Ambiguity and Deficiency of Permutations over Finite Fields with Linearized Difference Map

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

Abstract

The concepts of ambiguity and deficiency for a bijection on a finite Abelian group were recently introduced. In this work, we present some further fundamental results on the ambiguity and deficiency of functions; in particular, we note that they are invariant under the well-known CCZ-equivalence, we obtain upper and lower bounds on the ambiguity and deficiency of differentially k-uniform functions, and we give a lower-bound on the non-linearity of functions that achieve the lower-bound of ambiguity and deficiency. In addition, we provide an explicit formula in terms of the ranks of matrices on the ambiguity and deficiency of a Dembowski-Ostrom (DO) polynomial and using this technique we find exact values for known cases of DO permutations with few terms. We also derive exact values for the ambiguities and deficiencies of DO permutations obtained by trace functions. The key relationship between the above polynomials is that they all have linearized difference map.

Index Terms

Ambiguity, Deficiency, Non-linearity, Permutation Polynomials, Finite Fields, DO-Polynomials, Linearized Polynomials.

I. Introduction

Polynomials over finite rings can be viewed as maps between finite rings, or between finite groups. In this paper, we study mappings between two finite Abelian groups of the same cardinality, in particular, bijective mappings. A permutation polynomial over a finite ring $\mathcal{R}$ induces a bijective map from $\mathcal{R}$ to $\mathcal{R}$. Due to their applications in coding theory, combinatorics and cryptography, there has been considerable interest in studying these permutation polynomials [30], [31], [32]. We are chiefly interested in the finite field $\mathbb{F}_q$ and the finite ring $\mathbb{Z}_n$. For more background on permutation polynomials over finite fields we refer to [19, Chapter 7] and [23, Section 8.1]. For detailed surveys of open questions and results up to 1993 see [1], [17], [18], [21], [23]. For permutation polynomials over $\mathbb{Z}_n$, we refer the readers to [22], [27].

The ambiguity and deficiency of a given bijection F on a finite Abelian group $\mathcal{G}$ were introduced recently in [24], [26] to measure the surjectivity and injectivity of the *difference map* $\Delta_{F,a}(x) = F(x+a) - F(x)$ at $a \in \mathcal{G}$. In this work, we also primarily consider bijections, but we extend the definition to general maps between finite Abelian groups in a natural way. In the case of maps between finite fields, attaining the minimum ambiguity implies that F is *almost perfect non-linear* (APN), which means that each difference map for $a \neq 0$ is at worst 2-to-1. However, not every APN function attains the minimum ambiguity and deficiency. In particular, we give lower and upper bounds on the ambiguity and deficiency of all differentially k-uniform functions. These bounds are tight for differentially 2-uniform, equivalently APN, functions over binary fields.

The *non-linearity* of a function measures the distance of that function to the set of all affine functions [13]. Highly non-linear functions are desired due to their resistance to linear cryptanalysis [20]. We relate these two concepts

Daniel Panario, Brett Stevens, David Thomson and Qiang Wang are with the School of Mathematics and Statistics, Carleton University. E-mails: {daniel,brett,dthomson,wang}@math.carleton.ca.

Amin Sakzad is currently with the Department of Electrical and Computer Systems Engineering, Monash University, Australia. This work was initiated when he was with the Department of Mathematics and Computer Science, Amirkabir University of Technology, Tehran, Iran and completed at the Monash Software Defined Telecommunications Lab supported by the Talented Enhancement Scheme through the Monash Professorial Fellowship (MPF) program. E-mail: amin.sakzad@monash.edu.

A subset of this work was presented at ITW 2011, Paraty, Brazil. The statements of Lemma 1, Theorem 10 and Theorem 13 appear in the conference proceedings [25]. The proofs of Lemma 1 and Theorem 13 appear only in this paper (Theorem 10 is a known result and is given without proof). Furthermore, our statement of the deficiencies of these cases differs slightly from [25].

by finding a lower-bound on the non-linearity of a bijection which attains optimum ambiguity and deficiency. In the characteristic 2 case, similar relationships between known APN functions and functions with good non-linear characteristics can be found in [5]. In contrast, in this work we focus primarily on the non-linearity of bijections between finite fields of odd characteristics and on bijections between finite cyclic groups. Furthermore, in [5] Carlet analyzes the non-linearity of APN and almost bent (AB) functions as well as differential 4-uniform functions, and so on. Permutations with minimum ambiguity and deficiency (between non-2-groups) are APN, but not necessarily vice versa [24], [26]. Similarly, in this paper we show that these functions have strong non-linearity, but they are not necessarily perfectly balanced and therefore not necessarily bent.

Two notions of equivalence of functions which are significant in the cryptographic setting are *extended affine* (EA) and *Carlet-Charpin-Zinoviev* (CCZ) equivalence [6]. It is well-known that EA-equivalence implies CCZ-equivalence and the property of a function being APN is invariant under CCZ-equivalence [6]. The measures of ambiguity and deficiency are known to be EA-invariant parameters (that is, functions which are EA-equivalent have equal ambiguity and deficiency). In this work, we comment on the CCZ-invariance of the ambiguity and deficiency of functions.

If the group considered is the additive group of a finite field with even characteristic, a permutation attaining the minimum ambiguity is equivalent to an APN permutation [24]. The existence of an APN permutation of $\mathbb{F}_{2^6}$ was determined in [4], and searching for APN permutations over larger binary fields is still an open problem. Instead, in this work we investigate the ambiguity and deficiency of several well-known polynomials over finite fields without imposing the minimum restrictions on their ambiguities and deficiencies. The polynomials considered in this paper have a common property: all of them have linearized difference maps. These permutation polynomials are DO permutation polynomials [2] and permutation polynomials based on trace function [7].

A summary of the paper is as follows. In Section II, we provide some basic results on ambiguities and deficiencies. We supply some new results on ambiguities and deficiencies in Section III. In particular, we follow the well-known proof that the APN property is invariant under CCZ-equivalence and show that ambiguity and deficiency are also invariant under CCZ-equivalence. The lower and upper bounds on the ambiguity and deficiency of differentially k-uniform functions are provided in this section. Additionally, we show that functions with optimal ambiguity and deficiency also achieve good non-linearity, except over finite fields of characteristic two. In Section IV, we introduce some permutations of interest over finite fields and compute the ambiguities and deficiencies of them. Specifically, we derive a formula for the ambiguity and deficiency of any DO-polynomial in terms of ranks of matrices and analyze these matrices for some specific DO permutations. Permutations based on trace functions are also considered in this section. We present some conclusions and areas for future work in Section V.

II. Preliminaries

In order to make this work self-contained, we review the notions of ambiguity and deficiency of functions, as well as relevant results about ambiguity and deficiency.

Let us review the concept of APN functions first. Let $\mathcal{G}$ be a finite group, let $\mathcal{G}^* = \mathcal{G} \setminus \{0\}$ and let $a \in \mathcal{G}^*$. The *difference map* of a function F at $a \in \mathcal{G}^*$ is given by $\Delta_{F,a}(x) = F(x+a) - F(x)$. The function F is said to be *almost perfect non-linear* (APN) if $\Delta_{F,a}(x) = b$ has at most two solutions for all $a \in \mathcal{G}^*$ and all $b \in \mathcal{G}$. The *differential uniformity* of F is the minimum k such that $\Delta_{F,a}$ is at most k-to-1 for all a's.

Now we provide the definitions of ambiguity and deficiency of a function. These notions were introduced first in [26]. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be two finite Abelian groups (possibly of different cardinalities) and let F be a function from $\mathcal{G}_1$ to $\mathcal{G}_2$. Furthermore, let

$$n_k(F) = \left| \left\{ (a,b) \in \mathcal{G}_1^* \times \mathcal{G}_2 \colon \left| \Delta_{F,a}^{-1}(b) \right| = k \right\} \right|$$

for $0 \leq k \leq n$. We call $n_0(F)$ the *deficiency* of F and denote it by $\mathfrak{D}(F)$. Hence the deficiency 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 $\Delta_{F,a}$ collectively are to surjective. We also define the *row-a-deficiency* as

$$\mathfrak{D}_{r=a}(F) = \left| \left\{ b \colon \left| \Delta_{F,a}^{-1}(b) \right| = 0, b \in \mathcal{G}_2 \right\} \right|.$$

We similarly define a measure of the injectivity of the functions $\Delta_{F,a}$, called the *ambiguity* of F, such that the lower the ambiguity of F, the closer the $\Delta_{F,a}$ are to injective. The *(weighted) ambiguity* of F can be defined as

$$\mathfrak{A}(F) = \sum_{0 \le k \le n} n_k(F) \binom{k}{2}.$$

We explain this weighting as follows: contributions from n_0 and n_1 (that is, the number of elements of the codomain which have 0 or 1 preimage) vanish and the weighted ambiguity of F measures the replication of pairs x and x' such that $\Delta_{F,a}(x) = \Delta_{F,a}(x')$.

