On the Differential Uniformity of Polynomials over Galois Rings

Sondre Rønjom[1,2] and Arne Sandrib[1,2]

[1] University of Bergen, Department of Informatics, Bergen, Norway
[2] Nasjonal sikkerhetsmyndighet, Kolsås, Norway

Abstract

Design of hash functions and pseudo-random permutations over Galois extensions of $\mathbb{Z}_q$ for prime powers q has recently gained some interest in relation to recent directions in advanced cryptography, such as multiparty computation and zero-knowledge protocol design. Thus investigating optimality of cryptographic properties of S-boxes defined by polynomials over Galois rings is of interest. Of particular interest is the differential uniformity of such functions. To our knowledge, there are very few results on the differential uniformity for polynomials over Galois rings $\mathrm{GR}(p^k, m)$ when $k, m \geq 2$. Motivated by designing secure hash functions and block ciphers over Galois rings, a main contribution of this paper is an investigation into the differential properties of polynomials over Galois rings. Finally, we provide a classification of APN permutations in $\mathrm{GR}(4, 2)$ up to affine and CCZ-equivalence.

1 Introduction

One of the most fundamental constructions in symmetric cryptography is the substitution box (S-box), playing a key role in providing confusion during the encryption process. Traditionally, S-boxes have been defined as functions over binary fields, aiming for properties like low differential probability, high algebraic degree and high nonlinearity in order to achieve security. In recent years, however, there has been a growing interest in ring-based technologies. Examples include zero-knowledge (ZK) proof systems such as [LXY23, WZD+25b, WZD25a] and fully homomorphic encryption (FHE) schemes like BGV [BGV11] or BFV [BV11]. The Elisabeth cipher family defined over modular rings was designed to be FHE-friendly [CHMS22]. One key advantage of defining ciphers over rings is that many FHE protocols are defined over ring structures, often relying on some lattice problem being difficult to solve. Defining functions over the same algebraic structures may ease both implementation and efficiency when the need for conversion between data structures is eliminated.

This paper focuses on the construction of S-boxes over Galois rings. They are in some sense the unification of modular rings and finite fields (see e.g. [McD74, p. 307]), and their versatility could therefore make them well-suited for various cryptographic designs. In particular, we investigate *differential uniformity* of S-boxes over Galois rings which, in some sense, measures how close the function is to being linear. A function with low differential uniformity provides strong resistance to differential cryptanalysis, which was introduced by Biham and Shamir in [BS91]. The reader may note that there have been multiple attempts to construct symmetric ciphers over rings, like the SAFER family of cryptosystems [Mas94] whose S-boxes were defined to be APN (almost perfect nonlinear) functions over $\mathbb{Z}_{256}$, as well as the AES finalist RC6 [RRSY], which relied on multiple different operations over $\mathbb{Z}_{2^w}$, including XOR. However, none of these seem to be in widespread use today.

Emails: sondre.ronjom@uib.no (Sondre Rønjom), arne.sandrib@student.uib.no (Arne Sandrib)

Date of this document: 2026-07-08.

Despite the versatility of Galois rings, and apart from some earlier applications like [Hel96] using them for universal hash functions, Galois rings have not seen nearly the same amount of use in real-world (symmetric) cryptosystems as the finite binary fields. Furthermore, the amount of published research on differential properties of functions defined over Galois rings is close to non-existent. While [DGM09] provided an enumeration of APN permutations over $\mathbb{Z}_n$ for $n < 19$ and [YW13] found a general bound for differential uniformity in the context of $\mathbb{Z}_N$ where N is composite, there is very little research on Galois extensions of these rings. This lack of research on fundamental properties may in part explain the very limited use that Galois rings have seen in cryptography. To enable future construction of strong ciphers, the study of differential properties of these functions seems essential.

The main contribution of this paper is establishing rudimentary results on the differential uniformity of functions defined over Galois rings. Of particular interest are the permutations, and we establish a bound for both permutations and non-permutations when the functions are polynomials. We demonstrate that such functions have differential uniformity which is much higher than what is possible when resorting to table-based definitions of functions. We give a class of permutation polynomials achieving the lower bound for differential uniformity for certain parameters p, m, k. Finally, we enumerate all APN permutations over $\mathrm{GR}(2^2, 2)$ up to affine and CCZ-equivalence.

2 Preliminaries

We begin by recalling some basic properties of Galois rings and polynomials over them. The reader is referred to [McD74] for a more rigorous treatment of Galois rings. For a prime p and $k, m \geq 1$, a Galois ring $\mathrm{GR}(p^k, m)$ of p^{mk} elements is a degree m Galois extension of $\mathbb{Z}_{p^k}$. Any such ring is isomorphic to $\mathbb{Z}_{p^k}[\alpha]/(g(\alpha))$, where $g(\alpha) \in \mathbb{Z}_{p^k}[\alpha]$ is a monic polynomial of degree m whose reduction modulo p is irreducible over $\mathbb{Z}_p$. For $q = p^k$, denote this ring by $R_{q^m} = \mathrm{GR}(p^k, m)$. Setting $k = 1$ gives the usual Galois field $\mathrm{GF}(p^m) = \mathbb{F}_{p^m}$. Any Galois ring is a local principal ideal ring, and contains the chain

$$(0) \subset (p^{k-1}) \subset \cdots \subset (p) \subset R_{q^m}$$

of ideals generated by powers of the prime p. Moreover, note that $\mathbb{F}_{p^m} \cong R_{q^m}/(p)$, and we will henceforth denote the latter field by F. Elements in this field are just cosets of (p) and will be denoted by $\overline{x} \in F$, where by definition $\overline{x} = x + (p)$. An element $u \in R_{q^m}$ is a unit if and only if $\overline{u} \neq 0$, and we denote by $R_{q^m}^\times$ the unit group of R_{q^m}. The projection $R_{q^m} \to F$ extends coefficientwise to the polynomial ring, and for any polynomial $f(x) \in R_{q^m}[x]$ we denote its projection by $\overline{f}(x) \in F[x]$. Note that polynomial evaluation is well defined under this projection, since the fact that polynomial functions map cosets to cosets, i.e., $f(a + (p)) \subseteq f(a) + (p)$, implies that

$$\overline{f}(\overline{a}) = \overline{f(a)} \tag{1}$$

for every $a \in R_{q^m}$. Finally, for any polynomial $f(x) = \sum_{i=0}^{n} c_i x^i \in R_{q^m}[x]$, denote its formal derivative by $f'(x) = \sum_{i=1}^{n} c_i i x^{i-1}$.

It is well known that not all functions on R_{q^m} are induced by polynomials (see e.g. [BM92]). A function $\hat{f} \colon R_{q^m} \to R_{q^m}$ induced by a polynomial $f(x) \in R_{q^m}[x]$ is called a *polynomial function*, or simply *polyfunction*. We will usually refer to a polyfunction by a polynomial that induces it. A polynomial inducing a permutation of R_{q^m} is called a *permutation polynomial*.

Lifting roots of a reduced polynomial $\overline{f}(x) \in F[x]$ to roots of a polynomial $f(x) \in R_{q^m}[x]$ is central to this paper, and this is typically done with Hensel's lemma. It holds in general for so-called *Henselian* rings, and in particular for local rings with nilpotent maximal ideal. We state it for the latter case, which is all we need for Galois rings.

Theorem 1 (Hensel's lemma)**.** *Let R be a commutative ring with a nilpotent maximal ideal $\mathfrak{m}$. Suppose $H(x) \in R[x]$ is a polynomial with reduction $h(x) \in (R/\mathfrak{m})[x]$. If $\hat{w} \in R/\mathfrak{m}$ has*

$$h(\hat{w}) = 0 \qquad \text{and} \qquad h'(\hat{w}) \neq 0,$$

then there is a unique $w \in R$ such that $H(w) = 0$ and $w \equiv \hat{w} \mod \mathfrak{m}$.

Note that the requirement in Theorem 1 that $h'(\hat{w}) \neq 0$ is equivalent to $\hat{w}$ being a *simple root* of $h(x)$, i.e. that $(x - \hat{w})^d$ divides $h(x)$ for $d = 1$, but not for $d = 2$. We will refer to simple roots many times throughout the paper. A *multiple root* is a root which is not simple.

Now suppose that the root $\hat{w} \in R/\mathfrak{m}$ of $h(x)$ is not simple. Then an element $w \in R$ such that $w \equiv \hat{w} \mod \mathfrak{m}$ cannot automatically be ruled out as a root of $H(x)$. In the Galois ring setting, if $f(x) \in R_{q^m}[x]$ has reduction $\overline{f}(x) \in F[x]$ and $\overline{w} \in F$ is a multiple root of $\overline{f}(x)$, then a separate argument is needed to determine which elements in the coset $w + (p) \subseteq R_{q^m}$ that are roots of $f(x)$. In general, the number of such elements can range from zero to the size of the coset itself. This phenomenon will be the foundation of some worst-case bounds presented later in the paper.

Finally, we remark that many versions of Hensel's lemma require that $H(x)$ be monic, but this is not necessary for the simple root-lifting version of the result.

