Ambiguity and deficiency of reversed Dickson permutations

Daniel Panario, Amin Sakzad, and David Thomson

Abstract. We give the ambiguity and deficiency of two classes of binary reversed Dickson polynomials. The determination of their ambiguity and deficiency depends on new results on the 2-divisibility of binomial coefficients. We also give some conjectures regarding the ambiguity and deficiency for the other two classes of binary reversed Dickson polynomials.

1. Introduction

Linear and differential cryptanalysis are two well-known attacks against symmetric key cryptosystems which use S-boxes as part of the encryption-decryption procedure [**Bih91, Mat94**]. An S-box can be considered as a map between finite groups, most commonly the additive and multiplicative groups of a finite field. The S-box should be perfect non-linear (PN) or almost perfect non-linear (APN) in order to best resist against both linear and differential cryptanalysis. One of the most well-known parameters to measure against linear cryptanalysis is nonlinearity [**Car04, Dra10**].

The ambiguity and deficiency of a function were introduced in [**Pan11-1, Pan10**] and a thesis on the topic appears in [**Thom12**]. Theoretical results on the ambiguity and deficiency of permutation functions were presented in [**Pan11-1**] and [**Pan13**]. In particular, lower bounds on the ambiguity and deficiency are derived for permutations of both additive and multiplicative groups of finite fields. Functions that achieve these lower bounds were constructed in [**Pan11-1**]. Like other differential properties of functions, the ambiguity and deficiency are both invariant under extended-affine (EA) and Carlet-Charpin-Zinoviev (CCZ) [**Car98**] equivalences [**Pan11-1, Pan13**]. Attaining the minimum ambiguity implies that the function itself is almost perfect non-linear. In the case of finite fields, the reverse is true only in characteristic 2 [**Pan11-1**]. It has also been shown that permutations that achieve the lowest possible ambiguity are also highly non-linear (that is, they achieve a high non-linearity). The ambiguity and deficiency of functions whose difference map is a linearized polynomial are derived in [**Pan13**]. Numerical experiments on the ambiguity and deficiency of monomials and (reversed) Dickson polynomials are also provided in [**Pan11-2**].

Key words and phrases. Dickson polynomials, almost perfect non-linear functions, ambiguity and deficiency.

In this paper, we study the ambiguity and deficiency of binary reversed Dickson polynomials. Studying these values for Dickson polynomials entails the study of 2-divisibility of expressions of the form $\frac{n}{n-j}\binom{n-j}{j}$ that appear in the coefficients of these polynomials. In Section 3, we provide results of the 2-divisibility of binomial coefficients. We apply those computations in Section 4 to provide the ambiguity and deficiency to two of four known types of binary reversed Dickson permutations. We give some comments on the ambiguity and deficiency of the remaining cases based on some numerical computations in Sage.

Notation. We use capital letters to denote functions. Capital calligraphic letters are used for sets. The elements of a set and numbers are denoted by small letters and Greek letters. Matrices are denoted by bold capital letters.

2. Background material

We briefly recall the definitions of reversed Dickson polynomials. Then we review the concepts of ambiguity and deficiency related to permutation polynomials.

2.1. Reversed Dickson polynomials. In this paper, we are interested in computing the ambiguity and deficiency of reversed Dickson polynomials. One motivation for our interest is that reversed Dickson polynomials have close relations to APN functions [**Hou10, Hou09**]. Hence, studying differential properties of these polynomials may shed some light on the differential behaviour of these important functions. Next we define a Dickson polynomial first, then we introduce reversed Dickson polynomials.

Dickson polynomials [**Lidl93**] [**Lidl97**] are defined as the (unique) bi-variate polynomial D_n defined by the equation $D_n(x_1+x_2, x_1x_2) = x_1^n+x_2^n$. The univariate Dickson polynomial is denoted $D_n(x,c) \in \mathbb{F}_q$, where $c \in \mathbb{F}_q$. If $c = 0$, then $D_n(x,0)$ is a monomial. A *reversed Dickson polynomial* is obtained by reversing the role of the variable and parameter of the univariate D_n, thus considering instead $D_n(c,x)$. To be precise, let $q = p^e$ be a prime power; then the reversed Dickson polynomial is

$$D_n(c,x) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j}(-x)^j c^{n-2j}. \tag{1}$$

It can be shown that the permutation behaviour of Dickson polynomials depends only whether $c = 0$ or $c \neq 0$. For $c \neq 0$, it is well-known that the Dickson polynomial $D_n(x,c)$ defines a permutation of $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$. In the reversed Dickson case, only some sufficient conditions for $D_n(c,x)$ to define a permutation of $\mathbb{F}_q$ are known. In particular, a *desirable* pair [**Hou10**] $(q,n) = (p^e, n)$ indicates that $D_n(c,x)$ is a permutation polynomial over $\mathbb{F}_q$. Table 1 gives the list of known desirable pairs when $p = 2$.

n	condition
$2^k + 1$	$(k, 2e) = 1$ (Gold)
$2^e + 2^k + 1,\ k > 0$	$(k-1, e) = 1$, e even (cubic)
$2^{2k} - 2^k + 1$	$(k, 2e) = 1$ (Kasami)
$2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$	$e = 5k$ (Dobbertin)

Table 1. Reversed Dickson permutation polynomials, $D_n(1,x)$, over $\mathbb{F}_{2^e}$.

