Classification of \((q, q)\)-Biprojective APN Functions

Faruk Göloğlu

Abstract—In this paper, we classify \((q, q)\)-biprojective almost perfect nonlinear (APN) functions over \(\mathbb{L} \times \mathbb{L}\) under the natural left and right action of GL(2, \(\mathbb{L}\)) where \(\mathbb{L}\) is a finite field of characteristic 2. This shows in particular that the only quadratic APN functions (up to CCZ-equivalence) over \(\mathbb{L} \times \mathbb{L}\) that satisfy the so-called subfield property are the Gold functions and the function \(\kappa : \mathbb{F}_{2^4} \rightarrow \mathbb{F}_{2^6}\) which is the only known APN function that is equivalent to a permutation over \(\mathbb{L} \times \mathbb{L}\) up to CCZ-equivalence as shown in Browning et al. (2010). Deciding whether there exist other quadratic APN functions CCZ-equivalent to permutations that satisfy subfield property or equivalently, generalizing \(\kappa\) to higher dimensions was an open problem listed for instance in Carlet (2015) as one of the interesting open problems on cryptographic functions.

Index Terms—Perfect nonlinearity, almost perfect nonlinear (APN) functions, permutations.

I. INTRODUCTION

Almost perfect nonlinear (APN) functions are cryptographically important functions over a vector space over the finite field of order two that provides the best resistance against differential cryptanalysis. Arguably the most important open problem on APN functions is the question on the existence of APN permutations over even dimensional vector spaces. There are no APN permutations over \(\mathbb{F}_2^2\) and \(\mathbb{F}_2^4\) [1]. Existence of an APN permutation over \(\mathbb{F}_2^6\) was shown in [2]. The function is CCZ-equivalent (see Sections II and III for the definitions of the concepts that are used in Introduction) to the quadratic function \(\kappa : \mathbb{F}_{2^6} \rightarrow \mathbb{F}_{2^6}\). Note that we will view the finite field \(\mathbb{F}_{2^6}\) as a vector space \(\mathbb{F}_{2^2}^6\) and also as \(\mathbb{F}_{2^2} \times \mathbb{F}_{2^2}\). When \(\kappa\) is viewed as a polynomial over the finite field \(\mathbb{F}_{2^6}\) it falls into the class of Dembowski-Ostrom polynomials that satisfy the subfield property introduced in [2]. These polynomial functions when viewed as functions over \(\mathbb{F}_{2^2} \times \mathbb{F}_{2^2}\) form the class of \((q, q)\)-biprojective functions. Of course a natural question that arises is to determine whether Dembowski-Ostrom polynomials that satisfy the subfield property (or, equivalently, the class of \((q, q)\)-biprojective functions) contain APN functions that are CCZ-equivalent to permutations for \(l > 3\). The question is viewed as an important problem. For instance it was included by Carlet in a list of interesting research questions regarding cryptographic functions.

[3, Section 3.7] as an important subproblem of the major problem of deciding whether there exists an APN permutation when \(l > 3\). The problem also appeared in [4, Problem 15].

This paper, we solve this problem.

Theorem 1: Let \(q = 2^k\), \(r = 2^l\), \(\mathbb{L} = \mathbb{F}_{2^r}\) with \(0 < k < l\) and \(F : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}\) be a \((q, q)\)-biprojective function. Then \(F\) is APN if and only if \(\gcd(k, l) = 1\), and

1) \(l\) is even, and \(F \simeq_{\mathbb{L}} G_{q+1}\) or \(F \simeq_{\mathbb{L}} G_{q+r}\), or
2) \(l\) is odd, \(k\) is odd, and \(F \simeq_{\mathbb{L}} G_{q+1}\), or
3) \(l\) is odd, \(k\) is even, and \(F \simeq_{\mathbb{L}} G_{q+r}\), or
4) \(l = 3\) and \(F \simeq_{\mathbb{L}} \kappa\).

We have the following clarifications for the statement of the theorem.

- The equivalence relation \(\simeq_{\mathbb{L}}\) is introduced by the natural action of GL(2, \(\mathbb{L}\)) over the univariate notation with a suitable identification of the vector spaces.
- The biprojective maps \(G_s : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}\) with \(s \in \{q + 1, q + r\}\) are the so-called Gold maps \(X \mapsto X^s\) in the univariate notation with a suitable identification of the vector spaces.
- The Gold maps \(G_{2^l(2^{k+1})}\) over \(\mathbb{L} \times \mathbb{L}\) are APN whenever \(\gcd(j, 2l) = 1\) by [5]. APN Gold maps over \(\mathbb{L} \times \mathbb{L}\) are not CCZ-equivalent to permutations by [6]. Thus, a \((q, q)\)-biprojective APN function \(F\) over \(\mathbb{L} \times \mathbb{L}\) is CCZ-equivalent to a permutation if and only if \(l = 3\) and \(F \simeq_{\mathbb{L}} \kappa\).
- The special case \(k = 1\) was solved in [7] using results from [8], [9], and [10]. Thus, our theorem generalizes the main results of [7], [8], [9], and [10].
- The so-called Kim function \(\kappa : \mathbb{F}_{2^6} \rightarrow \mathbb{F}_{2^6}\) is the only known APN function on an even dimensional \(\mathbb{F}_2\)-vector space that is CCZ-equivalent to a permutation (up to CCZ-equivalence) as shown in [2]. It is defined by \(\kappa : X \mapsto X^3 + X^{10} + UXX^{24}\) where \(U \in \mathbb{F}_{2^6}\) satisfies \(U^6 + U^4 + U^3 + U = 1\).
- In the literature, another idea that was used to attack the problem (partially) was to identify a class of functions (a) that includes \(\kappa\) when \(l = 3\) and (b) that are CCZ-equivalent to permutations for larger \(l\). This is the case of the so-called butterfly construction [11] which requires \(l\) to be odd. In [12] and [13], butterflies were shown not to be APN when \(l > 3\). We will show in Remark 20 that a subcase of our Proposition 18 (which is a subcase of the main theorem) strictly generalizes the butterfly construction. Thus, our theorem also generalizes the main results of [12] and [13].
• The proof is based on three concepts:
  – zeroes of projective polynomials [14],
  – properties of Dillon-Dobbertin difference sets [15], and
  – recent classification of fractional projective permutations over finite fields [16].
• The proof avoids the use of Weil bound and is purely combinatorial.