The following lemma is also needed for establishing many of the results of this paper. It is an expression for the directional derivative $D_a f(x) = f(x + a) - f(x)$, and is closely related to the Taylor formula on rings (see e.g., [Wan03, p. 332]).

Lemma 1. *Suppose that $f(x) = \sum_{i=0}^{n} c_i x^i \in R[x]$ and $a \in R$, where R is any commutative ring. Then*

$$D_a f(x) = af'(x) + a^2 \sum_{i=1}^{n} c_i \sum_{j=2}^{i} \binom{i}{j} x^{i-j} a^{j-2}.$$

In particular, if $a^2 = 0$, then $D_a f(x) = af'(x)$.

Proof. By the binomial formula, we have

$$c_i(x + a)^i - c_i x^i = c_i \sum_{j=1}^{i} \binom{i}{j} x^{i-j} a^j = aic_i x^{i-1} + c_i \sum_{j=2}^{i} \binom{i}{j} x^{i-j} a^j$$

for any $i > 0$. For the entire polynomial we then get

$$\begin{aligned} D_a f(x) = f(x + a) - f(x) &= \sum_{i=1}^{n} [c_i(x + a)^i - c_i x^i] \\ &= \sum_{i=1}^{n} \left[aic_i x^{i-1} + c_i \sum_{j=2}^{i} \binom{i}{j} x^{i-j} a^j \right] \\ &= af'(x) + a^2 \sum_{i=1}^{n} c_i \sum_{j=2}^{i} \binom{i}{j} x^{i-j} a^{j-2}. \end{aligned}$$

The latter claim follows immediately. □

S-boxes are typically required to be permutations, and to this end we recall the following well-known conditions from [McD74] for a polynomial in $R_{q^m}[x]$ to induce a permutation. We include a proof for the benefit of the reader.

Theorem 2. *Suppose $q = p^k$ with $k > 1$. Then $f(x) \in R_{q^m}[x]$ is a permutation polynomial if and only if*

1. *$\overline{f}(x)$ permutes F and*
2. *the formal derivative $\overline{f}'(x)$ is nonzero on all of F.*

Proof. Assume conditions (1) and (2). For each $b \in R_{q^m}$, define $g_b(x) = f(x) - b \in R_{q^m}[x]$. For each b, there is by (1) some unique $\overline{y} \in F$ such that $\overline{g}_b(\overline{y}) = \overline{0}$, and by (2) we have $\overline{g}_b'(\overline{y}) \neq 0$. Then, by Theorem 1, there is some unique $w \in R_{q^m}$ with $\overline{w} = \overline{y}$ such that $g_b(w) = 0$. Equivalently, w is the unique input giving $f(w) = b$, so f is injective, and hence bijective by the finiteness of R_{q^m}.

If (1) does not hold, then f maps two different cosets to the same coset, contradicting injectivity. If (2) does not hold, then there is some $a \in R_{q^m}$ such that $f'(a) \in (p)$. Then for any $t \in R_{q^m}$, Lemma 1 gives

$$f(a + tp^{k-1}) = f(a) + p^{k-1}tf'(a) = f(a),$$

i.e., f is constant on the coset $a + (p^{k-1})$. □

Heuristically, the first condition listed in Theorem 2 means that the polynomial permutes the cosets of $(p) \subseteq R_{q^m}$, while the second condition ensures that the restriction of f to any coset $a + (p)$ maps injectively into the coset $f(a) + (p)$.

We remark that for certain parameters of R_{q^m}, there are given exact criteria for a polynomial to be a permutation. For example, when $m = 1$ and $q = 2^k$ for any $k > 1$, there is a complete classification by Rivest in [Riv01] giving exact criteria that a polynomial permutes $\mathbb{Z}_{2^k}$. In general, however, we must decide whether $\overline{f}$ permutes F, and as pointed out in [LN96, p. 347], this is a rather complicated matter. It is further complicated by the additional requirement that the derivative be nonzero on all of F.

We state some general properties of permutation polynomials in the setting of Galois rings. The following results are direct consequences of Theorem 2.

Corollary 1. *Let $f(x)$ be a permutation polynomial for $\mathrm{GR}(p^k, m)$. Then*

1. *for any integer $k' > k$ and lift $\hat{f}(x) \in \mathrm{GR}(p^{k'}, m)[x]$ of $f(x)$ such that $\hat{f}(x) \equiv f(x) \mod (p^k)$, the polynomial $\hat{f}(x)$ permutes $\mathrm{GR}(p^{k'}, m)$;*
2. *for any integer $1 < k' < k$, the reduction $f(x) \mod (p^{k'})$ in $\mathrm{GR}(p^{k'}, m)$ permutes $\mathrm{GR}(p^{k'}, m)$.*

Corollary 2. *A polynomial that only has terms that are multiples of p, except for degree-1 coefficient $a_1 \notin (p)$, will permute R_{q^m}.*

Proposition 1. *If $f(x) \in R_{q^m}[x]$ has only integer coefficients and permutes R_{q^m}, then f permutes $\mathbb{Z}_q$.*

It is in principle possible to use the above properties to design block ciphers or hash functions with S-boxes, linear layers and security analysis over $\mathbb{F}_{2^m}$, and then lift the cipher to R_{q^m} for any $q = 2^k$ as one sees fit, thus opening up the possibility for versatile cryptographic designs meeting several practical requirements (e.g. different ZK/MPC protocols) at once while relying on one security analysis. In the following, we analyse the differential properties of such S-boxes.

3 Differential Uniformity in $\mathrm{GR}(p^k, m)$

For a function $f\colon R \to R$ over a finite ring R, the differential uniformity of f measures the maximum number of solutions to the equation $D_a f(x) = f(x + a) - f(x) = b$ for a pair $a \neq 0, b \in R$. For $a, b \in R$ define

$$\delta_f(a, b) = |\{x \in R \mid f(x + a) - f(x) = b\}|$$

to be the entries of the $|R| \times |R|$ table δ which we call the *Difference Distribution Table* (DDT). The *differential uniformity* of f is simply $\Delta_f = \max_{a \neq 0, b} \delta_f(a, b)$. The *differential probability* corresponding to the pair of input/output differences (a, b) is given by $DP_f(a, b) = \delta_f(a, b)/|R|$, and we define $DP_f^{\max} = \Delta_f/|R|$. Let

$$N_f(c) = |\{(a, b) \in (R \setminus \{0\}) \times R \mid \delta_f(a, b) = c\}|.$$

Then the *differential spectrum* of f is given by $(N_f(0), N_f(1), \ldots) = (N_f(i))_{i\in\mathbb{Z}_{\geq 0}}$, where $N_f(c)$ counts the number of times the value $c \in \mathbb{Z}_{\geq 0}$ appears in the DDT of f.

Differential cryptanalysis is one of the main threats against symmetric ciphers and motivates the use of S-boxes defined by polynomials with low differential uniformity. In general, functions with low differential uniformity provide better resistance to such attacks than functions with higher differential uniformity. Any function $f(x)$ with differential uniformity 2 is called an *almost perfect nonlinear* (APN) function and achieves the lowest possible differential uniformity over $\mathbb{F}_{2^m}$. For rings with odd characteristic, differential uniformity equal to 1 can be possible, and a function attaining this bound is called a *perfect nonlinear* (PN) function.

3.1 Bound for Polynomials

We establish a lower bound on the differential uniformity for a polyfunction over a Galois ring.

Proposition 2. *The differential uniformity of a polyfunction $f(x) \in R_{q^m}[x]$ for $k > 1$ is lower bounded by the size of the maximal ideal of R_{q^m}. I.e., $\Delta_f \geq |(p)| = p^{m(k-1)}$.*

Proof. Let $f(x) \in R_{q^m}[x]$ be given by $f(x) = \sum_i c_i x^i$ and let $a = p^{k-1}y \in (p^{k-1})$. Using Lemma 1, for any $x = pz \in (p)$ we get

$$\begin{aligned} D_a f(x) &= p^{k-1} y f'(pz) \\ &= p^{k-1} y \sum_{i\geq 1} i c_i (pz)^{i-1} \\ &= p^{k-1} y c_1, \end{aligned}$$

which is constant for every such choice of a, x. □

The proof of Proposition 2 shows that the existence of zero divisors in R_{q^m} causes the differential uniformity of polyfunctions to be relatively high compared to the finite field case. We will later see that even though the values of $\delta_f(a, b)$ may be low for a, b units, Proposition 2 shows that there are always $a, b \in (p)$ such that $\delta_f(a, b) \geq p^{m(k-1)}$.

3.2 Bound for Permutation Polynomials

Recall the following basic result that will be needed for establishing a bound on differential uniformity for permutation polynomials over Galois rings. Its justification can be found in [McD74].

