Two New Measures for Permutations: Ambiguity and Deficiency

Daniel Panario, *Senior Member, IEEE,* Amin Sakzad, Brett Stevens, and Qiang Wang

***Abstract*—We introduce the concepts of weighted ambiguity and deficiency for a mapping between two finite Abelian groups of the same size. Then, we study the optimum lower bounds of these measures for permutations of an Abelian group. A construction of permutations, by modifying some permutation functions over finite fields, is given. Their ambiguity and deficiency is investigated; most of these functions are APN permutations. We show that, when they are not optimal, the Möbius function in the multiplicative group of $\mathbb{F}_q$ is closer to being *optimal* in ambiguity than the inverse function in the additive group of $\mathbb{F}_q$. We note that the inverse function over $\mathbb{F}_{2^8}$ is used in AES. Finally, we conclude that a twisted permutation polynomial of a finite field is again closer to being optimal in ambiguity than the APN function employed in the SAFER cryptosystem.**

***Index Terms*—Almost perfect non-linear (APN), permutation, Abelian group.**

I. Introduction

A permutation polynomial over a finite ring R induces a bijective map from R to R. In recent years, there has been considerable interest in studying permutation polynomials, partly due to their applications in coding theory, combinatorics and cryptography. We are interested in the finite field $\mathbb{F}_q$ or the integer ring $\mathbb{Z}_n$. For more background on permutation polynomials over finite fields we refer to Chapter 7 of [14]. For detailed surveys of open questions and results up to 1993 see [12], [13], [17]. For permutation polynomials over $\mathbb{Z}_n$ and $\mathbb{F}_q$, we refer the readers to [18], [21], [22], [23]. Polynomials over finite rings can be viewed as maps between finite rings, or between finite groups. This motivated us to study mappings between two finite Abelian groups of the same cardinality, in particular, bijective mappings.

Currently, substitution components called S-boxes are among the most popular tools for making a cryptosystem secure. The critical task of an S-box is to offer more confusion. This situation results in security. These S-boxes are based on Boolean functions [9]. For example, the SAFER cryptosystem introduced by Massey [15], uses S-boxes in its structure. Also the Advanced Encryption System (AES), proposed by Daemen and Rijmen in [5], employs an instance of an S-box to increase the amount of confusion.

D. Panario, B. Stevens and Q. Wang are with School of Mathematics and Statistics, Carleton University, Emails: {daniel,brett,wang}@math.carleton.ca

A. Sakzad is with the Department of Mathematics and Computer Science, Amirkabir University of Technology, Email: amin_sakzad@aut.ac.ir

The authors are partially supported by NSERC and the Ontario MRI.

Manuscript received ???? ??, ????; revised ????? ??, ????.

Differential cryptanalysis, which was initiated in [19], is one of the methods that can be used to attack S-boxes. Functions that have the best resistance to this type of cryptanalysis are called *Almost Perfect Non-linear (APN)*. Let $f : G_1 \to G_2$ be any map, or partial map, between two Abelian groups of the same sizes. For $a \in G_1$, $a \neq 0$, we can define a difference map

$$\Delta_{f,a}(x) = f(x + a) - f(x)$$

which measures the degree of "linearity" of f. The function f is called perfect non-linear (PN) if $\Delta_{f,a}$ is injective and almost perfect non-linear (APN) if $\Delta_{f,a}$ is at worst 2-to-1. These functions have received significant attention because of their resistance to linear cryptanalysis and differential cryptanalysis. In particular, we note that the APN functions 45^x and $\log_{45} x$ in $\mathbb{Z}_{256}$ were used in the SAFER cryptosystem [15]. In addition, AES uses the inverse function which is a differentially 4 uniform function (it means that $\Delta_{f,a}(x)$ is at worst 4-to-1) in $\mathbb{F}_{2^8}$ [5]; however, the inverse function is an APN function over some other fields.

One of the known measures for this resistance is *non-linearity* (see for example [1]). The non-linearity of a function is defined by the Fourier transform of that function. In this case, non-linearity is closely related to the selection of a "character" in its definition. For more precise information, we refer the reader to [9] and references therein. At the end of this article we calculate this measure for several of our functions and find correlations between these and our measures.

In this paper, we attempt to understand the injectivity and surjectivity of $\Delta_{f,a}$ when f is a bijection. This helps us to understand how close a bijection f is to being an APN function and how much better than 2-to-1 is $\Delta_{f,a}$. In Section II we define two generalized measures of injectivity and surjectivity of $\Delta_{f,a}$ which we call the *ambiguity* and the *deficiency* of f, respectively; this definition does not require f to be a bijection. When f is a bijection, we show these measures are invariant under certain affine transformations. Moreover, strong connections between permutations, Costas arrays and almost perfect non-linear functions are also explained in Section II. In Section III we prove bounds on these measures which then allow us to define notions of optimality with respect to them. This generalizes the results to arbitrary finite Abelian groups, where in [20] only $G_1 = G_2 = \mathbb{Z}_n$ is considered. In Section IV we study the ambiguity and deficiency of some permutations of the cyclic group $\mathbb{Z}_n$, where $n = p^m - 1$, or of the group $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, through exploiting several known permutation functions over finite fields. In the former case, we use permutation functions over finite fields

fixing 0 and discrete logarithms to construct two families of permutations of $\mathbb{Z}_n$ which achieve the optimum lower bounds. For the latter case, we show that optimal ambiguity and APN property are the same notion for permutations of finite fields of even characteristic. Moreover, we use SAGE [24], a free open-source mathematics software system, to computationally verify ambiguity and deficiency of several known APN permutations of finite fields when the characteristic is odd. In Section V we study how close an APN function is to being optimal in terms of ambiguity. The conclusion and further research topics are commented in Section VI.

II. Definitions and connections

A. Definitions

Let G_1 and G_2 be finite Abelian groups of the same cardinality n and $f : G_1 \to G_2$. Let $G_1^* = G_1 \setminus \{0\}$ and $G_2^* = G_2 \setminus \{0\}$. For any $a \in G_1^*$ and $b \in G_2$, we denote $\Delta_{f,a}(x) = f(x+a) - f(x)$ and $\lambda_{a,b}(f) = \#\Delta_{f,a}^{-1}(b)$. Let $\alpha_i(f) = \#\{(a,b) \in G_1^* \times G_2 \mid \lambda_{a,b}(f) = i\}$ for $0 \le i \le n$. We call $\alpha_0(f)$ the *deficiency* of f, denoted by $D(f)$. Hence $D(f) = \alpha_0(f)$ measures the number of pairs (a,b) such that $\Delta_{f,a}(x) = b$ has no solutions. This is a measure of the surjectivity of $\Delta_{f,a}$; the lower the deficiency the closer the $\Delta_{f,a}$ are to surjective.

Moreover, we define the *(weighted) ambiguity* of f as

$$A(f) = \sum_{0 \le i \le n} \alpha_i(f) \binom{i}{2}.$$

From this definition, we can see that the weighted ambiguity of f measures the total replication of pairs of x and x' such that $\Delta_{f,a}(x) = \Delta_{f,a}(x')$ for some $a \in G_1^*$. This is a measure of the injectivity of the functions $\Delta_{f,a}$; the lower the ambiguity of f the closer the $\Delta_{f,a}$ are to injective.

For a fixed a the values of $\Delta_{f,a}(x)$ are the entries in the ath row of what is often referred to as the *difference triangle* of f (when the domain of f is $\mathbb{Z}$ [2], [7]) or what we might call the *difference array* (when the domain of f is a finite group G). Thus for a fixed a, we define the *row-a-ambiguity of f* as

$$A_{r=a}(f) = \sum_b \binom{\lambda_{a,b}(f)}{2}.$$

These measure the injectivity of the individual $\Delta_{f,a}$. Similarly, we define the *row-a-deficiency* as $D_{r=a}(f) = \#\{b \mid \lambda_{a,b}(f) = 0, b \in G_2\}$, which measures the number of b's such that $\Delta_{f,a}(x) = b$ has no solutions for a fixed a. Likewise, we define the *column-b-ambiguity* as $A_{c=b}(f) = \sum_a \binom{\lambda_{a,b}(f)}{2}$ and the *column-b-deficiency* as $D_{c=b}(f) = \#\{a \mid \lambda_{a,b}(f) = 0, a \in G_1^*\}$, which measures the number of a's such that $\Delta_{f,a}(x) = b$ has no solutions for a fixed b.

