CCZ and EA Equivalence between Mappings over Finite Abelian Groups

Alexander Pott, Yue Zhou

CCZ and EA Equivalence between Mappings over Finite Abelian Groups

Alexander Pott[1] and Yue Zhou[1,2]

[1] Faculty of Mathematics, Otto-von-Guericke-University Magdeburg, 39106 Magdeburg, Germany
[2] Department of Mathematics and System Sciences, Science College, National University of Defense Technology, 410073 Changsha, P.R.China
alexander.pott@ovgu.de,yue.zhou@st.ovgu.de

Abstract. CCZ- and EA-equivalence, which are originally defined for vectorial Boolean functions, are extended to mappings between finite abelian groups G and H. We obtain an extension theorem for CCZ-equivalent but not EA-equivalent mappings. Recent results in [1] are improved and generalized.

Keywords: Abelian groups; Extended affine equivalence; Carlet-Charpin-Zinoviev equivalence

1 Introduction

In [6], Carlet, Charpin and Zinoviev introduced an equivalence relation, as a generalization of the *extended affine equivalence*, on the set of vectorial Boolean functions used as S-boxes in cryptosystems. Later, in [2] this equivalence is named after these three authors, and abbreviated to CCZ-equivalence. In [2], Budaghyan, Carlet and Pott proved that CCZ-equivalence is strictly more general than EA-equivalence , by exhibiting APN functions which are CCZ-equivalent to the APN function $F(x) = x^3$ on $\mathbb{F}_{2^n}$, but which are provably EA-inequivalent to it and (for n odd) to its inverse (for APN functions, see the recent survey [5]). In [1] and [3], Budaghyan, Carlet and Helleseth further proved:

Result 1 *Let p be a prime and n be a positive integer. Two functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_2$ are CCZ-equivalent if and only if they are EA-equivalent;*

Result 2 *Let p be a prime, and*

$$C = \begin{cases} 6, \, p = 2; \\ 3, \, \textit{otherwise.} \end{cases}$$

Let $n \geq C$ and $k > 1$ be the smallest divisor of n. Then for any $m \geq k$, the CCZ-equivalence of functions from $\mathbb{F}_{p^n}$ to $\mathbb{F}_{p^m}$, is strictly more general than their EA-equivalence.

In this paper, we generalize CCZ-and EA-equivalence to the mappings between finite abelian groups G and H, and consider whether CCZ-equivalence coincide with EA-equivalence for given G and H. Our results cover Result 1, and improve Result 2: we do not need the smallest divisor condition. This paper shows that the problems about the connection between CCZ and EA equivalence of functions $f : G \to H$ are related to the automorphisms of $G \times H$ and have nothing to do with the finite field or vector space structure of $\mathbb{F}_p^n$. The purpose of this presentation is to show how to extend the CCZ and EA concept to finite abelian groups.

Let f be a mapping from G to H, we call the set $\mathcal{G}_f = \{(x, f(x))|x \in G\} \subseteq G \times H$ the *graph* of f . We can generalize CCZ- and EA-equivalence to mappings between groups.

Definition 1. *Let f and g be two mappings from G to H, where G and H are abelian groups. Then f and g are called CCZ-equivalent, if there exists $\varphi \in \mathrm{Aut}(G \times H)$ and $c \in G \times H$, such that*

$$\varphi(\mathcal{G}_f) = \mathcal{G}_g + c.$$

Furthermore, f and g are called extended affine equivalent, which is abbreviated to EA-equivalent, if φ fixes $\{(0, y)|y \in H\}$, i.e., there exist $\varphi_1 \in \mathrm{Aut}(G)$, $\varphi_2 \in \mathrm{Aut}(H)$, $c_1 \in G$, $c_2 \in H$ and $\psi \in \mathrm{Hom}(G, H)$, such that