Lemma 2. *If the Galois ring R_{q^m} has $\operatorname{char} R_{q^m} = p^k = q$, then for every $0 \leq i \leq k$,*

$$p^i a = p^i b \iff a + (p^{k-i}) = b + (p^{k-i}).$$

We now have all the ingredients needed to prove the main theorem of this section:

Theorem 3. *The differential uniformity of a permutation polynomial $f(x) \in R_{q^m}[x]$ for $k > 1$ is lower bounded by twice the size of the maximal ideal of R_{q^m}. I.e., $\Delta_f \geq 2|(p)| = 2p^{m(k-1)}$.*

Proof. As in the proof of Proposition 2, set $a = p^{k-1}y \in (p^{k-1})$ and write $D_a f(x) = p^{k-1} y f'(x)$. Since f is a permutation, condition (2) of Theorem 2 implies that $\overline{f}'(\overline{x}) \neq \overline{0}$ for every $\overline{x} \in F$. The latter condition combined with the pigeonhole principle implies that there are (at least) two distinct elements $\overline{\alpha}, \overline{\beta} \in F$ such that $\overline{f}'(\overline{\alpha}) = \overline{f}'(\overline{\beta})$. Using Equation (1), note that every element of $(\alpha + (p)) \cup (\beta + (p))$ is mapped to some fixed coset $\mu + (p)$ by f'. Then, using Lemma 2 with $i = k - 1$, we have $p^{k-1} y f'(x) = p^{k-1} y f'(x')$ for every pair $x, x' \in (\alpha + (p)) \cup (\beta + (p))$. Hence, $\Delta_f \geq |(\alpha + (p)) \cup (\beta + (p))| = 2|(p)|$. □

Remark 1. Note that the bounds established by Proposition 2 and Theorem 3 are identical to the bounds established by Theorem 6 and Corollary 2 of [YW13] for polynomial functions over rings such as $\mathbb{Z}_{p^k}$, which is isomorphic to R_{q^m} with $m = 1$. However, they do not treat the general case of $m > 1$.

Corollary 3. *Every permutation polynomial on $\mathbb{Z}_{2^k}$ has differential uniformity 2^k, i.e., the highest attainable for functions on $\mathbb{Z}_{2^k}$.*

3.3 The DDT for Polynomials in $\mathrm{GR}(2^k, m)$

In this section, we establish results about the DDT of polynomials over R_{q^m}. First we show that if q is even, then $\delta_f(a, b)$ is even for each $a, b \in R_{q^m}$. Then we prove some results connecting δ_f with properties of the polynomials $\overline{f}$ and $\overline{f}'$ in $F[x]$.

In the case of a ring of characteristic 2 and a function f, all DDT values $\delta_f(a, b)$ are even, because if w solves the equation $f(x + a) - f(x) = b$ for x, then also $a + w$ is a solution. When the characteristic increases, this relation no longer holds. In the following, we show that polynomial functions over R_{q^m} with even q have only even numbers in their DDTs. First, we establish two basic lemmas.

Lemma 3. *Let $(p^{k-1}) \subset R_{q^m}$ denote the minimal ideal. The restriction of a polynomial map $f\colon R_{q^m} \to R_{q^m}$, to some coset $a + (p^{k-1})$ is constant if and only if $f'(a) \in (p)$. Otherwise the restricted map is injective, i.e., $f(a + (p^{k-1})) = f(a) + (p^{k-1})$.*

Proof. By Lemma 1, we have

$$f(a + p^{k-1}y) = f(a) + p^{k-1}yf'(a).$$

If $f'(a) \in (p)$, then the restriction of f to $a + (p^{k-1})$ is constantly equal to $f(a)$. Otherwise, for every pair y, y' such that $a+p^{k-1}y \neq a+p^{k-1}y'$, we have $p^{k-1}yf'(a) \neq p^{k-1}y'f'(a)$, as $f'(a)$ is a unit. □

Lemma 4. *Fix $q = 2^k$ and let $f(x) \in R_{q^m}[x]$. If the restriction of $D_af(x)$ to some coset $x_0 + (2^{k-1})$ is injective for some $a \notin (2)$, then the restriction of $D_af(x)$ to $x_0 + a + (2^{k-1})$ is also injective.*

Proof. Observe that since $\operatorname{char} F = 2$, we have $\overline{D_af(x)} = \overline{D_af(x + a)}$ as polynomials, implying that $\overline{(D_af)'(x)} = \overline{(D_af)'(x + a)}$. Equivalently,

$$(D_af)'(x) - (D_af)'(x + a) \in (2).$$

Since $2 \nmid (D_af)'(x_0)$, we must have that $2 \nmid (D_af)'(x_0 + a)$. Concluding by Lemma 3, we have that $D_af(x)$ is injective when restricted to the coset $x_0 + a + (2^{k-1})$. □

We are ready to prove that the entries of the DDT of functions over Galois rings with even characteristic are all even.

Proposition 3. *For $q = 2^k$ and $f(x) \in R_{q^m}[x]$, every entry $\delta_f(a, b)$ of the DDT of f is even.*

Proof. Fix $a \neq 0, b \in R_{q^m}$ for q even. Consider every coset of the minimal ideal (2^{k-1}). We will show that the number of solutions to $D_af(x) - b = 0$ inside each coset is either the size of the coset, one, or zero. If it is one, then we show that there is a (uniquely determined) corresponding coset whose contribution is also one. The sum of these contributions is, of course, even.

When the equation $D_af(x) - b$ has no solutions, the number of solutions is trivially even.

Suppose that w solves $D_af(x) - b = 0$ and $2 \mid (D_af)'(w)$. Then, by Lemma 3, the restriction of $D_af(x)$ to $w + (2^{k-1})$ is constant, thus, the contribution of the coset $w + (2^{k-1})$ is the size of the coset, which is even.

Suppose that w solves $D_af(x) - b = 0$ and $2 \nmid (D_af)'(w)$. Then $a \notin (2)$, since if $a \in (2)$,

$$\overline{D_af(x)} = \overline{f}(\overline{x} + \overline{a}) - \overline{f}(\overline{x}) = \overline{f}(\overline{x}) - \overline{f}(\overline{x}) = \overline{0},$$

implying that $\overline{D_af(x)}$ is the zero polynomial, contradicting $(D_af)'(w) \notin (2)$. Then there is exactly one solution in $w + (2^{k-1})$ since the restriction of $D_af(x)$ to this coset is injective by Lemma 3. Consider the equation $\overline{D_af(x) - b} = \overline{0}$ over the field $F = \mathbb{F}_{2^m}$. Since the characteristic is 2, the value $\overline{w + a}$ is also a solution. We note that $\overline{x + a} \neq \overline{x}$ since $\overline{a} \neq \overline{0}$. We claim that the root $\overline{w + a}$ is simple over F. A sufficient condition is that the derivative of $\overline{D_af(x) - b}$ be nonzero at $\overline{x + a}$. Note that $\overline{D_af(w)} = \overline{D_af(w + a)}$ are equal as polynomials over F. Combining with the assumption that $2 \nmid (D_af)'(w)$, we get

$$\overline{D_af}(\overline{w}) = \overline{D_af}(\overline{w} + \overline{a}) \implies \overline{(D_af)}'(\overline{w} + \overline{a}) = \overline{(D_af)}'(\overline{w}) \neq \overline{0}$$

We conclude that $\overline{w + a}$ is a simple root of $\overline{D_af(x) - b}$. This allows for the use of Theorem 1: There is a unique root $w' \in R_{q^m}$ of $D_af(x) - b$ such that $w' \equiv w + a \mod (2)$. This implies that $w' \neq w$. Since $2 \nmid (D_af)'(w')$, the restriction of D_af to the coset $w' + (2^{k-1})$ is injective, so the coset contributes with 1 to the entry (a, b) of the DDT of $f(x)$. Furthermore, by the uniqueness of lifted simple roots, this coset is uniquely determined by w. □

The lifting technique showcased in the proof above suggests that the DDT of a polynomial over a Galois ring has strong connections to the DDT of the polynomial projected onto $F[x]$. We illustrate one further such connection, by bounding $\delta_f(a, b)$ for some polynomial $f(x) \in R_{q^m}[x]$ in terms of its behavior on $F[x]$, when a is a unit.

Proposition 4. *Let $f(x) \in R_{q^m}[x]$ with $n = \deg \overline{f}$ and $(a, b) \in R_{q^m}^\times \times R_{q^m}$ and $q = p^k$ with $k > 1$. Then*

1. $\delta_f(a, b) \leq \delta_{\overline{f}}(\overline{a}, \overline{b})p^{m(k-1)} \leq \Delta_{\overline{f}}p^{m(k-1)}$;
2. $\delta_f(a, b) \leq \frac{n-1}{2} \cdot p^{m(k-1)}$ *if n is odd and $\overline{D_af(x)}$ non-constant;*
3. $\delta_f(a, b) \leq 1 + \frac{n-2}{2} \cdot p^{m(k-1)}$ *if n is even and $\overline{D_af(x)}$ is non-constant.*

Proof. Let $b \in R_{q^m}$ and $h(x) = D_af(x) - b$.

We start with proving (1). There are $\delta_{\overline{f}}(\overline{a}, \overline{b})$ solutions to $\overline{h}(x) = 0$ in F. Each such solution $\overline{w} \in F$ is the projection of some element in the coset $w + (p) \subseteq R_{q^m}$, and hence gives rise to at most $|w + (p)| = p^{m(k-1)}$ solutions of $h(x)$ in R_{q^m}. Consequently, $\delta_f(a, b) \leq \delta_{\overline{f}}(\overline{a}, \overline{b})|(p)| \leq \Delta_{\overline{f}}p^{m(k-1)}$.