One of the early motivations for studying ambiguity and deficiency specifically was an application to design theory. Briefly, if $F : \mathcal{G}_1 \to \mathcal{G}_2$ is a function between two Abelian groups with $|\mathcal{G}_1| = |\mathcal{G}_2| = n$, then we can construct an orthogonal doubly resolvable block design on n^2 points with n^2 blocks of size n [9, Section II.7.7]. The point set is $\mathcal{V} = \mathcal{G}_1 \times \mathcal{G}_2$. The block set is also indexed by $\mathcal{G}_1 \times \mathcal{G}_2$, where $(a, b) \in \mathcal{G}_1 \times \mathcal{G}_2$, gives the block $\mathcal{B}_{a,b} = \{(x, F(x + a) + b) \colon x \in \mathcal{G}_1\}$. The two resolutions correspond to the different $a \in \mathcal{G}_1$ and the different $b \in \mathcal{G}_2$, respectively. This design is used specifically to schedule a tournament which is broken into n rounds with n separate venues. In the scheduling of this tournament we are interested in the number of times any pair of players play together in the same venue in the same round. More specifically we want to minimize the number of pairs that miss each other totally and minimize the number of pairs that play together repeatedly. One of the first solutions to this problem came from a modification of the affine plane and achieved a globally minimal number of repetitions, but the schedule is rejected because there are n pairs of players that *always* play together in every round. A subsequent restraint was added that forbids any pair playing together more than twice. Ambiguity and deficiency are now the natural target measures. A deficiency of d corresponds to a tournament in which $(d - n + 1)n^2/2$ pairs miss playing together, and bounds on deficiency (see Theorem 1) give the best possible behaviour in this measure. Ambiguity is now the simplest measure in which achieving the minimum bounds *guarantees* that the worst repetitions are size two. Equivalently, ambiguity is a modification of counting the cardinality of the set $\{(x, y, \mathcal{B}) : \mathcal{B} \in \{\mathcal{B}_{a,b}\}, \quad x \neq y, \quad x, y \in \mathcal{B}\}$ which is a frequently encountered set in design theory. It was only later that we recognized the connections to PNs, APNs and cryptographic applications.

Some related measures for cryptographic applications are introduced in the literature; for example, the *differential spectrum* of F is the multi-set of the $n_k(F)$. Thus, knowing the entire differential spectrum of a function implies knowledge of the ambiguity and deficiency. The differential spectra of functions $F(x) = x^{2^t-1} \in \mathbb{F}_{2^n}[x]$ is considered in [3], generalizing known results on inverse functions. We therefore immediately inherit the corresponding results on ambiguity and deficiency of these functions. The presentation of ambiguity and deficiency has some advantages. For example, the proof of Theorem 1 below, which appears in [25], uses the equality of the ambiguity of a function with the sum of both its row-ambiguities (with fixed *direction*, a, of the derivative $\Delta_{F,a}$) and column-ambiguities (with fixed image $b \in \mathcal{G}_2$). These are quite natural notions in the language of ambiguity and deficiency.

The optimum ambiguity and deficiency of a mapping can be derived using the following theorem cited from [24].

Theorem 1: Let $F : \mathcal{G} \to \mathcal{G}$ be a permutation, where $\mathcal{G}$ is an Abelian group of order n. Let $\mathcal{I}$ be the set of elements of order 2 in $\mathcal{G}$ such that $\iota = |\mathcal{I}|$. Then, both the ambiguity and deficiency of F are bounded below by

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

In [24] the deficiency numbers are cited as these less a factor of $n-1$. This is because in [24] the authors consider $b \in \mathcal{G} \setminus \{0\}$ since $\Delta_{F,a}(x) \neq 0$ for permutation functions. In this paper we consider the entire codomain, since the inclusion of 0 to the codomain of $\Delta_{F,a}$ maintains consistency across all functions (not necessarily permutations). We note, however, that all of the results cited in [24] are correct in their setting.

A function whose ambiguity (deficiency) achieves the lower-bound of the above theorem is said to have *optimum ambiguity* (*optimum deficiency*, respectively). Let $\mathrm{OA}_F(\mathcal{G})$ and $\mathrm{OD}_F(\mathcal{G})$ denote the optimum ambiguity and optimum deficiency of a permutation F on $\mathcal{G}$, respectively. Let p be a prime number, $q = p^e$ and $\mathbb{F}_q$ denote the finite field of order q. If we suppose that $\mathcal{G} = (\mathbb{F}_q, +)$, then the ambiguity and deficiency depend on the characteristic p of $\mathbb{F}_q$. The following corollary is a simple consequence of the above theorem and the fact that every non-zero element of $\mathbb{F}_q$, $\mathrm{char}(\mathbb{F}_q) = 2$, has order 2.

TABLE I
THE OPTIMUM AMBIGUITY AND DEFICIENCY OF PERMUTATIONS OVER $\mathbb{F}_q$.

	$\mathrm{OA}_F(\mathbb{F}_q)$	$\mathrm{OD}_F(\mathbb{F}_q)$
p odd	$2(q-1)$	$2(q-1)$
p even	$(q-1)(\frac{q}{2})$	$(q-1)(\frac{q}{2})$

Corollary 1: The optimum ambiguity and deficiency of a permutation F over a finite field $\mathbb{F}_q$ is given in Table I.

Optimal functions with respect to ambiguity have the APN property. In other words, if a permutation $F : \mathcal{G} \to \mathcal{G}$ achieves the minimal ambiguity, then F is APN. The reverse of this statement is generally true only if the cardinality of $\mathcal{G}$ is a power of 2; see [24]. The ambiguity and deficiency of some well-known permutations such as twisted binomials and Möbius transformations are computed in [24]. These are evaluated on both additive and multiplicative groups of the finite field $\mathbb{F}_q$.

III. NEW RESULTS ON AMBIGUITY AND DEFICIENCY

In this section, we present some new important results about the ambiguity and deficiency measures. In particular, we note that these measures are invariant under certain common types of equivalence for cryptography, we provide lower and upper bounds on the ambiguity and deficiency of differentially k-uniform functions, and we give a connection between functions with good (low) ambiguity and deficiency and highly non-linear functions.

A. CCZ-invariance of ambiguity and deficiency

It is a simple exercise to see that a permutation and its compositional inverse have the same ambiguity and deficiency. Using this as motivation, we note that the ambiguity and deficiency of a function are invariant parameters under some other transformations. For example, adding a fixed element or applying an automorphism of $\mathcal{G}$ to the left or right of F, does not affect these two measures for permutations on $\mathcal{G}$ [24]. We extend this to common equivalence classes of cryptographic functions.

Definition 1: A function $L\colon \mathcal{G}_1 \to \mathcal{G}_2$ is *linear* if $L(x+y) = L(x) + L(y)$ for all $x, y \in \mathcal{G}_1$. A function $K\colon \mathcal{G}_1 \to \mathcal{G}_2$ is *affine* if $K(x+y) = K(x) + K(y) + c$ for a fixed constant $c \in \mathcal{G}_2$ and every $x, y \in \mathcal{G}_1$.

In the classical definition of EA-equivalence, $\mathcal{G}_1 = \mathcal{G}_2 = (\mathbb{F}_{2^e}, +)$. While this is the most common practical case, our scope is more general and so we relax the restrictions on the domain and codomain.

Definition 2: Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be arbitrary groups. Two functions F_1 and $F_2 : \mathcal{G}_1 \to \mathcal{G}_2$ are *extended affine equivalent* (EA-equivalent), denoted $F_1 \overset{\mathrm{EA}}{\sim} F_2$, if there exist affine permutations $K_1\colon \mathcal{G}_2 \to \mathcal{G}_2, K_2\colon \mathcal{G}_1 \to \mathcal{G}_1$ and an affine function $K_3\colon \mathcal{G}_1 \to \mathcal{G}_2$ such that

$$F_2 = K_1 \circ F_1 \circ K_2 + K_3.$$

If $K_3 = 0$, then F_1 and F_2 are *affine equivalent*.

The nomenclature is well-defined: EA-equivalence is an equivalence relation on functions. EA-invariance of ambiguity and deficiency was shown in [24]. We present another standard definition of equivalence, introduced in [6]. As in EA-equivalence, we extend the usual definition to arbitrary groups. First, we introduce some necessary notation. Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be arbitrary groups. If $F\colon \mathcal{G}_1 \to \mathcal{G}_2$ be a function, then the *graph* of F is defined as

$$\mathcal{G}_F = \{(x, F(x)) : x \in \mathcal{G}_1\} \subseteq \mathcal{G}_1 \times \mathcal{G}_2.$$

Definition 3: The relation $\overset{\mathrm{CCZ}}{\sim}$ defined on the set of functions $\mathcal{G}_1 \to \mathcal{G}_2$ such that $F_1 \overset{\mathrm{CCZ}}{\sim} F_2$ if and only if

$$K(\mathcal{G}_{F_1}) = \mathcal{G}_{F_2}$$

for some affine permutation $K\colon \mathcal{G}_1 \times \mathcal{G}_2 \to \mathcal{G}_1 \times \mathcal{G}_2$ is an equivalence relation. Functions in the same equivalence class are said to be *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent).

It is easy to see that EA-equivalence implies CCZ-equivalence. In other words, if two functions are EA-equivalent, then they are CCZ-equivalent. Ambiguity and deficiency are shown to be EA-invariant parameters in [24]. Since CCZ-equivalence classes are larger than EA-equivalence classes, showing CCZ-invariance of these parameters is a

stronger result. We note that the proof is similar to that of the APN case, indeed the proof that the APN property is preserved also shows that differential uniformity is preserved. For these reasons, we do not include the proof of the following theorem.