There are also some known conditions for reversed Dickson polynomials to be permutations in odd characteristic [**Hou10**]. However, in this paper we only focus on the binary case.

2.2. Differential properties: ambiguity and deficiency. Let $\mathcal{G}$ be a finite Abelian group of cardinality n and let F be a bijective map on $\mathcal{G}$. Let $\mathcal{G}^* = \mathcal{G} \setminus \{0\}$. For any $a \in \mathcal{G}^*$, the *difference map* of F with parameter a is $\Delta_{F,a}(x) = F(x+a) - F(x)$. Properties of a function's difference maps are critical in determining its resistance to differential cryptanalysis. In particular, differential cryptanalysis requires finding pairs of plaintexts and their corresponding ciphertexts whose *differences* occur with "significant" probability. Thus, the difference maps of a candidate function should be as close to injective as possible.

Let

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

for $0 \le i \le n$.

Definition 2.1. Let $\mathcal{G}$ be a finite Abelian group and let $F \colon \mathcal{G} \to \mathcal{G}$. The *deficiency* of F, denoted $\mathfrak{D}(F)$, is given by

$$\mathfrak{D}(F) = \alpha_0(F) = \left| \left\{ (a,b) \in \mathcal{G}^* \times \mathcal{G} : \Delta_{F,a}^{-1}(b) = \emptyset \right\} \right| .$$

When the function is clear, we simply write $\alpha_i = \alpha_i(F)$. The deficiency measures the number of pairs (a,b) such that $\Delta_{F,a}(x) = b$ has no solutions. Thus, the deficiency is a collective measure of the surjectivity of the difference maps $\Delta_{F,a}$, where a ranges over $\mathcal{G}^*$: the lower the deficiency the closer the $\Delta_{F,a}$ are to surjective.

Definition 2.2. Let $\mathcal{G}$ be a finite Abelian group and let $F \colon \mathcal{G} \to \mathcal{G}$. The *(weighted) ambiguity* of F, denoted $\mathfrak{A}(F)$, is given by

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

Analogously to the deficiency, the ambiguity of F is a collective measure of the injectivity of the difference maps $\Delta_{F,a}(x)$: the lower the ambiguity of F the closer the $\Delta_{F,a}$ are to injective. We explain this weighting as follows: contributions from α_0 and α_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 number of distinct pairs x and x' such that $\Delta_{F,a}(x) = \Delta_{F,a}(x')$.

Some related measures are introduced in the literature. In particular, the *differential spectrum* of F is the (multi-)set of $\alpha_i(F)$; see [**Blon11**], for a treatment of the differential spectrum of some special functions. Lower bounds on the ambiguity and deficiency of a permutation function can be derived using the following theorem.

Theorem 2.3. [**Pan11-1**] *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*

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

Moreover, over the finite field with 2^e elements, the optimum (smallest) ambiguity and deficiency of a permutation, denoted Opt $\mathfrak{A}(2^e)$ *and* Opt $\mathfrak{D}(2^e)$*, respectively, are given by* $2^{e-1}(2^e-1)$.

The ambiguity and deficiency of a number of well-known permutations such as linearized polynomials, twisted binomials, Möbius transformations, Dembowski-Ostrom polynomials [**Blokh01, Dem68**], permutations from [**Char08**] and some cases of Dickson polynomials are computed in [**Pan11-1, Pan11-2, Pan13**]. These are evaluated on either the additive or multiplicative groups of the finite field $\mathbb{F}_q$.

3. Divisibility of binomial coefficients

The coefficients of reversed Dickson polynomials involve expressions of the form $\frac{n}{n-j}\binom{n-j}{j}$. Studying the ambiguity and deficiency of reversed Dickson polynomials first requires studying the divisibility of binomial coefficients. Since we are chiefly concerned with the binary case, we require only the parity of the binomial coefficients. The exact divisibility is given by Goethegluck [**Goe87**], however for our purposes we apply Lucas' lemma, see, for example, [**Fine47**].

Theorem 3.1. *Let p be a prime, and let $n=\sum_{i=0}^{r} n_i p^i$ and $k=\sum_{i=0}^{r} k_i p^i$, with $0\le n_i, k_i<p$. Then*

$$\binom{n}{k}=\binom{n_0}{k_0}\binom{n_1}{k_1}\cdots\binom{n_r}{k_r} \pmod{p}.$$

Moreover, the form of the coefficients of Dickson polynomials leads to an important simplification which we use throughout this work.

Lemma 3.2. *Let n be a positive integer, then*

$$\frac{n}{n-j}\binom{n-j}{j}=2\binom{n-j-1}{j-1}+\binom{n-j-1}{j}.$$

Hence, the parity of $\frac{n}{n-j}\binom{n-j}{j}$ is equal to the parity of $\binom{n-j-1}{j}$.

Proof. We have

$$\begin{aligned}\frac{n}{n-j}\binom{n-j}{j} &= \frac{n-j+j}{n-j}\binom{n-j}{j}=(1+\frac{j}{n-j})\binom{n-j}{j}\\ &=\binom{n-j}{j}+\frac{j}{n-j}\binom{n-j}{j}=\binom{n-j}{j}+\binom{n-j-1}{j-1}.\end{aligned}$$

Using Pascal's rule $\binom{n-j}{j}=\binom{n-j-1}{j}+\binom{n-j-1}{j-1}$ yields the conclusion. □

As we will see, computing the base-2 expansion of the coefficients becomes more complicated as the number of non-zero elements in the expansion of n grows. Thus, Lemma 3.2 is particularly useful to calculate $\binom{m}{v}$ when m is odd. We encounter this situation in each case below by considering $\binom{n-j-1}{j}=\binom{(n-1)-j}{j}$.