$$g(x) = \varphi_2(f(\varphi_1(x) + c_1)) + \psi(x) + c_2.$$

If we take G and H to be linear spaces over $\mathbb{F}_2$, then it is easy to see that the definition of CCZ-equivalence (EA-equivalence) above coincides with the original one defined between vectorial Boolean functions. For any automorphism $\varphi \in \mathrm{Aut}(G \times H)$, if $\varphi(\mathcal{G}_f)$ is the graph of some mapping from G to H, then we call φ a CCZ-transformation of f, and we define $\mathrm{CCZ}(f) = \{g \mid \varphi(\mathcal{G}_f) = \mathcal{G}_g\}$, namely the mappings from G to H obtained by CCZ-transformations of f on $\mathcal{G}_f$. Furthermore, if φ fix $\{(0, y)|y \in H\}$, then we call φ an extended affine transformation (EA-transformation) of f, and we define $\mathrm{EA}(f) = \{g \mid \varphi(\mathcal{G}_f) = \mathcal{G}_g, \varphi(0, H) = (0, H)\}$. It is pointed out that CCZ equivalence preserves linear and differential properties of functions for the case of abelian groups as well, see Remark 1 of [2], and [7], [10].

Obviously, for any mapping f between two finite abelian groups G and H, $\mathrm{CCZ}(f) \supseteq \mathrm{EA}(f)$. However, for some cases, they are the same. For example,

- $f(x) = \psi(x) + a$, where $\psi \in \mathrm{Hom}(G, H)$ and $a \in H$;
- f is a planar function over a finite field with odd characteristic, see [9];
- As a generalization of the previous example, let $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, and all its derivatives are surjective, see [4].

Therefore, it is natural to ask, for given abelian groups G and H, whether there is a mapping $f : G \to H$, such that $\mathrm{CCZ}(f) \neq \mathrm{EA}(f)$. Obviously when $\gcd(|G|, |H|) = 1$, any $\varphi \in \mathrm{Aut}(G \times H)$ always fixes H, hence CCZ-equivalence coincides with EA-equivalence. Result 1 is another example. On the other hand,

we expected that for most pairs of abelian groups (G, H) with $\gcd(|G|, |H|) \neq 1$, there always exists mappings $f, g : G \to H$, such that f and g are CCZ-equivalent but not EA-equivalent, for example:

- $f, g : \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ defined by

$$f = \begin{pmatrix} 0\,1\,2\,3 \\ 0\,0\,1\,1 \end{pmatrix}, \quad g = \begin{pmatrix} 0\,1\,2\,3 \\ 0\,1\,0\,1 \end{pmatrix};$$

- Let n be an integer strictly greater than 8, and let mappings f and g be defined from $\mathbb{Z}/n\mathbb{Z}$ to itself as follows:

$$f : \begin{pmatrix} 0\,1\,2 & 3 & 4 \cdots & n-2 & n-1 \\ 2\,0\,1 & -3 & 0 \cdots & 0 & 0 \end{pmatrix},$$

$$g : \begin{pmatrix} 0 & 1\,2\,3\,4 \cdots & n-2 & n-1 \\ -3 & 0\,2\,1\,0 \cdots & 0 & 0 \end{pmatrix}.$$

It is just elementary calculation to prove that the two examples above are CCZ but not EA-equivalent. Furthermore, for $n = 6, 8$, similar pairs of (f, g) can also be found. Moreover, for $n = 3,\ 5,\ 7$, we used MAGMA for an exhaustive search, and it showed that for any mapping $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, we have $\mathrm{CCZ}(f) = \mathrm{EA}(f)$.

The organization of this paper is as follows: In next section, we show how to "extend" mappings $f, g : G \to H$ which are CCZ-equivalent but not EA-equivalent to mappings $f', g' : G \times K \to H \times L$. As a corollary, Result 2 is improved. In section 3, we consider $H = \mathbb{Z}/2\mathbb{Z}$. Finally, we give the conclusions.

2 Extension Theorem

Our goal of this section is to prove the Extension Theorem as follows:

Theorem 1. *Let G, H, G' and H' be finite abelian groups, and $G' = G \times K$, $H' = H \times L$. Assume that $f, g : G \to H$ are CCZ-equivalent, but not EA-equivalent. Then there exist mappings $f', g' : G' \to H'$, which are CCZ-equivalent, but not EA-equivalent.*

The following two lemmas are about how to get CCZ-equivalent but EA-inequivalent mappings from G to H, by using some known mappings defined on two subgroups of G and H.