Theorem 2: The differential spectrum of functions is invariant (up to permutation) under CCZ-equivalence.

Corollary 2: Let $F\colon \mathcal{G}_1 \to \mathcal{G}_2 \overset{\text{CCZ}}{\sim} F'\colon \mathcal{G}_1 \to \mathcal{G}_2$. The properties of PN, APN, ambiguity and deficiency are all invariant between F and F'.

B. Results on differentially k-uniform functions

We give next our second result of this section: upper and lower bounds for the ambiguity and deficiency of differentially k-uniform functions.

Theorem 3: Let $F\colon \mathcal{G} \to \mathcal{G}$ be a function with differential uniformity k. Suppose further that $|\mathcal{G}| = n = rk + s$, for some r, s with $0 \leq s < n$. Then the ambiguity of F satisfies

$$\binom{k}{2} \leq \mathfrak{A}(F) \leq (n-1)\left(r\binom{k}{2} + \binom{s}{2}\right),$$

and the deficiency of F satisfies

$$k - 1 \leq \mathfrak{D}(F) \leq (n-1)\left(n - r + \delta_s\right),$$

where $\delta_s = 0$ if $s = 0$ and $\delta_s = 1$ otherwise.

Proof: Let $F\colon \mathcal{G} \to \mathcal{G}$ be a function having differential uniformity k. Thus, $\Delta_{F,a}(x) = b$ has at most k solutions for all $(a, b) \in (\mathcal{G}^*, \mathcal{G})$. As in the hypothesis, suppose $|\mathcal{G}| = n = rk + s$ for some r, s with $0 \leq s < n$.

For the lower bound, suppose $\Delta_{F,a}(x) = b$ has k solutions for a single pair (a, b), and has either a unique solution or no solution for all other pairs $(a', b') \neq (a, b)$. Contributions to the ambiguity come only from the pair (a, b). The lower bound on the deficiency occurs in the same scenario. In this case, $|\Delta_{F,a}(\mathcal{G})| = n - k + 1$ and $\Delta_{F,a'}(\mathcal{G}) = \mathcal{G}$ for $a' \neq a$.

The upper bound is attained when $\Delta_{F,a}(x) = b$ has either k solutions or no solution for all pairs (a, b). Additionally, if k does not divide n, the maximum ambiguity and the maximum deficiency are both attained when, for each a, the images of the remaining s elements of $\Delta_{F,a}$ coincide. ■

C. Connections to non-linearity

The resistance of an S-box to linear cryptanalysis can be measured by the *non-linearity* of the function used in that S-box, with highly non-linear functions preferred. We present the notions in full generality and later restrict the definitions to the particular cases in which we use them. The general form of the non-linearity of a mapping between any two finite groups was introduced in [13].

Let $(\mathcal{G}, +)$ be a finite Abelian group. The Fourier transform of any complex-valued function Φ on $\mathcal{G}$ is given by

$$\widehat{\Phi}(\chi) = \sum_{x \in \mathcal{G}} \Phi(x)\chi(x),$$

where χ is a character of $\mathcal{G}$. Since the group of characters of $\mathcal{G}$, denoted by $\widehat{\mathcal{G}}$, is isomorphic to $\mathcal{G}$ itself, denote χ_α to be the image of α under an arbitrary but fixed isomorphism of $\mathcal{G}$ to $\widehat{\mathcal{G}}$. Then we write

$$\widehat{\Phi}(\alpha) = \sum_{x \in \mathcal{G}} \Phi(x)\chi_\alpha(x).$$

We can therefore consider $\widehat{\Phi}$ to be defined on the group $\mathcal{G}$.

If F is a function between finite Abelian groups $\mathcal{G}_1$ and $\mathcal{G}_2$, then identifying ψ_β as the image of $\beta \in \mathcal{G}_2$ under any isomorphism from $\mathcal{G}_2 \to \widehat{\mathcal{G}_2}$, we define the Fourier transform of F at $\alpha \in \mathcal{G}_1$ and $\beta \in \mathcal{G}_2$ by

$$\widehat{F}(\alpha, \beta) = \sum_{x \in \mathcal{G}_1} (\psi_\beta \circ F)(x)\chi_\alpha(x),$$

for all $x \in \mathcal{G}_1$.

Definition 4: If $F\colon \mathcal{G}_1 \to \mathcal{G}_2$, the *linearity* of F is given by

$$\mathfrak{L}(F) = \max_{\alpha\in\mathcal{G}_1,\beta\in\mathcal{G}_2^*} |\widehat{F}(\alpha,\beta)|.$$

The non-linearity of a function is finally given by the following normalized measure.

Definition 5: Let $\mathcal{G}_1$, $\mathcal{G}_2$ be finite Abelian groups, and $F\colon \mathcal{G}_1 \to \mathcal{G}_2$. The *non-linearity* of F is given by

$$\mathfrak{NL}(F) = \frac{|\mathcal{G}_1| - \mathfrak{L}(F)}{|\mathcal{G}_2|}.$$

The non-linearity of F is 0 if and only if F is an affine function. In the remainder of this section, we derive a lower-bound on the non-linearity of a bijective function which achieves the minimum ambiguity and deficiency over the additive group of a finite field (of both odd and even characteristic) and over a finite cyclic group. We recall that such a permutation function is APN.

1) The additive group of a finite field: In what follows, we assume $\mathcal{G}_1 = \mathcal{G}_2 = (\mathbb{F}_q, +)$, for some prime power q. Lower-bounds on the optimum ambiguity and deficiency of F in terms of its domain and codomain are given in Theorem 1. We note that when q is even, functions which meet the bound in Theorem 1 are precisely the APN functions [24]. We give bounds on the non-linearity of F depending on whether q is odd or even.

Let $\lambda_F(a,b) = \sum_{x\in\mathcal{G}_1} \chi(aF(x)+bx)$, where χ is an additive character $\mathcal{G}_1 \to \mathbb{C}$, that is $\lambda_F(a,b) = \widehat{F}(b,a)$. Thus,

$$\begin{aligned}
|\lambda_F(a,b)|^2 &= \sum_{x\in\mathcal{G}_1} \chi(aF(x)+bx)\overline{\sum_{y\in\mathcal{G}_1} \chi(aF(y)+by)} \\
&= \sum_{x\in\mathcal{G}_1} \chi\left(aF(x)+bx\right) \sum_{y\in\mathcal{G}_1} \chi\left(-aF(y)-by\right) \\
&= \sum_{x,y\in\mathcal{G}_1} \chi\left(a(F(x)-F(y))+b(x-y)\right),
\end{aligned}$$

and letting $z = x - y$, we get

$$\begin{aligned}
|\lambda_F(a,b)|^2 &= \left| \sum_{z,y\in\mathcal{G}_1} \chi\left(a(F(y+z)-F(y))+bz\right) \right| \\
&= \left| \sum_{z\in\mathcal{G}_1} \chi(bz) \sum_{y\in\mathcal{G}_1} \chi(a\Delta_{F,z}(y)) \right| \\
&= \left| n + \sum_{z\in\mathcal{G}_1, z\neq 0} \chi(bz) \sum_{y\in\mathcal{G}_1} \chi(a\Delta_{F,z}(y)) \right|. \qquad (1)
\end{aligned}$$

Since F is a permutation, for any $z \in \mathcal{G}_1, z \neq 0$ we have $\Delta_{F,z}(y) = F(y+z) - F(y) \neq 0$. Thus, by the Pigeon-Hole Principle, there is a repeated image of $\Delta_{F,z}$, call this image $\widetilde{r_{0,z}} := r_{0,z}/a$.

a) Odd characteristic: Since F has optimum deficiency, for each $z \in \mathcal{G}_1, z \neq 0$, there is exactly one $c \in \mathcal{G}_1\backslash\{0\}$ such that $\Delta_{F,z}(x) = c$ has no solution. Thus, by the Pigeon-Hole Principle there is one omitted value of $\Delta_{F,z}$, call this $\widetilde{o_z} := o_z/a$ and a corresponding repeated image of $\Delta_{F,z}$ denoted $\widetilde{r_z} := r_z/a$.

We must separate the case $b = 0$. If $b = 0$, then with $z \neq 0$ we have

$$|\lambda(a,0)|^2 = \left| n + \sum_{z\neq 0, y\in\mathcal{G}_1} \chi(a\Delta_{F,z}(y)) \right|.$$

We know that $\sum_{x\in\mathcal{G}_1} \chi(x) = 0$ and for each $z \neq 0$ we have that the image multiset of $\Delta_{F,z}$ is given by $\Delta_{F,z}(\mathcal{G}_1) = \mathcal{G}_1\backslash\{0, \widetilde{o_z}\} \cup \{\widetilde{r_{0,z}}, \widetilde{r_z}\}$. We note that $\widetilde{r_{0,z}} \neq \widetilde{r_z}$ due to the minimality condition on the ambiguity. Thus,

$$\sum_{y\in\mathcal{G}_1} \chi(a\Delta_{F,z}(y)) = 0 - \chi(0) - \chi(o_z) + \chi(r_{0,z}) + \chi(r_z)$$

and $|\lambda(a,0)|^2 \leq n + 4(n-1) = 5n - 4$.