The natural actions of the groups \( \text{GL}(2, \mathbb{L}) \times \text{GL}(2, \mathbb{L}) \) (left and right application of non-singular \( \mathbb{L} \)-linear transformations) and \( (\mathbb{L}^x \times \mathbb{L}^x) \times \text{GL}(2, \mathbb{L}) \) (scaling on both components and right application of non-singular \( \mathbb{L} \)-linear transformations) on bivariate vectorial Boolean functions of type

\[
F : \mathbb{L} \times \mathbb{L} \to \mathbb{L} \times \mathbb{L}
\]

and the action of \( \mathbb{L}^x \times \text{GL}(2, \mathbb{L}) \) on bivariate vectorial Boolean functions of type

\[
f : \mathbb{L} \times \mathbb{L} \to \mathbb{L}
\]

are important for this paper. The set of \((q, q')\)-biprojective functions is fixed (setwise) by the action \( (\mathbb{L}^x \times \mathbb{L}^x) \times \text{GL}(2, \mathbb{L})\) (actually, \((q, q')\)-biprojectivity is defined in such a way to accommodate this property). This and other niceties introduced by \( \text{PGL}(2, \mathbb{L}) \) on \( q \)-projective functions allows one to prove the rather straightforward fact [17, Lemma 3.6] that whether these functions are APN can be checked in a simple way using parametrization from \( \mathbb{P}^1(\mathbb{L}) \) instead of \( \mathbb{L} \times \mathbb{L} \) which also hints why we have many such families. A method to find new biprojective APN families was given as well in [17, Lemma 4.2] along with two biprojective APN families. These group actions and biprojectivity were instrumental in giving a method (in joint works with Lukas Kölsch) to check equivalences between biprojective APN functions [18, Theorem 3] and isomorphisms between biprojective semifields [19, Theorem 5.10], which leads to the solution of the equivalence problem for all biprojective APN families and, in the semifields case, generalizing a result of Albert [20] to give a solution to a 60-year old problem of Hughes [21] on determining the autotopism group of Knuth semifields [22]. The first ever family of commutative semifields of odd order that contains an exponential number of non-isotropic semifields [19, Corollary 6.4], and a family containing an exponential number of inequivalent APN functions [18, Theorem 5] were given recently using this method. In the case of APN functions, Kaspers and Zhou were the first [23] to prove such a result with a different method. They showed that the Taniguchi family [24], which is also \((q, q')\)-biprojective, contains an exponential number of inequivalent APN functions. In the \((q, q)\)-biprojective case, even the larger action \( \text{GL}(2, \mathbb{L}) \times \text{GL}(2, \mathbb{L}) \) fixes the set of \((q, q)\)-biprojective functions (setwise). This fact can be seen as the main reason that the classification in this paper is possible which we will heavily exploit (see Section III ff.) together with the above mentioned properties introduced by these classical groups on \((q, q)\)-biprojective functions. Note that these are natural and well-known group actions which were used previously on \((1, q)\)-biprojective semifields [25], [26].

Of course, the study of bivariate functions and semifields (not necessarily biprojective) has a long history. In the case of semifields, the bivariate idea dates back almost a century to Dickson [27], Hughes and Kleinfeld [28] and Knuth [29]. For the APN functions, the initial work on bivariate functions was by Carlet [30] who found the first biprojective APN family, and then Zhou and Pott [31] introduced another family of biprojective APN functions as well as a family of commutative semifields that contains a quadratic number of inequivalent members. Carlet, then introduced [32] a method to find bivariate (but not necessarily biprojective) APN functions from his previous biprojective family. Further work on biprojective APN functions includes the family of Taniguchi [24], and quite recently the papers [33], [34] which derive both biprojective and non-biprojective APN families from the family of [17] (or by extending it). The method of [32] was further investigated in [35]. Further work that do not involve constructions of bivariate functions but study their important properties include [36], [37], [38], [39].

In Section II we will explain the notions related to vectorial Boolean functions, including the definitions of biprojective functions, Dembowski-Ostrom polynomials and APN functions that we mentioned in Introduction. In Section III we will explain the various actions we introduced above (and more) on vectorial functions and the corresponding equivalence relations including \( \approx_{\text{CCZ}} \) and \( \equiv_{\text{G}} \) mentioned above. We also determine the equivalence classes of one of these actions. This will give us a representative set of biprojective functions that will reduce the problem of classification of all biprojective functions to the problem of classification of functions in the representative set. Section IV contains results required in the proof of the main theorem related to zeroes of projective polynomials, Dillon-Dobbertin difference sets and the recent classification of fractional projective permutations over finite fields. Finally, in Section V, we prove our main theorem.