In this paper we restrict our attention to $f : G_1 \to G_2$ that are bijections. This has the implication that $\Delta_{f,a}(x) = b$ can never have solutions for $b = 0$, thus we use the corresponding form in all our definitions that restrict $b \in G_2^*$; this also includes summations and universal quantifiers. Another effect of this to note is that the domain and co-domain of $\Delta_{f,a}$ are now sizes n and $n-1$, respectively; this is particularly important to remember when reading the proofs otherwise our references to "$n-1$" will seem odd. The ambiguity and deficiency of a function and its compositional inverse are the same since row-a-deficiency becomes column-a-deficiency, and reciprocally.

It is clear that the ambiguity and deficiency are strongly correlated although they are not exactly related. In this context, when we have $a \in G_1^*$, we can explicitly give the relationship between ambiguity and deficiency. For example, if $a \in G_1^*$, then we get $D_{r=a}(f) = n - 1 - \#\{\Delta_{f,a}(x) \mid x \in G_1\}$.

Lemma 1. *Let $f : G_1 \to G_2$ be a bijection. If a row-a-deficiency of f is equal to d, then row-a-ambiguity of f satisfies*

$$d + 1 \le A_{r=a}(f) \le \binom{d+2}{2}.$$

Proof: Because $D_{r=a}(f) = n - 1 - \#\{\Delta_{f,a}(x) \mid x \in G_1\}$, the size of the value set $\{\Delta_{f,a}(x) \mid x \in G_1\}$ is $n - 1 - d$ for a given row-a-deficiency d. The maximum row-a-ambiguity, $A_{r=a}(f) = \binom{d+2}{2}$, occurs when the n images, $\Delta_{f,a}(x)$, are distributed with $n - 2 - d$ values of x giving distinct images and the remaining $d+2$ values all agreeing. The minimum value, $A_{r=a}(f) = d + 1$, occurs when the n images are distributed with $d + 1$ pairs of $\{x, x'\}$ having $\Delta_{f,a}(x) = \Delta_{f,a}(x')$ and the remaining $n - 2(d+1)$ images are distinct. It is simple to check that $d \le n/2 - 1$ and that it is necessary for the sets $\Delta_{f,a}^{-1}(b)$ to have cardinality zero, one or two when $A_{r=a}(f)$ achieves its minimum. ∎

If we can view both G_1 and G_2 as vector spaces V_1 and V_2 over the same scalar field F, then ambiguity and deficiency measures are invariant under bijective affine transformations from V_1 and V_2.

Lemma 2. *Let $f, \bar{f} : G_1 \to G_2$ be bijections such that $\bar{f} = A_1 \circ f \circ A_2 + A$ where A_1, A_2 are bijective affine transformations and A is an affine transformation. Then for each pair (a,b) there exists a unique pair $(\bar{a}, \bar{b})$ such that $\lambda_{a,b}(f) = \lambda_{\bar{a},\bar{b}}(\bar{f})$. In particular, f and $\bar{f}$ have the same ambiguity, deficiency, and corresponding row ambiguities and row deficiencies.*

Proof: Clearly, $\bar{f}(x+a) - \bar{f}(x) = b$ is equivalent to $A_1 \circ (f \circ A_2(x+a) - f \circ A_2(x)) = b - A(a)$ because A_1 and A are affine transformations. Using the bijectivity of A_1 and A_2, we obtain $\lambda_{a,b}(f) = \lambda_{\bar{a},\bar{b}}(\bar{f})$, where $\bar{a} = A_2(a)$ and $\bar{b} = A_1^{-1}(b - A(a))$. ∎

Even when the groups are not vector spaces, the ambiguity and deficiency are invariant under some transformations, namely adding a fixed element or applying an automorphism of G_1 before applying the map f, and similarly adding an element or applying an automorphism of G_2 after the application of f.

B. Connections

Costas arrays [4] are $n \times n$ permutation matrices with ambiguity functions taking only the values 0 and (possibly) 1. These arrays have applications to radar and sonar systems [10].

Definition 3. *A* Costas array *is a permutation matrix (that is, a square matrix with precisely one 1 in each row and column*

and all other entries 0) for which all the vectors joining the pairs of 1's are distinct.

It is clear that a permutation f, from the columns to the rows (i.e. to each column x we assign one and only one row $f(x)$), gives a Costas array if and only if for $x \neq y$ and $k \neq 0$, $f(x+k)-f(x) \neq f(y+k)-f(y)$. We note that in the standard definition of Costas array, the arithmetic takes place inside $\mathbb{Z}$ and the vectors are in $\mathbb{Z} \times \mathbb{Z}$. The Costas array definition is precisely the property of $A(f) = 0$ when $f : [1, n] \subset \mathbb{Z} \to [1, n] \subset \mathbb{Z}$.

A special class of Costas arrays is the so called singly periodic Costas array, which is an $n \times \infty$ matrix built by infinitely and repeatedly horizontally concatenating an $n \times n$ Costas array with the property that any $n \times n$ window is a Costas array. This is equivalent to considering the injection $f : \mathbb{Z}_n \to [1, n] \subset \mathbb{Z}$ and asking again that f have zero ambiguity.

If we consider $f : \mathbb{Z}_n \to \mathbb{Z}_n$, the bounds from our Theorem 6 below show that zero ambiguity is impossible and thus "doubly periodic Costas arrays" cannot exist. However the bounds from Theorem 6 also tell us precisely what it means to be as close as possible to a "doubly periodic Costas array": we require the ambiguity, and correspondingly the deficiency, to be as small as possible. In Theorems 14 and 15 we build families of permutations f for an infinite number of orders, n, which are optimum with respect to both the ambiguity and deficiency.

Perfect and almost perfect non-linear functions can also be defined within the terminology of ambiguity and deficiency.

Definition 4. *[8] Let G_1 and G_2 be finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. We say that f is a* perfect non-linear function *if*

$$f(x + a) - f(x) = b$$

has exactly one solution for all $a \neq 0 \in G_1$ and all $b \in G_2$.

This corresponds again to zero ambiguity. This property is often too strong to require and particularly in the case of bijections f, it can never be satisfied. Thus a relaxed definition is frequently useful.

Definition 5. *[8] Let G_1 and G_2 be finite Abelian groups of the same cardinality and $f : G_1 \to G_2$. We say that f is an* almost perfect non-linear function *if*

$$f(x + a) - f(x) = b$$

has at most two solutions for all $a \neq 0 \in G_1$ and all $b \in G_2$.

The two subjects of Costas arrays and APN functions have been connected before by Drakakis, Gow and McGuire in [8] where they use the Welch construction of singly periodic Costas arrays to build APN permutations, $f : \mathbb{Z}_{p-1} \to \mathbb{Z}_{p-1}$ for p a prime. We note that our constructions have optimum and therefore lower ambiguity than those coming from the Welch construction and thus are closer to being PN functions. Additionally they are defined on the larger set of $n = q - 1$ where q is a prime power. Our construction methods in Section IV modify known families of permutation polynomials of finite fields. Frequently our permutations are optimum in both ambiguity and deficiency.

III. Bounds for general groups

In this section we determine a lower bound on the ambiguity and the deficiency of a bijection between two Abelian groups. Then in the next section we construct permutations achieving these bounds for an infinite number of values of n, the size of our group.

When G_1 and G_2 are arbitrary Abelian groups we can derive bounds on the ambiguity and deficiency. First let $I_1 \subset G_1$ be the elements of order 2 in G_1,

$$\gamma_1 = \sum_{g \in I_1} g,$$

and let $\iota_1 = |I_1|$. Similarly let $I_2 \subset G_2$ be the elements of order 2 in G_2,

$$\gamma_2 = \sum_{g \in I_2} g,$$

and let $\iota_2 = |I_2|$. Furthermore, let $f : G_1 \to G_2$ be a bijection and let $I_1^0 \subset I_1$ be

$$I_1^0 = \{a \in I_1 \mid D_{r=a}(f) = 0\}.$$

Also define

$$N_1^0 = \{a \in G_1 \setminus I_1 \mid D_{r=a}(f) = 0\}.$$

Similarly define I_2^0 and N_2^0.