If $b \neq 0$, a similar derivation gives

$$\begin{aligned}
|\lambda(a,b)|^2 &= \left| n + \sum_{z \in \mathcal{G}_1, z \neq 0} \chi(bz) \left(0 - \chi(0) - \chi(o_z) + \chi(r_{0,z}) + \chi(r_z)\right) \right| \\
&= \left| n - \sum_{z \in \mathcal{G}_1, z \neq 0} \chi(bz) - \sum_{z \in \mathcal{G}_1, z \neq 0} \chi(bz + o_z) + \sum_{z \in \mathcal{G}_1, z \neq 0} \chi(bz + r_{0,z}) + \sum_{z \in \mathcal{G}_1, z \neq 0} \chi(bz + r_z) \right| \\
&\leq n + 4.
\end{aligned}$$

Hence we have the following theorem.

Theorem 4: Let $\mathcal{G} = (\mathbb{F}_q, +)$ with q odd and let F be a permutation of $\mathcal{G}$ with optimum ambiguity and deficiency. The non-linearity of F satisfies

$$\mathfrak{NL}(F) \geq \frac{q - \sqrt{5q-4}}{q}.$$

b) Even characteristic: When q is even, $(\mathbb{F}_q, +)$ is a 2-group, so the number of order 2 elements is $q - 1$. Thus, we fit in the third case of Theorem 1. We note that functions which achieve the lower-bound of Theorem 1 are APN functions, that is $\Delta_{F,a}$ is 2-to-1 for all $a \in \mathbb{F}_q^*$.

The balanced property of APN functions is somehow the worst possible for the analysis and the Fourier transform does not simplify beyond Equation (1); the multiset $\{a\Delta_{F,z}(\mathcal{G})\}$ contains $n/2$ elements, each repeated twice. Thus,

$$|\lambda(a,b)|^2 \leq \left| n + 2 \sum_{z,y \in \mathcal{G}_1, z \neq 0} \chi(y_{1,z}) + \chi(y_{2,z}) + \cdots + \chi(y_{n/2,z}) \right| \leq n.$$

The bound on the linearity in this case using the coarse bounding of the triangle inequality is equal to the highest possible from Parseval's identity. We note that expanding the sum across all z has potential to vastly improve this bound: if the $\Delta_{f,z}(y)$ are evenly distributed across all $z \neq 0$ and all y, then $|\lambda(a,b)| = \sqrt{n}$, which is the smallest allowable by Parseval's identity.

Indeed, there is only one known APN permutation on finite fields of order 2^e for even e. Its polynomial form is complicated and so we refer the reader to [4]. Using SAGE [29], we calculate the non-linearity of this APN permutation to be $3/4$, hence the linearity of the APN permutation is $2^{\lceil \frac{n+1}{2} \rceil}$.

2) Finite cyclic groups: In what follows, suppose $\mathcal{G}_1 = \mathcal{G}_2$ is the finite cyclic group of order n (isomorphic to $\mathbb{Z}_n$). The characters of $\mathcal{G}_1$ are given by $\psi_j \colon \mathcal{G}_1 \to \mathbb{C}$ with $\psi_j(g^k) = e^{2\pi i j k/n}$, where g is a generator of $\mathcal{G}_1$ and $i = \sqrt{-1}$. In particular, every character is a power of ψ_1.

Let $\alpha \in \mathcal{G}_1$ and let $\beta \in \mathcal{G}_1^*$ (written multiplicatively so that $\beta \neq 1$). We have $\widehat{F}(\alpha,\beta) = \sum_{x \in \mathcal{G}_1} (\phi_\beta \circ F)(x) \chi_\alpha(x)$, where χ_α and ϕ_β are the characters obtained by some injection $\mathcal{G}_1 \to \mathbb{C}$. We note that χ_1 is the trivial character (in what follows, we think of $\alpha' = 0$) and for $\alpha \neq 1$, we set $\chi_\alpha = \psi_1^{\alpha'}$ and $\phi_\beta = \psi_1^{\beta'}$. Then

$$\begin{aligned}
\widehat{F}(\alpha,\beta) &= \sum_{x \in \mathcal{G}_1} \left(\psi_1^{\beta'} \circ F\right)(x) \psi_1^{\alpha'}(x) \\
&= \sum_{x \in \mathcal{G}_1} \exp(2\pi i \beta' \log_g(F(x))/n) \exp(2\pi i \alpha' \log_g(x)/n) \\
&= \sum_{x \in \mathcal{G}_1} \exp\left(2\pi i/n \left(\beta' \log_g(F(x)) + \alpha' \log_g(x)\right)\right) \\
&= \sum_{x \in \mathcal{G}_1} \exp\left(2\pi i/n \left(\log_g(F(x)^{\beta'} x^{\alpha'})\right)\right) \\
&= \sum_{x \in \mathcal{G}_1} \psi_1\left(F(x)^{\beta'} x^{\alpha'}\right).
\end{aligned}$$

Thus,

$$|\widehat{F}(\alpha,\beta)|^2 = \left|\sum_{x\in\mathcal{G}_1}\psi_1\left(F(x)^{\beta'}x^{\alpha'}\right)\overline{\sum_{y\in\mathcal{G}_1}\psi_1\left(F(y)^{\beta'}y^{\alpha'}\right)}\right|$$
$$= \left|\sum_{x,y\in\mathcal{G}_1}\psi_1\left(\left(\frac{F(x)}{F(y)}\right)^{\beta'}\left(\frac{x}{y}\right)^{\alpha'}\right)\right|.$$

Set $z = x/y$ to obtain

$$|\widehat{F}(\alpha,\beta)|^2 = \left|\sum_{y,z\in\mathcal{G}_1}\psi_1\left(\left(\frac{F(zy)}{F(y)}\right)^{\beta'}z^{\alpha'}\right)\right|$$
$$= \left|\sum_{y,z\in\mathcal{G}_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}z^{\alpha'}\right)\right|$$
$$= \left|\sum_{z\in\mathcal{G}_1}\psi_1\left(z^{\alpha'}\right)\sum_{y\in\mathcal{G}_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}\right)\right|.$$

We remark that if $z = 1$, $\log_g(z) = \log_g(\Delta_{F,z}) = 0$ and so the sum splits as

$$|\widehat{F}(\alpha,\beta)|^2 \le n + \left|\sum_{z\in\mathcal{G}_1,z\neq 1}\psi_1\left(z^{\alpha'}\right)\sum_{y\in\mathcal{G}_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}\right)\right|. \tag{2}$$

In a group of order $n \equiv 0 \pmod 2$, there is only one element of order 2 (isomorphic to $n/2$ in $\mathbb{Z}_n$), and so we need consider only the first two cases of Theorem 1.

a) $n \equiv 1 \pmod 2$*:* Identical to the odd characteristic case ((Case a) above), the image multiset of $\Delta_{F,z}$, for each $z \neq 1$, is given by $\mathcal{G}_1 \setminus \{1, o_z\} \cup \{r_{0,z}, r_z\}$. We note that $r_{0,z} \neq r_z$ due to the minimality condition on the ambiguity.

We recall that $\alpha = 1$ maps to the trivial character (equivalently, consider $\alpha' = 0$), so that $\psi_1(z^{\alpha'}) = 1$ for all z. Therefore, for any $z \neq 1$ we have that

$$\sum_{y\in\mathcal{G}_1}\psi_1(\Delta_{F,z}(y)^{\beta'}) = (0 - \psi_1(1) - \psi_{\beta'}(o_z) + \psi_{\beta'}(r_{0,z}) + \psi_{\beta'}(r_z))$$

and so Equation (2) gives $|\widehat{F}(1,\beta)|^2 \le 5n - 4$.

If $\alpha \neq 1$, the precise value of $|\widehat{F}(\alpha,\beta)|^2$ depends on the number of values that $z^{\alpha'}$ takes over the finite cyclic group of order n. It is easy to see that the number of images is $n/\gcd(n,\alpha') - 1$. We note that in the worst case, this cannot exceed $n - 1$. Thus, Equation (2) gives $|\widehat{F}(\alpha,\beta)|^2 \le 5n - 4$, as in the $\alpha = 1$ case.

b) $n \equiv 0 \pmod 2$ *and* $\iota_1 = \iota_2 = 1$*:* The difference in the derivation when $n \equiv 0 \pmod 2$ is only in the row corresponding to the order-2 element γ. For the $z = \gamma$ row, the row-deficiency is 1 and the image multiset of $\Delta_{F,\gamma}$ is $\mathcal{G}_1 \setminus \{1\} \cup \{r\}$, where r is some repeated value. Every other row appears exactly as in the $n \equiv 1 \pmod 2$ case.

The case where $\alpha = 1$ and when $\alpha \neq 1$ provide identical upper-bounds by the same reasoning as the $n \equiv 1 \pmod 2$ case. So consider $\alpha = 1$. Equation (2) becomes

$$|\widehat{F}(1,\beta)|^2 \le n + \left|\sum_{y\in\mathcal{G}_1}\psi_1\left(\Delta_{F,\gamma}(y)^{\beta'}\right)\right| + \left|\sum_{\substack{z\in\mathcal{G}_1\\ z\neq 1,z\neq\gamma}}\sum_{y\in\mathcal{G}_1}\psi_1\left(\Delta_{F,z}(y)^{\beta'}\right)\right|$$
$$\le 5n - 6.$$

TABLE II
THE LOWER-BOUNDS ON THE NON-LINEARITY OF OPTIMUM FUNCTIONS IN TERMS OF AMBIGUITY AND DEFICIENCY.