A. A Guide to the Proof

• We first introduce three group actions and their equivalence relations \( \sim_{\text{GR}} , \sim_{\text{G}} , \approx_{\text{C}} \).
• We determine equivalence classes of \( \sim_{\text{GR}} \) and a set \( S_{q,L} \) of representatives from these equivalence classes. This simplifies the classification of \((q, q)\)-biprojective APN functions under \( \approx_{\text{G}} \). These are done in Section III.
• We analyze the representatives in \( S_{q,L} \) case by case. One of the cases, which includes \( \kappa \)-function, requires extra care. This is addressed in Section IV-A using techniques related to roots of \( q \)-projective polynomials and Dillon-Dobbertin difference sets.
• In the even \( l \) case, the recent classification of fractional \( q \)-projective permutations [16] almost immediately implies the rest of the current classification problem on APN functions.
• In the odd \( l \) case, the proof is more complicated. We again use the group actions to deduce the rest of the classification. These are done in Section V.
II. PRELIMINARIES

Let $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ be a vectorial Boolean function. A function $F$ is said to be almost perfect nonlinear (APN) if

$$F(x) + F(x + a) = b$$

has zero or two solutions for every $(a, b) \in \mathbb{F}_2^n \setminus \{0\} \times \mathbb{F}_2^n$. Every vectorial Boolean function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ can be written as an evaluation function of a polynomial over $\mathbb{F}_2^n[X]$ with (polynomial) degree at most $2^n - 1$, i.e., $F : X \mapsto F(X)$ where

$$F(X) = \sum_{i=0}^{2^n-1} A_i X^i.$$  

We will not make distinction between functions and their polynomial representations. The algebraic degree of a vectorial Boolean function is defined to be

$$\deg_{\text{alg}}(F) = \max\{ wt_2(i) \ A_i \neq 0 \},$$

where $wt_2$ denotes the weight of base-2 representation of an integer. When we say quadratic, affine or linear, we refer to this notion of degree. We will need the usual polynomial degree as well which will be denoted by

$$\deg(F) = \max\{ i \ A_i \neq 0 \}$$

as usual. The polynomials in $\mathbb{F}_2^n[X]$ that correspond to affine functions are

$$M(X) = \sum_{0 \leq i \leq n-1} C_i X^{2^i} + D.$$  

If $D = 0$, they are called linear functions and are $\mathbb{F}_2$-linear vector-space endomorphisms of $\mathbb{F}_2^n$ when viewed as a $\mathbb{F}_2$-vector space. As polynomials in $\mathbb{F}_2^n[X]$, they are known as linearized polynomials. We are particularly interested in the class of quadratic polynomials in $\mathbb{F}_2^n$, namely

$$Q(X) = \sum_{0 \leq i < j \leq n-1} B_{ij} X^{2^{i+j}} + \sum_{0 \leq i \leq n-1} C_i X^{2^i} + D.$$  

The subclass of the above class of polynomials that contains only the non-affine parts is known as Dembowski-Ostrom (DO) polynomials, i.e.,

$$D(X) = \sum_{0 \leq i \neq j \leq n-1} B_{ij} X^{2^{i+j}}.$$  

When $n = 2l$, a further subclass of DO polynomials is important. The class of polynomials

$$R(X) = AX^{q+1} + BX^{d(q+1)} + CX^{q+2^l} + DX^{2q+1},$$

where $q = 2^k$ with $0 < k < l$, satisfying the subfield property

$$R(aX) = a^{q+1}R(X), \quad \text{for all } a \in \mathbb{F}_{2^l},$$

contains (up to CCZ-equivalence) the only known APN function $\kappa$ that is CCZ-equivalent to a permutation for even $n$ (we will describe various notions of equivalences of vectorial Boolean functions further below). Let $L = \mathbb{F}_{2^l}$. Identifying $\mathbb{F}_2^{2^l} = \mathbb{L}(\xi) = \mathbb{L}^\xi + \mathbb{L} \cong \mathbb{L} \times \mathbb{L}$, we can write the above class of functions $X \mapsto R(X)$ as $(x, y) \mapsto R(x, y)$ with

$$R(x, y) = \left( (a_0 x^{q+1} + b_0 x^{d(q+1)} + c_0 y^{q+1}), (a_1 x^{q+1} + b_1 x^{d(q+1)} + c_1 y^{q+1} + d_1 y^{q+1}) \right) = (f(x, y), g(x, y))$$

where $X = (x, y)$. This motivates the following definition.

**Definition 2:** Let $q = 2^k$ with $0 < k < l$.

- Let $f \in \mathbb{L}[x, y]$ be a polynomial of the form
  $$f(x, y) = a_0 x^{q+1} + b_0 x^{d(q+1)} + c_0 y^{q+1} + d_0 y^{q+1}.$$  

Then $f$ is called a $q$-biprojective polynomial.

- Let $R : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}$ be a function of the form
  $$R : (x, y) \mapsto R(x, y) = (f(x, y), g(x, y))$$

where $f$ and $g$ are $q$-biprojective polynomials. Then $R$ is called a $(q, q')$-biprojective function.

