\phi$ under several different measures of nonlinearity that are useful in cryptography and coding. Pott in [13] uses $S_\phi$ 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 $S_\phi$. 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 $N = G = \mathbb{Z}_2^n$, $S_\phi$ is called the graph $\mathcal{G}_\phi$ of $\phi$ and is used to define CCZ-equivalence [4], 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 In [23], $\{(x, \phi(x)) : x \in G\}$ is called the graph of $\phi$ but we swap coordinates for consistency with [13,6,7], without loss of generality.
nonlinearity, differential uniformity and, for functions of algebraic degree \( \geq 2 \), 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 \( S_\phi \) 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 \( \phi : G \to N \) (called bundles \( b(\phi) \)) using the theory of group extensions. When \( N = G = \mathbb{Z}_n^2 \), the bundle equivalence relation between normalised functions \( \phi : \mathbb{Z}_2^n \to \mathbb{Z}_2^n \) differs slightly from EA-equivalence, but the author’s affine bundle \( \hat{b}(\phi) \) is identical to the EA-equivalence class of \( \phi \) [10, Lemma 1].

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

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

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