Lemma 1. *Let H, G and K be finite abelian groups, and $G' = G \times K$. Assume that mappings $f, g : G \to H$ are CCZ-equivalent, but not EA-equivalent.*

Then the mappings $\bar{f}, \bar{g} : G' \to H$, which are defined as

$$\bar{f}(x, y) = f(x),$$

$$\bar{g}(x, y) = g(x)$$

for any $(x, y) \in G \times K$, are CCZ-equivalent, but not EA-equivalent.

Proof. First, let us assume that G can not be expressed as a nontrivial direct product $M \times N$, such that, for $u \in M, v \in N$, $f(u,v)$ and $g(u,v)$ are EA-equivalent to some functions f' and g' respectively, which only depend on u. Otherwise, when the above f' and g' exist, then we can consider the extension of $f', g' : M \to H$ to $M \times (N \times K) \to H$ directly.

By the definition of CCZ-equivalence, there are some $\psi \in \mathrm{Aut}(G \times H)$ and $c \in G \times H$, such that

$$\psi(\mathcal{G}_f) = \mathcal{G}_g + c.$$

Since there always exists some $\bar{\psi} \in \mathrm{Aut}(G' \times H)$, such that $\bar{\psi}|_{G \times H} = \psi$, we have

$$\bar{\psi}(\mathcal{G}_{\bar{f}}) = \mathcal{G}_{\bar{g}} + c.$$

which means $\bar{f}$ is CCZ-equivalent to $\bar{g}$.

Without loss of generality, we assume that $f(0) = g(0) = 0$. Assume that $\bar{f}$ and $\bar{g}$ are EA-equivalent, then there exist $\bar{\varphi}_1 \in \mathrm{Aut}(G')$, $\varphi_2 \in \mathrm{Aut}(H)$, $\bar{\psi}_1 \in \mathrm{Hom}(G, H)$, $\bar{\psi}_2 \in \mathrm{Hom}(K, H)$, $\bar{a} \in G'$ and $b \in H$, such that

$$g(x) = \bar{g}(x,y) = \varphi_2 \circ \bar{f}(\bar{\varphi}_1(x,y) + \bar{a}) + \bar{\psi}_1(x) + \bar{\psi}_2(y) + b, \tag{1}$$

for any $(x,y) \in G'$. Denote $\bar{\varphi}_1(x,y)$ as $(\bar{\varphi}_1^{(1)}(x,y), \bar{\varphi}_1^{(2)}(x,y))$, for any different $y_1, y_2 \in K$, by (1) we have

$$f(\bar{\varphi}_1^{(1)}(x,y_1) + a) - f(\bar{\varphi}_1^{(1)}(x,y_2) + a) = \varphi_2^{-1} \circ \bar{\psi}_2(y_2 - y_1)\ , \tag{2}$$

where a is the G-component of $\bar{a} \in G \times K$.

Furthermore, denote $\bar{\varphi}_1^{(1)}(x,y) = \nu(x) + \omega(y)$, where $\nu \in \mathrm{Hom}(G,G)$ and $\omega \in \mathrm{Hom}(K,G)$. According to the definition of $\bar{f}$, we have

$$\bar{f}(\bar{\varphi}_1^{(1)}(x,y), \bar{\varphi}_1^{(2)}(x,y)) = f(\bar{\varphi}_1^{(1)}(x,y)) = f(\nu(x) + \omega(y))\ .$$