We will use the shorthand notation

$$f = (a_0, b_0, c_0, d_0)_q,$$

and

$$R = ((a_0, b_0, c_0, d_0)_q, (a_1, b_1, c_1, d_1)_q) = (f, g).$$

The subfield property can be recognized in this form. For a $(q, q')$-biprojective map $F = (f, g)$, one has

$$(f(cx, cy), g(cx, cy)) = c^{q+1}f(x, y), g(y)),$$

for all $c, x, y \in \mathbb{L}$.

**Remark 3:** One can generalize the concept to $(q, q')$-biprojective functions

$$F : (x, y) \mapsto F(x, y) = ((a_0, b_0, c_0, d_0)_q, (a_1, b_1, c_1, d_1)_q')$$

where $q' = 2^{k'}$ (here one allows $0 \leq k, k' < l$). These functions satisfy a modified form of the subfield property

$$(f(cx, cy), g(cx, cy)) = c^{q+1}f(x, c^{q'}g(y)),$$

for all $c, x, y \in \mathbb{L}$. In this paper, we are only interested in $(q, q)$-biprojective functions. See [17] and [18] for more on $(q, q')$-biprojective APN functions and their constructions, equivalences and enumerations.

Define

$$D_0^0(x, y) = b_0 x^q + c_0 x + d_0 y^q + d_0 y,$$

$$D_0^\infty(x, y) = a_0 x^q + a_0 x + c_0 y^q + b_0 y,$$

$$D_0^1(x, y) = (a_0 u + b_0) x^q + (a_0 u^q + c_0)x + (c_0 u + d_0) y^q + (b_0 u^q + d_0) y,$$

for $u \in \mathbb{L}^\times$. The following lemma was proved in [17].

**Lemma 4:** Let $F = (f, g)$ be a $(q, q')$-biprojective function. Then $F$ is APN if and only if $D_0^1(x, y) = 0 = D_0^u(x, y)$ has exactly two solutions for each $u \in \mathbb{P}^1(\mathbb{L})$.  

A. The Trace Map and Hilbert’s Theorem 90

Let \( \mathbb{L} \) be the finite field with \( p^l \) elements, \( q = p^k \) for \( k > 0 \) and let \( \mathbb{D} \subset \mathbb{L} \) of order \( p^d \) with \( \delta = \gcd(l, k) \). The trace map is defined as

\[
\text{tr}_{\mathbb{L}/\mathbb{D}}(x) = \sum_{j=0}^{l/\delta-1} x^{(p^d)^j}.
\]

When \( \mathbb{D} = \mathbb{F}_p \) then we simply write

\[
\text{tr}(x) = \text{tr}_{\mathbb{L}/\mathbb{F}_p}(x).
\]

The following is the finite fields version of Hilbert’s Theorem 90.

Lemma 5 (Hilbert’s Theorem 90): Let \( \gcd(j, l) = 1 \) and \( a \in \mathbb{L} \). Then \( \text{tr}_{\mathbb{L}/\mathbb{D}}(a) = 0 \) if and only if \( a = x^{(p^d)^j} - x \) for some \( x \in \mathbb{L} \).

The \( \mathbb{D} \)-linear vector-space endomorphisms of \( \mathbb{L} \) can be written as

\[
L(x) = \sum_{j=0}^{l/\delta-1} a_j x^{(p^d)^j}, \quad a_j \in \mathbb{L},
\]

and are called \( \mathbb{D} \)-linearized polynomials. Determining kernels of such endomorphisms in \( \mathbb{L} \), especially of the form \( L(x) = ax^q - bx \) and the zeroes of its translates \( L(x) + c \), is important for this paper. This can simply be done by observing

\[
ax^q - bx = 0
\]

for some nonzero \( r \in \mathbb{L} \) if and only if \( r^{q-1} = b/a \). In that case \( L(rx)/rb = x^q - x \).

Then one can deduce that the zeroes of \( L(x) \) are 0 and \( er \) for \( e \in \mathbb{D}^\times \) if such \( r \) exists. Then the case \( L(x) + c \) can be handled using Hilbert’s Theorem 90. The following lemma is relevant and will be needed.

Lemma 6: For a prime \( p \),

i) \( \gcd(p^k - 1, p^l - 1) = p^{\gcd(k, l)} - 1 \).

ii)

\[
\gcd(p^k + 1, p^l - 1) = \begin{cases} 1 & \text{if } \gcd(k, l) \text{ is odd and } p = 2, \\ 2 & \text{if } \gcd(k, l) \text{ is odd and } p \text{ is odd,} \\ p^{\gcd(k, l)} + 1 & \text{if } \gcd(k, l) \text{ is even.} \end{cases}
\]

B. Difference Sets With Singer Parameters and Multisets

Let \( M \) be a multiset whose elements are \( s_i \) with repetition \( d_i \) for \( 1 \leq i \leq r \), denoted by

\[
M = \{ s_1^{d_1}, \ldots, s_r^{d_r} \},
\]

where we write \( \text{mult}_M(s_i) = d_i \). When all \( s_i \) have the same repetition number \( d \), we write \( M = S[d] \), where \( S = \{ s_1, \ldots, s_r \} \).

For two multisets \( S, T \) we denote by

\[
S/T = \{ s/t \mid s \in S, t \in T \}
\]

the direct division of two multisets.