For (2) and (3), denote $d = \deg \overline{h}$. Assume that $\overline{h}(x)$ is non-constant (which happens if and only if $\overline{D_af(x)}$ is non-constant) and note that $1 \leq d \leq \deg \overline{f} - 1$. Then there are at most d roots of $\overline{h}(x)$. Let s be the number of simple roots and t be the number of multiple roots, and thus $s + 2t \leq d$. Since every simple root of $\overline{h}$ may be lifted to a unique root of h, and every multiple root of $\overline{h}$ may be lifted to at most $|(p)|$ roots of h, we get

$$\delta_f(a, b) \leq s + t|(p)| = s + tp^{m(k-1)}, \tag{2}$$

which is maximized when d and t are as large as possible. If d is odd, then we maximize $s + tp^{m(k-1)}$ by setting $t = (d - 1)/2$ and setting $s = 1$, which gives $\delta_f(a, b) \leq 1 + p^{m(k-1)} \cdot (d-1)/2$. If d is even, set $t = d/2$ and get $\delta_f(a, b) \leq d/2 \cdot p^{m(k-1)}$.

Finally, if $n = \deg \overline{f}$ is odd, then Equation (2) is maximized when d is the maximal even or maximal odd number less than n, so

$$\delta_f(a, b) \leq \max\left\{(n - 1)/2 \cdot p^{m(k-1)}, 1 + (n - 3)/2 \cdot p^{m(k-1)}\right\} = (n - 1)/2 \cdot p^{m(k-1)}.$$

Similarly, if $\deg \overline{f}$ is even, we have

$$\delta_f(a, b) \leq \max\left\{(n - 2)/2 \cdot p^{m(k-1)}, 1 + (n - 2)/2 \cdot p^{m(k-1)}\right\} = 1 + (n-2)/2 \cdot p^{m(k-1)},$$

concluding the proof. □

Next, we establish some upper bounds on $\delta_f(a,b)$ in the case of a being a non-unit. These play an essential role in building towards criteria for determining that a polynomial in R_{q^m} achieves optimal differential uniformity, which will be explored in the next section. First, we show a useful lemma.

Lemma 5. *Suppose that $a = p^s u$ for some unit $u \in R_{q^m}^\times$ with $1 \leq s < k$, and that $f(x) \in R_{q^m}[x]$. Then $D_a f(x) \equiv D_a f(y) \mod (p^{s+1})$ if and only if $\overline{f}'(\overline{x}) = \overline{f}'(\overline{y})$. In particular,*

$$\overline{f}'(\overline{x}) \neq \overline{f}'(\overline{y}) \implies D_a f(x) \neq D_a f(y).$$

Proof. Let $a = p^s u \in (p)$ where $1 \leq s < k$ such that $u \in R_{q^m}^\times$ is a unit, and let $x, y \in R_{q^m}$. Note that $a^2 = p^{2s}u^2 \equiv 0 \mod p^{s+1}$ since $2s \geq s+1$. Thus, by Lemma 1, we have that $D_a f(x) \equiv a f'(x) \mod (p^{s+1})$. Then,

$$D_a f(x) - D_a f(y) \equiv p^s u(f'(x) - f'(y)) \mod (p^{s+1}),$$

which is zero mod (p^{s+1}) if and only if $\overline{f}'(\overline{x}) = \overline{f}'(\overline{y})$ since u is a unit. Hence, if $\overline{f}'(\overline{x}) \neq \overline{f}'(\overline{y})$, then

$$D_a f(x) - D_a f(y) \equiv a(f'(x) - f'(y)) \not\equiv 0 \mod (p^{s+1}),$$

and hence $D_a f(x) \neq D_a f(y)$. □

Lemma 5 shows that if $a \in (p) \setminus \{0\}$, then $D_a f(x) = D_a f(y)$ only if $\overline{f}'(\overline{x}) = \overline{f}'(\overline{y})$. An immediate consequence is the following important bound on $\delta_f(a,b)$ for $a \in (p) \setminus \{0\}$. Recall that a *fiber* is just the inverse image of a singleton set in the codomain of a function.

Proposition 5. *Suppose that $f(x) \in R_{q^m}[x]$ is a polynomial, $a \in (p) \setminus \{0\}$, $b \in R_{q^m}$ and let $t = \max_{y \in F} |(\overline{f}')^{-1}(y)|$ be the maximum size of some fiber of $\overline{f}'$. Then $\delta_f(a,b) \leq t p^{m(k-1)}$.*

Proof. Let a, b be as stated, and suppose w solves $D_a f(x) = b$. Let $A = (\overline{f}')^{-1}(\overline{f'(w)})$, and observe that $|A| \leq t$. By Lemma 5, if $\overline{w}' \notin A$, then $w' \in R_{q^m}$ does not solve $D_a f(x) = b$, implying that only lifts of elements in A to R_{q^m} may be roots of $D_a f(x) = b$. Hence, $\delta_f(a,b) \leq |A||(p)| = t p^{m(k-1)}$. □

In the next section, we draw some conclusions based on these results, especially regarding the optimality of certain polynomial functions.

3.4 On Optimal Differential Uniformity of Polynomials

Given a prime p and $k, m \geq 1$, we have $|(p)| = (p^{k-1})^m$. Then for the special case of $\mathbb{Z}_4$, $k = 2$ and $m = 1$, we do get that $|(2)| = 2$, being the only Galois ring with zero divisors for which APN polynomials can exist. While it is easy to verify that there are APN polynomials in $\mathbb{Z}_4$, Theorem 3 shows that none of them are permutations. In particular, there are no APN permutation polynomials for R_{q^m} when $k > 1$. This may seem like an unfortunate limitation, but it also motivates a new notion of optimal differential uniformity.

Definition 1. Let f be a polyfunction over a Galois ring R_{q^m}. We say that

1. f is *poly-APN* if $\Delta_f = p^{m(k-1)}$;
2. f is *permutation-poly-APN* (*ppoly-APN*) if $\Delta_f = 2p^{m(k-1)}$ and f is a permutation.

An immediate consequence of Theorem 3 is that the maximal differential probability for ppoly-APN polynomials is independent of k, i.e., $\max_{a \neq 0, b} DP(a,b) = 2p^{-m}$, which is in stark contrast to the case of permutation polynomials over $\mathbb{F}_{2^k}^m$ where this probability decreases as k increases.

Drawing from the previous section, we deduce criteria ensuring that a function is poly-APN.

Theorem 4. *A polynomial $f(x) \in R_{q^m}[x]$, is poly-APN if and only if $\overline{f}'$ is bijective on F.*

Proof. Suppose $\overline{f}'$ is bijective on F. If $0 \neq a \in (p)$, then $\delta_f(a,b) \leq p^{m(k-1)}$ by Proposition 5.

For $a \in R_{q^m}^\times$, define the polynomial $h(x) = D_a f(x) - b$. Then $\overline{h}'(x) = \overline{f}'(x+\overline{a}) - \overline{f}'(x)$ is nonzero for every $x \in F$, since $\overline{f}'$ is injective, implying that every root of $\overline{D_a f(x) - b}$ is simple and lifts uniquely to R_{q^m}. Hence, $\delta_f(a,b) = \delta_{\overline{f}}(\overline{a},\overline{b})$ for every unit $a \in R_{q^m}^\times$, and of course $\delta_{\overline{f}}(\overline{a},\overline{b}) \leq |F| \leq p^{m(k-1)}$, so f is indeed poly-APN.

Conversely, if f is poly-APN and $\overline{f}'$ is not injective on F, then by the same argument as in Theorem 3, we get $\Delta_f \geq 2p^{m(k-1)}$. □

For the case of permutation polynomials, the situation is more complex due to condition (2) of Theorem 2 requiring that the map $\overline{f}'$ be non-injective. Hence, candidates for being ppoly-APN must, for now, be treated in a case-by-case fashion. Nevertheless, we summarize sufficient criteria as a direct consequence of Proposition 5, where the cases of a being a unit and a non-unit must be treated separately.

Proposition 6. *Let $f(x) \in R_{q^m}[x]$ be a permutation polynomial. Then f is ppoly-APN if the maximal fiber size of $\overline{f}'$ is 2 and for each unit $a \in R_{q^m}^\times$ the relation $\delta_f(a,b) \leq 2p^{m(k-1)}$ holds.*

In order to prove that a specific function is ppoly-APN, one may combine Proposition 6 with Proposition 4. We demonstrate this in Section 4.2. For some polynomial $f(x) \in R_{q^m}[x]$, that would require either that $\Delta_{\overline{f}}$ is low enough, or that $\deg f$ is sufficiently low with $\overline{D_a f(x)}$ nonconstant for every unit a.