Since the deficiency is simply the sum of the row deficiencies and for any $a \notin I_1^0 \cup N_1^0$, $D_{r=a}(f) \geq 1$, we have

$$D(f) = \sum_{a \in G_1^*} D_{r=a}(f) \geq (n-1) - |I_1^0 \cup N_1^0|.$$

When $a \in I_1^0 \cup N_1^0$ then $D_{r=a}(f) = 0$ and the pigeonhole principle gives us that there is a single repeated value, r, in the multiset $\{f(x + a) - f(x) \mid x \in G_1\} \subseteq G_2^*$. In the case where $\gamma_2 \neq 0$ we have

$$\begin{aligned} 0 &= \sum_{x \in G_1} f(x + a) - \sum_{x \in G_1} f(x) \\ &= \sum_{x \in G_1} (f(x + a) - f(x)) = r + \sum_{y \in G_2^*} y = r + \gamma_2, \end{aligned}$$

and thus the repeated value r is γ_2. That is, there exist $x_1, x_2 \in G_1^*$ such that

$$f(x_1 + a) - f(x_1) = \gamma_2, \;\; f(x_2 + a) - f(x_2) = \gamma_2.$$

Letting $y_1 = f(x_1)$ and $y_2 = f(x_2)$, this is equivalent to

$$f^{-1}(y_1 + \gamma_2) - f^{-1}(y_1) = a, \;\; f^{-1}(y_2 + \gamma_2) - f^{-1}(y_2) = a.$$

The fact that for every $a \in I_1^0 \cup N_1^0$ we get that $a \in \text{Range}(f^{-1}(y + \gamma_1) - f^{-1}(y))$ gives us the left hand of Inequality (1) below. The fact that for every $a \in I_1^0 \cup N_1^0$ there is a pair of distinct values of $y \in G_2^*$ which have identical values of $f^{-1}(y+\gamma_2) - f^{-1}(y)$ gives the right hand of Inequality (1). Thus,

$$n - 1 - (|I_1^0 \cup N_1^0|) \geq D_{c=\gamma_2}(f) \geq (|I_1^0 \cup N_1^0|) - 1. \quad (1)$$

If $f(x+a)-f(x)=b$ then $f(x+a+a)-f(x+a)=b$ since $a \in I_1$ and $b \in I_2$. If $|I_2| \geq 2$, $b_1, b_2 \in I_2$ and there exists an $a \in I_1^0$ then $D_{r=a}(f) = 0$ and in particular there exist $x_1, x_2 \in G_1$ such that $f(x_1+a)-f(x_1) = b_1$ and $f(x_2+a)-f(x_2) = b_2$. But then, by the previous comments we also have $f(x_3+a)-f(x_3) = b_1$ and $f(x_4+a)-f(x_4) = b_2$ for $x_3 = x_1+a$ and $x_4 = x_2+a$. Again since $D_{r=a}(f) = 0$, there must be a solution, $x \in G_1$ of $f(x+a)-f(x) = b$ for *every* $b \in G_2^*$ but only $n-4$ elements of $G_1 \setminus \{x_1, x_2, x_3, x_4\}$ remain to provide solutions for all $n-3$ elements $b \in G_2^* \setminus \{b_1, b_2\}$ which is impossible. Thus if $|I_2| \geq 2$ then $I_1^0 = \emptyset$.

If n is odd or γ_2 is the identity, the corresponding versions of Inequality (1) give that the repeated value r is $r = 0$ but this is not possible since $f(x+a)-f(x) \in G_2^*$, thus no $D_{r=a}(f) = 0$ and $D(f) \geq n-1$. The same applies when we consider f^{-1}.

Theorem 6. *Let G_1 and G_2 be Abelian groups of order n with ι_1 and ι_2 elements of order 2, respectively. Let $f : G_1 \to G_2$ be a bijection. Then the deficiency of f, $D(f)$, is bounded below by*

$$\begin{cases} n-1 & n \equiv 1 \pmod 2, \\ n-3 & n \equiv 0 \pmod 2 \text{ and } \iota_1 = \iota_2 = 1, \\ n-1-\frac{3\min\{\iota_1,\iota_2\}}{2}+\frac{\iota_1\iota_2}{2} & n \equiv 0 \pmod 2 \text{ and } \iota_1\iota_2 > 1. \end{cases}$$

The ambiguity of f, $A(f)$, is bounded below by

$$\begin{cases} 2(n-1) & n \equiv 1 \pmod 2, \\ 2(n-2) & n \equiv 0 \pmod 2 \text{ and } \iota_1 = \iota_2 = 1, \\ 2(n-1)-\frac{3\min\{\iota_1,\iota_2\}}{2}+\frac{\iota_1\iota_2}{2} & n \equiv 0 \pmod 2 \text{ and } \iota_1\iota_2 > 1. \end{cases}$$

Proof: The lower bound on deficiency when n is odd is straightforward. Indeed, there are no $a \in G_1^*$ for which $D_{r=a}(f) = 0$ so $D_{r=a}(f) \geq 1$ for all a. Summing these over all non-zero a gives the required lower bound $D(f) \geq n-1$. By Lemma 1, $A_{r=a}(f) \geq 2$. Summing these over all non-zero a gives the required lower bound for ambiguity of f, that is, $A(f) \geq 2(n-1)$.

When n is even and $\iota_1 = \iota_2 = 1$, then $I_1 = \{\gamma_1\}$, $I_2 = \{\gamma_2\}$, which are both nonzero, and if $a \in I_1^0 \cup N_1^0$ the repeated value of $f(x+a)-f(x)$ must be γ_2. Recall the deficiency can be computed from either the row or column deficiencies

$$\sum_{a \neq 0} D_{r=a}(f) = \sum_{b \neq 0} D_{c=b}(f).$$

Using Inequality (1) and its row deficiency analog, we get

$$\begin{aligned} D(f) &= \frac{1}{2}\left(\sum_{a \in G_1^*} D_{r=a}(f) + \sum_{b \in G_2^*} D_{c=b}(f)\right) \\ &= \frac{1}{2}\left(\sum_{a \neq 0,\gamma_1} D_{r=a}(f) + \sum_{b \neq 0,\gamma_2} D_{c=b}(f) + \right. \\ &\quad \left. + D_{c=\gamma_2}(f) + D_{r=\gamma_1}(f) \right) \\ &\geq \frac{1}{2}\left((n-2-|I_1^0 \cup N_1^0|) + (n-2-|I_2^0 \cup N_2^0|)\right. \\ &\quad \left. + |I_1^0 \cup N_1^0| - 1 + |I_2^0 \cup N_2^0| - 1\right) \\ &= n-3. \end{aligned}$$

Again, by Lemma 1, a row-a-deficiency value of d contributes at least $d+1$ to the ambiguity, so we get that the total ambiguity for f is at least $n-1+n-3 = 2(n-2)$.

Now let $\iota_1\iota_2 > 1$. Without loss of generality, suppose $\iota_2 \geq \iota_1$ and thus $\iota_2 > 1$. If $D_{r=a}(f) = 0$, then there can only be a single repeated value, r, in the multiset $\{f(x+a)-f(x) \mid x \in G_1\} \subseteq G_2^*$. By the fundamental theorem of Abelian groups, we have

$$\begin{aligned} 0 &= \sum_{x \in G_1} f(x+a) - \sum_{x \in G_1} f(x) \\ &= \sum_{x \in G_1} (f(x+a)-f(x)) = r + \sum_{y \in G_2^*} y = r, \end{aligned}$$

which is a contradiction. Thus, $D_{r=a}(f) \geq 1$ for all $a \in G_1$ when $\iota_2 > 1$.