A subset \( D \) of cardinality \( k \) of a group \( G \) (written multiplicatively) of order \( v \) is said to be a \((v, k, \lambda)\)-difference set if

\[
D/D = \{ 1 \}^k \cup (G \setminus \{ 1 \})^\lambda.
\]

We are mostly interested in the cyclic difference sets in the multiplicative group \( \mathbb{L}^\times \) in characteristic 2. The parameters \( (2^l - 1, 2^l - 1, 2^l - 1 - 2^l - 2) \) and \( (2^l - 1, 2^l - 1 - 2^l - 2) \) are called Singer parameters, since they are the parameters of the Singer sets (i.e., hyperplanes of \( \mathbb{L} \)),

\[
\mathcal{H} = \{ x \in \mathbb{L} \mid \text{tr} (x) = 1 \},
\]

and \( \mathcal{H} \setminus \{ 0 \} \) where

\[
\mathcal{H} = \{ x \in \mathbb{L} \mid \text{tr} (x) = 0 \},
\]

respectively. Dillon-Dobbertin difference sets are another important example of cyclic difference sets with Singer parameters [15] (see Lemmas 13, 15) which we will use frequently in this paper.

C. Equivalences of Vectorial Boolean Functions

Let \( F : \mathbb{F} \to \mathbb{F} \) be a vectorial Boolean function and \( \mathbb{F} = \mathbb{F}_2^n \). The widest known notion of equivalence that keeps the APN property invariant is called the CCZ-equivalence [40]. Define the graph of the function \( F \) by

\[
\Gamma_F = \{ (x, F(x)) \mid x \in \mathbb{F} \}.
\]

Then \( F \) is said to be CCZ-equivalent to \( F' \) if there exists \( \mathbb{F}_2 \)-linear endomorphisms \( A, B, C, D \) of \( \mathbb{F} \), elements \( u, v \in \mathbb{F} \) and a permutation \( \pi : \mathbb{F} \to \mathbb{F} \) such that

\[
\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} x \\ F(x) \end{pmatrix} + \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} \pi(x) \\ F'(\pi(x)) \end{pmatrix}.
\]

In that case we write \( F \approx_{\text{CCZ}} F' \). A narrower notion of equivalence that keeps the algebraic degree of \( F \) invariant is called the extended affine (EA) equivalence. We write \( F \approx_{\text{EA}} F' \) if

\[
A_1 \circ F \circ A_2(x) + A_3(x) = F'(x),
\]

for affine maps \( A_1, A_2, A_3 : \mathbb{F} \to \mathbb{F} \) with \( A_1, A_2 \) bijective. It can easily be shown that EA-equivalence is a special case of CCZ-equivalence where one sets \( B = 0 \). An important theorem for quadratic APN functions is that for two quadratic APN functions \( F, G \) we have by a result of Yoshiara [41],

\[
F \approx_{\text{EA}} G \iff F \approx_{\text{CCZ}} G.
\]

We can restrict the equivalence even more if, for instance, we want to keep the property of being a permutation invariant. The functions \( F \) and \( F' \) are said to be linearly equivalent if

\[
L_1 \circ F \circ L_2 = F',
\]

for \( L_1, L_2 \in \text{GL}(n, 2) \). Note that this is equivalent to setting \( B = C = 0 \) and \( u = v = 0 \) in (2) (when only \( B = C = 0 \) holds, they are called affinely equivalent). We denote this equivalence by \( F \approx_{\text{GL}(n, 2)} F' \). In the following, we will even restrict this equivalence to the case where \( L_1, L_2 \in \text{GL}(2, 2^l) < \text{GL}(2l, 2) \) when \( n = 2l \) with the obvious
motivation that the (left and right) action of $\text{GL}(2, 2^l)$ keeps the $(q,q)$-biprojective property of $F(x,y) = (f(x,y), g(x,y))$ invariant.

III. ACTIONS OF $\text{GL}(2, L)$ AND $\text{PGL}(2, L)$

In this section we outline the basics of several actions of $\text{GL}(2, L)$ and $\text{PGL}(2, L)$ on biprojective functions. Most of this section can be considered standard. Let

$$V_{q,L} = \{(a, b, c, d)_q \mid a, b, c, d \in L\},$$

be the set of all $q$-biprojective polynomials. Let $f, g \in V_{q,L}$ be two $q$-biprojective polynomials and

$$F : L \times L \rightarrow L \times L$$

$$(x, y) \mapsto (f(x,y), g(x,y))$$

be the associated $(q,q)$-biprojective function. Define $\mathcal{F}_{q,L}$ to be the set of all $(q,q)$-biprojective functions, i.e.,

$$\mathcal{F}_{q,L} = V_{q,L} \times V_{q,L}.$$

Let $\mathcal{L}(L)$ be the group of all nonsingular $L$-linear transformations of $L \times L$, i.e.,

$$\text{GL}(2, L) \cong \mathcal{L}(L) = \{(x, y) \mapsto (tx + uy, vx + wy) : t, u, v, w \in L \mid tw - uv \neq 0\}.$$

We are mainly interested in the standard action of $\text{GL}(2, L) \times \text{GL}(2, L)$ on $(q,q)$-biprojective functions $F \in \mathcal{F}_{q,L}$. That is

$$F'(x, y) = L_1 \circ F \circ L_2(x, y).$$

This action defines an equivalence relation which we denote by $F' \approx_L F$. Define also the action of the group $L^\times \times \text{GL}(2, L)$ on $q$-biprojective polynomials $f \in V_{q,L}$ where $L^\times < \text{GL}(2, L)$ acts on $f$ by scaling, and the action of $\text{GL}(2, L)$ is the usual right action, i.e.,

$$f'(x, y) = \alpha(f \circ L(x, y)),$$

$$= \alpha(a(tx + uy)^{q+1} + b(tx + uy)^q(vx + wy) + c(tx + uy)(vx + wy)^q + d(vx + wy)^{q+1}),$$

where $(\alpha, L) \in L^\times \times \text{GL}(2, L)$. In this case we say that $f \approx_L f'$.