Theorem 3.3.

(1) *Let $n=2^k+1$ and $j\le n$; then for some i,*

$$\begin{cases} 2\nmid \frac{n}{n-j}\binom{n-j}{j} & j=0 \text{ or } j=2^i,\ 0\le i\le k-1,\\ 2\mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise.}\end{cases}$$

(2) *Let* $n = 2^e + 2^k + 1$, $e > k > 0$, *then*

$$\begin{cases} 2 \nmid \frac{n}{n-j}\binom{n-j}{j} & j = 0,\ j = 2^i,\ i \neq k,\ i \leq e-1,\ \text{or } j = 2^i + 2^s,\ i \geq k,\ s < k, \\ 2 \mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise.} \end{cases}$$

(3) *Let* $n = 2^{2k} - 2^k + 1$, *then*

$$\begin{cases} 2 \nmid \frac{n}{n-j}\binom{n-j}{j} & j = 0 \text{ or } j = 2^i - 2^k + 2^s,\ i \geq k,\ 0 \leq s < k, \\ 2 \mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise.} \end{cases}$$

(4) *Let* $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$ *and* $j \leq n$, *then*

$$\begin{cases} 2 \nmid \frac{n}{n-j}\binom{n-j}{j} & j = \delta_r 2^r + \delta_s 2^s + \delta_t 2^t + \delta_w \left(2^w + \cdots + 1\right), \\ 2 \mid \frac{n}{n-j}\binom{n-j}{j} & \text{otherwise,} \end{cases}$$

where $\delta_r, \delta_s, \delta_t, \delta_w \in \{0, 1\}$ *with*

$$\begin{cases} 6k \leq r \leq 8k-1, \\ 4k \leq s \leq 6k-1, \\ 2k-1 \leq t \leq 4k-1, \\ 0 \leq w \leq 2k-2, \end{cases}$$

satisfy the conditions:

(a) *If* $\delta_{2k-1} = 1$, *then* $w = 2k-2$ *and* $\delta_w = 1$; *otherwise,*
(b) *If* $\delta_t = 0$, *then* $\delta_{4k} = 0$,
(c) *if* $\delta_s = 0$, *then* $\delta_{6k} = 0$,
(d) *if* $\delta_r = 0$, *then* $\delta_{8k} = 0$.

Proof. We prove each of the cases above separately.

Part (1)**:** $n = 2^k + 1$**.** By Lemma 3.2, the parity of $\frac{n}{n-j}\binom{n-j}{j}$ is equal to the parity of $\binom{(n-1)-j}{j} = \binom{2^k-j}{j}$.

We use Theorem 3.1 to find the parity of $\frac{n}{n-j}\binom{n-j}{j}$. By Lemma 3.2, we require the 2-ary expansion of $2^k - j$ for all j. Let $j = \sum_{i=0}^{k-1} j_i 2^i$ and denote by b the smallest index such that $j_b = 1$. To compute the 2-ary expansion of $2^k - j$, we make use of diagrams of the form

$$\begin{array}{r||ccccccc} & k & k-1 & & \cdots & b & \cdots & 0 \\ \hline\hline 2^k & 1 & 0 & & \cdots & 0 & \cdots & 0 \\ j & 0 & 0 & & \cdots & 1 & \cdots & 0 \\ \hline 2^k - j & 0 & 1 & {}_{k-2}\text{complement}_{b+1} & & 1 & \cdots & 0 \end{array},$$

where ${}_{\alpha}\text{complement}_{\beta}$ means to replace each bit j_i with $\overline{j_i} = 1 - j_i$ for $\alpha \geq i \geq \beta$. The method is grade-school subtraction in base 2.

By Theorem 3.1, the parity of $\binom{2^k-j}{j}$ is 0 whenever there is a 0 in the bottom row (corresponding to a bit of $2^k - j$) and a 1 in the middle row (corresponding to the same bit of j). This occurs whenever j has more than one non-zero bit in its expansion; that is, when $j \neq 0, 2^b$ for some b, as required.

Part (2)**:** $n = 2^e + 2^k + 1,\ k > 0$**.** By Lemma 3.2, the parity of $\frac{n}{n-j}\binom{n-j}{j}$ is equal to the parity of $\binom{(n-1)-j}{j} = \binom{2^e+2^k-j}{j}$. Similar to Part (1), we require the 2-ary expansion of $2^e + 2^k - j$ and $2^e + 2^k - 2j$ for $0 < j < 2^{e-1} + 2^{k-1}$. If $j = \sum_{i=0}^{e-1} j_i 2^i$, let b be the first index less than k for which $j_b = 1$ and let t be the first index greater than k for which $j_t = 1$ (if they exist). An example of the corresponding diagram is of the form

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 1 & \cdots & j_k & \cdots & 1 & \cdots & 0 \\ \hline
2^e + 2^k - j & & & & & & & & &
\end{array}.$$

We now have cases according to the form of j and the existence and values of b and t, as well as the expansion of j at its k-th bit. If j_t, respectively j_b, does not exist we say $j_t = 0$, respectively $j_b = 0$. Some cases are trivial: if $j_t = j_b = 0$, then $j = 0$ or $j = 2^k$.