Therefore, when $y_1 = y$, $y_2 = 0$, (2) becomes

$$f(\nu(x) + \omega(y) + a) = f(\nu(x) + a) + L(y), \tag{3}$$

where $L = -\varphi_2^{-1} \circ \bar{\psi}_2 \in \mathrm{Hom}(K,H)$. Here ν can not be invertible, otherwise let $y = 0$ in (1), we have that f is EA-equivalent to g, which contradicts the assumption. Thus $\mathrm{Im}(\nu)$ and $\mathrm{Im}(\omega)$ contain subgroups M and $\{0\} \neq N \in G$ respectively, such that $G = M \times N$. By (3), f can be considered as

$$f(u + a_1, v + a_2) = f(u + a_1, a_2) + L'(v),$$

where $L' \in \mathrm{Hom}(N,H)$ and $a = (a_1, a_2) \in M \times N$ (L' is well-defined, since the value of $L(y)$ does not depend on y, but on $\omega(y)$.) Therefore, f is EA-equivalent to $f'(u + a_1, v + a_2) := f(u + a_1, a_2)$, whose value only depends on u. Simultaneously, since $g(x) = \varphi_2 \circ f(\nu(x) + a) + \bar{\psi}_1(x) + b$, g is also EA-equivalent to some function $g'(u,v)$ which only depends on the value of u. Hence, f and g contradict our assumption at the beginning of the proof. □

As a generalization of Proposition 2 for the binary fields case in [1], one can prove similar to [1]:

Lemma 2. *Let H, G and L be finite abelian groups, and $H' = H \times L$. If mappings $f, g : G \to H$ are CCZ-equivalent, but not EA-equivalent, then the mappings $\bar{f}, \bar{g} : G \to H'$, which are defined as,*

$$\bar{f}(x) = (f(x), 0),$$

$$\bar{g}(x) = (g(x), 0),$$

for any $x \in G$, are CCZ-equivalent, but not EA-equivalent.

By Lemma 1 and Lemma 2, we can easily prove Theorem 1. Furthermore, we can improve Result 2 as follows:

Corollary 1. *There exists mapping $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^m}$, such that $\mathrm{CCZ}(f) \neq \mathrm{EA}(f)$, in the following cases:*

- *$p = 2$, $\min\{n, m\} \geq 4$ or $n \geq 6$ together with $m \geq 2$;*
- *$p = 3$, $n \geq 4$ and $m > 1$ or $n = m = 3$;*
- *$p = 5, 7$, $n \geq 2$, $m \geq 1$;*
- *$p > 7$, n and $m \geq 1$.*

For $p = 2$, we use the mappings $f : \mathbb{F}_{2^n} \to \mathbb{F}_{2^m}$ with $\mathrm{CCZ}(f) \neq \mathrm{EA}(f)$, constructed in [1] when $n = m = 4$ or $n = 6$ together with $m = 2$, as a "start point" to do extension. Then the result follows.

For $p = 3$, we do not find any start point better than Result 2. But we do not need the "smallest divisor of n" anymore by Theorem 1

For $p = 5, 7$, we can construct some mapping from $(\mathbb{Z}/p\mathbb{Z})^2$ to $\mathbb{Z}/p\mathbb{Z}$, which will appear in the full version of this paper. Then by Theorem 1, the result follows.

For $p > 7$, the statement holds by Theorem 1 and the example listed at the end of Section 1 .

3 The case $H = \mathbb{Z}/2\mathbb{Z}$

It is well known that a finite abelian group is isomorphic to a product of cyclic groups by the fundamental theorem of finitely generated abelian groups. About the automorphism groups of finite abelian groups, the first complete characterization is contained in [11]. For an accessible and modern treatment, see [8] by Hillar and Rhea.

Let $H_p = \prod_{i=1}^{n} \mathbb{Z}/p^{e_i}\mathbb{Z}$, where p is a prime, $1 \leq e_1 \leq \cdots \leq e_n$. Let $\pi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}\mathbb{Z}$ be the standard quotient mapping $\pi_i(h) = \bar{h}$, and $\pi : \mathbb{Z}^n \to H_p$ be the homomorphism given by

$$\pi(h_1, \ldots, h_n) = (\pi_1(h_1), \ldots, \pi_n(h_n)) = (\bar{h}_1, \ldots, \bar{h}_n)$$

For convenience, sometimes we also use column vectors to express the element in H_p, especially when we interpret a homomorphism by a matrix as follows:

Lemma 3. *[8] Let the set R_p be defined as*

$$R_p = \{(a_{ij}) \in \mathbb{Z}^{n\times n} : p^{e_i - e_j} \text{ divides } a_{ij} \text{ for all } i,j \text{ satisfying } 1 \le j \le i \le n\}.$$

Then, the map $\psi : R_p \to End(H_p)$ given by

$$\psi(A)(\bar{h}_1, \ldots, \bar{h}_n)^T = \pi(A(h_1, \ldots, h_n)^T)$$

is a surjective ring homomorphism. Furthermore, an endomorphism $M = \psi(A)$ is an automorphism if and only if $(A \mod p) \in \mathrm{GL}_n(\mathbb{F}_p)$

The lemma above shows that there is a close connection between linear mappings and automorphisms of abelian p-groups. Since it seems more common to use column vectors, when linear mappings are expressed by matrices, we decided to use "column notation" in this section.

As we mentioned in the introduction, Budaghyan and Carlet recently proved that for n-variable Boolean functions, CCZ-equivalence coincides with EA-equivalence [1]. In this section, we will generalize this result to mappings from finite abelian groups to $\mathbb{Z}/2\mathbb{Z}$, using another proof method.

Theorem 2. *Let G be a finite abelian group, then there do not exist mappings $f, g : G \to \mathbb{Z}/2\mathbb{Z}$, such that f and g are CCZ-equivalent, but not EA-equivalent. In other words, for the mappings from G to $\mathbb{Z}/2\mathbb{Z}$, CCZ-equivalence coincides with EA-equivalence.*

Proof. Let f be a mapping from G to $\mathbb{Z}/2\mathbb{Z}$. For any CCZ-transformation of f, if we can prove that it can be expressed by the composition of several EA-transformations, then we prove the claim in the theorem.

Let μ be a CCZ-transformation of f, which can be expressed as

$$\mu \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \varphi_1(x) + \psi_1(y) \\ \varphi_2(x) + \psi_2(y) \end{pmatrix},$$

where $\varphi_1 \in \mathrm{Hom}(G, G)$, $\varphi_2 \in \mathrm{Hom}(G, \mathbb{Z}/2\mathbb{Z})$, $\psi_1 \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, G)$, and $\psi_2 \in \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$.

Next, we consider two cases depending on the invertibility of φ_1:

Case 1. If φ_1 is invertible, i.e. then we can define $\nu \in \mathrm{Aut}(G \times \mathbb{Z}/2\mathbb{Z})$ as $\nu(x, y)^T = (\varphi_1^{-1}(x), y - \varphi_2 \circ \varphi_1^{-1}(x))^T$. Then we have,

$$\nu \circ \mu \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + \varphi_1^{-1} \circ \psi_1(y) \\ \psi_2(y) - \varphi_2 \circ \varphi_1^{-1} \circ \psi_1(y) \end{pmatrix}.$$

Since $\nu \circ \mu$ is an automorphism, $\psi_2 - \varphi_2 \circ \varphi_1^{-1} \circ \psi_1$ is the identity automorphism of $\mathbb{Z}/2\mathbb{Z}$. Denoting $\varphi_1^{-1} \circ \psi_1$ by ψ, we have

$$\nu \circ \mu \begin{pmatrix} x \\ f(x) \end{pmatrix} = \begin{pmatrix} x + \psi(f(x)) \\ f(x) \end{pmatrix}.$$

If ψ is the zero homomorphism, then we have

$$\mu(x, f(x))^T = \nu^{-1}(x, f(x))^T,$$

which means that μ (the CCZ-transformation of f), can be achieved by an EA-transformation of f, since ν^{-1} is also an EA-transformation.

If ψ is not the zero homomorphism, then we denote $a = \psi(1)$, and obviously, $\mathrm{ord}(a) = 2$. For any $s \in G$, if $f(s) = 1$ and $s + a = t$, then $f(t) = 1$, otherwise, $x + \psi(f(x))$ will not be a permutation of G (consider the value of $x + \psi(f(x))$ for $x = s$ and $x = s + a$). Furthermore, $t + a = s$, since $\mathrm{ord}(a) = 2$. That means, by adding $\psi \circ f(x)$, we just permute the elements $\{s \in G | f(s) = 1\}$ in G, and the graph is still that of f. Therefore, we have

$$\nu \circ \mu(\mathcal{G}_f) = \mathcal{G}_f,$$

which means again that μ can be achieved by an EA-transformation of f, since ν^{-1} is also an EA-transformation.