Set $\phi_f(x) = f(x, 1)$. A polynomial $\phi_f \in L[x]$ for $f \in V_{q,L}$ is called a $q$-projective polynomial. The projective version of the above action on the bivariate $q$-projective polynomial $f$, on the univariate $q$-projective polynomial $\phi_f$ can be given using the fractional linear (Möbius) transformations over the finite field $L$, i.e.,

$$\text{PGL}(2, L) \cong \mathcal{M}(L) = \left\{ x \mapsto \frac{tx + u}{wx + w} : t, u, v, w \in L \mid tw - uv \neq 0 \right\}.$$

Now, define the action

$$\phi_{f'}(x) = \alpha(xw + w)^{q+1}(\phi_f \circ \mu(x)),$$

for $(\alpha, \mu) \in L^\times \times \text{PGL}(2, L)$ and $\mu : x \mapsto \frac{tx + u}{wx + w}$. One addresses the zero of the denominator $(vx + w)$ by introducing $\infty = \beta/0$ for all $\beta \in L^\times$. We define $\mathbb{P}^1(L) = \mathbb{L} \cup \{\infty\}$. By defining $\mu(\infty) = t/v$, we see that all $\mu \in \mathcal{M}(L)$ permutes $\mathbb{P}^1(L)$. Note that we view the action as

$$\phi_{f'}(x) = \alpha(a(tx + u)^{q+1} + b(tx + u)^q(vx + w) + c(tx + u)(vx + w)^q + d(vx + w)^{q+1}),$$

so that $\phi_{f'}$ is a $(q$-projective) polynomial over $L[x]$ and we do not have to deal with $\infty$ (but we will do that later, since it is helpful). We write $\phi_f \sim_{\mathcal{M}} \phi_{f'}$. The following lemma is straightforward.

Lemma 7: We have $f \sim_{\mathcal{L}} f'$ if and only if $\phi_f \sim_{\mathcal{M}} \phi_{f'}$. We will not use $\phi_f$ to refer to univariate $q$-projective version of $f$ and instead use $f$ for both univariate and bivariate functions and polynomials. We will also use $V_{q,L}$ as the ambient space of both types of functions/polyomials.

Our aim is to classify the APN functions in $\mathcal{F}_{q,L}$ under the equivalence $\approx_{\mathcal{L}}$. We say that $\mathcal{S}_{q,L} \subseteq V_{q,L}$ is a representative set of $V_{q,L}$ if (denoting by $[f]_{\approx}$ the equivalence class of $f$ under $\approx$)$\mathcal{S}_{q,L} \sim_{\mathcal{L}} \bigcup_{f \in \mathcal{S}_{q,L}} [f]_{\approx} = V_{q,L}$.

In the following we will find a representative set $\mathcal{S}_{q,L}$ using univariate $q$-projective polynomials and their equivalence $\sim_{\mathcal{M}}$. Then it will be clear that checking $(f,g) \in \mathcal{S}_{q,L} \times V_{q,L}$ is enough for our classification under $\approx_{\mathcal{L}}$ since $f \sim_{\mathcal{L}} f'$ if and only if $f \sim_{\mathcal{L}} f'$.

Let $q = p^k$, $D = F_{p^k}$, $L = F_{p^l}$ where $\delta = \text{gcd}(k, l)$ and

$$f(x) = ax^{q+1} + bx^q + cx + d$$

be a nonzero $q$-projective polynomial. If $a = 0$, then $f$ is an affine polynomial and the set of zeroes of $f$ in $L$, i.e.,

$$Z_f \in \{x \in \mathbb{L} \mid f(x) = 0\}$$

satisfies $|Z_f| \in \{0, 1, p^3\}$. To see that, first observe that scaling, i.e., $f \mapsto \alpha f$ for $\alpha \in L^\times$, the translations $f(x) \mapsto f(x + \beta)$ for $\beta \in L$ and the dilations $f(x) \mapsto f(\gamma x)$ for $\gamma \in L^\times$ keep the number of zeroes of $f$ in $L$ invariant. Then we have only a few options to consider:

- **f = 1** has no $L$-zeroes—degenerate case (together with omitted $f = 0$).
- $f \in \{x, x^q\}$ has one $L$-zero.
- $f = x^q - cx - d$ where $c \neq 0$.

We have

- if $c = A^{q-1} \in \mathbb{L}^\times$, then $f$ has $p^3$ $L$-zeroes if $\text{tr}_{L/D}(d/A^{q}) = 0$, and
- no $L$-zeroes if $\text{tr}_{L/D}(d/A^{q}) \neq 0$; or
- one $L$-zero if $c \notin (\mathbb{L}^\times)^{q-1}$,

by Hilbert’s Theorem 90.
Now assume $a \neq 0$. We will show that $|Z'_f| \in \{0, 1, 2, p^3 + 1\}$. Assume $f$ has at least one $\mathbb{L}$-zero $r \in Z'_f$. Now consider
\[ f'(x) = f(x + r) = ax^{q+1} + b'x + c'x. \]
The reciprocal $f''(x) = x^{q+1}f'(1/x)$ is
\[ f''(x) = a + b'x + c'x^q, \]
where $\deg f'' < q + 1$. Now $f''$ has one fewer $\mathbb{L}$-zeroes than $f'$ (since we punctured the zero of $f'$ at 0) and thus we have
\[ |Z''_{f''}| + 1 = |Z'_{f''}| = |Z'_f| \in \{1, 2, p^3 + 1\}. \]