Let n be even and let $\iota_1\iota_2 > 1$. For each $a \in I_1$ we calculate a lower bound on $D_{r=a}(f)$. The difference map is $\Delta_{f,a} : G_1 \to G_2^*$. Define α_i to be the cardinality of the set $\{b \in G_2^* \mid \#\Delta_{f,a}^{-1}(b) = i\}$. If $\Delta_{f,a}(x) = b \in I_2$, then $\Delta_{f,a}(x+a) = b$ as well, and we have that $\alpha_1 \leq n-1-\iota_2$. Simple counting over the domain and co-domain sizes gives

$$\sum_{i=0}^{n} \alpha_i = n-1, \qquad \sum_{i=0}^{n} i\alpha_i = n.$$

Using

$$2\sum_{i=2}^{n} \alpha_i \leq \sum_{i=2}^{n} i\alpha_i = \left(\sum_{i=1}^{n} i\alpha_i\right) - \alpha_1 = n - \alpha_1,$$

we get

$$\begin{aligned} D_{r=a}(f) = \alpha_0 &= n-1-\sum_{i=1}^{n} \alpha_i = n-1-\alpha_1-\sum_{i=2}^{n} \alpha_i \\ &\geq n-1-\alpha_1-\frac{n-\alpha_1}{2} = \frac{n}{2}-1-\frac{\alpha_1}{2} \\ &\geq \frac{n}{2}-1+\frac{\iota_2}{2}+\frac{1}{2}-\frac{n}{2} = \frac{\iota_2-1}{2}. \end{aligned}$$

Let $N_1 = G_1^* \setminus I_1$. We now have

$$\begin{aligned} D(f) &= \sum_{a \in I_1} D_{r=a}(f) + \sum_{a \in N_1} D_{r=a}(f) \\ &\geq \iota_1\frac{\iota_2-1}{2} + n - 1 - \iota_1 = n-1-\frac{3\iota_1}{2}+\frac{\iota_1\iota_2}{2}. \end{aligned}$$

The same calculation can be done for the column deficiencies and thus

$$D(f) \geq n-1-\frac{3\min\{\iota_1,\iota_2\}}{2}+\frac{\iota_1\iota_2}{2}.$$

The ambiguity lower bounds are derived directly from the bounds on deficiency using Lemma 1. ∎

In the particular case $G_1 = G_2 = \mathbb{Z}_n$, we have the following Corollary [20].

Corollary 7. *Let $n \in \mathbb{N}$ and $f : \mathbb{Z}_n \to \mathbb{Z}_n$ be a bijection. The ambiguity of f is at least $2(n-1)$ when n is odd and $2(n-2)$ when n is even. The deficiency of f is at least $n-1$ if n is odd and at least $n-3$ when n is even.*

Functions that meet these bounds are of particular interest.

Definition 8. *If a permutation $f : G_1 \to G_2$ has an ambiguity equal to the lower bound from Theorem 6 we say it has* optimum ambiguity *and similarly we define* optimum deficiency *for a permutation if it achieves the lower bound for the deficiency.*

Next we show that optimum ambiguity implies the APN property for bijections from G_1 and G_2. For the optimum ambiguity, all the sets $\Delta_{f,a}^{-1}(b)$ have cardinality at most two. These observations allow us to connect our notion of ambiguity to APN functions.

Corollary 9. *Let G be a finite Abelian group. If a permutation $f : G \to G$ achieves the minimal ambiguity, then f is Almost Perfect Non-linear.*

Proof: Consideration of the forced equalities throughout the proof of Theorem 6 gives that the number of pairs of (a, b) such that $|\Delta_{f,a}^{-1}(b)| \geq 2$ is exactly the ambiguity and each inverse image has size zero, one or two. Thus f is APN [8]. ∎

This is not true for the deficiency. If n is odd, it is possible that the $D_{r=a}(f)$ be at its minimum, while $A_{r=a}(f) = 3 > 2$. In this case there is one missed value $g_m \in G_2^*$ and a value g_t which is hit three times by $\Delta_{f,a}$. In that case f is not APN. When n is even, $\iota_1 = \iota_2 = 1$ and the minimum deficiency is achieved, then any row where $D_{r=a}(f) = 0$ cannot contain values of b that are hit more than twice. Considering the equalities that are forced in $D_{r=\gamma_1}(f)$ (as discussed at the start of Section III) when the deficiency is optimal shows that the only repeated b values in this row must come from columns that have zero deficiency and thus these values are repeated only twice. But just as in the odd case any other row with $D_{r=a}(f) > 0$ could have a value hit three times by $\Delta_{f,a}$. In the case $\iota_1\iota_2 > 1$ we can be more precise. If $a \in I_1$ the consideration of the inequalities in the proof of Theorem 6 shows that if $D_{r=a}(f) = (\iota_2 - 1)/2$ then $\#\Delta_{f,a}^{-1}(b) = 0, 1, 2$ for this a. It is only when $a \notin I_1$ that f can fail to be APN. Thus if $G_1 = \mathbb{Z}_2^e$ with $n = 2^e$, $\iota_1 = n - 1$ and f attains deficiency $D(f) = n-1-(3\iota_1)/2+\iota_1\iota_2/2 = (n-1)(\iota_2-1)/2$, then f must be APN. In this case however, if $\iota_2 < \iota_1$ this bound is never attained so all we can say is that if $G_1 = G_2 = \mathbb{Z}_2^e$, then attaining the minimum deficiency does guarantee f to be APN.

However a permutation which is APN could have ambiguity as large as $(n - 1)\lfloor n/2 \rfloor$ and correspondingly deficiency as large as $(n - 1)(\lfloor n/2 \rfloor - 1)$.

Proposition 10. *Let G_1, G_2 be finite Abelian groups of order n. If $f : G_1 \to G_2$ is any APN permutation such that $\Delta_{f,a}(x) = f(x + a) - f(x)$ is 2-to-1 mapping for all $x \in G_1$ with at most one exception and for any $a \in G_1^*$, then the deficiency of f is $(n - 1)(\lfloor n/2 \rfloor - 1)$ and the ambiguity of f is $(n - 1)\lfloor n/2 \rfloor$.*

Proof: Suppose $\Delta_{f,a}$ is 2-to-1 mapping for each $a \in G_1^*$, then n is even and the deficiency of f is $(n - 1)(n/2 - 1)$ and the ambiguity of f is $(n - 1)n/2$. However, if $\Delta_{f,a}$ is 2-to-1 mapping for all $x \in G_1$ with at most one exception and for each $a \in G_1^*$, then n is odd. In this case, the deficiency of f is $(n - 1)((n - 1)/2 - 1)$ and the ambiguity of f is $(n - 1)(n - 1)/2$. Hence the proof is complete. ∎

Obviously this case is the worst possible scenario that can happen in terms of ambiguity and deficiency for APN functions.

When f is a bijection we only consider $b \in G_2^*$ and APN functions are clearly functions with small ambiguity and therefore small deficiency. Since a function can be APN and still have an ambiguity anywhere between the lower bound presented in Theorem 6 and the upper bound of $(n-1)\lfloor n/2 \rfloor$ in Proposition 10, our definition of ambiguity has a higher resolution power than just the definition of APN and thus can usefully be regarded as a refinement of the concept.

Example 11. *One APN permutation constructed in $\mathbb{Z}_{10}$ from the Welch Costas array constructions is $f(x) = (2^x \bmod 11) - 1$ or $f = (0)(1)(23768)(4)(59)$ and has ambiguity $19 > 2(10 - 2) = 16$ and deficiency $12 > (10 - 3) = 7$ although this construction does not attain the worst possible values for APN permutations.*

In general, the converse of Corollary 9 is not true. But it is true for finite fields of characteristic 2.

Corollary 12. *Let $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ be a bijective APN, then it has optimum ambiguity and deficiency.*

Proof: Since we are working in finite fields of characteristic 2, the solutions of every equation come in pairs. It means that every equation such as $\Delta_{f,a}(x) = b$ has either exactly two solutions or no solution because f is an APN function. Based on the proof of Lemma 1, the minimum value, $A_{r=a}(f) = d + 1$, happens only when the n images are distributed with $d+1$ pairs of $\{x, x'\}$ having $\Delta_{f,a}(x) = \Delta_{f,a}(x')$ and the remaining $n - 2(d + 1)$ images are distinct. Hence, in this case we get $d = 2^{m-1} - 1$ and the sets $\Delta_{f,a}^{-1}(b)$ having cardinality zero and two are necessary when $A_{r=a}(f)$ achieves its minimum. Therefore, f has optimum ambiguity because every row has optimum row-a-ambiguity. Finally, since optimum ambiguity is stronger than optimum deficiency, f has optimum deficiency as well. ∎

IV. Ambiguity and deficiency of some known functions

Next we provide our main constructions which produce permutations that achieve the minimum ambiguity and deficiency.

A. Functions in the multiplicative group of $\mathbb{F}_q$

Before we give our first construction, that applies to values of $n = q - 1$ for q a prime power, we introduce a way to obtain a permutation polynomial of fixed point 0 over a finite field $\mathbb{F}_q$ from another permutation polynomial of $\mathbb{F}_q$ which does not fix 0. Namely, let h be a permutation polynomial of $\mathbb{F}_q$ such that $h(0) = a \neq 0$ and $h(b) = 0$. Then we define g as

$$g(x) = \begin{cases} h(b) = 0, & x = 0; \\ h(0) = a, & x = b; \\ h(x), & x \neq 0, b. \end{cases}$$

It is obvious that g is again a permutation polynomial of $\mathbb{F}_q$ which fixes 0.