Case 2. If $\varphi_1 \notin \mathrm{Aut}(G)$, i.e. φ_1 is not invertible, then we have $\mathrm{Im}(\psi_1) \cong \mathbb{Z}/2\mathbb{Z}$ and $G \cong \mathrm{Im}(\varphi_1) \times \mathrm{Im}(\psi_1)$, since $\mathbb{Z}/2\mathbb{Z}$ does not have a nontrivial subgroup.

First we assume that $|G|$ is a power of 2, and $G \cong \prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z})$, $1 = e_1 \leq e_2 \leq \cdots \leq e_n$. By Lemma 3 and choosing proper "basis" of G, μ corresponds to an $(n+1) \times (n+1)$ matrix $M \in R_2$, such that $(M \mod 2) \in \mathrm{GL}_{n+1}(\mathbb{F}_2)$, and

$$M = \left(\begin{array}{c|cccc} t_1 & t_2 & t_3 & \cdots & t_{n+1} \\ \hline 1 & 0 & 0 & \cdots & 0 \\ s_2 & m_{21} & m_{22} & \cdots & m_{2n} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ s_n & m_{n1} & m_{n2} & \cdots & m_{nn} \end{array}\right),$$

which acts on $\mathbb{Z}/2\mathbb{Z} \times \prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times G$. As M is in R_2, which can be naturally considered as an $(n+1) \times (n+1)$ matrix over $\mathbb{Z}/2^{e_n}\mathbb{Z}$, we can do the elementary linear operations as those for the matrix over a field. Fix the first row of M, after a series of elementary row operations without interchanging of row i and row j, with $e_i \neq e_j$, we can get

$$\left(\begin{array}{c|cccc} t_1 & t_2 & t_3 & \cdots & t_{n+1} \\ \hline 1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & a_n & & & 1 \end{array}\right),$$

where $a_i = 2^{e_i - 1}$ or $0 \mod 2^{e_i}$, for $2 \leq i \leq n$. Finally, subtracting the rows $2, \ldots, n+1$ from the first row, we get

$$N = \left(\begin{array}{c|cccc} 0 & 1 & 0 & \cdots & 0 \\ \hline 1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 1 & & \\ \vdots & \vdots & & \ddots & \\ 0 & a_n & & & 1 \end{array}\right),$$

since ($M \mod 2$) is invertible. Moreover, it is easy to see that all these linear operations from M to N can also be expressed as a matrix A, which corresponds to an automorphism of $\mathbb{Z}/2\mathbb{Z} \times G$, denoted by α. Furthermore, α is an EA-transformation, because all the elementary row operations we have applied above correspond to EA-transformations.

Let $x = (x_1, x_2, \cdots, x_n) \in \prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z})$, then we have

$$A \cdot M \begin{pmatrix} f(x) \\ x \end{pmatrix} = \begin{pmatrix} \frac{x_1}{f(x)} \\ x_2 + a_2 x_1 \\ \vdots \\ x_n + a_n x_1 \end{pmatrix},$$

which means that for fixed $x_i' = x_i + a_i x_1$ with $2 \leq i \leq n$, there must be $f(x) = x_1$ or $x_1 + 1$ to ensure that $\alpha \circ \mu$ is a CCZ-transformation. Notice that if $f(x) = x_1$, then

$$A \cdot M(1, 1, x_2, \cdots, x_n)^T = (1, 1, x_2', \cdots, x_n')^T$$
$$A \cdot M(0, 0, x_2, \cdots, x_n)^T = (0, 0, x_2', \cdots, x_n')^T$$

If $f(x) = x_1 + 1$, then

$$A \cdot M(0, 1, x_2, \cdots, x_n)^T = (1, 0, x_2', \cdots, x_n')^T$$
$$A \cdot M(1, 0, x_2, \cdots, x_n)^T = (0, 1, x_2', \cdots, x_n')^T$$

Thus it is not difficult to see that $A \cdot M(f(x), x)^T$ is just the graph of $(f(x), x')^T$ with $x' = (x_1, x_2', \cdots, x_n')$, which means that $\alpha \circ \mu$ is an EA-transformation of f. Since α is also an EA-transformation, we have $\mathrm{CCZ}(f) = \mathrm{EA}(f)$.