Suppose $j_b = 0$. Then $j_t = 1$ and we reduce to the following diagram

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 1 & \cdots & j_k & \cdots & 0 & \cdots & 0 \\ \hline
2^e + 2^k - j & 0 & {}_{e-1}\text{complement}_{t+1} & 1 & \cdots & 1 - j_k & \cdots & 0 & \cdots &
\end{array}.$$

Now, suppose $j_b = 1$. First, we treat $j_k = 0$. Suppose also $j_t = 1$, then we reduce the diagram to

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \hline
2^e + 2^k - j & 0 & {}_{e-1}\text{complement}_{t+1} & 1 & \cdots & 0 & {}_{k-1}\text{complement}_{b+1} & 1 & \cdots &
\end{array}.$$

If $j_t = j_k = 0$, the diagram is

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 & \cdots & 0 \\ \hline
2^e + 2^k - j & 1 & \cdots & 0 & \cdots & 0 & {}_{k-1}\text{complement}_{b+1} & 1 & \cdots &
\end{array}. \tag{2}$$

Now consider the case $j_b = j_k = 1$. Suppose also $j_t = 1$, then the diagram is

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 1 & \cdots & 1 & \cdots & 1 & \cdots & 0 \\ \hline
2^e + 2^k - j & 0 & {}_{e-1}\text{complement}_{t+1} & 0 & \cdots & 1 & {}_{k-1}\text{complement}_{b+1} & 1 & \cdots &
\end{array},$$

and finally if $j_t = 0$, then we reduce

$$\begin{array}{r||ccccccccc}
 & e & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\ \hline\hline
2^e + 2^k & 1 & \cdots & 0 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & \cdots & 0 & \cdots & 1 & \cdots & 1 & \cdots & 0 \\ \hline
2^e + 2^k - j & 0 & \cdots & 1 & \cdots & 1 & {}_{k-1}\text{complement}_{b+1} & 1 & \cdots &
\end{array}. \tag{3}$$

This gives the 2-ary expansion of the differences $2^e + 2^k - j$. As in Part (1), by Theorem 3.1, the binomial coefficient $\binom{n-1-j}{j} \equiv 0 \pmod 2$ whenever there is a 0 in the bottom row (corresponding to a bit in the binary expansion of $n-1-j$) with a 1 in the same position of the middle row (corresponding to a bit in the binary expansion of j). Table 2 summarizes conditions for when the binomial coefficient, and hence the coefficient of the reversed Dickson polynomial, is even. The statement of the lemma is a simple restatement of these conditions.

j_b	j_k	j_t	other
0	0	1	$j_\ell = 1, \ell > t$
0	1	0	all
0	1	1	all
1	0	0	$j_\ell = 1, b+1 \leq \ell \leq k+1$
1	0	1	$j_\ell = 1, b+1 \leq \ell \leq k+1$ or $\ell > t$
1	1	0	$j_\ell = 1, b+1 \leq \ell \leq k+1$
1	1	1	all

TABLE 2. Conditions for when the binomial coefficient $\binom{2^e+2^k-j}{j}$ is even.

The proofs of Part (3) and (4) are similar; the main difference arises in the presence of the minus sign in each n in Part (3), and with both the presence of a minus plus an additional two non-zero bits in Part (4). In Part (3), the binary expansion of $2^e - 2^k$, for $e > k$, produces a run of 1s between the $(e-1)$-th and k-th bits. As always, if producing the diagram with the 2-ary expansion of $n-1$ on top, j in the middle row and $n-1-j$ on the bottom-most row, the parity of $\binom{n-1-j}{j}$ is even by Theorem 3.1 whenever there is a 0 on the bottom row with a corresponding 1 on the middle row. If this occurs in the s-th bit, then $j_s = 1$ and there is a 1 in the first row of the diagram corresponding either to a 1 in the first row, which is created by a borrow or is unaffected by a borrow.

We omit the full proofs of the remaining cases, and give one concrete example of Part (3) which illustrates the reasoning above. Suppose $n = 2^e - 2^k + 1$. If $k+1 = e$ (we include this case only for completeness, since we are chiefly concerned with the case $n = 2^{2k} - 2^k + 1$), then $2^e - 2^k = 2^k$, and the parity of $\binom{2^k}{j}$ is given determined in Part (1). Otherwise, we have a diagram of the form

$$\begin{array}{c||cccccccccc}
 & e & e-1 & \cdots & t & \cdots & k & \cdots & b & \cdots & 0 \\
\hline\hline
2^e - 2^k & 0 & 1 & \cdots & 1 & \cdots & 1 & \cdots & 0 & \cdots & 0 \\
j & & & \cdots & j_t & \cdots & j_k & \cdots & j_b & \cdots & 0 \\
\hline
2^e + 2^k - j & & & & & & & & & &
\end{array}.$$

Suppose $j = 2^{k+1} + 2^k + j_{k-1}2^{k-1} + \cdots + j_{b+1}2^{b+1} + 2^b$, for some $b < k$. Then the diagram is

$$\begin{array}{c||ccccccccccc}
 & e & e-1 & \cdots & k+2 & k+1 & k & \cdots & b & \cdots & 0 \\
\hline\hline
2^e - 2^k & 0 & 1 & \cdots & 1 & 1 & 1 & \cdots & 0 & \cdots & 0 \\
j & 0 & 0 & \cdots & 0 & 1 & 1 & \cdots & 1 & \cdots & 0 \\
\hline
2^e + 2^k - j & 0 & 1 & \cdots & 0 & 1 & 1 & {}_{k-1}\text{complement}_{b+1} & 1 & \cdots & 0
\end{array},$$

and the parity is even if and only if $j_\ell = 1$ for some $b+1 \leq \ell \leq k-1$, since 1s are created on the top row by the borrow from bit b. This exact reasoning shows that the parity is odd for $j = 2^b + 2^\ell - 2^k$ for $k+1 \leq \ell \leq e-1$.