$\mathcal{G}$	Property	Non-linearity lower-bound
$(\mathbb{F}_q, +)$	$\text{char}(\mathbb{F}_q) = 2$	$(q - \sqrt{(q^2+q)/2})/q$
	$\text{char}(\mathbb{F}_q) = p \neq 2$	$(q - \sqrt{5q-4})/q$
$(\mathbb{Z}_n, \cdot)$	n odd	$(n - \sqrt{5n-4})/n$
	n even	$(n - \sqrt{5n-6})/n$

Theorem 5: Let $\mathcal{G}$ be a finite cyclic group of order n and let F be a permutation of $\mathcal{G}$ with optimum ambiguity and deficiency. The non-linearity of F satisfies

$$\mathfrak{NL}(F) \geq \begin{cases} \frac{n-\sqrt{5n-4}}{n} & \text{if } n \text{ is odd,} \\ \frac{n-\sqrt{5n-6}}{n} & \text{if } n \text{ is even.} \end{cases}$$

APN permutations over $\mathbb{Z}_n$ are considered in [12] and their non-linearity is studied in [13]. A consequence of Parseval's identity gives that the linearity of an APN permutation F on $\mathbb{Z}_n$ satisfies $\sqrt{n} \leq \mathfrak{L}(F) \leq n$. In [13], the authors show that the linearity of their APN permutations over $\mathbb{Z}_p$ appears to be asymptotically $2p^{0.55}$. In particular, the APN permutation used in the SAFER cryptosystem for $p = 257$ has linearity 42.484. Our upper-bound on the linearity for the case of permutations with optimal ambiguity and deficiency for this parameter is ≈ 35.791. We conclude that permutations with optimal ambiguity and deficiency are very good candidates for S-box design due to *both* their strong linearity properties as well as their resistance to differential attacks.

We summarize the connection of ambiguity and deficiency of this function to its non-linearity in Table II.

IV. AMBIGUITY AND DEFICIENCY OF POLYNOMIALS

In this section we demonstrate different methods of computing the ambiguity and deficiency of polynomials. In particular we showcase a mix of classical methods, use the invariance of ambiguity and deficiency under EA-equivalence and we introduce a new method for calculating the ambiguity and deficiency of Dembowski-Ostrom polynomials based on analyzing matrices of a specific shape.

A. Specific permutations over finite fields

A *permutation function* over $\mathbb{F}_q$ is a bijective function F which maps the elements of $\mathbb{F}_q$ onto itself. Let $\text{Tr} : \mathbb{F}_{q^r} \to \mathbb{F}_q$ be the trace function, where $\text{Tr}(\alpha) = \sum_{j=0}^{r-1} \alpha^{q^j}$ for any $\alpha \in \mathbb{F}_{q^r}$ and positive integer r.

In the following, we review some well-known polynomials over the finite field $\mathbb{F}_q$. In this work we are interested in calculating ambiguity and deficiency of these functions in some specific cases of the parameters. We require the following terminology. For any positive integer s and any prime number p, we denote the p-weight of s to be the number of non-zero terms in its p-ary expansion. For example, the 2-weight of $13 = 8 + 4 + 1$ is 3.

- *Linearized polynomials* [19]: The polynomial $L \in \mathbb{F}_q[x]$ with

$$L(x) = \sum_{j=0}^{e-1} \ell_j x^{p^j} \tag{3}$$

  is a permutation polynomial over $\mathbb{F}_q$ if and only if L has no roots in $\mathbb{F}_q$ other than 0.
- *Direct constructions of Dembowski-Ostrom* (DO) *polynomials* [11]: A polynomial $f \in \mathbb{F}_q[x]$ such that

$$F(x) = \sum_{k,j=0}^{e-1} a_{k,j} x^{p^j + p^k}, \tag{4}$$

  is called a DO polynomial. Now, we give a list of DO permutation polynomials over $\mathbb{F}_q$.

  Theorem 6: [2] Let $q = 2^e$ and β be any primitive element of $\mathbb{F}_q$. Let k be any integer and set $d = (k, e)$. Suppose $F \in \mathbb{F}_q[X]$ is a DO polynomial satisfying $F(x) = xL(x)$ for some linearized polynomial L. Then F permutes $\mathbb{F}_q$ when any of the following conditions are satisfied:

1) $L(x) = x^{2^k}$ where e/d is odd;
2) $L(x) = x^{2^k} + cx^{2^{e-k}}$ where e/d is odd and $c \neq \beta^{t(2^d-1)}$ for any integer t;
3) $L(x) = x^{2^{2k}} + c^{2^k+1}x^{2^k} + cx$ where $e = 3k$ and $c \neq \beta^{t(2^d-1)}$ for any integer t.

- *DO Permutations based on trace functions* [2], [7]:
  1) Let q be even and r be odd. Then the polynomial
  $$F(x) = x(\mathrm{Tr}(x) + sx), \tag{5}$$
  permutes $\mathbb{F}_{q^r}$ for all $s \in \mathbb{F}_q \setminus \{0, 1\}$.
  2) Let $1 \leq k \leq e-1$ and $1 \leq s \leq 2^e - 2$. The polynomial $F \in \mathbb{F}_{2^e}[x]$ with
  $$F(x) = x^{2^k} + x + \mathrm{Tr}\left(x^s\right) \tag{6}$$
  is a permutation polynomial over $\mathbb{F}_{2^e}$ if and only if
  a) e is odd,
  b) $\gcd(k, e) = 1$
  c) s has 2-weight 1 or 2.
  3) Let $d \geq 1$ and $t \leq 2^e - 2$. The polynomial $F \in \mathbb{F}_{2^e}[x]$ defined as
  $$F(x) = x^d + \mathrm{Tr}\left(x^t\right) \tag{7}$$
  is a permutation polynomial over $\mathbb{F}_{2^e}$ if and only if
  a) e is even,
  b) $\gcd(d, 2^e - 1) = 1$
  c) $t \equiv s \cdot d \pmod{2^e - 1}$ for some $1 \leq s \leq 2^e - 2$, s has 2-weight 1 or 2.

We now compute the ambiguity and deficiency of members of the classes of permutation polynomials given above.

B. Linearized polynomials

The ambiguity and deficiency of linearized polynomials is treated next.

Lemma 1: Let $L(x) = \sum_{j=0}^{e-1} \ell_j x^{p^j}$ be a linearized polynomial over $\mathbb{F}_q$, $q = p^e$. Then $\mathfrak{D}(L) = (q-1)^2$ and $\mathfrak{A}(L) = (q-1)\binom{q}{2}$.

Proof: Let us consider $\Delta_{L,a}$ for an arbitrary $a \in \mathbb{F}_q^*$:

$$\begin{aligned}\Delta_{L,a}(x) = L(x+a) - L(x) &= \sum_{j=0}^{e-1} \ell_j (x+a)^{p^j} - \sum_{j=0}^{e-1} \ell_j x^{p^j} \\ &= \sum_{j=0}^{e-1} \ell_j \left(x^{p^j} + a^{p^j}\right) - \sum_{j=0}^{e-1} \ell_j x^{p^j} = \sum_{j=0}^{e-1} \ell_j a^{p^j}.\end{aligned}$$

Thus, $\Delta_{L,a}$ is a constant function for every $a \in \mathbb{F}_q^*$. In other words, for every $a \in \mathbb{F}_q^*$ there exists a unique $b = \sum_{j=0}^{e-1} \ell_j a^{p^j}$ such that $\Delta_{L,a}(x) = b$ has exactly q solutions and there are $q-1$ choices for $b' \in \mathbb{F}_q$, where $\Delta_{L,a}(x) = b'$ has no solution. Since there are $q-1$ elements like a in $\mathbb{F}_q$, $n_0 = \mathfrak{D}(L) = (q-1)^2$ and $n_q = q-1$. Hence we get $\mathfrak{A}(L) = n_q\binom{q}{2} = (q-1)\binom{q}{2}$. ∎

C. DO polynomials

In this section we compute the ambiguity and deficiency of some known DO permutation polynomials. The authors of [10] characterize DO polynomials as those (reduced) polynomials whose discrete difference polynomials are linearized. More specifically, they give the following equivalence on DO polynomials.

Theorem 7: [10] Let $F \in \mathbb{F}_q[X]$ with $\deg(F) < q$. Then the following conditions are equivalent:

1) $F = D + L + c$ where D is a DO polynomial, L is a linearized polynomial and $c \in \mathbb{F}_q$ is a constant;
2) for each $a \in \mathbb{F}_q^*$, $\Delta_{F,a} = L_a + c_a$ where L_a is a linearized polynomial and $c_a \in \mathbb{F}_q$ is a constant (both depending on a).