Example 13. *For any positive integer e such that $\gcd(e,n)=1$ and $m,a\neq 0\in\mathbb{F}_q$, the polynomial $h(x)=mx^e+a$ is a permutation polynomial of $\mathbb{F}_q$ which does not fix 0. Let b be the unique (non-zero) field element such that $h(b)=0$. Using the above construction, we let*

$$g(x)=\begin{cases} h(b)=0, & x=0;\\ h(0)=a, & x=b;\\ h(x)=mx^e+a, & x\neq 0,b.\end{cases}$$

Then g is a permutation polynomial of $\mathbb{F}_q$ which fixes 0.

It turns out that this twist of permutation polynomials can be very useful in constructing permutations of $\mathbb{Z}_n$ with optimum deficiency and optimum ambiguity.

1) Functions derived from permutation monomials:

Theorem 14. *Let q be a prime power, $n=q-1$ and α a primitive element in $\mathbb{F}_q$. For $\gcd(e,n)=1$ and $m,a\neq 0\in\mathbb{F}_q$, let $h:\mathbb{F}_q\to\mathbb{F}_q$ be defined by $h(x)=mx^e+a$ and let b be the unique (non-zero) field element such that $h(b)=0$. Let*

$$g(x)=\begin{cases} h(b)=0, & x=0;\\ h(0)=a, & x=b;\\ h(x)=mx^e+a, & x\neq 0,b.\end{cases}$$

If $q\not\equiv 0 \pmod 3$ then $f:\mathbb{Z}_n\to\mathbb{Z}_n$ defined by $f(i)=\log_\alpha(g(\alpha^i))$ has optimum deficiency. If, additionally, $q\equiv 2 \pmod 3$ (i.e., q is an odd power of a prime p where $p\equiv 2 \pmod 3$), then f has optimum ambiguity as well.

Proof: We have $f(i+a)-f(i)=\log_\alpha(g(\alpha^{i+a}))-\log_\alpha(g(\alpha^i))=\log_\alpha\left(\frac{g(\alpha^{i+a})}{g(\alpha^i)}\right)$. Let $d=\alpha^a$. We need to study the size v_d of the value set of $g(dx)/g(x)$ for $x\neq 0$. From the definition of g, we have

$$\frac{g(dx)}{g(x)}=\begin{cases}\frac{m(db)^e+a}{a}, & x=b;\\ \frac{a}{m(b/d)^e+a}, & x=b/d;\\ \frac{m(dx)^e+a}{mx^e+a}, & x\neq b,b/d.\end{cases}$$

First we show that $v_d\geq q-3$ for any $d\neq 0,1$. Let x,y be both different from $b,b/d$. Assume that

$$\frac{m(dx)^e+a}{mx^e+a}=\frac{m(dy)^e+a}{my^e+a}.$$

Then

$$\begin{aligned} & m^2d^ex^ey^e+amy^e+amd^ex^e+a^2\\ = \;& m^2d^ex^ey^e+amd^ey^e+amx^e+a^2.\end{aligned}$$

Since $m,a\neq 0$, we obtain $(d^e-1)y^e=(d^e-1)x^e$. Because $\gcd(e,q-1)=1$, we have $d^e\neq 1$ if $d\neq 1$. Hence $x^e=y^e$. Again, by $\gcd(e,q-1)=1$, we obtain $x=y$. Hence $v_d\geq q-3$ for any $d\neq 0,1$.

Moreover, if

$$\frac{m(db)^e+a}{a}=\frac{m(dx)^e+a}{mx^e+a},$$

then

$$m^2d^eb^ex^e+amx^e+amd^eb^e+a^2=amd^ex^e+a^2.$$

Hence

$$(m^2d^eb^e+am-amd^e)x^e=-amd^eb^e.$$

Since $mb^e=-a$, we obtain

$$(am-2amd^e)x^e=-amd^eb^e.$$

Again, $m,a\neq 0$. This implies that $(2d^e-1)x^e=d^eb^e$.

If q is odd, we can find a solution for x as long as $2d^e-1\neq 0$. On the other hand, there exists a unique d such that $d^e=1/2$ and

$$\frac{m(db)^e+a}{a}\neq\frac{m(dx)^e+a}{mx^e+a}.$$

Similarly, there exists a unique d such that $d^e=2$ and

$$\frac{a}{m(b/d)^e+a}\neq\frac{m(dx)^e+a}{mx^e+a}.$$

Hence $v_d=q-3=n-2$ if $d^e\neq 2$ or $1/2$, and $v_d=q-2=n-1$ if $d^e=2$ or $1/2$. Moreover $\frac{m(db)^e+a}{a}=\frac{a}{m(b/d)^e+a}$ is equivalent to $d^{2e}-d^e+1=0$.

We observe that if $\mathrm{char}(\mathbb{F}_q)=3$, then $2=1/2$ and $\frac{a}{m(b/d)^e+a}=\frac{m(db)^e+a}{a}$. Hence there is one row with row deficiency zero and the remaining rows have deficiency one. Thus $D(f)=n-2$ where $n=q-1$. It is obvious that $A(f)=2(n-2)+1=2n-3$ in this case.

If $\mathrm{char}(\mathbb{F}_q)>3$ then we consider two cases: $q\equiv 1 \pmod 3$ and $q\equiv 2 \pmod 3$. In the former case, $d^{2e}-d^e+1=0$ has two distinct roots r_1,r_2 for d^e which are not equal to 2 or $1/2$. Again $d^e=2,1/2$ give us two rows with row deficiency zero and row ambiguity one. When $d^e=r_1,r_2$ then we get two rows with row deficiency one and row ambiguity three. The remaining $n-5$ rows have row deficiency one and row ambiguity two. Thus for $q\equiv 1 \pmod 3$ we get $D(f)=2(0)+2(1)+(n-5)(1)=n-3$ which is optimal and $A(f)=2(1)+2(3)+(n-5)(2)=2(n-1)$. However, when $q\equiv 2 \pmod 3$, there are no roots for $d^{2e}-d^e+1=0$. Hence we have two rows with row deficiency zero and row ambiguity one, the remaining $n-3$ rows have row deficiency one and row ambiguity two. Hence $D(f)=2(0)+(n-3)(1)=n-3$ and $A(f)=2(1)+(n-3)(2)=2(n-2)$ are both optimal in the case that $q\equiv 2 \pmod 3$.

If q is even, we always find x such that

$$\frac{m(db)^e+a}{a}=\frac{m(dx)^e+a}{mx^e+a},$$

and

$$\frac{a}{m(b/d)^e+a}=\frac{m(dx)^e+a}{mx^e+a}.$$

Hence $v_d=q-3$, and $D(f)=\sum_{a\in\mathbb{Z}_n^*}D_{r=a}(f)=(n-1)(n-1-(q-3))=n-1$ when n is odd.

If q is an even power of two, then $d^{2e}+d^e+1=0$ has two solutions for d^e. Hence there exist two d's such that

$$\frac{m(db)^e+a}{a}=\frac{a}{m(b/d)^e+a}=\frac{m(dx)^e+a}{mx^e+a}.$$

In this case, we have $A(f) = 2 \cdot 3 + (n-3) \cdot 2 = 2n$ which is not optimal. However, in the case that q is an odd power of 2, there are no solutions to $d^{2e} + d^e + 1 = 0$, so we still have optimal ambiguity $A(f) = 2(n-1)$. ∎

We remark from the proof that if $q \equiv 1 \pmod 3$ then the ambiguity is $2(n-1)$ or $2n$ depending on whether q is odd or even, respectively. In these cases f is not APN. Also, if $q \equiv 0 \pmod 3$ then f has deficiency $n-2$ and ambiguity $2n-3$, both exactly one more than optimal. In this case, f is APN. Some of these cases were overlooked in [20].

2) Möbius function:

Theorem 15. *Let $q = p^m$, $n = q-1$ and α a primitive element in $\mathbb{F}_q$. Let $g : \mathbb{F}_q \to \mathbb{F}_q$ be defined as follows*

$$g(x) = \begin{cases} \frac{\beta x}{\gamma x + \eta} & x \neq \frac{-\eta}{\gamma}, \\ \frac{\beta}{\gamma} & x = \frac{-\eta}{\gamma}, \end{cases}$$

where $\beta, \gamma, \eta \neq 0$. If $q \not\equiv 0 \pmod 3$ then $f(i) = \log_\alpha\left(g(\alpha^i)\right)$ has optimum deficiency. Moreover, if $q \equiv 2 \pmod 3$ then f has optimum ambiguity. If $q \equiv 1 \pmod 3$ then the ambiguity is $2(n-1)$ or $2n$ depending on whether q is odd or even, respectively. Finally, if $q \equiv 0 \pmod 3$ then f has deficiency $n-2$ and ambiguity $2n-3$, both exactly one more than optimal.