Now, let $G \cong K \times \prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z})$ with $|K|$ odd, and we denote the elements of G by (k, l), where $k \in K$ and $l \in \prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z})$. Since $|K|$ is odd, we can write μ as

$$\mu(k, l, f(k, l))^T = (\mu_1(k), \mu_2(l, f(k, l)))^T.$$

Let EA-transformation $\tau = (\mu_1^{-1}, \mathrm{id})$, then $\tau \circ \mu(k, l, f(k, l))^T = (k, \mu_2(l, f(k, l)))^T$. In the proof when G is a $2-$group, we see that the EA-transformation α and x' only depend on μ_2. Therefore, we can also find some $\alpha \in \mathrm{Aut}(\prod_{i=1}^{n}(\mathbb{Z}/2^{e_i}\mathbb{Z}))$ here, such that

$$(\mathrm{id}, \alpha) \circ \tau \circ \mu(k, l, f(k, l))^T = (k, l', f(k, l))^T,$$

which means that $(\mathrm{id}, \alpha) \circ \tau \circ \mu$ is an EA-transformation of f, hence $\mathrm{CCZ}(f) = \mathrm{EA}(f)$. □

4 Conclusions

In Theorem 1, we need the condition that the extension of G (or H) is splitting. Naturally, one question is: whether these splitting conditions are really needed? Namely,

Question 1. Let G, H, G' and H' be finite abelian groups, and $H \leq H'$, $G \leq G'$. Assume that $f, g : G \to H$ are CCZ-equivalent, but not EA-equivalent. Is it true that we can always find mappings $f', g' : G' \to H'$, which are CCZ-equivalent, but not EA-equivalent?

One difficulty to extend the proof of Theorem 1 is: if G' or H' is not a splitting extension of G or H respectively, then it is possible that some automorphism φ of $G \times H$ is not induced, i.e. $\varphi \neq \psi|_{G\times H}$, for any $\psi \in \mathrm{Aut}(G' \times H')$. Therefore, it is difficult to construct f', g' from f, g, such that f' and g' are also CCZ-equivalent.

Let G and H be finite abelian groups, and $\gcd(|G|, |H|) > 1$. For any mapping $f : G \to H$, if G or H satisfies the following conditions, then $\mathrm{CCZ}(f) = \mathrm{EA}(f)$:

1. $G = \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}$ or $(\mathbb{Z}/2\mathbb{Z})^2$;
2. $H = \mathbb{Z}/2\mathbb{Z}$;
3. $H = (\mathbb{Z}/2\mathbb{Z})^n \times L$ with $|L|$ odd, when $G = \mathbb{Z}/4\mathbb{Z}$.

The proof is not difficult. For all the mappings $f : \mathbb{Z}/3\mathbb{Z} \to H$, we can assume that $f(0) = 0$ without loss of generality (otherwise we can use EA-transformation to subtract $f(x)$ by $f(0)$). Furthermore any CCZ-transformation can only permute 1 and -1 in $\mathbb{Z}/3$, which can be also achieved by the unique non-identity automorphism of $\mathbb{Z}/3\mathbb{Z}$. Therefore, for any mapping here, CCZ-equivalence always coincides with EA-equivalence. It is the same for any $f : \mathbb{Z}/2\mathbb{Z} \to H$.

