

Constructing Complete Permutations via the D-Class of Locally Crooked Permutations

Li Shuai

lis198707@gmail.com

Ningxia University

Research Article

Keywords: complete permutation, locally crooked permutation, CCZ equivalence, differential uniformity, nonlinearity, algebraic degree

Posted Date: October 16th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-11369322/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Constructing Complete Permutations via the $\mathcal{D}$ -Class of Locally Crooked Permutations

Li Shuai^{1*}

¹School of Information Engineering, Ningxia University, Yinchuan, 750021, Ningxia, People's Republic of China.

Corresponding author(s). E-mail(s): lis198707@gmail.com;

Abstract

A permutation f over $\mathbb{F}_{2^n}$ is *complete* (CP) if both f and $x \mapsto f(x) + x$ are permutations. CPs are central to the Lai–Massey framework and to nonlinear S-boxes. Building on the LCP–CP correspondence of Shuai and Li (where LCP stands for locally crooked permutation), we introduce the $\mathcal{D}$ -class: permutations of $\mathbb{F}_{2^{n+1}}$ whose derivative in a fixed direction has as image the complement of a fixed hyperplane H . We prove that $\mathcal{D}$ is closed under translation, under left multiplication by the linear group preserving H , and under right multiplication by the centralizer of the involution swapping H and its complement, and we characterize the local translations preserving it. The lifted CP subclass $\mathcal{D}^\uparrow$ is rigid under each individual operation; certain products of two operations escape rigidity. Using a piecewise-bijection criterion, we obtain necessary and sufficient conditions for two local conjugations to be CPs. Localized centralizer elements link the $\mathcal{D}$ -closure to these conjugations. They produce composites in the lifted subclass that restrict to these conjugations. We derive bounds on differential uniformity, nonlinearity, and algebraic degree under local modifications, and prove CCZ-inequivalence criteria. Two algorithms are presented: a backtracking search enumerating CPs and a greedy local search that accepts only improving local conjugations based on the full differential and Walsh spectra. Experiments on $H \cong \mathbb{F}_{32}$ illustrate their behavior, yield several $\delta = 4$ complete permutations with distinct differential spectra, and provide preliminary evidence for the conjectured connectivity of $\mathcal{D}^\uparrow$ under local-conjugation moves.

Keywords: complete permutation; locally crooked permutation; CCZ equivalence; differential uniformity; nonlinearity; algebraic degree

1 Introduction

1.1 From Latin Squares to S-boxes: The Role of CPs

A permutation f over a finite field is called *complete* if both f and the map $x \mapsto f(x) + x$ are permutations. The notion first appeared in Mann’s construction of orthogonal Latin squares [1]; complete mappings of finite groups were studied by Hall and Paige [2], and the finite-field case was developed by Niederreiter and Robinson [3]. In combinatorial design theory, complete mappings are precisely those permutations whose associated Latin square admits a transversal; in coding theory, they appear in the construction of perfect difference sets; and in sequence design, they are connected to low-correlation families. Recent constructions of complete permutations can be found in [4, 5].

The cryptographic significance of complete permutations (CPs) manifests itself at two distinct levels. At the *structural level*, a standard construction in the Lai–Massey framework [6] uses a round function built from a permutation σ ; Vaudenay’s analysis [7] showed that, under the usual hypotheses, to avoid a differential or linear distinguisher of probability 1, the map σ must be an orthomorphism, i.e., a complete permutation over the underlying additive group. This turns the existence of CPs with good differential and linear behavior into a design requirement rather than a curiosity.

At the *component level*, an early use of complete permutation polynomials with good nonlinearity in a nonlinear dynamic substitution device is due to Mitten-thal [8], thereby anticipating the modern use of CPs as building blocks for S-boxes with strong diffusion and confusion. The cryptographic indicators relevant to this paper—differential uniformity and nonlinearity—have their roots in the differential cryptanalysis of Biham and Shamir [9] and the introduction of the APN property by Nyberg [10].

1.2 Locally Crooked Permutations and the Shuai–Li Correspondence

A related class, which becomes wider after lifting, is that of *locally crooked permutations* (LCPs). A permutation f of $\mathbb{F}_{2^{n+1}}$ is an LCP if there exists $a \neq 0$ and a hyperplane H' such that the derivative $\Delta_a f$ has image exactly $\mathbb{F}_{2^{n+1}} \setminus H'$. Crooked functions were introduced in [11]; see also [12]. Every crooked function is an LCP, but the converse fails: a nonempty and, in small dimensions, large proportion of the LCP class consists of permutations that are not crooked in any direction.

This gap was exploited by Shuai and Li [13], who established a correspondence between normalized LCPs over $\mathbb{F}_{2^{n+1}}$ and CPs over $\mathbb{F}_{2^n}$. Their construction takes a known crooked function, applies an affine normalization (a linear change of coordinates mapping the distinguished hyperplane to a standard form, combined with a translation of the output), and lifts the resulting permutation to an LCP by defining it as the identity on the complement of the hyperplane; restricting back to the hyperplane $\mathbb{F}_{2^n}$ yields a CP. Because the starting point is a crooked function, their method is intrinsically a “crooked function $\rightarrow$ LCP $\rightarrow$ CP” path and, as stated, does not directly permit free movement within the LCP class itself.

We take a complementary direction: we work *inside* the LCP class and use its internal group actions to generate new LCPs, which we then project back to H to obtain CPs. The key observation is that the LCPs whose derivative in a fixed direction has as image a specific hyperplane complement—the $\mathcal{D}$ -class introduced below—form a set closed under three natural group actions. Composing these actions produces a construction chain

$$\text{CP} \xrightarrow{\uparrow} \text{LCP} \xrightarrow{\text{group action}} \text{new LCP} \xrightarrow{\downarrow} \text{new CP},$$

in which each arrow is an explicit algebraic operation. We sharpen this picture in two ways. First, we prove that the lifted CP subclass $\mathcal{D}^\uparrow \subseteq \mathcal{D}$ is rigid under each individual closure operation; hence, within this construction chain, new lifted CPs require products of operations. Second, we identify localized centralizer elements that turn these products into elements of $\mathcal{D}^\uparrow$, whose restrictions to H are exactly the two local conjugations f_1 and f_2 , respectively.

1.3 Contributions and Organization

Our contributions are the following.

- (1) **The $\mathcal{D}$ -class and its invariance.** We introduce the $\mathcal{D}$ -class, the set of permutations f of $\mathbb{F}_{2^{n+1}}$ whose derivative in the direction $q_1 = 2^n$ has image the complement of $H = \{x : x_n = 0\}$. We prove that $\mathcal{D}$ is closed under left translation, under left multiplication by GL_H , and under right multiplication by the centralizer $\mathcal{C}(t_{q_1})$ (Proposition 7), and we characterize the local translations that preserve $\mathcal{D}$ (Proposition 9).
- (2) **Rigidity and the construction chain.** We define the lifted subclass $\mathcal{D}^\uparrow$ and prove that it is rigid under each single operation; certain products of two operations escape rigidity. Localized centralizer elements link the $\mathcal{D}$ -closure to the two local conjugations f_1 and f_2 , producing composites in $\mathcal{D}^\uparrow$ that restrict to them (Theorem 22, Proposition 21).
- (3) **Exact CP criteria for f_1 and f_2 .** Using a piecewise-bijection criterion (Lemma 24), we prove that f_1 is a CP iff $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$, and that, for $a \in K$, f_2 is a well-defined CP iff $X_2 + a = f(X_2)$ (Propositions 25, 26).
- (4) **CCZ-inequivalence criteria.** We prove CCZ-inequivalence criteria via DDT and Walsh spectra, using the fact that CCZ equivalence preserves the DDT up to row and column permutations and preserves the multiset of absolute Walsh coefficients [14, 15], and we discuss the structural limitations of the construction chain.

The remainder of the paper is organized as follows: Section 2 fixes notation and states the basic definitions; Section 3 develops the $\mathcal{D}$ -class, its normalization, and its closure properties; Section 4 proves the CP– $\mathcal{D}$ equivalence, establishes rigidity, constructs the correcting maps g_{a,X_1}, g_{a,X_2} , and identifies the two local conjugations f_1 and f_2 ; Section 5 derives the cryptographic indicator bounds; Section 6 proves CCZ-inequivalence criteria and discusses structural limitations; Section 7 presents the

two algorithms; Section 8 reports the experiments; and Section 9 concludes and lists open problems.

2 Preliminaries

We collect here the notation, the finite-field conventions, the group-theoretic objects, and the cryptographic notions used throughout the paper [16]. Table 1 summarizes the main symbols.

Table 1 Summary of notation.

Symbol	Meaning
$\mathbb{F}_q$	finite field of order $q = 2^{n+1}$, identified with the vector space $\mathbb{F}_2^{n+1}$
q_1	$q_1 = 2^n$; also viewed as the corresponding element of $\mathbb{F}_q$
H	hyperplane $\{x \in \mathbb{F}_q : x_n = 0\} \cong \mathbb{F}_2^n$
K	complement $\mathbb{F}_q \setminus H = H + q_1$
$\mathcal{S}_q$	symmetric group on $\mathbb{F}_q$
$\mathcal{S}_{q_1}$	symmetric group on $H \cong \mathbb{F}_2^n$
s_a	multiplication by $a \in \mathbb{F}_q^*$ in $\mathbb{F}_q$, $x \mapsto ax$
t_a	translation in $\mathbb{F}_q$, $x \mapsto x + a$
$t_{a,X}$	local translation: $x \mapsto x + a$ for $x \in X$, and $x \mapsto x$ otherwise
GL	general linear group over $\mathbb{F}_q$
GL_H	general linear group preserving H
$\mathcal{C}$	centralizer of t_{q_1} in $\mathcal{S}_q$
$\mathcal{D}$	$\{f \in \mathcal{S}_q : \text{Im } \Delta_{q_1} f = K\}$
$f^\uparrow$	lift of $f \in \mathcal{S}_{q_1}$ to $\mathcal{S}_q$, identity on K
$\mathcal{D}^\uparrow$	lifted CP subclass $\{f^\uparrow : f \in \mathcal{S}_{q_1}, f \text{ is a CP}\}$
$\Delta_a f$	derivative $x \mapsto f(x) + f(x + a)$
$\delta(h)$	differential uniformity of h
$\text{nl}(h)$	nonlinearity of h
$\text{deg}(h)$	algebraic degree of h

2.1 Finite Field and Hyperplane Decomposition

Let $n \geq 1$ be an integer and set $q = 2^{n+1}$. We identify $\mathbb{F}_q$ with $\mathbb{F}_2^{n+1}$ using the standard binary encoding $\iota : \{0, 1\}^{n+1} \rightarrow \mathbb{F}_q$, so that an element $x \in \mathbb{F}_q$ corresponds to the binary vector $(x_n, x_{n-1}, \dots, x_0)$ with integer value

$$x = \sum_{i=0}^n x_i 2^i.$$

In this encoding, we do not distinguish between the integer 2^n and its corresponding element in $\mathbb{F}_q$; both are denoted by q_1 . Thus $q_1 \in \mathbb{F}_q$ and $|H| = |K| = q_1$. Field

addition is bitwise XOR. We fix the distinguished element $q_1 = 2^n$ and two subsets:

$$H = \{x \in \mathbb{F}_q : x_n = 0\}, \quad K = \mathbb{F}_q \setminus H = H + q_1.$$

Thus H is a hyperplane of $\mathbb{F}_q$, identified with $\mathbb{F}_2^n$ as an $\mathbb{F}_2$ -vector space, and K is its complement.