The Dobbertin case, Part (4), combines elements of both Parts (2) and (3), and we omit the proof for brevity. □

4. Ambiguity and deficiency of reversed Dickson polynomials

Let p be a prime and let $q = p^e$. A *linearized* polynomial L is of the form $L(x) = \sum_{i=0}^{e-1} a_i x^{p^i} \in \mathbb{F}_q[x]$. Linearized polynomials are equivalent to linear operators over finite fields. Furthermore, an *affine* polynomial is given by $L(x)+c$, where c is a constant in $\mathbb{F}_q$. Difference maps act on polynomials over finite fields in a similar fashion as differentiation over the reals; indeed, the difference map of a function is often called the (discrete) *derivative* of the function. Instead of reducing the degree of the polynomial by 1, taking the difference map of a monomial reduces its p-weight (that is, the sum of the digits in the p-ary expansion of its degree) by one. We use this fact to state the ambiguity and deficiency of an affine polynomial.

LEMMA 4.1. *Let $L(x)=\sum_{j=0}^{e-1}\ell_j x^{p^j}$ be a linearized polynomial over $\mathbb{F}_q$, $q=p^e$, and let $c\in\mathbb{F}_q$. Then $\mathfrak{D}(L+c)=(q-1)^2$ and $\mathfrak{A}(L+c)=(q-1)\binom{q}{2}$.*

PROPOSITION 4.2. *Let $F(x)=D_n(1,x)$ be the reversed Dickson polynomial over $\mathbb{F}_q$, $q=2^e$, $n=2^k+1$ and $(k,2e)=1$ obtained from the Gold function. The ambiguity and deficiency of F satisfies $\mathfrak{D}(F)=(q-1)(q-2)$ and $\mathfrak{A}(F)=(q-1)\binom{q}{2}$, respectively.*

PROOF. By Theorem 3.3, $D_n(1,x)=1+\mathrm{Tr}(x)$, which is a linearized polynomial, plus a constant. The ambiguity and deficiency follows from Lemma 4.1. □

The ambiguity and deficiency of the reversed Dickson polynomial $F_n(x)=D_n(1,x)$ for $q=2^e$, $n=2^e+2^2+1$, and $e\neq 4$ was given in [**Pan11-2**] and satisfy

$$\mathfrak{A}(F_n)=2^{2e-3}\binom{4}{2}+(2^e-4)\binom{2^{e-1}}{2}+\binom{2^e}{2}$$

and

$$\mathfrak{D}(F_n)=2^e(2^e-1)-\left(\frac{2^{2e}}{8}+2^e-3\right).$$

A generalization of this result to the cubic binary reversed Dickson permutations, see Table 1, is given next.

THEOREM 4.3. *Let $q=2^e$, with e even and let $n=2^e+2^k+1$. Moreover, let $\gcd(k-1,e)=1$ and let $\gcd(k,e)=d$. Then the ambiguity and deficiency of the reversed Dickson polynomial $F_n(x)=D_n(1,x)$ satisfy*

$$\mathfrak{A}(F_n)=\begin{cases}2^{2e-d-1}\binom{2^d}{2}+(2^e-2^d)\binom{2^{e-1}}{2}+(2^{d-1}-1)\binom{2^e}{2}, & k/d\equiv 1 \pmod 2,\\ 2^{2e-d-1}\binom{2^d}{2}+(2^e-2^{d+1})\binom{2^{e-1}}{2}+(2^{d}-1)\binom{2^e}{2}, & k/d\equiv 0 \pmod 2;\end{cases}$$

$$\mathfrak{D}(F_n)=\begin{cases}2^{2e}-2^{2e-d-1}-2^{e+1}+2^{d-1}+1, & k/d\equiv 1 \pmod 2,\\ 2^{2e}-2^{2e-d-1}-2^{e+1}+2^{d}+1, & k/d\equiv 0 \pmod 2.\end{cases}$$

PROOF. Let $k=2t$ and $G_{v,w}(x)=x^{2^v}+x^{2^{v+1}}+\cdots+x^{2^w}$ for $x\in\mathbb{F}_{2^e}$ (observe that $G_{0,e-1}(x)=\mathrm{Tr}(x)$, where Tr is the trace function from $\mathbb{F}_{2^e}$ to $\mathbb{F}_2$).