This key fact on the relation between linearized polynomials and DO polynomials helps us to compute the ambiguity and deficiency of some DO permutation polynomials. Let F be a polynomial defined over a ring $\mathcal{R}$. The *value set* of F is given by $V_F = \{F(x)\colon x \in \mathcal{R}\}$. The ambiguity and deficiency of a polynomial depend on the multiset of the images of $\Delta_{F,a}$ and the size of the value set of $\Delta_{F,a}$. When F is a DO polynomial, the values of the ambiguity and deficiency depend only on the value sets of the linearized polynomial L_a.

Theorem 8: [19, Page 362] For any linearized polynomial $L(x) = \sum_{j=0}^{r-1} \ell_j x^{q^j} \in \mathbb{F}_{q^r}$, denote by $\mathbf{L}$ the matrix

$$\begin{bmatrix} \ell_0 & \ell_{r-1}^q & \cdots & \ell_1^{q^{r-1}} \\ \ell_1 & \ell_0^q & \cdots & \ell_2^{q^{r-1}} \\ \vdots & \vdots & & \vdots \\ \ell_{r-1} & \ell_{r-2}^q & \cdots & \ell_0^{q^{r-1}} \end{bmatrix}. \tag{8}$$

Then L is a permutation polynomial over $\mathbb{F}_{q^r}$ if and only if $\det(\mathbf{L}) \neq 0$.
The same matrix in Equation (8) also provides the cardinality of the value set of L.

Corollary 3: [8], [14] Let $L(x) = \sum_{j=0}^{r-1} \ell_j x^{q^j} \in \mathbb{F}_{q^r}[x]$ be a linearized polynomial and let $\mathbf{L}$ be the matrix in Equation (8). Then the value set of L, $\mathcal{V}_L$, satisfies $|\mathcal{V}_L| = q^{\mathrm{rk}(\mathbf{L})}$, where $\mathrm{rk}(\mathbf{L})$ denotes the rank of the matrix $\mathbf{L}$, and the number of preimages of each image is given by $q^{r-\mathrm{rk}(\mathbf{L})}$.

Theorem 9: Let F be a DO polynomial and let $\Delta_{F,a} = L_a + c_a$, for any $a \in \mathbb{F}_{q^r}^*$, as in Theorem 7. Furthermore, let $\mathbf{L}_a$ be the matrix corresponding to L_a given in Equation (8). The ambiguity and deficiency of F are respectively given by

$$\mathfrak{A}(F) = \sum_{a \in \mathbb{F}_{q^r}^*} q^{\mathrm{rk}(\mathbf{L}_a)} \binom{q^{r-\mathrm{rk}(\mathbf{L}_a)}}{2},$$
$$\mathfrak{D}(F) = \sum_{a \in \mathbb{F}_{q^r}^*} \left(q^r - q^{\mathrm{rk}(\mathbf{L}_a)}\right).$$

Proof: Since L_a is a linearized polynomial, we have $|\mathcal{V}_{L_a}| = q^{\mathrm{rk}(\mathbf{L}_a)}$ and every $b \in \mathcal{V}_{L_a}$ contains the same number of preimages, $q^{r-\mathrm{rk}(\mathbf{L}_a)}$. The calculation of $\mathfrak{A}(F)$ and $\mathfrak{D}(F)$ are immediate from the definition. ■

We now present the ambiguity and deficiency of DO permutation polynomials coming from Theorem 6.

Theorem 10: Let k be any integer and set $d = (k, e)$. Suppose $F \in \mathbb{F}_{2^e}[x]$ is a DO polynomial satisfying $F(x) = xL(x) = x^{2^k+1}$. Then $\mathfrak{D}(F) = (2^e - 1)(2^e - 2^{e-d})$ and $\mathfrak{A}(F) = (2^e - 1)\,(2^{e-d})\binom{2^d}{2}$.
If $d = 1$, then F is the APN Gold function over $\mathbb{F}_{2^e}$ which has optimal ambiguity and deficiency [24]. The proof of this result appears in [25] using basic techniques and can also be derived using Theorem 9. We illustrate our new method, which involves analyzing the ranks of various forms of matrices, with the following theorem.

Theorem 11: Let β be any primitive element of $\mathbb{F}_{2^e}$. Let either $e = 3k$ or $2e = 3k$ with $d = \gcd(e, k) = e/3$. Also, let $F(x) = xL(x) \in \mathbb{F}_{2^e}[x]$ be the DO permutation polynomial, where $L(x) = x^{2^k} + cx^{2^{e-k}}$ and $c \neq \beta^{t(2^d-1)}$ for any integer t. Then, the deficiency of f is

$$\mathfrak{D}(F) = 2^e\,(2^e - 1) - (2^e - 1)\,2^{2d},$$

and the ambiguity of f is

$$\mathfrak{A}(F) = (2^e - 1)\,2^{2d}\binom{2^{e-2d}}{2}.$$

Proof: Assume that $2e = 3k$, as the proof when $e = 3k$ is analogous. Suppose F is given as in the hypothesis, then

$$\begin{aligned}\Delta_{F,a}(x) &= (x+a)\left((x+a)^{2^k} + c(x+a)^{2^{e-k}}\right) - x\left(x^{2^k} + cx^{2^{e-k}}\right) \\ &= ax^{2^k} + cax^{2^{e-k}} + \left(a^{2^k} + ca^{2^{e-k}}\right)x + c_a,\end{aligned}$$

where $c_a \in \mathbb{F}_{2^e}$. Let $L_a = \Delta_{f,a} - c_a$ and let $d = \gcd(e,k)$. Since $2e = 3k$, we have $d = e-k$, $e = 3d$ and $k = 2d$. The $e \times e$ matrix $\mathbf{L}_a$ in Equation (8) can be broken into diagonal blocks of size $d \times d$, where the j-th entry along the diagonal is given in the following expression and every other entry is equal to 0

$$\mathbf{L}_j = \begin{bmatrix} \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^j} & a^{2^{(e-k)+j}} & (ca)^{2^{k+j}} \\ (ca)^{2^j} & \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^{(e-k)+j}} & a^{2^{k+j}} \\ a^{2^j} & (ca)^{2^{(e-k)+j}} & \left(a^{2^k} + ca^{2^{e-k}}\right)^{2^{k+j}} \end{bmatrix}, \quad j = 0, 1, \ldots, e-k-1.$$

We substitute $d = e-k$ and $2d = k$ for clarity and perform the following row operations to $\mathbf{L}_a$:

1. $\mathrm{Row}_j \leftarrow \mathrm{Row}_j + \left(\dfrac{a^{2^{2d}} + ca^{2^d}}{a}\right)^{2^j} \mathrm{Row}_{2d+j}, \quad j = 0, 1, \ldots, d-1;$
2. $\mathrm{Row}_{d+j} \leftarrow \mathrm{Row}_{d+j} + c^{2^j}\mathrm{Row}_{2d+j}, \quad j = 0, 1, \ldots, d-1,$

to get a new block matrix of the form

$$\mathbf{L}_j \sim \begin{bmatrix} 0 & \Phi_j & \Phi_j^{2^{2d}} \\ 0 & \frac{a^{2^j}}{a^{2^{d+j}}}\Phi_j & \frac{a^{2^j}}{a^{2^{d+j}}}\Phi_j^{2^{2d}} \\ a^{2^j} & (ca)^{2^{d+j}} & \left(a^{2^{2d}} + ca^{2^d}\right)^{2^{2d+j}} \end{bmatrix},$$

where

$$\Phi_j = \left(a^{2^d} + \frac{\left(a^{2^{2d}} + ca^{2^d}\right)c^{2^d}a^{2^d}}{a}\right)^{2^j}.$$

It is clear that $\mathrm{rk}(\mathbf{L}_j) \leq 2$ and thus $\mathrm{rk}(\mathbf{L}_a) \leq 2d$. To show equality, we determine that $\Phi_j \neq 0$ for any j, $0 \leq j \leq d-1$ and for any $a \in \mathbb{F}_{2^e}$.

Suppose that $\Phi_0 = 0$, then re-arranging gives

$$a = c^{2^d}a^{2^{2d}} + c^{2^d+1}a^{2^d}. \tag{9}$$

Raise to the power of 2^{2d} and multiply by c^{2^d} to obtain

$$c^{2^d}a^{2^{2d}} = c^{2^d+1}\left(a^{2^d} + c^{2^{2d}}a\right).$$

Substituting for the left-hand side using Equation (9) gives

$$a + c^{2^d+1}a^{2^d} = c^{2^d+1}a^{2^d} + c^{2^{2d}+2^d+1}a,$$

thus

$$1 = c^{2^{2d}+2^d+1} = c^{(2^{3d-1})/(2^d-1)},$$

contradicting that $c \neq \beta^{t(2^d-1)}$ for a primitive element β.