We denote by $\mathcal{S}_q$ the symmetric group on $\mathbb{F}_q$, i.e. the set of all permutations of $\mathbb{F}_q$, and by $\mathcal{S}_{q_1}$ the symmetric group on $H \cong \mathbb{F}_2^n$. Thus $f \in \mathcal{S}_q$ means that f is a permutation of $\mathbb{F}_q$, while $f \in \mathcal{S}_{q_1}$ means that f is a permutation of H . An element of $\mathcal{S}_{q_1}$ is extended to $\mathcal{S}_q$ by fixing every element of K ; in this way $\mathcal{S}_{q_1}$ is regarded as a subgroup of $\mathcal{S}_q$.

For a subset $X \subseteq \mathbb{F}_q$ and a map $\phi : \mathbb{F}_q \rightarrow \mathbb{F}_q$, we write $X^\phi = \{\phi(x) : x \in X\}$.

We denote by s_a the multiplication-by- a map, $s_a(x) = a \cdot x$, which is a linear permutation whenever $a \neq 0$.

We denote by t_a the translation map, $t_a(x) = x + a$, which is an affine permutation.

The derivative of f in direction $a \in \mathbb{F}_q$ is

$$\Delta_a f(x) = f(x) + f(x + a), \quad x \in \mathbb{F}_q.$$

2.2 Cryptographic Functions: APN, LAP, LCP, Crooked, and CP

The notion of almost perfect nonlinearity was introduced by Nyberg [10] in the study of S-boxes resisting differential cryptanalysis [9]. Crooked functions, introduced in [11], form a distinguished subclass of APN functions that are simultaneously locally crooked; see [12] for a survey. The following definition collects the APN, locally APN (LAP), and locally crooked permutation (LCP) notions, which differ in the strength of the condition imposed on the derivative images.

Definition 1 (APN, LAP, LCP). Let $f \in \mathcal{S}_q$.

- (i) f is *APN* if $|\text{Im } \Delta_a f| = q_1$ for every $a \neq 0$.
- (ii) f is *LAP* (locally APN) if $|\text{Im } \Delta_a f| = q_1$ for at least one $a \neq 0$.
- (iii) f is *LCP* (locally crooked permutation) if there exist $a \neq 0$ and a hyperplane $H' \subseteq \mathbb{F}_q$ such that $\text{Im } \Delta_a f = \mathbb{F}_q \setminus H'$.

The relations among these classes are as follows. Every APN function is LAP, and every LCP is LAP, because a hyperplane complement in $\mathbb{F}_q$ has exactly q_1 elements. The converses fail: an LAP function need not have the maximal image size in every direction, and an LAP function whose derivative image has size q_1 need not have that image equal to the complement of a hyperplane. Every crooked function is an LCP, but the converse fails: a nonempty and, in small dimensions, large proportion of the LCP class consists of permutations that are not crooked in any direction. Complete permutations, defined below, are not a subclass of $\mathcal{S}_q$ but rather of $\mathcal{S}_{q_1}$; they are linked to LCPs over $\mathbb{F}_{2^{n+1}}$ by the Shuai–Li correspondence [13].

Definition 2 (Complete permutation). Let $f \in \mathcal{S}_{q_1}$, viewed as a permutation of $H \cong \mathbb{F}_2^n$. We say f is a *complete permutation* (CP) if both f and $x \mapsto f(x) + x$ are permutations of H .

Complete permutations are also called complete mappings or orthomorphisms; see [2–5]. The CP condition does not depend on a field structure on H : it only uses the additive group of H . This matches the standard usage in the Lai–Massey literature, where a complete permutation is an orthomorphism of the underlying additive group.

2.3 The $\mathcal{D}$ -class and the Groups Acting on It

Definition 3 ($\mathcal{D}$ -class). Define

$$\mathcal{D} = \{f \in \mathcal{S}_q : \text{Im } \Delta_{q_1} f = K\}.$$

The class $\mathcal{D}$ is the object whose invariance we exploit; its elements are precisely the LCPs with respect to the fixed direction q_1 and the fixed hyperplane H . Proposition 6 shows that every LCP can be brought into $\mathcal{D}$ by applying a linear map $L \in \text{GL}$ with $L(a) = q_1$ and $L(H') = H$ (where H' is a distinguished hyperplane of the LCP and a a distinguished direction) and a translation of the output, i.e., by an affine normalization.

Definition 4 (Related groups). We denote by

$$\mathcal{T} = \{t_a : t_a(x) = x + a, x \in \mathbb{F}_q\}$$

the translation group of $\mathbb{F}_q$,

$$\text{GL} = \{g \in \mathcal{S}_q : g(x + y) = g(x) + g(y) \ \forall x, y \in \mathbb{F}_q\}$$

the general linear group,

$$\text{GL}_H = \{g \in \text{GL} : g(H) = H\}$$

the subgroup of GL preserving the hyperplane H , and

$$\mathcal{C} = \mathcal{C}(t_{q_1}) = \{g \in \mathcal{S}_q : gt_{q_1}g^{-1} = t_{q_1}\}$$

the centralizer of the involution t_{q_1} in the symmetric group.

Equivalently, $g \in \mathcal{C}$ if and only if $g(x + q_1) = g(x) + q_1$ for all $x \in \mathbb{F}_q$; this follows by evaluating $gt_{q_1}g^{-1} = t_{q_1}$ at $g(x)$. That is, g commutes with the involution that swaps H and K .

Definition 5 (Local translation). For $a \in \mathbb{F}_q$ and $X \subseteq \mathbb{F}_q$,

$$t_{a,X}(x) = \begin{cases} x + a, & x \in X, \\ x, & x \notin X. \end{cases}$$

The map $t_{a,X}$ is a permutation of $\mathbb{F}_q$ if and only if $X + a = X$ (which includes the case $a = 0$); in general, $t_{a,X}$ is not a permutation. This fact is essential for the analysis of the local translations that preserve $\mathcal{D}$ (Proposition 9).

For $f \in \mathcal{S}_{q_1}$, define its lift $f^\uparrow \in \mathcal{S}_q$ by

$$f^\uparrow(x) = \begin{cases} f(x), & x \in H, \\ x, & x \in K. \end{cases}$$

Then the lifted CP subclass is

$$\mathcal{D}^\uparrow = \{f^\uparrow : f \in \mathcal{S}_{q_1}, f \text{ is a CP}\}.$$

2.4 Cryptographic Indicators

For a function $f : \mathbb{F}_q \rightarrow \mathbb{F}_q$, its differential distribution table (DDT) is the $q \times q$ matrix

$$D_f = (\nu_f(a, b))_{a, b \in \mathbb{F}_q}, \quad \nu_f(a, b) = \#\{x \in \mathbb{F}_q : f(x + a) + f(x) = b\}.$$

If row maxima of the DDT are needed, we write

$$\delta_f(a) = \max_{b \in \mathbb{F}_q} \nu_f(a, b), \quad \delta(f) = \max_{a \in \mathbb{F}_q \setminus \{0\}} \delta_f(a).$$

We denote by $\text{nl}(f)$ the nonlinearity of f , and by $\deg(f)$ its algebraic degree.

Two permutations $f, g \in \mathcal{S}_q$ are *extended-affine (EA) equivalent* if there exist affine permutations A, B of $\mathbb{F}_q$ and an affine map C of $\mathbb{F}_q$ such that

$$g = A \circ f \circ B + C.$$

They are *CCZ-equivalent* if their graphs

$$\Gamma_f = \{(x, f(x)) : x \in \mathbb{F}_q\}, \quad \Gamma_g = \{(x, g(x)) : x \in \mathbb{F}_q\}$$

are related by an affine transformation of $\mathbb{F}_q^2$. CCZ equivalence was introduced in [14]. The two notions are related by the implication

$$\text{EA-equivalent} \implies \text{CCZ-equivalent},$$

but the converse does not hold in general. For permutations, CCZ equivalence preserves the differential distribution table up to row and column permutations, and preserves the multiset of absolute Walsh coefficients; see [14, 15]. In particular, differential uniformity and nonlinearity are preserved under CCZ equivalence.

3 Normalization of LCPs and Invariance of $\mathcal{D}$

This section develops the two structural facts on which the construction chain rests. First, every LCP can be normalized into $\mathcal{D}$ by a linear change of coordinates (Proposition 6). Second, $\mathcal{D}$ is stable under the three group actions that we will use as elementary building blocks of our constructions (Proposition 7), together with a family of local translations (Proposition 9). The local translations play a distinguished role: they are the mechanism by which the two local conjugations f_1 and f_2 of Section 4 enter the picture.

Proposition 6 (Normalization of LCPs). *Let $f \in \mathcal{S}_q$ be an LCP. Then there exist $a \in \mathbb{F}_q^*$ and $g \in \text{GL}$ such that*

$$g \circ f \circ s_{a/q_1} \in \mathcal{D}.$$

Proof Since f is an LCP, there exist $a \in \mathbb{F}_q^*$ and a hyperplane H' such that $\text{Im } \Delta_a f = \mathbb{F}_q \setminus H'$. Set $K' = \mathbb{F}_q \setminus H'$. The general linear group GL acts transitively on hyperplanes of $\mathbb{F}_q$, so we may choose $g \in \text{GL}$ with $g(H') = H$, hence $g(K') = K$. Put $h = g \circ f \circ s_{a/q_1}$. For every $x \in \mathbb{F}_q$,

$$\Delta_{q_1} h(x) = g\left(f(s_{a/q_1}(x)) + f(s_{a/q_1}(x) + a)\right) = g(\Delta_a f(s_{a/q_1}(x))),$$

where we used $s_{a/q_1}(x + q_1) = s_{a/q_1}(x) + a$ and the additivity of g . Passing to images,

$$\text{Im } \Delta_{q_1} h = g(\text{Im } \Delta_a f) = g(K') = K.$$

Hence $h \in \mathcal{D}$. □

Both $g \in \text{GL}$ and s_{a/q_1} are affine, so normalization preserves the EA-class and hence the CCZ-class.