Proof: First of all suppose that $\mathrm{char}(\mathbb{F}_q) \neq 2$. It is easy to see that g is a permutation function over $\mathbb{F}_q$ and $g(0) = 0$. We have

$$\begin{aligned} f(i+a) - f(i) &= \log_\alpha\left(g(\alpha^{i+a})\right) - \log_\alpha\left(g(\alpha^i)\right) \\ &= \log_\alpha\left(\frac{g(\alpha^{i+a})}{g(\alpha^i)}\right). \end{aligned}$$

Suppose that $d = \alpha^a$. We have to evaluate the value set v_d of $g(dx)/g(x)$ for $x \neq 0$ where $d \neq 0, 1$. Based on the definition of g, we get

$$\frac{g(dx)}{g(x)} = \begin{cases} \frac{d(\gamma x + \eta)}{\gamma d x + \eta} & x \neq \frac{-\eta}{\gamma}, \frac{-\eta}{d\gamma}, \\ \frac{d}{d-1} & x = \frac{-\eta}{\gamma}, \\ 1 - d & x = \frac{-\eta}{d\gamma}. \end{cases}$$

Let us first assume that x, y are both different from $\frac{-\eta}{\gamma}, \frac{-\eta}{d\gamma}$. Then

$$\begin{aligned} \frac{g(dx)}{g(x)} = \frac{g(dy)}{g(y)} &\iff \frac{d(\gamma x + \eta)}{\gamma d x + \eta} = \frac{d(\gamma y + \eta)}{\gamma d y + \eta} \\ &\iff \gamma\eta x + \gamma\eta d y = \gamma\eta y + \gamma\eta d x \\ &\iff (x-y)(d-1) = 0 \\ &\iff x = y. \end{aligned} \tag{2}$$

Hence $v_d \geq q - 3$ for any $d \neq 0, 1$. In addition, we have

$$\frac{d(\gamma x + \eta)}{\gamma d x + \eta} = \frac{d}{d-1} \iff x = \frac{\eta(d-2)}{\gamma}, \tag{3}$$

and also

$$\frac{d(\gamma x + \eta)}{\gamma d x + \eta} = 1 - d \iff x = \frac{\eta(1-2d)}{\gamma d^2}. \tag{4}$$

Let $\mathrm{char}(\mathbb{F}_q) \neq 2$. So, the expressions (2) and (3) imply that if $d \neq 2$, then we have a unique non-zero solution and for these values of d we have the row deficiency one. But if $d = 2$, then $x = 0$ and it means that for this d and for some a such that $2 = \alpha^a$, we have the row deficiency zero. Hence $v_d = q - 3 = n - 2$ if $d^e \neq 2$ or $1/2$, and $v_d = q - 2 = n - 1$ if $d^e = 2$ or $1/2$. Moreover $\frac{d}{d-1} = 1 - d$ is equivalent to $d^2 - d + 1 = 0$. Then the rest of the proof follows in the same way as the proof of Theorem 14. ∎

B. Additive group of a finite field

1) APN permutations in a field of characteristic 2:

Let $q = 2^m$ and $f : \mathbb{F}_q \to \mathbb{F}_q$ be the inverse function defined as follows

$$f(x) = \begin{cases} x^{-1} & x \neq 0, \\ 0 & x = 0. \end{cases}$$

It is easy to see that f is permutation function over $\mathbb{F}_q$ and $f(0) = 0$.

Theorem 16. *Let $q = 2^m$, m odd. The inverse function $f(x) = x^{-1}$ over $\mathbb{F}_q^*$ has optimum ambiguity and deficiency. For even m, the ambiguity and deficiency are*

$$A(f) = (2^m - 1)\left(2^{m-1} + 4\right),$$

and

$$D(f) = (2^m - 1)2^{m-1}.$$

Proof: Based on the definition of f, we get

$$f(x+a) - f(x) = \begin{cases} \frac{-a}{x(x+a)} & x \neq 0, -a, \\ \frac{1}{a} & x = 0, -a. \end{cases}$$

Let us assume first x, y are both different from $0, -a$. Then

$$\begin{aligned} & f(x+a) - f(x) = f(y+a) - f(y) \\ \iff\ & \frac{-a}{x(x+a)} = \frac{-a}{y(y+a)} \\ \iff\ & (x-y)(a+x+y) = 0. \end{aligned}$$

Hence for every x there is exactly one y such that $f(x+a) - f(x) = f(y+a) - f(y)$. In addition, we have

$$\frac{-a}{x(x+a)} = \frac{1}{a} \Leftrightarrow x^2 + ax + a^2 = 0. \tag{5}$$

This equation has solutions in $\mathbb{F}_{2^m}$ if and only if m is even. Indeed, for $a \neq 0$, $x^2 + ax + a^2 = 0$ is equivalent to $(x/a)^2 + (x/a) + 1 = 0$, which is equivalent to $(x/a)^3 = 1$ provided $x \neq a$. Hence this happens if and only if $3 \mid 2^m - 1$, namely, m is even.

Now, we distinguish between two cases.

1) For even m, we have two distinct solutions to $x^2 + ax + a^2 = 0$ for every $a \neq 0$. Therefore, all the elements in $\mathbb{F}_{2^m}$ are 2 to 1 except one of them which is 4 to 1 and that is happening when we have Equation (5). We note that four solutions are $x = 0, -a$ and the other two solutions come from equation $x^2 + ax + a^2 = 0$. In this case, the number of $b \neq 0$'s such that we do not have a solution for $\Delta_{f,a}(x) = b$ is $\frac{q-2}{2} + 1 = \frac{q}{2}$. Also we have $q - 1$ choices for $a \in \mathbb{F}_q^*$. Hence $D(f) = (q-1)\frac{q}{2}$. Moreover, there exist $\frac{q}{2} - 2$, $b \neq 0$'s for which we do

have two solutions for $\Delta_{f,a}(x) = b$. Therefore, $A(f) = \binom{2}{2}\alpha_2(f) + \binom{4}{2}\alpha_4(f)$ equals

$$(q-1)\left(\frac{q}{2}-2\right) + \binom{4}{2}(q-1) = (q-1)\left(\frac{q}{2}+4\right).$$

2) For odd m this function is APN and Corollary 12 applies.

In both cases we have to use lower bounds from general groups. Since in the additive group of $\mathbb{F}_q$, $q = 2^m$, all the elements have order 2, we get $\iota_1 = \iota_2 = q-1$. Hence, based on the lower bounds of Theorem 6, the lower bounds on deficiency and ambiguity of the inverse function on the additive group of $\mathbb{F}_q$ are $(q-1) - \frac{3(q-1)}{2} + \frac{(q-1)^2}{2} = (q-1)\left(\frac{q}{2}-1\right)$ and $2(q-1) - \frac{3(q-1)^2}{2} + \frac{(q-1)^2}{2} = (q-1)\frac{q}{2}$, respectively. ■

We note that for odd m, the inverse function is APN and thus has optimum ambiguity and deficiency. For even m, the inverse function is not optimal in terms of ambiguity, nor APN. We observe that the inverse function in the even m case $\mathbb{F}_{2^8}$ is used in the S-box of AES.

2) APN permutations over finite fields of odd characteristic:

There is a sharp contrast with the above situation when we consider APN permutations over a finite field $\mathbb{F}_{p^e}$ of characteristic $p > 2$. More precisely, Corollary 12 is not true if we change the characteristic of our finite field to odd prime numbers p. In the following we determine the ambiguity and deficiency of some well-known APN permutations on $\mathbb{F}_{p^e}$ and $p > 2$. In Table I, we report on some APN permutations of the form x^d for some special values of d, and for finite fields with characteristic $p > 2$. We found the deficiency and ambiguity of them in the following theorem.

d	Condition
3	$p \neq 3$
$p^e - 2$	$p > 2$ and $p^e \equiv 2 \pmod 3$
$\frac{2p^e-1}{3}$	$p^e \equiv 2 \pmod 3$
$\frac{p^k+1}{2}$	$p = 5$ and $(2e, k) = 1$

TABLE I
FOUR APN FUNCTIONS x^d OVER FINITE FIELDS $\mathbb{F}_{p^e}$ OF ODD CHARACTERISTIC [11].