By Theorem 3.3, the reversed Dickson polynomial $F_n(x)=D_n(1,x)$ satisfies

$$\begin{aligned}F_n(x) &= \sum_{j=0}^{2^{e-1}+2^{2t-1}}\frac{n}{n-j}\binom{n-j}{j}(-x)^j\\ &= 1+\mathrm{Tr}(x)+x^{2^{2t}}+G_{0,2t-1}(x)G_{2t,e-1}(x).\end{aligned}$$

Hence, the difference map $\Delta_{F_n,a}(x)=F_n(x+a)-F_n(x)$ satisfies

$$\begin{aligned}\Delta_{F_n,a}(x) &= \mathrm{Tr}(a)+a^{2^{2t}}+G_{0,2t-1}(a)G_{2t,e-1}(x)\\ &\quad +G_{0,2t-1}(x)G_{2t,e-1}(a)+G_{0,2t-1}(a)G_{2t,e-1}(a).\end{aligned}$$

We observe that $\Delta_{F_n,a}$ is of the form $C_a + L_a(x)$, where $C_a \in \mathbb{F}_q$ is a constant (depending only on a) and $L_a \in \mathbb{F}_q[x]$ is a linearized polynomial whose coefficients depend on a.

We recall the result of [**Pan13**, Corollary 3]: for any linearized polynomial $L(x) = \sum_{i=0}^{e-1} a_i x^{q^i}$, its value set has size $q^{\mathrm{rk}(\mathbf{A})}$, where $\mathrm{rk}(\mathbf{A})$ is the rank of the $e \times e$ auto-circulant matrix $\mathbf{A}$ with defining column $(a_0, a_1, \ldots, a_{e-1})$. Moreover, the number of times each image is repeated is precisely $q^{e-\mathrm{rk}(\mathbf{A})}$. If $a_0, a_1, \ldots, a_{e-1} \in \mathbb{F}_q$, then the auto-circulant matrix is simply circulant and has *associated polynomial* $A(x) = a_0 + a_1 x + \cdots + a_{e-1}x^{e-1}$. In addition, it is well-known [**Ing56**] that an $e \times e$ circulant matrix has rank equal to $e - \deg(\gcd(A(x), x^e - 1))$.

If $\mathrm{Tr}(a) = 0$, then $G_{0,2t-1}(a) = G_{2t,e-1}(a)$, and the linearized part of $\Delta_{F_n,a}$, $L_a(x) = G_{0,2t-1}(a)\mathrm{Tr}(x)$.

First, we determine when $G_{0,2t-1}(a) = 0$. By telescoping, $(1+a)G_{0,2t-1}(a) = a^{2^{2t}} + a = 0$ implies $a \in \mathbb{F}_{2^{2t}}$; that is, $G_{0,2t-1}(a) = 0$ implies $a \in \mathbb{F}_{2^{2t}} \cap \mathbb{F}_{2^e} = \mathbb{F}_{2^d}$. Moreover, for $a \in \mathbb{F}_{2^d}$, $G_{0,2t-1}(a) = (2t/d)\mathrm{Tr}_d(a)$, where Tr_d is the trace function from $\mathbb{F}_{2^d}$ to $\mathbb{F}_2$. If $2t/d$ is odd, then $G_{0,2t-1}(a) = 0$ if and only if a is a trace-0 element of $\mathbb{F}_{2^d}$. Otherwise if $2t/d$ is even, then $G_{0,2t-1}(a) = 0$ for all $a \in \mathbb{F}_{2^d}$. Whenever $G_{0,2t-1}(a) = 0$, $\Delta_{F_n,a}(x) = a$ for all x.

For all a with $\mathrm{Tr}(a) = 0$ and $G_{0,2t-1}(a) \neq 0$, there are exactly two values of $b \in \mathbb{F}_{2^e}$ such that $\Delta_{F_n,a}(x) = b$ has solutions for x in $\mathbb{F}_{2^e}$, namely $b = a^{2^{2t}} + G_{0,2t-1}(a)t_0$, where $t_0 \in \{0, 1\}$. Moreover, for each such pair (a, b), the equation $\Delta_{F_n,a}(x) = b$ has exactly 2^{e-1} solutions. This can be also be realized by observing that the first column of the auto-circulant matrix $\mathbf{A}$ has every entry equal to $G_{0,2t-1}(a)$, hence has rank 1 whenever $G_{0,2t-1}(a) \neq 0$ and rank 0 otherwise.

Now, consider those $a \in \mathbb{F}_{2^e}$ with $\mathrm{Tr}(a) = 1$. With $G_{0,2t-1}(a) = 1 + G_{2t,e-1}(a)$, we have $\Delta_{F_n,a}(x) = C_a + G_{0,2t-1}(a)\mathrm{Tr}(x) + G_{0,2t-1}(x)$, where C_a is a constant depending only on a. Thus, we need to consider only the value set of $G_{0,2t-1}(a)\mathrm{Tr}(x) + G_{0,2t-1}(x)$, which is linearized. We observe that $(G_{0,2t-1}(a) + \delta)^{2^i} = G_{i,2t-1+i}(a) + \delta$, with indices taken modulo e and with $\delta = 0, 1$. We further denote $G_{i,2t-1+i}(a) + \delta$ by $G_i^{(\delta)}$. Let

$$\mathbf{A}_{2t,a} = \begin{pmatrix} G_0^{(1)} & \cdots & G_{2t-1}^{(0)} & G_{2t}^{(0)} & \cdots & G_{e-1}^{(1)} \\ G_0^{(1)} & \cdots & G_{2t-1}^{(0)} & G_{2t}^{(0)} & \cdots & G_{e-1}^{(1)} \\ \vdots & & \vdots & \vdots & & \vdots \\ G_0^{(1)} & \cdots & G_{2t-1}^{(1)} & G_{2t}^{(0)} & \cdots & G_{e-1}^{(0)} \\ G_0^{(0)} & \cdots & G_{2t-1}^{(1)} & G_{2t}^{(1)} & \cdots & G_{e-1}^{(0)} \\ \vdots & \vdots & \vdots & & \vdots & \\ G_0^{(0)} & \cdots & G_{2t-1}^{(0)} & G_{2t}^{(0)} & \cdots & G_{e-1}^{(0)} \\ G_0^{(0)} & \cdots & G_{2t-1}^{(0)} & G_{2t}^{(0)} & \cdots & G_{e-1}^{(1)} \end{pmatrix}.$$