Proposition 7 (Invariance of $\mathcal{D}$). *Let $f \in \mathcal{D}$. Then*

- (i) $t_a \circ f \in \mathcal{D}$ for every $a \in \mathbb{F}_q$;
- (ii) $g \circ f \in \mathcal{D}$ for every $g \in \text{GL}_H$;
- (iii) $f \circ h \in \mathcal{D}$ for every $h \in \mathcal{C}$.

Proof (i) Translations cancel in differences:

$$\Delta_{q_1}(t_a \circ f)(x) = f(x) + a + f(x + q_1) + a = f(x) + f(x + q_1) = \Delta_{q_1} f(x),$$

so $\text{Im } \Delta_{q_1}(t_a \circ f) = \text{Im } \Delta_{q_1} f = K$.

(ii) Since $g \in \text{GL}_H$, we have $g(H) = H$, hence $g(K) = K$. By additivity,

$$\Delta_{q_1}(g \circ f)(x) = g(\Delta_{q_1} f(x)),$$

so $\text{Im } \Delta_{q_1}(g \circ f) = g(K) = K$.

(iii) Let $h \in \mathcal{C}$, i.e., $h(x + q_1) = h(x) + q_1$ for all x . Then

$$\Delta_{q_1}(f \circ h)(x) = f(h(x)) + f(h(x) + q_1) = \Delta_{q_1} f(h(x)).$$

Since h is a permutation of $\mathbb{F}_q$, the image of this map is $\text{Im } \Delta_{q_1} f = K$. □

Remark 8. Left multiplication $g \circ f$ with $g \in \text{GL}_H$ is EA-equivalent to f ; translation $t_a \circ f$ is also EA-equivalent to f . Right multiplication $f \circ h$ is EA-equivalent to f when h is affine; for non-affine $h \in \mathcal{C}$, it need not be EA-equivalent to f . The centralizer $\mathcal{C}$ contains many non-affine elements, e.g. local translations $t_{a,X}$ with $X + q_1 = X$ and $X + a = X$, and the localized maps g_{a,X_1}, g_{a,X_2} introduced in Section 4.

Proposition 9 (Local translations preserving $\mathcal{D}$). *Let $f \in \mathcal{D}$, $a \in \mathbb{F}_q$, and $X \subseteq \mathbb{F}_q$. Assume that X is a union of orbits of the dihedral group*

$$\mathcal{G} = \langle t_a, f t_{q_1} f^{-1} \rangle.$$

Equivalently,

$$X^{t_a} = X, \quad X^{f t_{q_1} f^{-1}} = X.$$

Then $t_{a,X} \circ f \in \mathcal{D}$.

Proof The condition $X^{t_a} = X$ means $X + a = X$, so $t_{a,X}$ is an involutive permutation. Let $p = f \circ t_{q_1} \circ f^{-1}$. For any $x \in \mathbb{F}_q$, putting $y = f(x)$ gives

$$f(x + q_1) = f(f^{-1}(y) + q_1) = p(y),$$

hence $\Delta_{q_1} f(x) = y + p(y)$. The condition $X^p = X$ says $y \in X \Leftrightarrow p(y) \in X$, so $t_{a,X}$ either adds a to both y and $p(y)$ or to neither, and in either case

$$t_{a,X}(y) + t_{a,X}(p(y)) = y + p(y).$$

Consequently

$$\Delta_{q_1}(t_{a,X} \circ f)(x) = \Delta_{q_1} f(x)$$

for every x , and passing to images gives $\text{Im } \Delta_{q_1}(t_{a,X} \circ f) = K$. $\square$

Remark 10. The condition $X^{f t_{q_1} f^{-1}} = X$ is equivalent to $f^{-1}(X) + q_1 = f^{-1}(X)$, i.e., $f^{-1}(X)$ is a union of $\langle q_1 \rangle$ -cosets. Together with $X^{t_a} = X$, this means X is a union of orbits of the dihedral group $\mathcal{G}$.

4 From CP to LCP and Back: Rigidity and the Construction Chain

We now assemble the pieces of Section 3 into the three-step chain

$$f \text{ CP} \implies f^\uparrow \text{ LCP} \implies t_{a,X}(f^\uparrow) \text{ LCP} \implies t_{a,X}(f^\uparrow) g_{a,X_i}|_H \text{ CP},$$

where $i = 1$ if $a \in H$ and $i = 2$ if $a \in K$. Subsection 4.1 establishes the first arrow via the embedding $\uparrow$ and proves rigidity. Subsection 4.2 introduces the correcting maps $g_{a,X_1}, g_{a,X_2} \in \mathcal{C}$, whose role is to bring $t_{a,X}(f^\uparrow)$ back to a permutation that fixes K pointwise. Subsection 4.3 identifies the two branches of the chain with the local conjugations f_1 and f_2 , and gives proofs of their CP property via a general lemma on piecewise permutations.

4.1 Embedding CPs into $\mathcal{D}$ via the Lift $\uparrow$

Definition 11 (Standard lift). Let $f \in \mathcal{S}_{q_1}$. The *standard lift* of f is the permutation $f^\uparrow \in \mathcal{S}_q$ defined by

$$f^\uparrow(x) = \begin{cases} f(x), & x \in H, \\ x, & x \in K. \end{cases}$$

Conversely, if $u \in \mathcal{S}_q$ satisfies $u|_K = \text{id}_K$, we write $u^\downarrow \in \mathcal{S}_{q_1}$ for its restriction to H ; this restriction is a permutation of H . We define the lifted CP subclass

$$\mathcal{D}^\uparrow = \{f^\uparrow : f \in \mathcal{S}_{q_1}, f \text{ is a CP}\} = \{u \in \mathcal{D} : u|_K = \text{id}_K\}.$$

Proposition 12 (CP- $\mathcal{D}$ equivalence). *Let $f \in \mathcal{S}_{q_1}$. Then f is a CP if and only if $f^\uparrow \in \mathcal{D}$.*

Proof We compute $\Delta_{q_1} f^\uparrow$ on the two cosets of H . If $x \in H$, then $x + q_1 \in K$, so

$$\Delta_{q_1} f^\uparrow(x) = f(x) + (x + q_1) = (f(x) + x) + q_1.$$

If $y \in K$, write $y = x + q_1$ with $x \in H$; the same computation gives $\Delta_{q_1} f^\uparrow(y) = (f(x) + x) + q_1$. Hence

$$\text{Im } \Delta_{q_1} f^\uparrow = \{f(x) + x : x \in H\} + q_1.$$

This image equals $K = H + q_1$ if and only if $\{f(x) + x : x \in H\} = H$, i.e., if and only if $x \mapsto f(x) + x$ is a permutation of H . Since f is itself a permutation of H , this is exactly the CP condition. $\square$

Lemma 13 (Descent). *Let $u \in \mathcal{D}$. Then $u \in \mathcal{D}^\uparrow$ if and only if $u|_K = \text{id}_K$. In that case $u = (u|_H)^\uparrow$.*

Proof If $u \in \mathcal{D}^\uparrow$, then $u = f^\uparrow$ for some CP f , and hence $u|_K = \text{id}_K$. Conversely, if $u \in \mathcal{D}$ and $u|_K = \text{id}_K$, then $u = (u|_H)^\uparrow$, and Proposition 12 above shows that $u|_H$ is a CP. Thus $u \in \mathcal{D}^\uparrow$. $\square$

Remark 14. Not every element of $\mathcal{D}$ arises as $f^\uparrow$ for some CP f . Indeed, the lift $f^\uparrow$ fixes K pointwise by construction, whereas a general element of $\mathcal{D}$ may move K . To recover a CP from a general $u \in \mathcal{D}$ we must apply a suitable correction on K , which is the role played by the maps g_{a,X_1} and g_{a,X_2} introduced below.

Theorem 15 (Rigidity of $\mathcal{D}^\uparrow$). *Let $f \in \mathcal{S}_{q_1}$ be a CP and let $u = f^\uparrow \in \mathcal{D}^\uparrow$. Then:*

- (i) $t_a \circ u \in \mathcal{D}^\uparrow$ implies $a = 0$;
- (ii) $g \circ u \in \mathcal{D}^\uparrow$ with $g \in \text{GL}_H$ implies $g = \text{id}$;
- (iii) $u \circ h \in \mathcal{D}^\uparrow$ with $h \in \mathcal{C}$ implies $h = \text{id}$;
- (iv) if $a \neq 0$ and $t_{a,X} \circ u \in \mathcal{D}^\uparrow$ under the hypotheses of Proposition 9, then $X = \emptyset$.

Proof By Lemma 13, $u \in \mathcal{D}^\dagger$ iff $u|_K = \text{id}_K$, and $u|_K = \text{id}_K$.

- (i) For $x \in K$, $(t_a \circ u)(x) = x + a$, so $x + a = x$ for all $x \in K$; hence $a = 0$.
- (ii) For $x \in K$, $(g \circ u)(x) = g(x)$. Thus $g|_K = \text{id}_K$. Since g is linear and K spans $\mathbb{F}_q$, $g = \text{id}$.
- (iii) For $x \in K$, $u(h(x)) = x$. If $h(x) \in K$, then $h(x) = x$. If $h(x) \in H$, then $u(h(x)) \in f(H) = H$, contradicting $x \in K$. Hence $h|_K = \text{id}_K$. Using $h(x + q_1) = h(x) + q_1$, we get $h = \text{id}$.
- (iv) Let $p = ut_{q_1}u^{-1}$. Then p swaps H and K . If $t_{a,X} \circ u \in \mathcal{D}^\dagger$, then for $x \in K$,

$$t_{a,X}(u(x)) = t_{a,X}(x) = x.$$

Since $a \neq 0$, this forces $x \notin X$. Hence $X \cap K = \emptyset$. Now $X^p = X$ and $p(X \cap H) \subseteq X \cap K = \emptyset$, so $X \cap H = \emptyset$. Therefore $X = \emptyset$. $\square$

Remark 16. Rigidity constrains each single operation. The construction chain below shows that a product of two operations escapes rigidity.