The lower bounds on differential uniformity established in the previous sections suggest that the non-units are primarily responsible for high numbers appearing in the DDT of some polynomial function. However, explicit testing shows that when both $a, b \in R_{q^m}^\times$, we may still have $\delta_f(a,b) > 2p^{m(k-1)}$, even if the polynomial behaves *optimally* on the non-units. For instance, the permutation polynomial

$$f(x) = x + (5\alpha + 3\alpha^2)x^2 + (3\alpha + 3\alpha^2)x^3 + (2 + \alpha + 5\alpha^2)x^4 + (3 + 3\alpha^2)x^5 + 5x^6$$

in $R_{8^3}[x]$ has

$$\max_{(a,b)\in((p)\setminus\{0\})\times R_{q^m}} \delta_f(a,b) = 128 = 2 \cdot 2^{3(3-1)} \quad \text{and} \quad \max_{a,b\notin(p)} \delta_f(a,b) = 136,$$

where the latter maximum is achieved when both a, b are units. We are able to computationally verify that for every lift $\hat{f}$ of f to $R_{16^3}[x]$ has $\delta_{\hat{f}}(a,b)$ achieving its maximum on non-units a, b. The same behavior can be observed for multiple other polynomials, suggesting the following conjecture:

Conjecture 1. *Given a permutation polynomial $f(x) \in R_{q^m}[x]$ with $q = p^k$ such that the maximal fiber size of $\overline{f}'$ is 2, then there is some $n \geq k$ such that $q' = p^n$ such that any lift $\hat{f}$ of f to $R_{(q')^m}[x]$ achieves the lower bound of $\Delta_{\hat{f}} = 2p^{m(n-1)}$.*

We conclude the section with one final conjecture. The reasoning is that an APN permutation polynomial, when lifted to the Galois ring, will have a differential uniformity which is *too low* to be a permutation of the ring due to Theorem 3.

Conjecture 2. *An APN permutation polynomial $f : \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$ cannot be lifted to a permutation polynomial over R_{q^m} for $q = 2^k$.*

If true, the conjecture would, by Theorem 2 imply that the formal derivative of an APN permutation vanishes in at least one point of its domain.

4 Explicit Constructions

4.1 Power Functions

Consider the polynomial $f(x) = x^d \in R_{q^m}[x]$ for some $d > 1$. Then f is a well-known APN function for many values of d when $k = 1$. When k increases, the differential uniformity of the function obviously also increases, and it loses the property of being a permutation by condition (2) of Theorem 2. The following result tells us exactly when a power polynomial is poly-APN.

Theorem 5. *Let $q = p^k$, $d > 1$, $m > 0$ and $k > 1$. Then the power polynomial $x^d \in R_{q^m}[x]$ is poly-APN if and only if $\gcd(d-1, p^m - 1) = \gcd(d, p) = 1$. In particular, if $\gcd(d-1, p^m - 1) > 1$, then $\Delta_f \geq 2p^{m(k-1)}$, and if $\gcd(d, p) > 1$, then $\Delta_f = p^{km} = |R_{q^m}|$.*

Proof. Suppose that $\gcd(d-1, p^m - 1) = \gcd(d, p) = 1$ and that $f(x) = x^d$. Then $\overline{f}'(x) = \overline{d}x^{d-1}$, which is injective on F if and only if d is a unit and $x^{d-1} \in F[x]$ is a permutation. The first is ensured by $\gcd(d, p) = 1$, and the latter by $\gcd(d-1, p^m - 1) = 1$. Hence, by Theorem 4, $f(x)$ is poly-APN.

Conversely, let $\gcd(d-1, p^m - 1) > 1$ and $a = p^{k-1}u$ with $u \in R_{q^m}^\times$. Then, by Lemma 1, $D_a f(x) = p^{k-1}udx^{d-1}$. Then there are $r, s \in R_{q^m}$ such that $\overline{r} \neq \overline{s}$, and $\overline{r}^{d-1} = \overline{s}^{d-1}$ since $\overline{x} \mapsto \overline{x}^{d-1}$ is not injective. Consequently, if $x, x' \in (r+(p)) \cup (s+(p))$, we have $x^{d-1} \equiv (x')^{d-1} \mod (p)$, and hence by Lemma 2, we have $p^{k-1}dx^{d-1} = p^{k-1}d(x')^{d-1}$, implying that $\Delta_f \geq 2p^{m(k-1)}$.

Finally, let $\gcd(d, p) > 1$ and $a = p^{k-1}u$ with $u \in R_{q^m}^\times$. Then $d = py$ for some $y \in R_{q^m}$, and hence $D_a f(x) = p^{k-1}dx^{d-1} = p^{k-1}pyx^{d-1} = 0$, so $\Delta_f = p^{km} = |R_{q^m}|$. □

Over the finite field $\mathbb{F}_{2^m}$, the Gold function x^{2^i+1} is APN when i and m are coprime. For $q = 2^k$, it is poly-APN over R_{q^m} if and only if $(d-1, p^m-1) = (d, p) = 1$, by Theorem 5. Indeed, inserting $d = 2^i + 1$ and $p = 2$ yields

$$\gcd((2^i + 1) - 1, 2^m - 1) = 1 \qquad \text{and} \qquad \gcd(2^i + 1, 2) = 1.$$

Hence, we conclude with the following corollary.

Corollary 4. *For $k > 1$, $q = 2^k$ and $m > 0$, the Gold function $x^{2^i+1} \in R_{q^m}[x]$ is poly-APN for every $i > 0$.*

4.2 Dickson Polynomials

Definition 2. Choose some unit $u \in R_{q^m}^\times$ and some degree $d > 0$. Define the corresponding Dickson polynomial $g_d(x, u) \in R_{q^m}[x]$ to be

$$g_d(x, u) = \sum_{j=0}^{\lfloor d/2 \rfloor} \frac{d}{d-j} \binom{d-j}{j} (-u)^j x^{d-2j}$$

where $\frac{d}{d-j}\binom{d-j}{j}$ is evaluated in $\mathbb{Z}$ before any modulo reduction in R_{q^m}, and hence the expression is always well defined.

The work done in [BGC91] provided exact conditions that the Dickson polynomial be a permutation polynomial in $\mathrm{GR}(p^k, m)$: for a fixed prime p, a unit $u \in R_{q^m}^\times$ and $k > 1$, the Dickson polynomial $g_d(x, u)$ is a permutation polynomial for $\mathrm{GR}(p^k, m)$ if and only if the equalities $\gcd(d, p^{2m} - 1) = \gcd(d, p) = 1$ hold. From our experiments we see that many Dickson permutation polynomials are ppoly-APN for R_{q^m} when m is odd. For the even case, however, our observations do not indicate that permutation polynomials with this property exist.

A possible advantage of using Dickson polynomials for cryptographic applications is that they can be defined in a way in which all coefficients lie in $\mathbb{Z}_q \subset R_{q^m}$. In fact, this happens every time u is chosen to be a unit in $\mathbb{Z}_q$.

The following result establishes a class of degree 5 Dickson polynomials which are permutations for $p = 2$ and odd m, and have optimal differential uniformity of $2 \cdot 2^{m(k-1)}$. This, in fact, gives an infinite class of ppoly-APN permutations.

Theorem 6. *Let $q = 2^k$ and m odd. The permutation given by the polynomial $g_5(x, u) = x^5 - 5ux^3 + 5u^2x \in R_{q^m}[x]$ for any unit u achieves the lowest possible differential uniformity of $2^{m(k-1)+1}$.*

Proof. Since m is odd and $d = 5$, we have

$$2^{2m} - 1 \equiv 4^m - 1 \equiv (-1)^m - 1 \equiv -1 - 1 \equiv 3 \mod 5,$$

so $\gcd(5, p^{2m} - 1) = 1$. Moreover, $\gcd(5, 2) = 1$, so $g_5(x, u)$ is indeed a permutation.

We know by Theorem 3 that $\Delta_f \geq 2 \cdot 2^{m(k-1)}$. We show that the differential uniformity is also upper bounded by this quantity, proving the theorem. Note that

$$\begin{aligned} D_a f(x) &= 5ax^4 + 10a^2x^3 + (10a^3 - 15ua)x^2 + (5a^4 - 15ua^2)x + (5u^2a - 5ua^3 + a^5) \\ &= a\Big(5x^4 + 10ax^3 + (10a^2 - 15u)x^2 + (5a^3 - 15ua)x + (5u^2 - 5ua^2 + a^4)\Big). \end{aligned}$$

and define

$$h(x) = 5x^4 + 10ax^3 + (10a^2 - 15u)x^2 + (5a^3 - 15ua)x + (5u^2 - 5ua^2 + a^4)$$

so that $D_a f(x) = ah(x)$.

When $a \notin (2)$, the polynomial $\overline{D_a f(x)}$ is non-constant. Furthermore, since $\deg \overline{f} = 5$, statement (2) in Proposition 4 implies that $\delta_f(a, b) \leq \frac{4}{2} 2^{m(k-1)} = 2^{m(k-1)+1}$ for every $b \in R_{q^m}$.

Now suppose $a \in (2)$. It is routine to check that $\overline{f}'(x) = x^4 + x^2 + 1 \in F[x]$ is 2-to-1 on F. We conclude that $\overline{f}'(x)$ has maximal fiber size 2, and hence by Proposition 5, we have $\delta_f(a, b) \leq 2 \cdot 2^{m(k-1)}$.

□

We conclude the part on Dickson polynomials with a few observations for $p = 2$, motivating further research.

There are many Dickson permutation polynomials other than g_5, such as $g_{11}(x, u)$. While the latter polynomial is ppoly-APN in R_{q^3}, it is not a permutation over R_{q^5}, and it has higher differential uniformity than optimal permutations. Hence, a ppoly-APN Dickson polynomial does not automatically give rise to an infinite class of ppoly-APN functions.