■

A different proof, suggested by an anonymous referee, can be provided using the following equations

$$\begin{cases} x^{2^k+1} + cx^{2^{e-k}+1} = x^{2^k+1} + cx^{2^{2k}+1} = \left(x + cx^{2^{2k}}\right) \circ x^{2^k+1} & e = 3k, \\ x^{2^k+1} + cx^{2^{e-k}+1} = x^{2^k+1} + cx^{2^{k/2}+1} = \left(x^{2^k} + cx\right) \circ x^{2^{k/2}+1} & e = 3k/2. \end{cases} \tag{10}$$

The polynomial $x + cx^{2^{2k}}$ has no non-zero roots, since $x + cx2^{2k} = x(1 + cx^{2^{2k}-1})$ and if $\beta \neq 0$ is a root, $c = \beta^{-(2^{2k}-1)}$, contradicting the condition on c. A similar argument can be applied to $x^{2^k} + cx$. Thus, both of these polynomials are permutation polynomials. Therefore, $x^{2^k+1} + cx^{2^{e-k}+1}$ and $x^{2^k+1} + cx^{2^{e-k}+1}$ are EA-equivalent to x^{2^k+1} and $x^{2^{k/2}+1}$, respectively. Since ambiguity and deficiency are EA-invariant parameters, their ambiguity and deficiency are the same as the DO polynomials given in Theorem 10 with the further constraint $3d = e$.

Theorem 12: Let β be any primitive element of $\mathbb{F}_{2^e}$ and let $F(x) = xL(x)$ be the DO permutation polynomial over $\mathbb{F}_{2^e}$ where $L(x) = x^{2^{2k}} + c^{2^k+1}x^{2^k} + cx$ for which $e = 3k$ and $c \neq \beta^{t(2^d-1)}$ for any integer t. Then the deficiency of F is

$$\mathfrak{D}(F) = 2^e\,(2^e-1) - (2^e-1)\,2^{2k}$$

and the ambiguity of F is

$$\mathfrak{A}(F) = (2^e-1)\,2^{2k}\binom{2^k}{2}.$$

Proof: For $e = 3k$, the polynomial $F(x) = x^{2^{2k}+1}+c^{2^k+1}x^{2^k+1}+cx^2$ is EA-equivalent to $x^{2^{2k}+1}+c^{2^k+1}x^{2^k+1}$, and $x^{2^{2k}+1}+c^{2^k+1}x^{2^k+1}$ is also EA-equivalent to the first polynomial in Equation (10). The rest of the proof follows from Theorem 10 and the EA-invariance of ambiguity and deficiency. ■

D. DO permutations based on traces

First, we use the matrix method of Theorem 9 to give the ambiguity and deficiency of the DO permutation polynomial coming from a trace function given in Equation (5).

Theorem 13: Let $s \in \mathbb{F}_q \setminus \{0,1\}$ and $F(x) = x(\mathrm{Tr}(x) + sx)$ be the DO permutation polynomial over $\mathbb{F}_{q^r}$ for even q and odd r. Then the deficiency of F is

$$\mathfrak{D}(F) = q^r(q^r-1) - (q^r - q^{r-1})q^{r-1} - (q^r - q)$$

and the ambiguity of F is

$$\mathfrak{A}(F) = \left(q^r - q^{r-1}\right)q^{r-1}\binom{q}{2} + (q^r - q)\binom{q^{r-1}}{2}.$$

Proof: Let us consider $\Delta_{F,a}(x)$ for $a \in \mathbb{F}_{q^r}^*$; we have

$$\begin{aligned}\Delta_{F,a}(x) &= (x+a)(\mathrm{Tr}(x+a) + s(x+a)) - x(\mathrm{Tr}(x) + sx)\\ &= x\mathrm{Tr}(a) + a\mathrm{Tr}(x) + a\mathrm{Tr}(a) + sa^2.\end{aligned}$$

The corresponding matrix $\mathbf{L}_a$ as in Equation (8) is

$$\mathbf{L}_a = \begin{bmatrix} a+\mathrm{Tr}(a) & a^q & a^{q^2} & \cdots & a^{q^{r-1}} \\ a & (a+\mathrm{Tr}(a))^q & a^{q^2} & \cdots & a^{q^{r-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a & a^q & a^{q^2} & \cdots & (a+\mathrm{Tr}(a))^{q^{r-1}} \end{bmatrix}.$$

If $\mathrm{Tr}(a) = 0$, then $\mathrm{rk}(\mathbf{L}_a) = 1$. Let us suppose that $\mathrm{Tr}(a) \neq 0$, then the following elementary row operations

1. $\mathrm{Row}_j \leftarrow \mathrm{Row}_j - \mathrm{Row}_1, \quad j = 2, \ldots, r;$
2. $\mathrm{Column}_1 \leftarrow \mathrm{Column}_1 - \mathrm{Column}_j, \quad j = 2, \ldots, r,$

reduce $\mathbf{L}_a$ to

$$\mathbf{L}'_a = \begin{bmatrix} 0 & a^q & a^{q^2} & \cdots & a^{q^{r-1}} \\ 0 & \mathrm{Tr}\,(a^q) & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathrm{Tr}\left(a^{q^{r-1}}\right) \end{bmatrix},$$

where we have used the identities $\mathrm{Tr}\,(a) = \mathrm{Tr}\,(a^q) = \mathrm{Tr}(a)^q$. Thus we have $\mathrm{rk}\,(\mathbf{L}'_a) = r-1$. Theorem 9, with the observation that there are both q^{r-1} trace-0 and q^{r-1} trace-1 elements, completes the proof. ■

Theorem 13 illustrates the power of the matrix method of Theorem 9 when the difference map is a linearized polynomial with high weight, in contrast to the previously considered low-weight DO binomial (Gold polynomial) and trinomials. Now, we treat the permutation polynomials based on traces introduced in Equations (6) and (7), see also [7], using a classical method due to the more complicated expression of their difference maps.

Theorem 14: Let $1 \leq k \leq e-1$ and $1 \leq s \leq 2^e - 2$. Let $F(x) = x^{2^k} + x + \mathrm{Tr}\,(x^s) \in \mathbb{F}_{2^e}[x]$, where e is odd, $\gcd(k, e) = 1$ and s has 2-weight 1 or 2. If s has 2-weight 1, then the ambiguity and deficiency are respectively given by

$$\begin{aligned}\mathfrak{A}(F) &= (2^e - 1)\binom{2^e}{2},\\ \mathfrak{D}(F) &= 2^e\,(2^e - 1) - (2^e - 1) = (2^e - 1)^2.\end{aligned}$$

If s has 2-weight 2, then the ambiguity and deficiency are respectively given by

$$\begin{aligned}\mathfrak{A}(F) &= \left(2^{e+1} - 2^2\right)\binom{2^{e-1}}{2} + \binom{2^e}{2}\\ \mathfrak{D}(F) &= 2^e\,(2^e - 1) - \left(2^{e+1} - 2^2\right) - 1.\end{aligned}$$

Proof: If s has 2-weight 1, then f is linearized and the result follows from Lemma 1. Suppose now that s has 2-weight 2, that is $s = 2^w + 2^j$ for some $0 \leq w < j$. Then,

$$\begin{aligned}\Delta_{F,a}(x) &= a^{2^k} + a + \mathrm{Tr}\left((x+a)^{2^w+2^j}\right) + \mathrm{Tr}\left(x^{2^w+2^j}\right)\\ &= a^{2^k} + a + \mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right).\end{aligned}$$

Since e is odd, $\mathrm{Tr}(1) = 1$ and it follows that $(a, b) = (1, 1)$ is the only pair with exactly 2^e solutions for $\Delta_{F,a}(x) = b$.

There are 2^{e-1} elements $x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}$ satisfying

$$\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) = t_0 \in \mathbb{F}_2,$$

so we only need to enumerate the number of pairs

$$(a, b) = (a, a^{2^k} + a + t_0)$$

such that $a \in \mathbb{F}_{2^e} \setminus \{0, 1\}$. It is simple to see that the number of pairs is $2(2^e - 2)$. This completes the proof. ■

We note that the linearized portion of Equation (6) (i.e., $x^{2^k} + x = F(x) - \mathrm{Tr}(x^s)$) does not affect the ambiguity or deficiency of F, since its difference map is constant. Thus, the ambiguity and deficiency of F would remain unchanged by replacing $x^{2^k} + x$ with any linearized polynomial. However, such a change may affect the permutation properties of F.

The polynomial given in Equation (7) can be decomposed as $F(x) = (x + \mathrm{Tr}(x^s)) \circ x^d$, where the monomial x^d defines a permutation polynomial. Since ambiguity and deficiency are invariant under EA-equivalence, we treat here the initial case $d = 1$.

Theorem 15: Let $F(x) = x + \mathrm{Tr}(x^s) \in \mathbb{F}_{2^e}[x]$, where e is even and s has 2-weight 1 or 2. The ambiguity and deficiency of F are respectively given by

$$\begin{aligned}\mathfrak{A}(F) &= (2^e - 1)\binom{2^e}{2},\\ \mathfrak{D}(F) &= (2^e - 1)^2,\end{aligned}$$

when s has 2-weight 1 and

$$\begin{aligned}\mathfrak{A}(F) &= \left(2^{e+1} - 2^3\right)\binom{2^{e-1}}{2} + 3\binom{2^e}{2},\\ \mathfrak{D}(F) &= 2^e\,(2^e - 1) - \left(2^{e+1} - 2^3\right) - 3,\end{aligned}$$

when s has 2-weight 2.