4.2 The Correcting Maps $g_{a,X_1}, g_{a,X_2} \in \mathcal{C}$

Throughout this subsection, fix a CP $f \in \mathcal{S}_{q_1}$ and its lift $f^\dagger \in \mathcal{D}$. We distinguish two cases.

Case $a \in H$. Let $X_1 \subseteq H$ be a union of orbits of the dihedral group

$$\mathcal{G}_1 = \langle t_a, f^{-1}t_a f \rangle,$$

so that

$$X_1 + a = X_1, \quad f(X_1) + a = f(X_1).$$

Set $X^{(1)} = f(X_1) \cup (X_1 + q_1) \subseteq \mathbb{F}_q$.

Case $a \in K$. Write $a = a_H + q_1$ with $a_H \in H$. Let $X_2 \subseteq H$ be a union of orbits of the cyclic group

$$\mathcal{G}_2 = \langle t_{a_H} f \rangle,$$

so that

$$X_2 + a_H = f(X_2).$$

Set $X^{(2)} = f(X_2) \cup (X_2 + q_1) \subseteq \mathbb{F}_q$.

In both cases, $X^{(i)}$ satisfies the hypotheses of Proposition 9:

$$(X^{(i)})^{t_a} = X^{(i)}, \quad (X^{(i)})^{f^\dagger t_{q_1} (f^\dagger)^{-1}} = X^{(i)}.$$

Define the *shadow* of $X^{(i)}$ on H by

$$(X^{(i)})' = (X^{(i)} \cap K) + q_1.$$

In the case $a \in H$, we have $(X^{(1)})' = X_1$. In the case $a \in K$, we have $(X^{(2)})' = X_2$.

Definition 17 (The correcting maps g_{a,X_1} and g_{a,X_2}). Define $g_{a,X_1} \in \mathcal{S}_q$ (for $a \in H$) and $g_{a,X_2} \in \mathcal{S}_q$ (for $a \in K$) by their values on the two cosets of H as follows.

Case $a \in H$: definition of g_{a,X_1} .

$$g_{a,X_1}(y) = \begin{cases} y + a, & y \in X_1, \\ y, & y \in H \setminus X_1, \\ y + a, & y \in X_1 + q_1, \\ y, & y \in (H \setminus X_1) + q_1. \end{cases}$$

Equivalently, g_{a,X_1} acts on $X_1 \cup (X_1 + q_1)$ by translation $y \mapsto y + a$, and on its complement by the identity. In particular, g_{a,X_1} preserves both H and K setwise.

Case $a \in K$: definition of g_{a,X_2} . Write $a = a_H + q_1$ with $a_H \in H$.

$$g_{a,X_2}(y) = \begin{cases} f^{-1}(y + a_H) + q_1, & y \in X_2, \\ y, & y \in H \setminus X_2, \\ f^{-1}(y + a), & y \in X_2 + q_1, \\ y, & y \in (H \setminus X_2) + q_1. \end{cases}$$

Remark 18. For g_{a,X_2} in the case $a \in K$, the argument $y + a_H$ lies in H : indeed, $y \in X_2 \subseteq H$, $a_H \in H$, so $y + a_H \in H$. Thus $f^{-1}(y + a_H)$ is well-defined. In the third branch, $y \in X_2 + q_1 \subseteq K$, so $y + a \in H$, and $f^{-1}(y + a)$ is well-defined. In both branches the value of g_{a,X_2} is therefore a well-defined element of $\mathbb{F}_q$.

In both cases the values on the two cosets are linked by the compatibility condition

$$g_{a,X_i}(y + q_1) = g_{a,X_i}(y) + q_1 \quad \text{for all } y \in \mathbb{F}_q, \ i = 1, 2,$$

which we verify below. This is exactly the defining relation of the centralizer $\mathcal{C}$.

Lemma 19. (i) If $a \in H$ and $X_1 \subseteq H$ satisfies $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$, then g_{a,X_1} is a permutation of $\mathbb{F}_q$ and lies in $\mathcal{C} = \mathcal{C}(t_{q_1})$.
(ii) If $a \in K$, write $a = a_H + q_1$, and $X_2 \subseteq H$ satisfies $X_2 + a_H = f(X_2)$, then g_{a,X_2} is a permutation of $\mathbb{F}_q$ and lies in $\mathcal{C} = \mathcal{C}(t_{q_1})$.

Proof We prove the two cases separately.

Case $a \in H$. Compatibility. If $y \in X_1$, then $y + q_1 \in X_1 + q_1$, and

$$g_{a,X_1}(y + q_1) = (y + q_1) + a = y + a + q_1 = g_{a,X_1}(y) + q_1.$$

If $y \in H \setminus X_1$, then $y + q_1 \in (H \setminus X_1) + q_1$ and

$$g_{a,X_1}(y + q_1) = y + q_1 = g_{a,X_1}(y) + q_1.$$

The same identities hold for $y \in X_1 + q_1$ and $y \in (H \setminus X_1) + q_1$ by symmetry. Hence $g_{a,X_1} \in \mathcal{C}$.

Bijectivity. On H , g_{a,X_1} acts by translation $y \mapsto y + a$ on X_1 and by the identity on $H \setminus X_1$. Since $X_1 + a = X_1$, these two pieces are injective with disjoint images X_1 and $H \setminus X_1$, whose union is H . Hence g_{a,X_1} is a bijection of H , and compatibility makes it a bijection of K .

Case $a \in K$. Write $a = a_H + q_1$ with $a_H \in H$.

Compatibility. If $y \in X_2$, then $y + q_1 \in X_2 + q_1$, and

$$g_{a,X_2}(y + q_1) = f^{-1}((y + q_1) + a) = f^{-1}(y + a_H) = g_{a,X_2}(y) + q_1.$$

If $y \in H \setminus X_2$, then $y + q_1 \in (H \setminus X_2) + q_1$ and $g_{a,X_2}(y + q_1) = y + q_1 = g_{a,X_2}(y) + q_1$. The remaining two cases follow by symmetry. Hence $g_{a,X_2} \in \mathcal{C}$.

Bijectivity. On H , the two pieces of g_{a,X_2} are:

$$y \mapsto f^{-1}(y + a_H) + q_1 \text{ on } X_2, \quad y \mapsto y \text{ on } H \setminus X_2.$$

Their images are $X_2 + q_1$ (because $X_2 + a_H = f(X_2)$) and $H \setminus X_2$, which are disjoint. On K , write a point as $y + q_1$ with $y \in H$. The two pieces are:

$$y + q_1 \mapsto f^{-1}(y + a_H) \text{ for } y \in X_2, \quad y + q_1 \mapsto y + q_1 \text{ for } y \in H \setminus X_2.$$

Their images are X_2 and $(H \setminus X_2) + q_1$, respectively. Hence the four images are $X_2 + q_1$, $H \setminus X_2$, X_2 , and $(H \setminus X_2) + q_1$, which partition $\mathbb{F}_q$. Therefore g_{a,X_2} is a bijection of $\mathbb{F}_q$. $\square$

Remark 20. In the case $a \in H$, the condition $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$ ensures that X_1 is a union of orbits of $\mathcal{G}_1 = \langle t_a, f^{-1}t_a f \rangle$. In the case $a \in K$, the condition $X_2 + a_H = f(X_2)$ ensures that X_2 is a union of orbits of $\mathcal{G}_2 = \langle t_{a_H} f \rangle$. These are exactly the conditions appearing in Propositions 25 and 26.

Proposition 21 (Construction chain). *Let $f \in \mathcal{S}_{q_1}$ be a CP and $f^\uparrow \in \mathcal{D}$ its lift.*

- (i) *If $a \in H$ and $X_1 \subseteq H$ satisfies $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$, set $X^{(1)} = f(X_1) \cup (X_1 + q_1)$. Then*

$$u := t_{a,X^{(1)}} \circ f^\uparrow \circ g_{a,X_1} \in \mathcal{D}$$

and $u|_K = \text{id}_K$. Consequently $u^\downarrow \in \mathcal{S}_{q_1}$ is a CP, and $u^\downarrow = f_1$ as defined in Proposition 25.

- (ii) *If $a \in K$, write $a = a_H + q_1$, and $X_2 \subseteq H$ satisfies $X_2 + a_H = f(X_2)$, set $X^{(2)} = X_2 + q_1 \cup f(X_2)$. Then*

$$u := t_{a,X^{(2)}} \circ f^\uparrow \circ g_{a,X_2} \in \mathcal{D}$$

and $u|_K = \text{id}_K$. Consequently $u^\downarrow \in \mathcal{S}_{q_1}$ is a CP, and $u^\downarrow = f_2$ as defined in Proposition 26 with parameter a_H and subset X_2 .

Proof We prove the two cases.

Case $a \in H$. By Proposition 9, $t_{a,X^{(1)}} \circ f^\uparrow \in \mathcal{D}$. By Lemma 19(i), $g_{a,X_1} \in \mathcal{C}$, and Proposition 7(iii) gives

$$u = t_{a,X^{(1)}} \circ f^\uparrow \circ g_{a,X_1} \in \mathcal{D}.$$

We claim $u|_K = \text{id}_K$. Let $x \in K$; write $x = x' + q_1$ with $x' \in H$, so that $x' \in X_1$ if and only if $x \in X^{(1)}$ (since $X^{(1)} \cap K = X_1 + q_1$). If $x' \in X_1$, then $g_{a,X_1}(x) = x' + a + q_1 \in K$. Hence $f^\uparrow(g_{a,X_1}(x)) = x' + a + q_1$, and since $x' + a + q_1 \in X_1 + q_1 \subseteq X^{(1)}$, we have

$$t_{a,X^{(1)}}(x' + a + q_1) = (x' + a + q_1) + a = x' + q_1 = x.$$

If $x' \in H \setminus X_1$, then $g_{a,X_1}(x) = x' + q_1$ and $x' + q_1 \notin X^{(1)}$, hence $f^\uparrow(g_{a,X_1}(x)) = x' + q_1$ and $t_{a,X^{(1)}}(x' + q_1) = x' + q_1 = x$. Thus $u|_K = \text{id}_K$. By Proposition 12, $u^\downarrow$ is a CP. Comparing with Proposition 25 gives $u^\downarrow = f_1$.