As before, we reduce $\mathbf{A}_{2t,a}$ by the row operation (with rows indexed by 0)

(1) Row $j \leftarrow$ Row j $-$ Row $j-1$ for $1 \leq j \leq e-1$, and
(2) Row $0 \leftarrow$ Row 0 $-$ Row $e-1$.

What remains is the circulant matrix with defining column $\mathbf{v} = (v_i)_{i=0}^{e-1}$, with $v_0 = v_{2t} = 1$ and $v_i = 0$ for $i \neq 0, 2t$. The associated polynomial $V(x) = \sum_{i=0}^{e-1} v_i x^i = 1 + x^{2t}$. The rank of the matrix defined by $\mathbf{v}$ is given by $e - \deg(\gcd(1+x^{2t}, 1+x^e)) =$

$e - \gcd(2t, e) = e - d$. In each case, the value set has cardinality 2^{e-d} and each image is repeated exactly 2^d times.

We give all values of $\alpha_i > 0$ for $i > 0$ in the following table.

	α_{2^d}	$\alpha_{2^{e-1}}$	α_{2^e}
$2t/d \equiv 1 \pmod 2$	$2^{e-1} \cdot 2^{e-d}$	$2(2^{e-1} - 2^{d-1})$	$2^{d-1} - 1$
$2t/d \equiv 0 \pmod 2$	$2^{e-1} \cdot 2^{e-d}$	$2(2^{e-1} - 2^{d})$	$2^{d} - 1$

Moreover, the deficiency of F_n, $\mathfrak{D}(F_n) = \alpha_0$ is given by subtracting the row-sum from $2^e(2^e - 1)$ in the appropriate row of the above table. □

Numerical results on the differential spectrum and ambiguity and deficiency of the Kasami and Dobbertin binary reversed Dickson permutation polynomials from Table 1 are calculated using a SAGE program and provided in Tables 3–5.

e	k	α_0	α_2	α_4	α_6	α_8	α_{10}
5	3	596	316	60	40	0	0
7	3	9703	5146	1239	168	0	0
7	5	9829	4950	1260	210	7	0
8	3	39775	19510	5072	740	149	34
8	5	39889	19398	4960	860	123	50
9	5	159634	77670	20286	3648	340	54
9	7	159070	78354	20520	3348	322	18

TABLE 3. Differential spectrum of the Kasami reversed Dickson polynomial $D_n(1, x)$ for $q = 2^e$, $n = 2^{2k} - 2^k + 1$ and $(k, 2e) = 1$.

e	k	α_0	α_2	α_4	$\alpha_{2^{e-1}}$	$\alpha_{2^{e-1}+2}$
4	3	159	58	16	5	2
6	5	2769	951	281	24	7
8	7	46317	13196	5640	91	36

TABLE 4. Differential spectrum of the reversed Dickson polynomial $D_n(1, x)$ for $q = 2^e$, $n = 2^{2k} - 2^k + 1$ and $k = e - 1$.

We can draw some inferences from our tables. As we observe in Theorem 4.3, the form of the ambiguity and deficiency for reversed Dickson permutations can be case dependent, which is confirmed for the Kasami case by comparing Tables 3 and 4. In Table 3, we observe that the i for which α_i are non-zero are "low", in comparison to those i in Table 4. Moreover, based on Table 4, in the particular case $k = e - 1$ we can draw the conjecture that the Kasami reversed Dickson polynomial $D_n(1, x)$ over $\mathbb{F}_q$ with $q = 2^e$, $n = 2^{2k} - 2^k + 1$ satisfies $\alpha_{2^{e-1}} + \alpha_{2^{e-1}+2} = 2^{e-1} - 1$.

One of our motivations for studying the reversed Dickson polynomials was their connection to almost perfect nonlinear functions [**Hou10, Hou09**]. The *differential uniformity* of a function is the largest i such that $\alpha_i > 0$. If a function is almost perfect nonlinear, it has differential unifomity at most 2, and in the case of permutations in even-degree extensions of $\mathbb{F}_2$, only one known almost perfect non-linear permutation is known [**Bro10**]. Therefore, functions with differential uniformity

e	k	$(\mathfrak{D}(F), \text{Opt } \mathfrak{D}(2^e))$	$(\mathfrak{A}(F), \text{Opt } \mathfrak{A}(2^e))$	MC
5	1	$(656, 496)$	$(1396, 496)$	$(10, 5)$
10	2	$(655774, 523776)$	$(1296588, 523776)$	$(28, 30)$

Table 5. Ambiguity and deficiency of the Dobbertin reversed Dickson polynomial $D_n(1, x)$ for $e = 5k$ and $n = 2^{8k} + 2^{6k} + 2^{4k} + 2^{2k} - 1$.

at most 4 are preferred, such as the inverse map used in the *Advanced Encryption Standard*.