Furthermore, it is not enough for a permutation to be 4-uniform over F to be ppoly-APN over R_{q^m}. One example is $g_{13}(x, u)$ over $\mathrm{GR}(2^k, 3)$ whose differential uniformity over F is 4, but for example when $k = 2$, it has differential uniformity 40 and not 16, which is the lowest possible for permutations in R_{4^3}. This holds for any $g_{13}(x, u)$ with $u \in R_{q^m}^\times$.

For $g_6(x, u)$, we observe that while it is APN over $\mathbb{F}_{2^m}$ for various m, it achieves maximal differential uniformity of q^m over R_{q^m} whenever $k > 1$. This can be shown by writing out the expression for g_6 as in the proof of Theorem 6, and writing $D_a g_6(x) = a h_a(x)$ for some $h_a(x)$, and we get $\overline{h_a(x)}$ is by no means 2-to-1 when $a \in (2)$.

Finally, we have not observed any Dickson polynomial over R_{q^m} for m even which is ppoly-APN. Nevertheless, the question of existence of ppoly-APN polynomials for even m is answered in the affirmative in the following section.

4.3 Polynomials with Integer Coefficients

As mentioned in the context of Dickson polynomials, there are upsides to considering polynomials with only integer coefficients. Not only does this ease the study of the functions, but it has various advantages in cryptographic applications.

By computing the differential uniformity of all permutation polynomials over R_{4^2} restricted to having integer coefficients, it becomes evident that the differential uniformity never goes below 10, slightly above the lower bound 8. I.e., none of the 32 integral permutation polynomials are ppoly-APN. For the case of R_{8^2}, the differential uniformity lower bound is easily achieved with integer coefficient polynomials, e.g., $f(x) = x(1 + x^4 + x^6)$ is ppoly-APN with $\Delta_f = 32$. There is currently no reason to believe that there is any lack of ppoly-APN functions with integer coefficients in the general setting.

5 A Classification of All APN Permutations over $\mathrm{GR}(4, 2)$

If we do not require a polynomial representation of the function, but resort to a table-based implementation, we find many APN permutations over Galois rings. We remark that due to the isomorphism $(R_{q^m}, +) \cong (\mathbb{Z}_q^m, +)$, studying the difference distribution tables in the Galois ring setting is essentially the same as defining functions over the Cartesian product of m copies of $\mathbb{Z}_q$.

We classify APN permutations in $\mathrm{GR}(4, 2)$ up to affine and CCZ-equivalence. Two functions $f, g\colon \mathbb{Z}_q^m \to \mathbb{Z}_q^m$ are *affine equivalent* if there are invertible matrices A, B over $\mathbb{Z}_q$ and $a, b \in \mathbb{Z}_q^m$ such that

$$g(x) = B(f(Ax + a)) + b$$

for all $x \in \mathbb{Z}_q^m$. A more general notion of equivalence is that of CCZ-equivalence. Define $\Gamma_f = \{(x, f(x)) \mid x \in \mathbb{Z}_q^m\}$ to be the graph of the function f. Then f, g are said to be *CCZ-equivalent* if there exists an invertible $2m \times 2m$ matrix A and $a \in \mathbb{Z}_q^{2m}$ such that $A\Gamma_f + a = \Gamma_g$. Both these notions of equivalence preserve differential uniformity and differential spectrum, but CCZ-equivalence is strictly more general than affine equivalence.

5.1 Exhaustive Search on $\mathrm{GR}(4, 2)$

We performed an exhaustive search of all affine equivalence classes of permutations of $R_{4^2} \cong \mathbb{Z}_4^2$, thereby classifying all APN permutations up to affine equivalence. Following a search technique very similar to that of [LP07], we use the fact that every permutation of $\mathbb{Z}_{2^k}^m$ is affine equivalent to one fixing $(0, \ldots, 0)$ and all standard basis vectors. The ring-analogue of their result allowed us to fix three points for every permutation, namely $(0, 0), (1, 0)$ and $(0, 1)$, drastically reducing the search space. Before stating the results in Section 5.2, we justify fixing these points and explain how we determine CCZ-equivalence of two functions. Finally, we provide code[3] for the search, and refer the reader to `README.md` for its details.

Fixing coordinates in the search. Recall the notion of *affine span* $\mathrm{Aff}(x_0, \ldots, x_m) = x_0 + \mathrm{Span}(x_1 - x_0, \ldots, x_m - x_0)$ which is independent of the choice of base point within the set $\{x_0, \ldots, x_m\}$. The vectors $x_0, \ldots, x_m$ are said to be *affine independent* if $\mathrm{Span}(x_1 - x_0, \ldots, x_m - x_0)$ has rank m over $\mathbb{Z}_{2^k}$, where $\mathrm{Span}(\{x_i - x_s\}_{i \neq s})$ again is independent of choice of base point x_s. The following is the ring-analogue of Lemma 1 in [LP07].

Lemma 6. *Given a bijection $f\colon \mathbb{Z}_{2^k}^m \to \mathbb{Z}_{2^k}^m$, there are two sets of affine independent vectors $A = \{x_0, \ldots, x_m\}$ and $B = \{y_0, \ldots, y_m\}$ such that $f(x_i) = y_i$ for every $0 \leq i \leq m$.*

Proof. We give a proof by induction on t. Suppose $A_t = \{x_0, \ldots, x_t\}$ and $B_t = \{y_0, \ldots, y_t\}$ with $f(x_i) = y_i$ for every $i \leq t$ and suppose A_t and B_t both are affine

[3] https://github.com/arnesandrib/Galois-Ring-APN-Classification

independent sets. Let $C_t = f^{-1}(\mathrm{Aff}(B_t))$ and observe that $|\mathrm{Aff}(A_t)| = |\mathrm{Aff}(B_t)| = |C_t| = 2^{kt}$.

We seek $x_{t+1} \in \mathbb{Z}_{2^k}^m$ such that $y_{t+1} = f(x_{t+1})$ and $y_{t+1} \notin \mathrm{Aff}(B_t)$. Hence, x_{t+1} must be chosen from $\mathbb{Z}_{2^k}^m \setminus (\mathrm{Aff}(A_t) \cup C_t)$, which is guaranteed to be a nonempty set when $|\mathrm{Aff}(A_t) \cup C_t| < |\mathbb{Z}_{2^k}^m| = 2^{km}$. Note that for each x_i with $i \leq t$, we have $f(x_i) = y_i \in \mathrm{Aff}(B_t)$, implying that $x_i \in C_t$. Consequently, $\mathrm{Aff}(A_t) \cap C_t \neq \emptyset$, and hence

$$|\mathrm{Aff}(A_t) \cup C_t| < |\mathrm{Aff}(A_t)| + |C_t| = 2^{kt} + 2^{kt} = 2^{kt+1}.$$

Since $t \leq m-1$, we have $|\mathrm{Aff}(A_t) \cup C_t| < 2^{kt+1} \leq 2^{k(m-1)+1} \leq 2^{km} = |\mathbb{Z}_{2^k}^m|$. Hence, the set $\mathbb{Z}_{2^k}^m \setminus (\mathrm{Aff}(A_t) \cup C_t)$ is non-empty, and choosing x_{t+1} to be any of its elements completes the induction step. □

Given Lemma 6, one may transform any permutation $f\colon \mathbb{Z}_{2^k}^m \to \mathbb{Z}_{2^k}^m$ into some permutation g fixing $(0,\ldots,0)$ and all the standard basis vectors e_i, where the i-th entry equals 1 and the remaining entries are 0, in the following way: Let $X = \{x_0,\ldots,x_m\}$ and $Y = \{y_0,\ldots,y_m\}$ be sets such that $f(x_i) = y_i$ for each i. Set $a = x_0$ and let A be the $m \times m$ matrix whose i-th column is $x_i - x_0$. Let C be the $m \times m$ matrix whose i-th column is given by $y_i - y_0$. Both sets X and Y are affine independent, and equivalently, both A and C are invertible. Finally, choose $B = C^{-1}$, and $b = -By_0$. Then define $g(x) = Bf(Ax + a) + b$. Observe that $g(0) = Bf(x_0) + b = By_0 + b = 0$. Furthermore, evaluating g at e_i gives

$$g(e_i) = Bf(Ae_i + a) + b = Bf((x_i - x_0) + x_0) + b = By_i - By_0 = B(y_i - y_0) = e_i$$

using that $B = C^{-1}$.

The consequence for our search for permutations over $\mathbb{Z}_4^2$ was that three inputs could be fixed. Then the search space was significantly reduced to only $13! \approx 2^{32.5}$ permutations. Finding all APN permutations with fixed points was done in a matter of minutes on a modern laptop. Then we made a set consisting of all the obtained APN permutations. By selecting one representative, we could easily eliminate from the set all permutations to which it was affine equivalent. This process yielded a complete list of representatives of equivalence classes of APN permutations.