Case $a \in K$. Write $a = a_H + q_1$ with $a_H \in H$. By Proposition 9, $t_{a,X^{(2)}} \circ f^\uparrow \in \mathcal{D}$. By Lemma 19(ii), $g_{a,X_2} \in \mathcal{C}$, so $u = t_{a,X^{(2)}} \circ f^\uparrow \circ g_{a,X_2} \in \mathcal{D}$. Let $x \in K$; write $x = x' + q_1$ with $x' \in H$. If $x' \in X_2$, then $x \in X_2 + q_1 \subseteq X^{(2)}$. By Definition 17,

$$g_{a,X_2}(x) = f^{-1}(x + a) = f^{-1}(x' + a_H) \in X_2.$$

Hence $f^\uparrow(g_{a,X_2}(x)) = f(f^{-1}(x' + a_H)) = x' + a_H$. Since $x' \in X_2$, the condition $X_2 + a_H = f(X_2)$ gives $x' + a_H \in f(X_2) \subseteq X^{(2)}$. Thus

$$t_{a,X^{(2)}}(x' + a_H) = x' + a_H + a = x' + a_H + a_H + q_1 = x' + q_1 = x.$$

If $x' \notin X_2$, then $x \notin X_2 + q_1$. Also $x \notin f(X_2) \subseteq H$, so $x \notin X^{(2)}$. By Definition 17, $g_{a,X_2}(x) = x$, and since $x \in K$, $f^\uparrow(x) = x$; hence $t_{a,X^{(2)}}(x) = x$. Therefore $u|_K = \text{id}_K$. By Proposition 12, $u^\downarrow$ is a CP. Comparing with Proposition 26 gives $u^\downarrow = f_2$, where f_2 is taken with parameter $a_H = a + q_1 \in H$. $\square$

Theorem 22. *Let $f \in \mathcal{S}_{q_1}$ be a CP and $a \in \mathbb{F}_q \setminus \{0\}$.*

- (i) *If $a \in H$ and $X_1 \subseteq H$ satisfies $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$, set $X^{(1)} = f(X_1) \cup (X_1 + q_1)$. Then $g_{a,X_1} \in \mathcal{C}$, $u := t_{a,X^{(1)}} \circ f^\uparrow \circ g_{a,X_1} \in \mathcal{D}^\uparrow$, and $u|_H = f_1$ of Proposition 25 with subset X_1 .*
- (ii) *If $a \in K$, write $a = a_H + q_1$, and $X_2 \subseteq H$ satisfies $X_2 + a_H = f(X_2)$, set $X^{(2)} = X_2 + q_1 \cup f(X_2)$. Then $g_{a,X_2} \in \mathcal{C}$, $u := t_{a,X^{(2)}} \circ f^\uparrow \circ g_{a,X_2} \in \mathcal{D}^\uparrow$, and $u|_H = f_2$ of Proposition 26 with parameter a_H and subset X_2 . In particular, when $a = q_1$, the parameter a_H equals 0.*

Proof Immediate from Lemma 19 and Proposition 21. $\square$

Remark 23 (Connection between the two constructions). Theorem 22 shows that the two constructions are two faces of the same mechanism: the closure operation of Proposition 9 on $\mathcal{D}$, followed by right multiplication by g_{a,X_1} or $g_{a,X_2} \in \mathcal{C}$, descends via Lemma 13 to the local modification on H . Rigidity (Theorem 15) constrains each operation in isolation but not their product: for $a \in K$, $f^\uparrow \circ g_{a,X_2} \in \mathcal{D} \setminus \mathcal{D}^\uparrow$, but precomposing with $t_{a,X^{(2)}}$ repairs the defect.

4.3 The Two Local Conjugations f_1 and f_2

We isolate the two local conjugations appearing in Proposition 21 and prove directly that they are CPs. The proofs are short once we use the following elementary lemma [17, 18] on piecewise permutations.

Lemma 24 (Piecewise permutations). *Let $g, h : H \rightarrow H$ be permutations and let $X \subseteq H$. Then the map $u : H \rightarrow H$ defined by*

$$u(x) = \begin{cases} g(x), & x \in X, \\ h(x), & x \notin X, \end{cases}$$

is a permutation of H if and only if $g(X) = h(X)$.

Proof The map u is a permutation if and only if its images on X and $H \setminus X$ are disjoint and cover H :

$$g(X) \cap h(H \setminus X) = \emptyset, \quad g(X) \cup h(H \setminus X) = H.$$

Since h is a permutation, $h(H \setminus X) = H \setminus h(X)$. Substituting, the first condition becomes $g(X) \subseteq h(X)$, and the second becomes $g(X) \cup (H \setminus h(X)) = H$, i.e., $g(X) \supseteq h(X)$. Together they read $g(X) = h(X)$. $\square$

Proposition 25 (Local conjugation f_1). *Let $f \in \mathcal{S}_{q_1}$ be a CP, $a \in H \setminus \{0\}$, and let $X_1 \subseteq H$ be a union of orbits of the dihedral group*

$$\mathcal{G}_1 = \langle t_a, f^{-1}t_af \rangle.$$

Equivalently,

$$X_1 + a = X_1, \quad f(X_1) + a = f(X_1).$$

Define

$$f_1(x) = \begin{cases} f(x+a) + a, & x \in X_1, \\ f(x), & x \notin X_1. \end{cases}$$

Then f_1 is a CP. Moreover,

$$f_1 = t_{a,f(X_1)} \circ f \circ t_{a,X_1} = f + \mathbf{1}_{X_1} \cdot (\Delta_a f + a).$$

Conversely, if f_1 is a CP, then X_1 is necessarily a union of orbits of $\mathcal{G}_1$.

Proof Write $\phi(x) = x + f(x)$, a permutation of H because f is a CP. Apply Lemma 24 twice.

For f_1 , take $g = t_a \circ f \circ t_a$, $h = f$, $S = X_1$. Both g, h are permutations. Hence f_1 is a permutation iff

$$g(X_1) = h(X_1) \iff f(X_1 + a) + a = f(X_1).$$

For $x \mapsto x + f_1(x)$, on X_1 we have

$$x + f_1(x) = x + f(x+a) + a = \phi(x+a),$$

and on $H \setminus X_1$ we have $x + f_1(x) = \phi(x)$. Both maps are permutations, so $x + f_1(x)$ is a permutation iff

$$\phi(X_1 + a) = \phi(X_1) \iff X_1 + a = X_1,$$

by injectivity of ϕ . This proves the iff condition. The group description follows because $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$ mean that X_1 is invariant under t_a and under $f^{-1}t_af$, hence is a union of orbits of the dihedral group $\mathcal{G}_1 = \langle t_a, f^{-1}t_af \rangle$. The final identity is immediate. $\square$

Proposition 26 (Local conjugation f_2). *Let $f \in \mathcal{S}_{q_1}$ be a CP, $a \in H$, and let $X_2 \subseteq H$ be a union of orbits of the cyclic group*

$$\mathcal{G}_2 = \langle t_a f \rangle.$$

Equivalently,

$$X_2 + a = f(X_2).$$

Define

$$f_2(x) = \begin{cases} f^{-1}(x + a) + a, & x \in X_2, \\ f(x), & x \notin X_2. \end{cases}$$

Then f_2 is a well-defined CP. The case $a = 0$ is allowed: then the condition reads $f(X_2) = X_2$, and f_2 acts as f^{-1} on X_2 and as f on $H \setminus X_2$.

Proof Since X_2 is a union of orbits of $\langle t_a f \rangle$, we have $(t_a f)(X_2) = X_2$, i.e., $f(X_2) + a = X_2$, hence $X_2 + a = f(X_2)$. We first verify that f_2 is well-defined. For $x \in X_2$, $x + a \in f(X_2)$, so $f^{-1}(x + a)$ is well-defined; moreover $f^{-1}(x + a) \in X_2$, because otherwise $f(f^{-1}(x + a)) = x + a \in f(X_2)$ would contradict $f^{-1}(x + a) \notin X_2$. Hence f_2 is a well-defined map.

Apply Lemma 24 to

$$g(x) = f^{-1}(x + a) + a, \quad h(x) = f(x).$$

Both are permutations of H . Hence f_2 is a permutation of H iff

$$g(X_2) = h(X_2) \iff f^{-1}(X_2 + a) + a = f(X_2) \iff X_2 + a = f(X_2),$$

where the last equivalence uses the bijectivity of f and $|X_2 + a| = |X_2| = |f(X_2)|$.

It remains to show that $x \mapsto x + f_2(x)$ is a permutation of H . Let $\psi(x) = x + f(x)$, a permutation of H since f is a CP. If $x \in X_2$, put $y = f^{-1}(x + a) \in X_2$; then $x = f(y) + a$, and

$$x + f_2(x) = x + y + a = f(y) + a + y + a = f(y) + y = \psi(y).$$

As x ranges over X_2 , $y = f^{-1}(x + a)$ ranges over X_2 , so

$$\{x + f_2(x) : x \in X_2\} = \psi(X_2).$$

If $x \notin X_2$, then $x + f_2(x) = x + f(x) = \psi(x)$, so

$$\{x + f_2(x) : x \notin X_2\} = \psi(H \setminus X_2).$$

Since ψ is a bijection, $\psi(X_2)$ and $\psi(H \setminus X_2)$ are disjoint and their union is H . Hence $x \mapsto x + f_2(x)$ is a permutation of H . Combining this with the earlier verification that f_2 is a permutation of H , we conclude that f_2 is a CP. The case $a = 0$ is included: all steps remain valid because $0 + 0 = 0$ and $X_2 + 0 = X_2 = f(X_2)$. $\square$

Remark 27. The condition $X_2 + a = f(X_2)$ in Proposition 26 is genuinely necessary: if it fails, the definition of f_2 is not well-defined on X_2 , so the question of whether f_2 is a CP does not even arise. The stronger condition that X_2 is a union of orbits of the cyclic group $\langle t_a f \rangle$ is a natural sufficient condition that guarantees $X_2 + a = f(X_2)$. In particular, the case $a = 0$ corresponds to X_2 being a union of f -orbits.

5 Effects of Local Modifications on Cryptographic Indicators

We now quantify how the two local conjugations of Subsection 4.3 affect the three main cryptographic indicators: differential uniformity, nonlinearity, and algebraic degree.