For $G = (\mathbb{Z}/2\mathbb{Z})^2$, any $f : G \to H$ can be written as

$$\left(\begin{array}{cccc} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ \hline 0 & h_1 & h_2 & h_3 \end{array}\right),$$

by assuming that $f(0) = 0$ as in case 1. For any CCZ-transformation, there are corresponding $\psi \in \mathrm{Hom}(H, G)$ and $\varphi \in \mathrm{Hom}(G, G)$, such that

$$\nu := ((0,0), \psi(h_1), \psi(h_2), \psi(h_3)) + ((0,0), \varphi(1,0), \varphi(0,1), \varphi(1,1))$$

which contains all the elements of G as its entries. However, there always exists $\gamma \in \mathrm{Aut}(G)$, such that

$$((0,0), \gamma(1,0), \gamma(0,1), \gamma(1,1)) = \nu,$$

since there are totally $3! = 6$ possible ν, and $|\mathrm{Aut}(G)|$ also equals 6.

Case 2 is just Theorem 2.

For any mapping f from $G = \mathbb{Z}/4\mathbb{Z}$ to $H = (\mathbb{Z}/2\mathbb{Z})^n \times L$ with $2 \nmid |L|$ and $f(0) = 0$, we should first notice that the CCZ-transformation of a given mapping f on it, could only permute 1 and 3 in G. However, $\mathrm{Aut}(G)$ also permute them in this way. Therefore $\mathrm{CCZ}(f) = \mathrm{EA}(f)$.

In fact, this list is not complete. For example, we can use computer to show that $\mathrm{CCZ}(f) = \mathrm{EA}(f)$ for any $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$. However, we expect that there are only finite pairs of (G, H) except for these three cases. This expectation is

based on experience working with CCZ and EA equivalence problems, and it is not based on computational data. An asymptotic version of this question can be written as:

Question 2. Let G and H be finite abelian groups, and $\gcd(|G|, |H|) > 1$. Is there an integer B, such that when $\max\{|G|, |H|\} \geq B$, there always exist CCZ-equivalent but EA-inequivalent mappings f, g from G to H, except for the 3 cases mentioned above.

Acknowledgements

We are grateful to an anonymous referee for the valuable comments on the proof of Theorem 2. The second author is partially supported by China Scholarship Counsel.

References

1. Lilya Budaghyan and Claude Carlet. CCZ-equivalence of single and multi-output Boolean functions. In *Post-proceedings of the 9-th International Conference on Finite Fields and Their Applications Fq'09*, volume 518 of *Contemporary Math.*, pages 43–54. AMS, 2010.
2. Lilya Budaghyan, Claude Carlet, and Alexander Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Transactions on Information Theory*, 52(3):1141–1152, 2006.
3. Lilya Budaghyan and Tor Helleseth. On isotopisms of commutative presemifields and ccz-equivalence of functions. Cryptology ePrint Archive, Report 2010/507, 2010. `http://eprint.iacr.org/`.
4. Lilya Budaghyan and Tor Helleseth. New commutative semifields defined by new pn multinomials. *Cryptography and Communications*, 3:1–16, 2011.
5. Claude Carlet. *Boolean Functions*, volume 2, chapter Vectorial Boolean functions for cryptography. Cambridge University Press, in press.
6. Claude Carlet, Pascale Charpin, and Victor Zinoviev. Codes, bent functions and permutations suitable for des-like cryptosystems. *Des. Codes Cryptography*, 15(2):125–156, 1998.
7. Claude Carlet and Cunsheng Ding. Highly nonlinear mappings. *J. Complexity*, 20(2-3):205–244, 2004.
8. Christopher J. Hillar and Darren Rhea. Automorphisms of finite abelian groups. http://arxiv.org/abs/math.GR/0605185, 2006.
9. Gohar M. Kyureghyan and Alexander Pott. Some theorems on planar mappings. In *WAIFI '08: Proceedings of the 2nd international workshop on Arithmetic of Finite Fields*, pages 117–122, Berlin, Heidelberg, 2008. Springer-Verlag.
10. Alexander Pott. Nonlinear functions in abelian groups and relative difference sets. *Discrete Applied Mathematics*, 138(1-2):177–193, 2004.
11. Arthur Ranum. The group of classes of congruent matrices with application to the group of isomorphisms of any abelian group. *Transactions of the American Mathematical Society*, 8(1):71–91, 1907.