On Establishing CCZ-equivalence. To check whether two permutations f, g are CCZ-equivalent, we search for an invertible matrix $A \in \mathbb{Z}_4^{4\times 4}$ and $a \in \mathbb{Z}_4^4$ such that $A\Gamma_f + a = \Gamma_g$. We do this by checking all block matrices A with $A_{11}, A_{12} \in \mathbb{Z}_4^{2\times 2}$ such that

$$A = \begin{pmatrix} A_{11} & A_{12} \\ * & * \end{pmatrix}$$

and checking if $A_{11}x + A_{12}f(x)$ is a permutation so that $A(x, f(x)) = (A_{11}x + A_{12}f(x), *)$ indeed gives the graph of a function. Then determining the existence of A_{21}, A_{22} and a such that $A\Gamma_f + a = \Gamma_g$ reduces to solving linear equations over $\mathbb{Z}_4$. Details are available in `GR42_CCZ.sage` in the referenced code.

5.2 Results

The search yielded 15,576 APN permutations, and we extracted 32 unique representatives corresponding to each affine equivalence class. These representatives are provided in Table 1. The 32 representatives fall into 19 different CCZ-classes and yield 13 different differential spectra. See Table 2 for the complete list of differential spectra and CCZ-classes.

The provided tables should be interpreted using the following ordering of R_{q^m}: for each element $u = \sum_{i=0}^{m-1} u_i\alpha^i \in R_{q^m}$ associate the nonnegative integer given by $\sum_{i=0}^{m-1} u_i q^i \in \{0,1,\ldots,q^m-1\}$. If $x \in R_{q^m}$ corresponds to the integer x_i under this correspondence, then the x_i-th element of the table is an integer y_i representing the output y of the function when evaluated in x.

The number of entries equal to 2 in the DDTs of the APN permutations varied substantially, ranging from 64 in the *best case* to 112 in the *worst case*. A peculiar

Table 1: Collection of 32 representatives of the different affine equivalence classes of optimal APN permutations over GR$(4, 2)$.

H_0	0, 1, 2, 5, 4, 3, 7, 12, 13, 15, 6, 8, 14, 10, 9, 11
H_1	0, 1, 2, 5, 4, 3, 8, 10, 14, 13, 11, 12, 6, 9, 15, 7
H_2	0, 1, 2, 5, 4, 3, 9, 11, 12, 14, 8, 13, 10, 7, 15, 6
H_3	0, 1, 2, 5, 4, 3, 10, 6, 11, 14, 13, 15, 7, 8, 12, 9
H_4	0, 1, 2, 5, 4, 3, 10, 12, 8, 14, 11, 7, 13, 15, 9, 6
H_5	0, 1, 2, 5, 4, 3, 12, 15, 6, 13, 7, 10, 11, 9, 8, 14
H_6	0, 1, 2, 5, 4, 6, 3, 13, 7, 14, 9, 15, 12, 10, 8, 11
H_7	0, 1, 2, 5, 4, 6, 3, 14, 7, 8, 12, 15, 9, 11, 10, 13
H_8	0, 1, 2, 5, 4, 6, 8, 13, 11, 14, 3, 15, 9, 7, 12, 10
H_9	0, 1, 2, 5, 4, 7, 10, 12, 15, 13, 11, 6, 14, 8, 3, 9
H_{10}	0, 1, 2, 5, 4, 7, 11, 10, 9, 15, 3, 12, 6, 13, 8, 14
H_{11}	0, 1, 2, 5, 4, 7, 15, 11, 12, 14, 13, 8, 10, 3, 9, 6
H_{12}	0, 1, 2, 5, 4, 9, 11, 14, 12, 6, 13, 8, 15, 7, 3, 10
H_{13}	0, 1, 2, 5, 4, 10, 3, 11, 15, 14, 6, 8, 7, 12, 9, 13
H_{14}	0, 1, 2, 5, 4, 10, 7, 3, 11, 13, 15, 14, 6, 9, 8, 12
H_{15}	0, 1, 2, 5, 4, 10, 7, 3, 15, 8, 14, 12, 11, 9, 13, 6
H_{16}	0, 1, 2, 5, 4, 10, 14, 12, 9, 15, 13, 6, 11, 7, 3, 8
H_{17}	0, 1, 2, 5, 4, 12, 3, 10, 11, 15, 6, 14, 7, 8, 13, 9
H_{18}	0, 1, 2, 5, 4, 12, 10, 15, 6, 8, 3, 11, 13, 9, 7, 14
H_{19}	0, 1, 2, 5, 4, 15, 8, 12, 6, 9, 14, 7, 3, 11, 13, 10
H_{20}	0, 1, 2, 6, 4, 3, 10, 12, 11, 14, 5, 7, 13, 15, 9, 8
H_{21}	0, 1, 2, 6, 4, 8, 15, 9, 5, 7, 14, 10, 11, 13, 12, 3
H_{22}	0, 1, 3, 5, 4, 2, 9, 8, 10, 15, 7, 14, 11, 13, 12, 6
H_{23}	0, 1, 3, 5, 4, 7, 13, 9, 6, 12, 15, 2, 8, 10, 11, 14
H_{24}	0, 1, 3, 5, 4, 8, 10, 11, 13, 2, 6, 14, 15, 7, 9, 12
H_{25}	0, 1, 3, 5, 4, 9, 7, 13, 15, 11, 6, 14, 2, 8, 12, 10
H_{26}	0, 1, 3, 5, 4, 9, 8, 10, 6, 12, 15, 2, 11, 7, 13, 14
H_{27}	0, 1, 3, 5, 4, 10, 8, 9, 15, 2, 6, 12, 13, 7, 11, 14
H_{28}	0, 1, 3, 5, 4, 10, 13, 12, 7, 8, 6, 14, 9, 11, 2, 15
H_{29}	0, 1, 3, 5, 4, 12, 10, 13, 14, 6, 7, 8, 11, 2, 15, 9
H_{30}	0, 1, 3, 6, 4, 7, 15, 10, 5, 13, 14, 2, 11, 9, 8, 12
H_{31}	0, 1, 3, 6, 4, 11, 8, 13, 10, 7, 15, 5, 9, 2, 12, 14

case is the spectrum S_{12} of Table 2, where the value 1 appears only 16 times in the DDTs of the corresponding functions. The spectrum of these functions seems remarkably close to that observed for APN functions in the field case, while the remaining functions have differential spectra more concentrated at the value 1.

Checking each pair of optimal affine inequivalent representatives, we found that some of the APN permutations sharing differential spectrum fall into the same CCZ class. The CCZ classes have maximum size 2, suggesting that many of these functions are not affine equivalent to their inverse. We also observe that APN permutations with the same differential spectrum do not need to be CCZ-equivalent, as in S_9 where we observe 3 distinct CCZ classes with the same differential spectrum. For a list of the CCZ classes and complete differential spectra, consult Table 2.

The function $H_7 = [0, 1, 2, 5, 4, 6, 3, 14, 7, 8, 12, 15, 9, 11, 10, 13]$ is an example of an APN permutation achieving the *best* differential spectrum found in our search, in the sense that $N_{H_7}(2) = 64$ is the minimum value attained by any permutation. Its DDT is given in Table 3.

Table 2: Differential spectra of affine-inequivalent APN permutations of GR$(4, 2)$. Functions within the same brackets are CCZ-equivalent.

Spectrum ID	**Differential Spectrum**			**CCZ Classes**
	$N(0)$	$N(1)$	$N(2)$	
S_0	79	112	64	$\{H_7, H_{14}\}$
S_1	84	102	69	$\{H_9, H_{21}\}, \{H_{22}\}$
S_2	85	100	70	$\{H_{11}, H_{12}\}$
S_3	86	98	71	$\{H_6, H_{15}\}$
S_4	88	94	73	$\{H_2, H_4\}, \{H_8\}$
S_5	89	92	74	$\{H_{13}, H_{20}\}$
S_6	90	90	75	$\{H_{25}, H_{31}\}$
S_7	91	88	76	$\{H_0, H_3\}$
S_8	94	82	79	$\{H_{10}, H_{16}\}$
S_9	95	80	80	$\{H_1, H_5\}, \{H_{17}, H_{19}\}, \{H_{28}\}$
S_{10}	97	76	82	$\{H_{18}\}$
S_{11}	111	48	96	$\{H_{23}, H_{26}\}, \{H_{24}, H_{29}\}$
S_{12}	127	16	112	$\{H_{27}\}, \{H_{30}\}$

Table 3: The DDT of H_7.