Lemma 28 (Perturbation of the DDT). *Let $h, h' : H \rightarrow H$ and suppose h' differs from h on a set D with $|D| \leq m$. Then for every $u \neq 0$ and every v ,*

$$|\nu_{h'}(u, v) - \nu_h(u, v)| \leq 2m.$$

In particular,

$$\delta(h) - 2m \leq \delta(h') \leq \delta(h) + 2m.$$

Proof The difference $\nu_{h'}(u, v) - \nu_h(u, v)$ is supported on the set of $x \in H$ such that $x \in D$ or $x + u \in D$, i.e., $x \in D \cup (D + u)$. This set has size at most $|D| + |D + u| \leq 2m$. The second claim follows by maximizing over $u \neq 0$ and v . $\square$

Proposition 29 (Differential uniformity under local modification). *Let $f \in \mathcal{S}_{q_1}$ be a CP, $a \in H \setminus \{0\}$, and let $X_1, X_2 \subseteq H$ be as in Propositions 25 and 26, with $m_1 = |X_1|$ and $m_2 = |X_2|$. Then*

$$\delta(f) - 2m_1 \leq \delta(f_1) \leq \delta(f) + 2m_1, \quad \delta(f_1) \geq \max\{2, \delta_f(a), \delta(f) - 2m_1\},$$

and

$$\delta(f) - 2m_2 \leq \delta(f_2) \leq \delta(f) + 2m_2, \quad \delta(f_2) \geq \max\{2, \delta(f) - 2m_2\}.$$

Proof Both f_1 and f_2 differ from f only on X_1 and X_2 , respectively, so the sandwich bounds follow from Lemma 28. Since f_1 and f_2 are permutations of H , every nonzero row of their DDT has q_1 entries summing to q_1 , and each entry is even, giving $\delta(f_i) \geq 2$. For f_1 , under the conditions $X_1 + a = X_1$ and $f(X_1) + a = f(X_1)$ one has $\Delta_a f_1(x) = \Delta_a f(x)$ for every x , so $\Delta_a f_1 = \Delta_a f$ and $\delta(f_1) \geq \delta_f(a)$. $\square$

Proposition 30 (Nonlinearity under local modification). *Under the notation of Proposition 29,*

$$\text{nl}(f) - m_1 \leq \text{nl}(f_1) \leq \text{nl}(f) + m_1,$$

and

$$\begin{aligned} \text{nl}(f_2) &\geq \max\{0, \text{nl}(f) - m_2, \text{nl}(f^{-1}) - |H \setminus X_2|\}, \\ \text{nl}(f_2) &\leq \min\{\text{nl}(f) + m_2, \text{nl}(f^{-1}) + |H \setminus X_2|\}. \end{aligned}$$

Proof Let $\mathcal{A}$ denote the affine maps of H . The elementary bound $|\text{nl}(h) - \text{nl}(h')| \leq r$ holds whenever h, h' differ on at most r points, because Hamming distance to any fixed affine map changes by at most r . Applied to f_1 with $r = m_1 = |X_1|$, this gives the stated bounds. For f_2 , the same bound with $r = m_2 = |X_2|$ yields $|\text{nl}(f_2) - \text{nl}(f)| \leq m_2$. Separately, under the

condition $X_2 + a = f(X_2)$ we may form $g = t_a \circ f^{-1} \circ t_a$, whose nonlinearity equals $\text{nl}(f^{-1})$; since f_2 differs from g only on $H \setminus X_2$, we obtain $|\text{nl}(f_2) - \text{nl}(f^{-1})| \leq |H \setminus X_2|$. Combining the two estimates with the trivial $\text{nl}(f_2) \geq 0$ gives the bounds. $\square$

Proposition 31 (Algebraic degree under local modification). *Under the notation of Proposition 29,*

$$f_1 = f + \mathbf{1}_{X_1} \cdot (\Delta_a f + a).$$

Hence

$$\deg(f_1) \leq \max\{\deg(f), \deg(\mathbf{1}_{X_1}) + \deg(\Delta_a f)\}.$$

If $\deg(\mathbf{1}_{X_1}) + \deg(\Delta_a f) < \deg(f)$, then $\deg(f_1) = \deg(f)$. An analogous upper bound holds for f_2 , with f^{-1} in place of f and X_2 in place of X_1 .

Proof The identity for f_1 is immediate from Proposition 25. The degree bound follows from the fact that the degree of a sum is at most the maximum of the degrees of the summands. If the modification term has strictly smaller degree than f , then the leading monomial of f survives, so the degree does not drop. $\square$

Remark 32. Obtaining a sharp lower bound on $\deg(f_1)$ and $\deg(f_2)$ in terms of $\deg(f)$ and n remains open. The product $\mathbf{1}_{X_1} \cdot (\Delta_a f + a)$ can in principle reach $\deg(\mathbf{1}_{X_1}) + \deg(\Delta_a f)$.

6 CCZ-Inequivalence and Structural Limitations

The construction chain of Section 4 produces new CPs from a given one. The point of the construction is that the new CPs are, generically, CCZ-inequivalent to the original one. This section makes that statement precise and discusses the structural limitations imposed by affine seeds.

Theorem 33 (CCZ-inequivalence of the construction chain). *Let $f \in \mathcal{S}_{q_1}$ be a CP and $f^\uparrow \in \mathcal{D}$ its standard lift. Let $g \in \text{GL}_H$ and $h \in \mathcal{C}$ satisfy*

$$g \circ f^\uparrow \circ h = u^\uparrow$$

for some $u \in \mathcal{S}_{q_1}$. If the DDT of u is not obtainable from that of f by row and column permutations, or if the multiset of absolute Walsh coefficients of u differs from that of f , then u is a CP CCZ-inequivalent to f .

Proof By Proposition 7, $g \circ f^\uparrow \circ h \in \mathcal{D}$. By assumption this equals $u^\uparrow$, so $u^\uparrow \in \mathcal{D}$, and Proposition 12 shows that u is a CP. CCZ-equivalent permutations have the same DDT up to row and column permutations and the same multiset of absolute Walsh coefficients. Hence a difference in either invariant rules out CCZ-equivalence. $\square$

Proposition 34 (f_1 is CCZ-inequivalent to f). *Under the hypotheses of Proposition 25, if the multiset*

$$\{\delta_{f_1}(u) : u \in H \setminus \{0\}\}$$

differs from

$$\{\delta_f(u) : u \in H \setminus \{0\}\},$$

then f_1 is CCZ-inequivalent to f .

Proof The multiset of row maxima is determined by the DDT up to row permutations, which are preserved by CCZ equivalence. Hence a difference in this multiset rules out CCZ-equivalence. $\square$

Remark 35. The criteria above are sufficient, not necessary. A local modification $t_{a,X}$ may still produce a function CCZ-equivalent to the original one; the construction chain does not guarantee a new CCZ class at every step.

Proposition 36 (f_2 is CCZ-inequivalent to f). *Under the hypotheses of Proposition 26, if the Walsh spectrum multiset of f_2 differs from that of f , then f_2 is CCZ-inequivalent to f .*

Proof The Walsh spectrum multiset is a CCZ invariant. $\square$

Proposition 37 (f_1 and f_2 are mutually CCZ-inequivalent). *Under the hypotheses of Propositions 25 and 26, if f_1 and f_2 have different DDT multisets or different Walsh spectrum multisets, then f_1 and f_2 are CCZ-inequivalent.*

Proof The DDT multiset and the Walsh spectrum multiset are CCZ invariants. $\square$

7 Algorithms for Constructing Complete Permutations

We now translate the theoretical construction into two algorithms. The first produces a random CP from scratch, providing a rich supply of starting points. The second performs a greedy local search over the local conjugations of Subsection 4.3, maintaining two candidate direction pools and accepting only moves that strictly improve a quality function built from the full differential and Walsh spectra.

7.1 Algorithm 1: Random Complete Permutation

The first algorithm performs a randomized backtracking search over permutations of H while maintaining the additional constraint that $x \mapsto f(x) + x$ be injective. The search is driven by the observation that the two sets $U = \{f(x) : x \in H\}$ and $V = \{f(x) + x : x \in H\}$ must both have size q_1 at the end of the search; a partial assignment is extended if and only if both constraints can still be satisfied. In the description below, $\oplus$ denotes addition in $H \cong \mathbb{F}_2^n$, while indices are integers.

Algorithm 1 Random complete permutation over $H \cong \mathbb{F}_{2^n}$

Require: Integer $n \geq 2$.

Ensure: A complete permutation f of H .

```
1:  $q_1 \leftarrow 2^n$ ,  $S \leftarrow [0, 1, \dots, q_1 - 1]$  ▷ elements of  $H$ , in a fixed order
2:  $U \leftarrow \emptyset$ ,  $V \leftarrow \emptyset$  ▷ used values of  $f$  and of  $f + x$ 
3:  $f \leftarrow$  empty array of length  $q_1$ 
4:  $i \leftarrow 0$ 
5: while  $i < q_1$  do
6:    $x \leftarrow S[i]$ 
7:    $C \leftarrow \{y \in S \setminus U : y \oplus x \notin V\}$ 
8:   if  $C \neq \emptyset$  then
9:     Choose  $y \in C$  uniformly at random
10:     $f(x) \leftarrow y$ 
11:     $U \leftarrow U \cup \{y\}$ ,  $V \leftarrow V \cup \{y \oplus x\}$ 
12:     $i \leftarrow i + 1$ 
13:   else
14:     if  $i = 0$  then
15:       restart the algorithm
16:     end if
17:      $i \leftarrow i - 1$ ,  $x \leftarrow S[i]$ 
18:      $U \leftarrow U \setminus \{f(x)\}$ ,  $V \leftarrow V \setminus \{f(x) \oplus x\}$ 
19:   end if
20: end while
21: return  $f$ 
```

In practice, the algorithm terminates quickly for the dimensions considered here; no polynomial worst-case bound is claimed. On termination, $f(H) = H$ and $(f + \text{id})(H) = H$, i.e., f is a CP.

7.2 Algorithm 2: Greedy Local Search via Local Conjugations

The second algorithm performs a greedy local search over the local conjugations f_1 and f_2 of Subsection 4.3. It maintains two independent candidate direction pools:

$$A_1 := H \setminus \{0\}$$

for the f_1 -branch, and

$$A_2 := H$$

for the f_2 -branch (which, by Proposition 26, allows $a = 0$). At each iteration it picks a direction a from A_1 , computes the orbits of $\mathcal{G}_1 = \langle t_a, f^{-1}t_a f \rangle$, and then examines the admissible subsets X_1 in a uniformly random order rather than in a fixed enumeration order. If some candidate f_1 strictly improves the quality function, the current CP f is updated and both pools are reset. If no candidate improves $Q(f)$, the direction a is removed from A_1 . The same procedure is applied independently to A_2 for the f_2 -branch. The algorithm terminates when both A_1 and A_2 are empty.