Theorem 17. *Let f be one of the APN permutations in Table I over $\mathbb{F}_q$ where $q = p^e$. Then the deficiency of f is $(q-1)\left(\frac{q-3}{2}\right)$ and the ambiguity of f is $(q-1)\left(\frac{q-1}{2}\right)$.*

Proof: If $f(x) = x^3$ or $f(x) = x^{p^e-2}$, then $f(x+a) - f(x) = b$ is a quadratic equation. Now we show that for the third and fourth functions we have the same situation. Let f be the third function. The equation $(x+a)^d - x^d = b$ where $d = \frac{2p^e-1}{3}$ implies that $(x+a)^d = b + x^d$. Raising both sides of the last equation to the power 3, we get

$$(x+a)^{3d} = (b+x^d)^3 = x^{3d} + 3x^{2d}b + 3b^2x^d + b^3.$$

Since $3d \equiv 1 \pmod{(p^e-1)}$, we obtain

$$x + a = x + 3x^{2d}b + 3b^2x^d + b^3.$$

By a simple rearrangement, we have

$$3b\left(x^d\right)^2 + 3b^2x^d + b^3 - a = 0 \tag{6}$$

which is a quadratic equation in x^d. Therefore, it has at most two solutions in x^d. Each of these solutions gives a maximum of (d, p^e-1) solutions in x. Since f is a permutation, $(d, p^e-1) = 1$ and we conclude that finding the solutions of (6) is equivalent to providing the set of solutions of $3bx^2 + 3b^2x + b^3 - a = 0$. The former equation is a quadratic equation.

Now suppose that f is the last APN permutation in Table I. We closely follow the proof of Theorem 11 in [11]. Any $x \in \mathbb{F}_q$ can be represented as $x = \alpha + \alpha^{-1}$, where α and α^{-1} are the two roots in $\mathbb{F}_{q^2}^*$ of $z^2 - xz + 1 = 0$. A solution of $\Delta_{f,a} = (x+a)^d - x^d = b$ is equivalent to a solution of $a^d((x/a)+1)^d - a^d(x/a)^d = b$. Let $y = x/a$ and this corresponds to solutions of $(y+1)^d - y^d = ba^{-d}$. Hence, it is sufficient to find the number of solutions of

$$(x+1)^d - x^d = b. \tag{7}$$

Replacing x by $x+2$, we obtain $(x+3)^d - (x+2)^d = b$. Substituting $x = \alpha + \alpha^{-1}$, we conclude

$$\frac{(\alpha-1)^{2d} - (\alpha+1)^{2d}}{\alpha^d} = b,$$

which is equivalent to

$$\alpha^{\frac{5^k-1}{2}} + \alpha^{-\frac{5^k-1}{2}} = 2b. \tag{8}$$

The above equation has in general four solutions in $\mathbb{F}_{q^2}$ for any b (b can be in $\mathbb{F}_q$ or $\mathbb{F}_{q^2}$ but of course we are interested in the former). If one solution is α, then the remaining solutions (for $p = 5$) are $-\alpha$, α^{-1} and $-\alpha^{-1}$

These α's map onto x's; in general, this is a 2-to-1 mapping. In particular α and α^{-1} both map to the same x and so do the pair $-\alpha$ and $-\alpha^{-1}$. Thus we get, generally, two solutions of x for every b corresponding to α and $-\alpha$. When $\alpha = \alpha^{-1}$ ($\alpha = 1$ or 4) then Equation (8) has two solutions for α, but α and $-\alpha$ still map to distinct x's so Equation (7) still has two solutions. When $\alpha = -\alpha^{-1}$ ($\alpha = 2$, or 3), then Equation (8) has two solutions and in this case α and $-\alpha$ map to the same x so Equation (7) has one solution. Other than these two situations Equation (8) always has four solutions and thus Equation (7) has two solutions.

For all of the APN functions of Table I, $\Delta_{f,a} = b$ has either zero or two solutions for all b's except one where it has a single solution. It means that, for each a, there is only one b such that these two solutions are the same. Hence, based on Proposition 10 the deficiency of f is $(q-1)\left(\frac{q-1}{2}-1\right) = (q-1)\left(\frac{q-3}{2}\right)$ and the ambiguity of f is $(q-1)\left(\frac{q-1}{2}\right)$. ■

V. A MEASURE FOR BEING CLOSER TO OPTIMAL AMBIGUITY

Let $\mathrm{Opt}_{G_1,G_2}(f)$ denote the optimum ambiguity of the function $f : G_1 \to G_2$ for Abelian groups G_1 and G_2. Then, we can define the *normalized ambiguity* of a function f as the ratio

$$\mathrm{Opt}^*_{G_1,G_2}(f) = \frac{\mathrm{A}(f)}{\mathrm{Opt}_{G_1,G_2}(f)}.$$

It is obvious that $\mathrm{Opt}^*_{G_1,G_2}(f) \geq 1$. Furthermore, it can be easily seen that the functions with optimum ambiguity that we constructed in Section IV have normalized ambiguity equal to one.

Proposition 18. *All the functions with optimum ambiguity including the twisted monomial g introduced in Subsection IV-A for finite fields $\mathbb{F}_q$ such that $q \equiv 2 \pmod 3$, the Möbius function in the multiplicative group of a field $\mathbb{F}_q$ with $q \equiv 2 \pmod 3$, the inverse function in the additive group of a field of characteristic $p = 2$ with odd exponent, and the cubic function in a field of characteristic $p = 2$ have normalized ambiguity equal to 1.*

Therefore, this parameter can be imagined as a measure for functions to be close to optimal ambiguity. The closer $\mathrm{Opt}^*_{G_1,G_2}(f)$ is to one, the closer f is to being optimal in ambiguity. For example, let us recall the Möbius function. According to Lemma 2, ambiguity and deficiency of Möbius function on the additive group of a finite field $\mathbb{F}_q$ are equal to the ambiguity and deficiency of all of its linear transformations. Hence the ambiguity and deficiency of g in Theorem 15 are equal to the ambiguity and deficiency of the inverse function.

Proposition 19. *Let $q = 2^m$ where m is even. Then the Möbius function over the multiplicative group of $\mathbb{F}_q$ is closer to being optimal in ambiguity than the Möbius function (inverse function) over the additive group of $\mathbb{F}_q$ in terms of ambiguity.*

Proof: According to the above paragraph, the ambiguity of the Möbius function in the additive group of $\mathbb{F}_q$ is $(q-1)\left(\frac{q}{2}+4\right)$ while the optimum ambiguity is $(q-1)\frac{q}{2}$. So,

$$\mathrm{Opt}^*_{\mathbb{F}_q,\mathbb{F}_q}(g) = \frac{(q-1)\left(\frac{q}{2}+4\right)}{(q-1)\frac{q}{2}} = 1 + \frac{8}{q}.$$

In addition the worst case (m even) ambiguity of the Möbius function in the multiplicative group of $\mathbb{F}_q$ is $2n$ where $n = q-1$. Also the optimum ambiguity in this case is $2(n-1)$. Hence

$$\mathrm{Opt}^*_{\mathbb{Z}_n,\mathbb{Z}_n}(f) = \frac{2n}{2n-2} = 1 + \frac{2}{2n-2} = 1 + \frac{1}{q-2}.$$

It is clear that $\frac{1}{q-2} < \frac{8}{q}$ for $q > 2$, and this implies that the Möbius function over the multiplicative group of $\mathbb{F}_q$ is closer to be APN than the inverse function (Möbius function) over additive group of $\mathbb{F}_q$. ∎

Massey [15] uses $f(x) = (45^x \bmod 257) \bmod 256$ and its inverse in the SAFER cryptosystem. Drakakis, Gow and McGuire [8] show that the shift $g(x) = (45^x \bmod 257) - 1$ of the above permutation and its inverse are APN permutations in $\mathbb{Z}_{256}$. Thus both functions and their inverses have the same deficiency and ambiguity. For the S-box of the SAFER cryptosystem, as a map of $\mathbb{Z}_{256}$ to itself, our SAGE program calculates its deficiency and ambiguity as 10865 and 11120 respectively. We have shown in Theorems 14 and 15 that our twisted permutation polynomials in $\mathbb{Z}_{256}$ have optimum deficiency and ambiguity, 253 and 508, respectively. SAFER's S-box's deficiency and ambiguity are both more than 20 times larger than optimal. We also use SAGE program to calculate another important measure, linearity, of cryptographic functions [9]. We verify that the linearity of $f(x)$ used in SAFER cryptosystem is 42.484 (see [9]) and obtain the linearity of our twisted permutation polynomials, both those from Theorems 14 and 15, is 17.0312, which is very close to the lower bound 16.