When $f$ has no $\mathbb{L}$-zeroes, it can easily be seen that translations, dilations, reciprocation and scaling cannot make the first or the last coefficient zero. Blumer proved the existence of $f$ with no $\mathbb{L}$-zeroes [14, Theorem 5.6] for every parameter set where she gave exact enumeration results for the important subclass of $q$-projective polynomials of the form $x^{q+1} + x + a$. Therefore, in the general case (including $f$ has no $\mathbb{L}$-zeroes),
\[ |Z'_f| \in \{0, 1, 2, p^3 + 1\}. \]

This observation, together with the fact that $\text{PGL}(2, \mathbb{L})$ is generated by translations, dilations, reciprocation and inversions (for which the corresponding action is reciprocation), motivates us to ascribe $f(\infty) = 0$ if and only if $\deg f < q + 1$ so that $\sim_{\mathbb{M}}$ preserves the number of roots in $\mathbb{P}^1(\mathbb{L})$. Now we can define

**Definition 8:** The **$\mathbb{P}^1(\mathbb{L})$-zeroes** of a $q$-projective polynomial $f$ is defined as
\[ Z_f = \{x \in \mathbb{P}^1(\mathbb{L}) : f(x) = 0\}, \]
where we define $f(\infty) = 0$ if and only if $\deg f < q + 1$.

Thus we have

**Lemma 9:** Let $f \neq 0$ be a $q$-projective polynomial. Then,
\[ i) |Z_f| \text{ is invariant under } \sim_{\mathbb{M}}, \]
\[ ii) |Z_f| \in \{0, 1, 2, p^3 + 1\}. \]

**Proof:** Part (ii) is explained before the lemma. We will give a more detailed proof of Part (i) which, actually, also follows from the previous discussion.

Let $f' \sim_{\mathbb{M}} f$ via $(a, \mu) \in \mathbb{L}^\times \times \text{PGL}(2, \mathbb{L})$ with $\mu : x \mapsto \frac{tx + u}{t'x + u}$. Suppose $v \neq 0$. Define $T = \mathbb{L} \setminus \{w/v\}$, which satisfies $\mu(T) = \mathbb{L} \setminus \{t/v\}$. We see by (3) that $x \in T$ is a zero of $f' \iff \mu(x)$ is a zero of $f$.

By (4), we get $a = 0$ if and only if
\[ w/v = \mu^{-1}(\infty) \text{ is a zero of } f' \iff \infty \text{ is a zero of } f \]
if and only if $\deg f < q + 1$. Also by (4), since the coefficient of the $x^{q+1}$ term of $f'$ is $a't^{q+1} + b'tv + c'tv^q + dv'^{q+1} = v^{q+1}f(t/v)$, we have
\[ t/v = \mu(\infty) \text{ is a zero of } f \iff \infty \text{ is a zero of } f' \]
if and only if $\deg f' < q + 1$. Combining the three cases we get $\mu(Z_{f'}) = Z_f$ and $|Z_f| = |Z_{f'}|$. These facts also trivially follow when $v = 0$. □

Define the sets (suppressing $q$ and $\mathbb{L}$ from the notation for simplicity),
\[ D_0 = \{(0, 0, 0, 0)_q\}, \]
\[ D_1 = \{(0, 0, 0, 1)_q\} \sim_{\mathbb{M}}, \]
\[ D = D_1 \cup D_1, \]
\[ \Pi_j = \{f \in \nu_{\mathbb{L}} \setminus D : |Z_f| = j\}, \]
for $j \in \{0, 1, 2, p^3 + 1\}$.

In the following we will show that $\Pi_i$, for several $i \in \{0, 1, 2, p^3 + 1\}$, has only one equivalence class under $\sim_{\mathbb{M}}$, that is to say, if $f, g \in \Pi_i$, then $f \sim_{\mathbb{M}} g$. Recall that an action of a group $G$ on a set $S$ determines an equivalence relation $\sim$ on the elements of $S$, partitioning $S$ into equivalence classes. The action of $G$ is said to be **transitive** on $S$ if there is only one equivalence class of $\sim$ in $S$ (or equivalently, every $s \in S$ is mapped to $t \in S$ by some $g \in G$).

**Lemma 10:** We have
\[ i) \nu_{\mathbb{L}} = \bigcup_{i \in \{0, 1, 2, p^3 + 1\}} \Pi_i \cup D, \]
\[ ii) \Pi_1 = \{(0, 1, 1, 0)_q\} \sim_{\mathbb{M}} \text{ where } u \in \mathbb{L} \text{ satisfies } \text{tr}_{\mathbb{L}/\mathbb{D}}(u) = 1, \]
\[ iii) \Pi_{p^3 + 1} = \{(0, 1, 1, 0)_q\} \sim_{\mathbb{M}}. \]