Quality function.

Let $D(f)$ denote the *differential spectrum* of f , i.e. the multiset of DDT entries

$$D(f) = \{\nu_f(u, v) : u \in H \setminus \{0\}, v \in H\},$$

encoded as a map $d_f : \mathbb{N} \rightarrow \mathbb{N}$, $d_f(k) := \#\{(u, v) : \nu_f(u, v) = k\}$. Let $W(f)$ denote the *Walsh spectrum* of f , i.e. the multiset of absolute values of Walsh coefficients

$$W(f) = \{|\widehat{f}(u, v)| : u, v \in H\},$$

encoded similarly as a map $w_f : \mathbb{N} \rightarrow \mathbb{N}$. Define the quality function

$$Q(f) := (D(f), W(f)),$$

compared lexicographically. For two spectra d, d' , represented as maps $\mathbb{N} \rightarrow \mathbb{N}$, we compare them as follows: let $k_1 > k_2 > \dots > k_r$ be the keys appearing in d or d' , in descending order; write

$$\begin{aligned} D &:= [(k_1, d(k_1) \text{ or } 0), \dots, (k_r, d(k_r) \text{ or } 0)], \\ D' &:= [(k_1, d'(k_1) \text{ or } 0), \dots, (k_r, d'(k_r) \text{ or } 0)]. \end{aligned}$$

Then $d < d'$ iff D is lexicographically smaller than D' . This comparison is the natural encoding of the requirement that high DDT or Walsh values should occur as rarely as possible, with smaller spectral values tie-broken in the same way. In words, we first compare the multiplicity of the largest DDT value, then the next largest, and so on; if the DDT spectra coincide, we compare the Walsh spectra in the same way. With this convention we write $Q(g) < Q(f)$ iff $D(g) < D(f)$, or $D(g) = D(f)$ and $W(g) < W(f)$.

Algorithm 2 Greedy local search over local conjugations with randomized subset order

Require: A CP $f_0 \in \mathcal{S}_{q_1}$.

Ensure: A CP f that is locally Q-optimal.

```

1:  $f \leftarrow f_0$ 
2:  $A_1 \leftarrow H \setminus \{0\}$  ▷ candidate directions for the  $f_1$ -branch
3:  $A_2 \leftarrow H$  ▷ candidate directions for the  $f_2$ -branch (including 0)
4: while  $A_1 \neq \emptyset$  or  $A_2 \neq \emptyset$  do
5:    $g \leftarrow \text{null}$ 
6:   –  $f_1$ -branch –
7:   while  $A_1 \neq \emptyset$  and  $g = \text{null}$  do
8:     Randomly choose  $a \in A_1$ 
9:     Compute the orbits of  $\mathcal{G}_1 = \langle t_a, f^{-1}t_af \rangle$  on  $H$ ; let  $\text{orbs}_1$  be the list of
    orbits.
10:     $m_1 \leftarrow |\text{orbs}_1|$ 
11:    Randomly shuffle all nonempty proper subsets of  $\{1, \dots, m_1\}$ ; let  $L_1$  be the
    shuffled list.
12:    for  $S \in L_1$  do
13:       $X_1 \leftarrow \bigcup_{j \in S} \text{orbs}_1[j]$ 
14:       $h \leftarrow f_1$  with parameter  $a$  and subset  $X_1$ 
15:      if  $Q(h) < Q(f)$  then
16:         $g \leftarrow h$ 
17:        break
18:      end if
19:    end for
20:    if  $g = \text{null}$  then
21:       $A_1 \leftarrow A_1 \setminus \{a\}$ 
22:    end if
23:  end while
24:  –  $f_2$ -branch –
25:  while  $A_2 \neq \emptyset$  and  $g = \text{null}$  do
26:    Randomly choose  $a \in A_2$ 
27:    Compute the orbits of  $\mathcal{G}_2 = \langle t_a f \rangle$  on  $H$ ; let  $\text{orbs}_2$  be the list of orbits.
28:     $m_2 \leftarrow |\text{orbs}_2|$ 
29:    Randomly shuffle all nonempty proper subsets of  $\{1, \dots, m_2\}$ ; let  $L_2$  be the
    shuffled list.
30:    for  $S \in L_2$  do
31:       $X_2 \leftarrow \bigcup_{j \in S} \text{orbs}_2[j]$ 
32:       $h \leftarrow f_2$  with parameter  $a$  and subset  $X_2$ 
33:      if  $Q(h) < Q(f)$  then
34:         $g \leftarrow h$ 
35:        break
36:      end if
37:    end for
38:    if  $g = \text{null}$  then
39:       $A_2 \leftarrow A_2 \setminus \{a\}$ 
40:    end if
41:  end while
42:  if  $g \neq \text{null}$  then 22
43:     $f \leftarrow g$ 
44:     $A_1 \leftarrow H \setminus \{0\}$ 
45:     $A_2 \leftarrow H$  ▷ reset both candidate pools
46:  end if
47: end while
48: return  $f$ 

```

The algorithm always terminates. Indeed, every iteration either strictly decreases $Q(f)$ or removes one direction from one of the finite pools A_1, A_2 .

Complexity.

In the worst case, the enumeration of all nonempty proper subsets of $\{1, \dots, m_i\}$ is exponential in m_i . In the reported experiments with $n = 5$, the number of orbits is small in practice, and the search over subsets is stopped as soon as an improving move is found; hence the enumeration is feasible for these experiments. For larger n , one should replace the exhaustive subset enumeration by a randomized or heuristic subset search. The construction chain itself does not require exhaustive enumeration. The termination argument remains valid for any finite subset search strategy that either improves $Q(f)$ or removes a direction from the candidate pool.

8 Experiments

All experiments below are performed on $H \cong \mathbb{F}_{32}$ ($n = 5$). We compute all indicators directly from the permutation table using a Python implementation. Algorithm 2 is used in its randomized form: whenever a direction a is selected, the admissible subsets X_1 or X_2 are examined in a uniformly random order, rather than in a fixed enumeration order. In both experiments, Algorithm 2 is run independently 100 times.

8.1 Experiment 1: Greedy Search from the Linear Seed s_2

The seed is the linear complete permutation

$$f_0 = s_2, \quad s_2(x) = 2x, \quad x \in H \cong \mathbb{F}_{32}.$$

For this seed one has $\delta(f_0) = 32$, $\text{nl}(f_0) = 0$, and $\deg(f_0) = 1$. We run Algorithm 2 100 times from this seed. Table 2 records a representative trajectory until the first $\delta = 4$ complete permutation is found. Here, for the f_1 -branch, $X^{(1)} = f(X_1) \cup (X_1 + q_1)$; for the f_2 -branch, $X^{(2)} = f(X_2) \cup (X_2 + q_1)$. Thus $|X^{(i)}|$ is always even and at most 64.

Table 3 reports the distribution of the final indicators over the 100 independent runs.

8.2 Experiment 2: Greedy Search from Random CP Seeds

In the second experiment, each run starts from a random complete permutation generated by Algorithm 1, and then Algorithm 2 is run 100 times independently. Table 4 records a representative trajectory until the first $\delta = 4$ complete permutation is found.

Table 5 reports the final indicator distribution over the 100 independent runs.

8.3 Selected CPs and Differential Spectra

Table 6 lists selected $\delta = 4$ CPs found in the two experiments, together with the Dillon-based CP from Shuai-Li [13] as a reference. For $H \cong \mathbb{F}_{32}$, every differential

Table 2 Experiment 1: trajectory to the first $\delta = 4$ CP from the linear seed $s_2(x) = 2x$ on $H \cong \mathbb{F}_{32}$. Indicators after each accepted move.

Step t	Branch	a	$ X^{(i)} $	$\delta(f_t)$	$\text{nl}(f_t)$	$\text{deg}(f_t)$
0	—	—	—	32	0	1
1	f_1	11	40	32	0	3
2	f_1	1	16	32	0	3
3	f_2	19	46	18	4	4
4	f_1	31	8	16	4	4
5	f_1	29	44	10	6	4
6	f_2	21	20	8	4	4
7	f_2	21	34	8	8	4
8	f_2	30	8	8	6	4
9	f_1	19	20	8	6	4
10	f_2	20	46	8	8	4
11	f_2	12	56	6	8	4
12	f_2	24	46	6	6	4
13	f_2	20	54	6	6	4
14	f_2	0	58	6	6	4
15	f_1	26	28	6	8	4
16	f_2	24	8	6	8	4
17	f_1	30	12	6	8	4
18	f_1	14	40	4	8	4

Table 3 Experiment 1: indicator distribution over 100 independent runs of Algorithm 2 from the linear seed s_2 on $H \cong \mathbb{F}_{32}$.

Indicator	Min	Median	Max	Mean
δ	4.0	6.0	6.0	5.94
nl	6.0	8.0	8.0	7.90
deg	3.0	4.0	4.0	3.99

spectrum contains $31 \cdot 32 = 992$ entries, and

$$\delta(f) = \max\{k : d_f(k) > 0\}.$$

Thus $\text{cp}_{11}, \text{cp}_{12}, \text{cp}_{13}$ and $\text{cp}_{21}, \text{cp}_{22}, \text{cp}_{23}, \text{cp}_{24}$ are all $\delta = 4$, while the Dillon-based reference cp_0 has $\delta = 8$.

For completeness, the corresponding permutation tables over $H \cong \mathbb{F}_{32}$ are as follows.

$\text{cp}_0 = [0, 25, 30, 29, 17, 15, 23, 19, 27, 5, 13, 28, 31, 3, 1, 18, 7, 16, 9, 4, 26, 14, 8, 6, 24, 22, 21, 20, 10, 2, 11, 12]$
 $\text{cp}_{11} = [7, 21, 16, 1, 11, 31, 14, 2, 19, 13, 10, 18, 5, 29, 25, 23, 30, 28, 4, 24, 9, 20, 3, 8, 6, 26, 22, 17, 0, 27, 15, 12]$
 $\text{cp}_{12} = [12, 11, 31, 23, 10, 20, 21, 30, 22, 8, 1, 14, 25, 5, 9, 24, 18, 7, 13, 16, 29, 26, 6, 17, 4, 2, 0, 3, 28, 15, 19, 27]$

Table 4 Experiment 2: trajectory to the first $\delta = 4$ CP from a random CP seed generated by Algorithm 1 on $H \cong \mathbb{F}_{32}$. Indicators after each accepted move.