Proof: If s has weight 1, then F is linearized and the result follows from Lemma 1. Suppose now that s has 2-weight 2, that is $s = 2^w + 2^j$ for some $0 \leq w < j$. Then,

$$\begin{aligned}\Delta_{F,a}(x) &= a + \mathrm{Tr}\left((x+a)^{2^w+2^j}\right) + \mathrm{Tr}\left(x^{2^w+2^j}\right)\\ &= a + \mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right).\end{aligned}$$

Since e is even, $\mathrm{Tr}(1) = 0$ and $\mathbb{F}_4 \subseteq \mathbb{F}_{2^e}$. We claim the only pairs (a, b) with exactly 2^e solutions for $\Delta_{F,a}(x) = b$ satisfy that $a \in \mathbb{F}_4^*$. Let β be the primitive element of $\mathbb{F}_{2^e}$ and $\mathbb{F}_4^* = \{1, \eta, \eta+1\}$ with $\eta = \beta^{(2^e-1)/3}$. For a non-unit $a \in \mathbb{F}_4^*$, it is clear that $a^{2^k} = a$ when k is even and $a^{2^k} = a + 1$ otherwise. For every $a \in \mathbb{F}_4^*$, if the parity of w and j is the same, then

$$\begin{aligned}\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) &= \mathrm{Tr}\left(x^{2^w}a^{2^w} + a^{2^j}x^{2^j} + a^{2^{w+1}}\right)\\ &= \mathrm{Tr}\left(xa\right)^{2^w} + \mathrm{Tr}\left(xa\right)^{2^j} + \mathrm{Tr}\left(a^{2^{w+1}}\right)\\ &= \mathrm{Tr}(a).\end{aligned}$$

On the other hand, without loss of generality we can assume that w is even and j is odd and we have

$$\begin{aligned}\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) &= \mathrm{Tr}\left(x^{2^w}a + (a+1)x^{2^j} + a(a+1)\right)\\ &= \mathrm{Tr}\left(x^2a^2\right)^{2^{w-1}} + \mathrm{Tr}\left(x^2a^2\right)^{2^{j-1}} + \mathrm{Tr}\left(1\right)\\ &= 0.\end{aligned}$$

It is clear that there are 2^{e-1} elements satisfying

$$\mathrm{Tr}\left(x^{2^w}a^{2^j} + a^{2^w}x^{2^j} + a^{2^w+2^j}\right) = t_0,$$

for each choice of $t_0 \in \mathbb{F}_2$. So the number of pairs with

$$(a, b) = (a, a + t_0)$$

such that $a \in \mathbb{F}_{2^e} \setminus \{0, 1\}$ is of interest. A simple enumeration implies that the number of pairs is $2(2^e - 4)$. This completes the proof. ■

V. Concluding remarks and further work

In this work, we establish the CCZ-invariance of the ambiguity and deficiency parameters. We give an upper and a lower bound on the ambiguity and deficiency of differentially k-uniform functions, showing that ambiguity and deficiency are finer measures than differential uniformity. We give a lower-bound on the non-linearity of permutations which achieve optimal ambiguity and deficiency. For functions over finite cyclic groups and the additive group of a finite field of odd cardinality, we show that these permutations approach optimal non-linearity. We also study and derive explicit values of the ambiguity and deficiency of some permutation polynomials over finite fields including linearized polynomials, DO polynomials, including three specific DO permutations, and two polynomials based on the trace function.

For future work on the ambiguity and deficiency of permutations, we plan to study the ambiguity and deficiency of (reversed) Dickson Polynomials [15], [16] as well as Rédei functions [28].

Acknowledgments: We would like to thank two anonymous reviewers for their insightful comments and suggestions which improved both the presentation and the content of this manuscript.

References

[1] A. Akbary, D. Ghioca, and Q. Wang, "On constructing permutations of finite fields," *Finite Fields Appl.* vol. 17, pp. 51–67, 2011.

[2] A. Blokhuis, R.S. Coulter, M. Henderson, and C.M. O'Keefe, "Permutations amongst the Dembowski-Ostrom polynomials," *Proc. 5th Int'l Conf. Finite Fields and Appl.*, pp. 37–42, 2001.

[3] C. Blondeau, A. Canteaut and P. Charpin, "Differential properties of $x \to x^{2^t-1}$," *IEEE Trans. on Inform. Theory*, vol. 57, pp. 8127–8137, 2011.

[4] K.A. Browning, J.F. Dillon, M.T. Mcquistan, and A.J. Wolfe, "An APN permutation in dimension six," *Proc. 9th Int'l Conf. Finite Fields Appl.*, vol 518 of Contemporary Mathematics, pp. 33–42, 2010.

[5] C. Carlet, "Vectorial Boolean Functions for Cryptography", chapter of the monograph *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, Y. Crama and P. L. Hammer (eds.), Cambridge University Press, pp. 398-468, 2010.

[6] C. Carlet, P. Charpin, and V. Zinoviev, "Codes, bent functions and permutations suitable for DES-like cryptosystems," *Des. Codes Cryptogr.*, vol. 15, pp. 125–156, 1998.

[7] P. Charpin and G. Kyureghyan, "On a class of permutation polynomials over $\mathbb{F}_{2^n}$," *SETA '08 Proc. 5th Int'l Conf. Sequences and Their Applications*, pp. 368–376, 2008.

[8] W.-S. Chou, J. Gomez-Calderon, G.L. Mullen, D. Panario, and D. Thomson, "Subfield value sets of polynomials over finite fields," *to appear in Functiones et Approximatio, Commentarii Mathematici*, 20 pages, 2013.

[9] 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.

[10] R. Coulter and R.W. Matthews, "Planar functions and planes of Lenz-Barlotti class II," *Des. Codes and Crypto.*, vol. 10, pp. 167–184, 1997.

[11] P. Dembowski and T.G. Ostrom, "Planes of order n with collineation groups of order n," *Math. Z.* vol. 2, pp. 239–258, 1968.

[12] K. Drakakis, R. Gow, and G. McGuire, "APN permutations on $\mathbb{Z}_n$ and Costas arrays," *Discrete Appl. Math.*, vol. 157, pp. 3320–3326, 2009.

[13] K. Drakakis, V. Requena, and G. McGuire, "On the non-linearity of exponential Welch Costas functions," *IEEE Trans. on Inform. Theory*, vol. 56, pp. 1230–1238, 2010.

[14] X.-D. Hou, "Solution to a problem of S. Payne," *Proc. of the American Mathematical Society*, vol. 132, pp. 1–6, 2003.

[15] X.-D. Hou and T. Ly, "Necessary conditions for reversed Dickson polynomials to be permutational," *Finite Fields Appl.*, vol. 16, pp. 436–448, 2010.

[16] X.-D. Hou, G.L. Mullen, J.A. Sellers, and J. Yucas, "Reversed Dickson polynomials over finite fields," *Finite Fields Appl.*, vol. 15, pp. 748–773, 2009.

[17] 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, pp. 243–246, 1988.

[18] 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, pp. 71–74, 1993.

[19] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, second edition, 1997.

[20] M. Matsui, "Linear cryptanalysis method for DES cipher," *Advances in Cryptology – EUROCRYPT '93*, vol. 765 of *Lecture Notes Comput. Sci.*, pp. 386–397, 1994.

[21] 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 Pure and Appl. Math.*, pp. 131–151, 1993.

[22] G.L. Mullen and H. Stevens, "Polynomial functions (mod m)," *Acta Mathematica Hungarica*, vol. 44, pp. 237–241, 1984.

[23] G.L. Mullen and D. Panario, *Handbook of Finite Fields*, CRC Press, ISBN 9781439873786, to appear 2013.

[24] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, "Two new measures for permutations: ambiguity and deficiency," *IEEE Trans. on Inform. Theory*, vol. 57, pp. 7648–7657, 2011.

[25] D. Panario, A. Sakzad, B. Stevens, and Q. Wang, "Ambiguity and deficiency of permutations from finite fields," *Proc. Information Theory Workshop (ITW), 2011 IEEE*, pp. 165–169, 2011.

[26] D. Panario, B. Stevens, and Q. Wang, "Ambiguity and deficiency in Costas arrays and APN permutations," *LATIN 2012*, vol. 6034 of *Lecture Notes Comput. Sci., LATIN 2010*, pp. 397–406, 2010.

[27] R.L. Rivest, "Permutation polynomials modulo 2^w," *Finite Fields Appl.*, vol. 7, pp. 287–292, 2001.

[28] L. Rédei, "Uber eindeuting umkehrbare polynome in endlichen kopern," *Acta Scientarium Mathmematicarum*, vol. 11, pp. 85–92, 1946-48.

[29] SAGE Mathematics Software, Version 4.3, http://www.sagemath.org/.

[30] A. Sakzad, M-R. Sadeghi, and D. Panario, "Cycle structure of permutation functions over finite fields and their applications," *Adv. Math. Comm.*, vol. 6, pp. 347–361, 2012.

[31] A. Sakzad, D. Panario, M-R. Sadeghi, and N. Eshghi, "Self-inverse interleavers based on permutation functions for turbo codes," *Proc. 48th Ann. Allerton Conf. on Communication, Control, and Computing, (Allerton, Monticello, IL, USA), IEEE, 2010,* pp. 22–28, 2010.

[32] J. Sun and O.Y. Takeshita, "Interleavers for turbo codes using permutation polynomials over integer rings," *IEEE Trans. on Inform. Theory*, vol. 51, pp. 101–119, 2005.