VI. Conclusions

In this paper, we have studied a lower bound for the ambiguity and deficiency of permutations of finite Abelian groups. In particular, we obtained several constructions of permutations in the cyclic group $\mathbb{Z}_n$ where $n = p^m - 1$ which meet the optimum lower bound. In [20], we have given an example of permutation of $\mathbb{Z}_5$, which does not come from our construction but it does come from Table I. A natural question is to find more constructions achieving the optimum bound. Optimum ambiguity and deficiency of permutations of group $\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ are interesting as they are related to the concept of APN permutation of finite fields. We have shown optimum ambiguity implies APN and the converse also holds if the finite field has even characteristic. Some preliminary calculations have suggested that ambiguity and deficiency measures are related to the *linearity* of a function and we are currently investigating this. It is desirable to understand the distribution of ambiguity and deficiency of APN permutations of finite fields. We have checked that no functions from $\mathbb{Z}_3$ and $\mathbb{Z}_{15}$ to itself can achieve the optimum ambiguity which is $2n-2$; only $2n$ is possible and all these functions have two instances of 3-to-1 behaviour.

We have treated the case when the function between the two Abelian groups is a bijection. If the groups are the same size and the function is not bijective then the existence of Perfectly Non-linear (PN) functions shows that the ambiguity and deficiency are not bounded away from 0 in general. In fact the following are all equivalent

- a map, f, being a PN function,
- $A(f) = 0$,
- $D(f) = 0$.

We would like to know if there are certain groups where ambiguity and deficiency of non-bijections are bounded away from zero? Second, even if non bijections with zero ambiguity and deficiency could exist for maps between two groups, $G_1 \to G_2$, what is the spectrum of deficiencies and ambiguities that can be realized? This question is relevant for bijections as well. Finally we note that maps of deficiency zero between groups, not necessarily of the same size, have been used in efficient constructions for covering arrays [3], [6], [16] although the term "deficiency" was not defined nor used. Further studies of ambiguity and deficiency in these more general settings would be interesting and is open for further research.

References

[1] C. Carlet and C. Ding, "Highly nonlinear mappings", *J. Compl.*, vol. 20, no. 2, pp. 205–244, 2004.

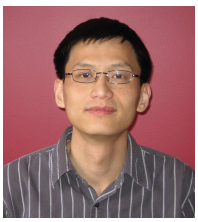
[2] C. J. Colbourn and J. H. Dinitz, editors, *Handbook of Combinatorial Designs*, Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[3] C. J. Colbourn, S. S. Martirosyan, G. L. Mullen, D. Shasha, G. B. Sherwood, and J. L. Yucas, "Products of mixed covering arrays of strength two", *J. Combin. Des.*, vol. 14 no. 2, pp. 124–138, 2006.
[4] J. P. Costas, "A study of a class of detection waveforms having nearly ideal range-doppler ambiguity properties", *Proceedings of IEEE*, vol. 72, pp. 996–1009, 1984.
[5] J. Daemen, and V. Rijmen, "*The Design of Rijndael: AES - The Advanced Encryption Standard*", Springer, 2002.
[6] P. Danziger, J. Lobb, and B. Stevens, "The use of cover starters to create strength two covering arrays", In preparation.
[7] K. Drakakis, "A review of Costas arrays", *J. Appl. Math.*, Art. ID 26385, 32, 2006.
[8] K. Drakakis, R. Gow, and G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays", *Discrete Applied Mathematics*, vol. 157, no. 15, pp. 3320–3326, 2009.
[9] K. Drakakis, V. Requena, and G. McGuire, "On the nonlinearity of exponential Welch Costas functions", *IEEE Trans. Inform. Theory*, vol. 56, no. 3, pp. 1230–1238, 2010.
[10] S. W. Golomb, and G. Gong, *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*, Cambridge University Press, Cambridge, 2004, New York, NY, USA.
[11] T. Helleseth, C. Rong, and D. Sandberg, "New families of almost perfect nonlinear power mappings", *IEEE Trans. Inform. Theory*, vol. 45, pp. 475-485, 1999.
[12] R. Lidl and G. L. Mullen, "Unsolved problems: when does a polynomial over a finite field permute the elements of the field?", *Amer. Math. Monthly*, vol. 95, no. 3, pp. 243–246, 1988.
[13] R. Lidl and G. L. Mullen, "Unsolved problems: when does a polynomial over a finite field permute the elements of the field? II", *Amer. Math. Monthly*, vol. 100, no. 1, pp. 71–74, 1993.
[14] R. Lidl and H. Niederreiter, *Finite Fields*, vol. 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, second edition, 1997.
[15] J. Massey, "SAFER K_{64}: A byte-oriented block-ciphering algorithm", *Fast Software Encryption*, pp. 1–17, 1993.
[16] K. Meagher and B. Stevens, "Group construction of covering arrays", *J. Combin. Des.*, vol. 13, no. 1, pp. 70–77, 2005.
[17] G. L. Mullen, Permutation polynomials over finite fields, *Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991)*, vol. 141 of *Lecture Notes in Pure and Appl. Math.*, pp. 131–151, 1993.
[18] G. L. Mullen and H. Stevens, "Polynomial functions (mod m)", *Acta Mathematica, Hungarica* vol.44 no. 3–4, pp. 237-241, 1984.
[19] K. Nyberg, "Differentially uniform mappings for cryptography", *Advances in cryptology—EUROCRYPT'93 (Lofthus, 1993)*, vol. 765 of *Lecture Notes in Comput. Sci.*, pp. 55–64, 1994.
[20] D. Panario, B. Stevens and Q. Wang, "Ambiguity and deficiency in Costas arrays and APN permutations" *LATIN 2010: Theoretical Informatics (Mexico, 2010)–LATIN 2010*, vol. 6034, *Lecture Notes in Comput. Sci.*, pp. 397–406, 2010.
[21] R. L. Rivest, "Permutation polynomials modulo 2^w", *Finite Fields and their Applications*, vol. 7, pp. 287–292, 2001.
[22] A. Sakzad, D. Panario, M-R. Sadeghi and N. Eshghi, "Self-inverse interleavers based on permutation functions for turbo codes", Proc. of 48th Ann. Allerton Conf. Commun. Control, and Computing, pp 22-28, 2010.
[23] J. Sun and O. Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings", *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 101–119, 2005.
[24] SAGE Mathematics Software, Version 4.3, http://www.sagemath.org/, Online; accessed 18-November-2010.

Daniel Panario was born in Uruguay where he studied Mathematics and Computer Science. He received a M.Sc. degree from the University of São Paulo (Brazil) and a Ph.D. from the University of Toronto (Canada). He is Professor of Mathematics at Carleton University in Ottawa (Canada), and a Senior Member of IEEE. His main research interests are in finite fields and applications, and in analysis of algorithms.

Amin Sakzad was born in Iran where he received the B.Sc., M.Sc. and Ph.D. degree from the Amirkabir University of Technology, Tehran, Iran, in 2005, 2007, and 2011 respectively, all in pure and applied Mathematics. He was a research visitor and a lecturer at Carleton University, Ottawa, ON, Canada, in 2010. He is currently a researcher and a lecturer at the Amirkabir University of Technology, Tehran (Iran). His research interests include lattice coding theory and applications, network coding and cryptography.

Brett Stevens was educated at the University of Chicago, University College London and the University of Toronto. His M.Sc. was in mathematical biology and his Ph.D. in mathematics, specifically combinatorics. He did post-doctoral work at Simon Fraser University and IBM T.J. Watson Laboratories. He is interested in combinatorics, applications of mathematics and the interaction of mathematics with other disciplines and culture. He is Professor in Mathematics at Carleton University.



Qiang Wang was born in China where he received B. Sc., M.Sc. degrees in Mathematics from ShaanXi Normal University (China). He received a M. Sc. Degree in information and System Science from Carleton University (Canada) and a Ph.D. in Mathematics from the Memorial University of Newfoundland (Canada). He is currently an Associate Professor at Carleton University in Ottawa (Canada). His main research interests are in finite fields and applications in coding theory, combinatorics, and cryptography.