The last column of Table 5 provides a pair which denotes the maximum collisions (MC). For example, $(10, 5)$ in last column of the first row of Table 5 means that there are exactly 5 pairs of $(a, b) \in \mathbb{F}_q^* \times \mathbb{F}_q$ such that $\Delta_{f,a}(x) = b$ has exactly 10 distinct solutions. Therefore, the differential uniformity of the first two cases of the Dobbertin reversed Dickson polynomial is 10, when $e = 5$ and 28 when $e = 10$, so unfortunately we do not believe that these functions will be suitable for use in systems where resistance against differential attacks is necessary.

Acknowledgement. We would like to thank Brett Stevens and Qiang (Steven) Wang for some initial discussions which were valuable to this work. In addition, we would like to thank an anonymous referee for their helpful comments which improved the presentation of this work.

References

[Bih91] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, J. Cryptology, vol. 4, 1991, pp. 3–72.

[Blokh01] A. Blokhuis, R. S. Coulter, M. Henderson and C. M. O'Keefe, *Permutations amongst the Dembowski-Ostrom polynomials*, Proceedings of the Fifth Conference on Finite Fields and Applications, Contemporary Mathematics, 2001, pp. 37–42.

[Blon11] C. Blondeau, A. Canteaut and P. Charpin, *Differential properties of $x \to x^{2^t-1}$*, IEEE Trans. Inform. Theory, vol. 57, 2011, pp 8127–8137.

[Bro10] K. A. Browning, J. F. Dillon, M. T. McQuistan and A. J. Wolfe, *An APN permutation in dimension six*, Proceedings of the Ninth Conference on Finite Fields and Applications, Contemporary Mathematics, vol. 518, 2010, pp. 33–42.

[Car98] C. Carlet, P. Charpin and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr., vol. 15, 1998, pp. 125–156.

[Car04] C. Carlet and C. Ding, *Highly non-linear mappings*, J. Complexity, vol. 20, 2004, pp. 205–244.

[Char08] P. Charpin and G. Kyureghyan, *On a class of permutation polynomials over $\mathbb{F}_{2^n}$*, SETA'08 Proceedings of the 5th International Conference on Sequences and Their Applications, 2008, pp. 368–376.

[Dem68] P. Dembowski and T. G. Ostrom, *Planes of order n with collineation groups of order n*, Math. Z. vol. 2, 1968, pp. 239–258.

[Dra10] K. Drakakis, V. Requena and G. McGuire, *On the non-linearity of exponential Welch Costas functions*, IEEE Trans. Inform. Theory, vol. 56, 2010, pp. 1230–1238.

[Fine47] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly, vol. 54, 1947, pp. 589–592.

[Goe87] P. Goetgheluck, *Computing binomial coefficients*, Amer. Math. Monthly, vol. 94, 1987, pp. 360–365.

[Hou10] X. Hou and T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl., vol. 16, 2010, pp. 436–448.

[Ing56] A. E. Ingleton, *The rank of circulant matrices* J. London Math. Soc., vol s1-31(4), 1956, pp. 445-460.

[Hou09] X. Hou, G. L. Mullen, J. A. Sellers and J. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl., vol. 15, 2009, pp. 748–773.

[Lidl93] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson Polynomials*, Longman Scientific & Technical, Essex, 1993.

[Lidl97] R. Lidl and H. Niederreiter, *Finite Fields (2nd ed.)*, Cambridge University Press, Cambridge, 1997.

[Mat94] M. Matsui, *Linear cryptanalysis method for DES cipher*, Advances in Cryptology EUROCRYPT'93, Lecture Notes Comput. Sci., vol. 765, 1994, pp. 386–397.

[Mul86] W.B. Müller and R. Nöbauer, *Cryptanalysis of the Dickson scheme*, Advances in Cryptology EUROCRYPT'85, Lecture Notes Comput. Sci., vol. 219, 1986, pp. 50–61.

[Pan11-1] D. Panario, A. Sakzad, B. Stevens and Q. Wang, *Two new measures for permutations: ambiguity and deficiency*, IEEE Trans. Inform. Theory, vol. 57, 2011, pp. 7648–7657.

[Pan11-2] D. Panario, A. Sakzad, B. Stevens and Q. Wang, *Ambiguity and deficiency of permutations from finite fields*, Proceedings of IEEE Information Theory Workshop (ITW), 2011, pp. 165–169.

[Pan13] D. Panario, A. Sakzad, B. Stevens, D. Thomson and Q. Wang, *Ambiguity and deficiency of permutations with linearized difference function from finite fields*, IEEE Trans. Inform. Theory, vol. 58, 2013, pp. 5616–5626.

[Pan10] D. Panario, B. Stevens and Q. Wang, *Ambiguity and deficiency in Costas arrays and APN permutations*, Proceedings of LATIN 2010, Lecture Notes Comput. Sci., vol. 6034, 2010, pp. 397–406.

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

[Thom12] D. Thomson, *On difference maps and their cryptographic applications*, PhD Thesis, Carleton University, 2012.

School of Mathematics and Statistics, Carleton University, Ottawa ON, Canada, K1S 5B6.

E-mail address: `daniel@math.carleton.ca`

Department of Electrical and Computer Systems Engineering, Monash University, Melbourne, VIC. 3800, Australia.

E-mail address: `amin.sakzad@monash.edu`

School of Mathematics and Statistics, Carleton University, Ottawa ON, Canada, K1S 5B6.

E-mail address: `dthomson@math.carleton.ca`