Step t	Branch	a	$ X^{(i)} $	$\delta(f_t)$	$\text{nl}(f_t)$	$\text{deg}(f_t)$
0	—	—	—	10	8	4
1	f_2	12	10	8	8	4
2	f_2	19	26	8	6	4
3	f_1	19	56	8	6	4
4	f_2	31	54	6	8	4
5	f_2	30	56	6	8	4
6	f_2	9	56	6	8	4
7	f_1	25	32	6	8	4
8	f_1	10	56	6	8	4
9	f_2	10	56	6	8	4
10	f_1	31	24	4	8	4

Table 5 Experiment 2: indicator distribution over 100 independent runs of Algorithm 2 from random CP seeds generated by Algorithm 1 on $H \cong \mathbb{F}_{32}$.

Indicator	Min	Median	Max	Mean
δ	4.0	6.0	6.0	5.92
nl	6.0	8.0	8.0	7.92
deg	4.0	4.0	4.0	4.00

$cp_{13} = [1, 24, 9, 3, 12, 23, 8, 25, 14, 28, 22, 16, 20, 7, 11, 27, 29, 30, 4, 0, 5, 10, 17, 19, 2, 26, 13, 6, 21, 31, 18, 15]$
 $cp_{21} = [0, 10, 27, 30, 13, 3, 9, 16, 29, 18, 21, 15, 26, 7, 2, 19, 24, 5, 28, 20, 23, 4, 12, 22, 8, 11, 31, 25, 17, 14, 6, 1]$
 $cp_{22} = [2, 1, 25, 9, 16, 21, 8, 0, 4, 12, 18, 22, 27, 17, 10, 29, 31, 28, 13, 24, 23, 19, 7, 30, 6, 15, 3, 26, 20, 14, 11, 5]$
 $cp_{23} = [2, 18, 1, 6, 13, 8, 14, 25, 30, 17, 4, 23, 24, 31, 9, 26, 10, 27, 5, 3, 21, 12, 11, 19, 20, 22, 28, 16, 7, 29, 15, 0]$
 $cp_{24} = [9, 7, 31, 21, 29, 16, 3, 28, 23, 4, 11, 19, 15, 5, 26, 0, 30, 22, 12, 25, 20, 2, 10, 6, 8, 27, 17, 1, 24, 14, 18, 13]$

8.4 Discussion

The experiments provide three main conclusions.

First, the randomized local-conjugation search constructs several $\delta = 4$ complete permutations that are CCZ-inequivalent. Indeed, the selected CPs in Table 6 realize multiple distinct differential spectra (with cp_{21} and cp_{22} sharing one spectrum). Since the DDT multiset is a CCZ invariant, any two CPs with distinct spectra are CCZ-inequivalent. Thus the construction chain of Section 4, implemented by Algorithm 2,

Table 6 Selected complete permutations and their differential spectra over $H \cong \mathbb{F}_{32}$. The spectrum is written as the frequency map $D(f) = \{k : d_f(k)\}$.

ID	Source	δ	Differential spectrum $D(f)$
cp_0	Dillon-based, Shuai-Li [13]	8	$\{0 : 578, 2 : 339, 4 : 69, 6 : 5, 8 : 1\}$
cp_{11}	Experiment 1	4	$\{0 : 568, 2 : 352, 4 : 72\}$
cp_{12}	Experiment 1	4	$\{0 : 589, 2 : 310, 4 : 93\}$
cp_{13}	Experiment 1	4	$\{0 : 556, 2 : 376, 4 : 60\}$
cp_{21}	Experiment 2	4	$\{0 : 577, 2 : 334, 4 : 81\}$
cp_{22}	Experiment 2	4	$\{0 : 577, 2 : 334, 4 : 81\}$
cp_{23}	Experiment 2	4	$\{0 : 607, 2 : 274, 4 : 111\}$
cp_{24}	Experiment 2	4	$\{0 : 580, 2 : 328, 4 : 84\}$

genuinely produces new CCZ classes of complete permutations rather than mere affine or CCZ-equivalent variants of the seed.

Second, the repeated appearance of identical differential spectra from different random seeds, and the tight concentration of the indicator distributions in Tables 3 and 5, provide preliminary evidence that the equivalence relation generated by the local-conjugation moves may have a single class on $\mathcal{D}^\uparrow$. This supports the conjecture stated in Open Problem 38.

Third, the Dillon-based reference cp_0 has $\delta(cp_0) = 8$, whereas the CPs produced by the local search all satisfy $\delta = 4$. Thus a CP derived from the well-known Dillon APN permutation does not dominate the CPs found here; in fact its differential uniformity is worse. This indicates that APN-based constructions and the local-conjugation mechanism explore different regions of the space of complete permutations. Since the LCP-CP correspondence maps crooked functions to differentially 4-uniform CPs, and the CPs obtained here are also $\delta = 4$, it is tempting to speculate that this may lead to APN permutations CCZ-inequivalent to the Dillon APN permutation. This is, however, only a heuristic indication; no such APN permutations are established here.

9 Conclusion and Open Problems

We introduced the $\mathcal{D}$ -class as the natural setting for LCPs with fixed distinguished direction and hyperplane. We proved its closure under three group actions and local translations, established rigidity of the lifted CP subclass $\mathcal{D}^\uparrow$, and used localized centralizer elements to explain the two local conjugations f_1 and f_2 as the two branches of the construction chain. We also derived bounds for differential uniformity, nonlinearity, and algebraic degree, proved CCZ-inequivalence criteria, and presented two algorithms. The two central open problems are the connectivity of $\mathcal{D}^\uparrow$ under local-conjugation moves and the existence of APN functions in $\mathcal{D}^\uparrow$.

Open Problem 38 (Connectivity of $\mathcal{D}^\uparrow$ under local conjugations). Define an equivalence relation $\sim$ on $\mathcal{D}^\uparrow$ by $f \sim g$ if there exists a sequence

$$u_0 = f, \quad u_{j+1} = t_{a_j, X_j} \circ u_j \circ g_{a_j, X_j}, \quad u_n = g,$$

with all $u_j \in \mathcal{D}^\dagger$. Is $\mathcal{D}^\dagger$ a single equivalence class under $\sim$? Equivalently, are all lifted CPs in $\mathcal{D}^\dagger$ connected by the local-conjugation moves? The experiments in Section 8 support the conjecture that the answer is affirmative; see the discussion in Section 8.

Open Problem 39 (APN functions in $\mathcal{D}^\dagger$). For a given $f \in \mathcal{D}^\dagger$, is the intersection

$$\text{APN}(\mathbb{F}_q) \cap \{t \circ L \circ f \circ g : t \in \mathcal{T}, L \in \text{GL}_H, g \in \mathcal{C}\}$$

nonempty? Here $\text{APN}(\mathbb{F}_q)$ denotes the set of APN permutations of $\mathbb{F}_q$. Give sufficient or necessary conditions for this intersection to be nonempty. In particular, if f is not APN, can right multiplication by a non-affine element of $\mathcal{C}$ produce an APN function?

Acknowledgements. This work is supported by the Natural Science Foundation of Ningxia (2026AAC030162). The authors would like to thank the editor and the anonymous reviewers for their valuable comments and suggestions that improved the quality of this paper.

References

- [1] H. B. Mann, *The construction of orthogonal Latin squares*, Ann. Math. Statist. **13** (1942), 418–423.
- [2] M. Hall and L. J. Paige, *Complete mappings of finite groups*, Pacific J. Math. **5** (1955), 541–549.
- [3] H. Niederreiter and K. H. Robinson, *Complete mappings of finite fields*, J. Austral. Math. Soc. Ser. A **33** (1982), 197–212.
- [4] A. Muratović-Ribić and E. Pasalic, *A note on complete polynomials over finite fields and their applications in cryptography*, Finite Fields Appl. **25** (2014), 306–315.
- [5] B. Sun, K. Li, J. Guo, and L. Qu, *New constructions of complete permutations*, IEEE Trans. Inform. Theory **67** (2021), 7561–7567.
- [6] X. Lai and J. L. Massey, *A proposal for a new block encryption standard*, in: Advances in Cryptology—EUROCRYPT’90, LNCS **473**, Springer, 1991, pp. 389–404.
- [7] S. Vaudenay, *On the Lai–Massey scheme*, in: Advances in Cryptology—ASIACRYPT’99, LNCS **1716**, Springer, 1999, pp. 8–19.
- [8] L. Mittenenthal, *Block substitutions using orthomorphic mappings*, Adv. Appl. Math. **16** (1995), 59–71.
- [9] E. Biham and A. Shamir, *Differential cryptanalysis of DES-like cryptosystems*, in: Advances in Cryptology—CRYPTO’90, LNCS **537**, Springer, 1991, pp. 2–21.

- [10] K. Nyberg, *Perfect nonlinear S-boxes*, in: Advances in Cryptology—EUROCRYPT’91, LNCS **547**, Springer, 1991, pp. 378–386.
- [11] T. D. Bending and D. Fon-Der-Flaass, *Crooked functions, bent functions, and distance regular graphs*, Electron. J. Combin. **5** (1998), R34.
- [12] P. Charpin, *Crooked functions*, in: Finite Fields and their Applications, J. A. Davis (Ed.), De Gruyter Proc. Math., Berlin, 2020, pp. 87–102.
- [13] L. Shuai and M. Li, *The locally crooked permutations and the complete permutations over $\mathbb{F}_{2^n}$* , Cryptogr. Commun. **17** (2025), 1583–1600.
- [14] C. Carlet, P. Charpin, and V. Zinoviev, *Codes, bent functions and permutations suitable for DES-like cryptosystems*, Des. Codes Cryptogr. **15** (1998), 125–156.
- [15] C. Carlet, *Boolean Functions for Cryptography and Coding Theory*, Cambridge University Press, 2021.
- [16] N. Jacobson, *Basic Algebra I*, 2nd ed., Dover, 2012 (reprint of the 1985 2nd edition).
- [17] L. Shuai, L. Wang, L. Miao, and X. Zhou, *Differential uniformity of the composition of two functions*, Cryptogr. Commun. **12** (2020), 205–220.
- [18] S. Li and L. Miao, *New differentially 4-uniform piecewise permutations over $\mathbb{F}_{2^{2k}}$ from the inverse function*, Symmetry **15** (2023), 131.