16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	2	2	2	1	2	0	1	1	0	1	0	1	2	0	1
0	1	2	1	1	1	1	1	2	1	0	1	1	1	1	1
0	2	2	2	1	1	0	2	1	0	1	0	1	1	0	2
0	2	1	2	0	0	1	1	2	1	1	1	1	0	2	1
0	1	2	1	2	1	1	0	1	1	1	1	2	1	1	0
0	1	0	1	1	0	2	2	1	0	1	2	2	1	1	1
0	0	1	2	1	2	2	0	0	2	1	2	1	1	0	1
0	1	0	1	0	2	1	1	0	2	2	2	0	1	1	2
0	0	1	0	0	2	2	2	2	1	1	1	2	1	0	1
0	0	0	0	1	1	2	2	0	1	2	1	1	2	2	1
0	0	1	0	2	1	0	1	2	1	1	1	0	2	2	2
0	2	1	2	1	1	2	0	2	1	1	1	0	1	1	0
0	2	1	0	1	1	0	1	0	2	1	2	1	0	2	2
0	1	0	1	2	1	1	1	1	2	1	0	1	2	2	0
0	1	2	1	2	0	1	1	1	1	1	1	2	0	1	1

6 On Using Polynomials vs Lookup Tables (LUTs)

The objective of this paper was to investigate the differential uniformity of polynomials and functions over Galois rings. While our results show that the optimal functions are not among those admitting a polynomial representation, we would like to shed some light on why using polynomials perhaps might have some benefit if our goal is to construct a sort of generic design. Advanced cryptography frequently requires symmetric cryptography over non-standard fields and rings, leading to a range of dedicated designs that rely on different security arguments and whose logical implementations share little in common. This could motivate designs of hash functions and block ciphers whose security arguments can be independent of the specific rings they are defined over, to have one single base design which can be re-used in many different advanced cryptographic schemes only by parameterizing the ring it is defined over. The obvious idea is to pick a ppoly-APN permutation with binary coefficients which remains ppoly-APN over R_{q^m} for a suitable range of parameters $q = p^k$ and m for the S-box layer together with a suitable linear layer. This generic design approach generally excludes picking table-based S-boxes. A possible direction for constructing generic designs is then as follows. A permutation polynomial $f(x) \in \mathbb{F}_p[x]$ is an *exceptional polynomial* if the induced map $f : \mathbb{F}_{p^m} \to \mathbb{F}_{p^m}$ is a permutation for infinitely many integers $m \geq 1$. The notion is naturally generalized to include the Galois ring.

Definition 3. Let $f(x) \in \mathbb{Z}[x]$. We say that f is *ring-exceptional* if the induced map $f\colon R_{q^m} \to R_{q^m}$ is a permutation for infinitely many tuples $q = p^k$ and m.

A block cipher or hash function is ring-exceptional if its components (S-boxes

and linear layers) are ring-exceptional for infinitely many numbers of compatible parameters p, k, m. To be more concrete, we fix $p = 2$. Recall that an $n \times n$ MDS matrix over $\mathrm{GR}(2^k, m)$ is a matrix whose square sub-matrices are all non-singular. Non-singularity is just the same as having determinant equal to a unit in the ring. The existence of MDS matrices in the context of Galois rings is a consequence of the following theorem.

Theorem 7 ([TP17, Theorem 1])**.** *An $n \times n$ matrix $M = (a_{ij})$ over $\mathrm{GR}(2^k, m)$ is MDS if and only if $\overline{M} = (\overline{a}_{ij})$ is an $n \times n$ MDS matrix over $\mathbb{F}_{2^m}$.*

Thus, one may construct a ring-exceptional Substitution Permutation Network (SPN) by picking a ring-exceptional S-box f for the S-box layer and a $n \times n$ MDS matrix for the linear layer over $\mathrm{GR}(2, m)$ and lift it to a suitable $\mathrm{GR}(2^k, m)$. One can deduce e.g. two-round differential probabilities based on the differential uniformity of f and the minimum number of active S-boxes in the usual way. For instance, by fixing m large enough in comparison to n, one can pick a MDS matrix over $\mathrm{GR}(2, m)$ for the linear layer and lift it to a MDS matrix over $\mathrm{GR}(2^k, m)$. For the S-box layer, one can pick e.g. the ppoly-APN Dickson polynomial $f(x) = L(x)x$ where $L(x) = x^4 + x^2 + 1$. A cryptanalyst can analyze a cipher with components defined over $\mathrm{GR}(2^k, m)$ by restricting it to a problem over $\mathrm{GR}(2, m)$, so the security of the design instantiated over the smallest ring $\mathrm{GR}(2, m)$ can give an indication of the security of the entire design.

7 Conclusion

The contents of this paper provide a foundation for further investigation into the differential properties of functions over Galois rings. The results suggest that it can be wise to build block ciphers and hash functions from functions that do not admit a polynomial representation. Even though we have knowledge of a class of optimal ppoly-APN functions, their high differential uniformity is still not advantageous in many applications. We leave many open problems, classifying polynomials with only integer coefficients in terms of differential uniformity, identifying a class of ppoly-APN functions for even m, improving criteria for determining that a function is ppoly-APN, and identifying a non-table-based representation of the APN permutations over R_{4^2}. Other obvious problems are for what Galois rings there exist APN functions, APN permutations and even PN functions.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback, as well as the organizers of the BFA 2025 workshop.

References

[BGC91] Priscilla S. Bremser and Javier Gomez-Calderon. Value sets of dickson polynomials over galois rings. *Journal of Number Theory*, 38(2):240–250, 1991. URL: https://www.sciencedirect.com/science/article/pii/0022314X9190087R, doi:10.1016/0022-314X(91)90087-R.

[BGV11] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. Fully homomorphic encryption without bootstrapping. Cryptology ePrint Archive, Paper 2011/277, 2011. URL: https://eprint.iacr.org/2011/277.

[BM92] Joel V. Brawley and Gary L. Mullen. Functions and polynomials over Galois rings. *Journal of Number Theory*, 41(2):156–166, 1992. URL: https://www.sciencedirect.com/science/article/pii/0022314X92901167, doi:10.1016/0022-314X(92)90116-7.

[BS91] Eli Biham and Adi Shamir. Differential Cryptanalysis of DES-like Cryptosystems. In Alfred J. Menezes and Scott A. Vanstone, editors, *Advances in Cryptology-CRYPTO' 90*, pages 2–21, Berlin, Heidelberg, 1991. Springer Berlin Heidelberg.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 505–524, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[CHMS22] Orel Cosseron, Clément Hoffmann, Pierrick Méaux, and François-Xavier Standaert. Towards globally optimized hybrid homomorphic encryption - featuring the elisabeth stream cipher. Cryptology ePrint Archive, Paper 2022/180, 2022. URL: https://eprint.iacr.org/2022/180.

[DGM09] Konstantinos Drakakis, Rod Gow, and Gary McGuire. APN permutations on Zn and Costas arrays. *Discrete Applied Mathematics*, 157(15):3320–3326, 2009. URL: https://www.sciencedirect.com/science/article/pii/S0166218X09002789, doi:10.1016/j.dam.2009.06.029.

[Hel96] Helleseth, Tor and Johansson, Thomas. Universal Hash Functions from Exponential Sums over Finite Fields and Galois Rings. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 31–44, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge, 2 edition, 1996.

[LP07] G. Leander and A. Poschmann. On the Classification of 4 Bit S-Boxes. In Claude Carlet and Berk Sunar, editors, *Arithmetic of Finite Fields*, pages 159–176, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[LXY23] Fuchun Lin, Chaoping Xing, and Yizhou Yao. More efficient zero-knowledge protocols over $\mathbb{Z}_{2^k}$ via galois rings. Cryptology ePrint Archive, Paper 2023/150, 2023. URL: https://eprint.iacr.org/2023/150.

[Mas94] James L. Massey. SAFER K-64: A byte-oriented block-ciphering algorithm. In Ross Anderson, editor, *Fast Software Encryption*, pages 1–17, Berlin, Heidelberg, 1994. Springer Berlin Heidelberg.

[McD74] B.R. McDonald. *Finite Rings with Identity*. Lecture notes in pure and applied mathematics. M. Dekker, New York, 1974.

[Riv01] Ronald L. Rivest. Permutation polynomials modulo 2w. *Finite Fields and Their Applications*, 7(2):287–292, 2001. URL: https://www.sciencedirect.com/science/article/pii/S107157970090282X, doi:10.1006/ffta.2000.0282.

[RRSY] Ronald L. Rivest, M. J. B. Robshaw, R. Sidney, and Y. L. Yin. The RC6 block cipher. In *First Advanced Encryption Standard (AES) Conference*. Slides from NIST AES1 (1998-08-21) and AES3 (2000-04-14) conferences. URL: https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.140.6264&rank=3.

[TP17] Chik How Tan and Theo Fanuela Prabowo. Orthogonal MDS Diffusion Matrices over Galois Rings. In Máire O'Neill, editor, *Cryptography and Coding*, pages 307–330, Cham, 2017. Springer International Publishing.

[Wan03] Z. Wan. *Lectures On Finite Fields And Galois Rings*. World Scientific Publishing Company, Singapore, 2003.

[WZD25a] Yuanju Wei, Xinxuan Zhang, and Yi Deng. Transparent SNARKs over galois rings. Cryptology ePrint Archive, Paper 2025/263, 2025. URL: https://eprint.iacr.org/2025/263.

[WZD+25b] Zhuo Wu, Xinxuan Zhang, Yi Deng, Yuanju Wei, Zhongliang Zhang, and Liuyu Yang. Polylogarithmic polynomial commitment scheme over galois rings. Cryptology ePrint Archive, Paper 2025/1767, 2025. URL: https://eprint.iacr.org/2025/1767.

[YW13] Yuyin Yu and Mingsheng Wang. Permutation polynomials and their differential properties over residue class rings. *Discrete Applied Mathematics*, 161(18):3104–3108, 2013. URL: https://www.sciencedirect.com/science/article/pii/S0166218X13002989, doi:10.1016/j.dam.2013.06.020.