**Proof:** The proof of Part (i) follows from the discussion before the lemma. For Parts (ii) and (iii), we have to show that the action is transitive on the sets $\Pi_i$ and $\Pi_{p^3 + 1}$. If $a \neq 0$, as in the discussion before the lemma, using $f'(x) = f(x + r)$ first, where $r$ is an $\mathbb{L}$-zero of $f$, and then using the reciprocal $f''(x) = x^{q+1}f'(1/x)$, one shows that $f \sim_{\mathbb{M}} f''$ with $\deg f'' < q + 1$. Now in both $p^3 + 1$ and one $\mathbb{P}^1(\mathbb{L})$-root cases, $f''$ has the form
\[ f''(x) = a + b'x + c'x^q, \]
with $-b'/c' = A_{q-1}$ for some $A \in \mathbb{L}^\times$. One can apply $x \mapsto xA$ and then scale to get $f'' \sim_{\mathbb{M}} x^q - x - d$ for some $d \in \mathbb{L}$, where $f$ has $p^3 + 1$ $\mathbb{P}^1(\mathbb{L})$-roots if and only if $\text{tr}_{\mathbb{L}/\mathbb{D}}(d) = 0$ and $f$ has one $\mathbb{P}^1(\mathbb{L})$-root if and only if $\text{tr}_{\mathbb{L}/\mathbb{D}}(d) \neq 0$ by Hilbert's Theorem 90, and the action is transitive on $\Pi_{p^3 + 1}$ since any $d$ with $\text{tr}_{\mathbb{L}/\mathbb{D}}(d) = 0$ can be written as $z^q - z = d$ for some $z \in \mathbb{L}$ and $f \sim_{\mathbb{M}} x^q - x$ after the application of $x \mapsto x + z$.

For the case $\text{tr}_{\mathbb{L}/\mathbb{D}}(d) \neq 0$, applying $x \mapsto cx$ where $c \in \mathbb{D}^\times$, and scaling by $1/c$, one can assume $\text{tr}_{\mathbb{L}/\mathbb{D}}(d) = 1$. Then the transitivity of the action follows again by translations. □

When $\gcd(p^k - 1, p^l - 1) = 1$, that is to say $\gcd(k, l) = 1$ and $p = 2$ by Lemma 6, we can say more.

**Lemma 11:** Let $p = 2, q = 2^k$, and $\delta = \gcd(k, l) = 1$. Then we have the following facts.
\[ i) \Pi_0 = \{g\} \sim_{\mathbb{M}}, \text{ for every fixed } g \in \Pi_0. \]
\[ ii) \Pi_2 = \{(0, 0, 1, 0)_q\} \sim_{\mathbb{M}}. \]
\[ iii) \text{If } l \text{ is odd, then } a) \Pi_1 = \{(1, 0, 0, 1)_q\} \sim_{\mathbb{M}}. \]
\[ iv) \text{If } l \text{ is even, then } a) \Pi_0 = \{(1, 0, 0, 1)_q\} \sim_{\mathbb{M}}, \]
\[ b) \Pi_2 = \{(1, 0, 1, 0)_q\} \sim_{\mathbb{M}}. \]

**Proof:**
\[ i) \text{This was proved in } \bullet [42, \text{Theorem 2.1}] \text{ when } l \text{ is even, and } \bullet [18, \text{Lemma 7}] \text{ for general } l. \]
We can now state the representative set $S_{q,l}$ we will use.

**Lemma 12**: Let $p = 2, q = 2^k, \delta = \gcd(k,l) = 1$, and

$S = \{(0, 0, 0, 0)q, (0, 0, 0, 1)q, (0, 0, 1, 0)q\}$

$\cup \{(1, 0, 0, a)q, a \in \mathbb{L}^\times\}$.

i) If $l$ is odd then

$S_{q,L} = S \cup \{(0, 1, 1, 0)q\} \cup I_0$.

ii) If $l$ is even then

$S_{q,L} = S \cup I_1$.

Then $S_{q,L}$ is a representative set for $V_{q,L}$.

**IV. FURTHER LEMMAS**

In this section we will give the results that are needed in the classification.

**A. The Zeroes of $x^{q+1} + x + b$**

Now we are going to restrict ourselves to a specific type of $q$-projective polynomials, namely

$P_b(x) = x^{q+1} + x + b$,

for $b \in \mathbb{L}$. Bluher studied these polynomials [14] and determined the cardinalities of the sets

$I_j = \{b \in \mathbb{L} \mid P_b \in I_j\}$,

where $j \in \{0, 1, 2, 3^p + 1\}$. In this section we are interested only in the $p = 2$ case and $\gcd(k,l) = 1$ where $\mathbb{L} = \mathbb{F}_{2^l}$ and $q = 2^k$. In the definitions of $I_j$ and $P_b$ (along with the previously defined sets) we suppress $q$ and $\mathbb{L}$ for notational simplicity.

The following is an important result on combinatorics of finite fields proved by Dillon and Dobbertin [15].

**Lemma 13**: Let $q = 2^k$ and $\gcd(k,l) = 1$. The set $I_1$ is a

i) $(2^l - 1, 2^{l-1} - 1, 2^{l-2} - 1)$-difference set in $\mathbb{L}^\times$ if $l$ is odd, and

ii) $(2^l - 1, 2^{l-1}, 2^{l-2})$-difference set in $\mathbb{L}^\times$ if $l$ is even.

**Proof**: Let $d = 4^k - 2^k + 1$ and

$\Delta = \begin{cases} 
\{x^d + (x+1)^d + 1 : x \in \mathbb{L} \setminus \mathbb{F}_2\} & \text{if } l \text{ is odd,} \\
\mathbb{L}^\times \setminus \{x^d + (x+1)^d + 1 : x \in \mathbb{L} \setminus \mathbb{F}_2\} & \text{if } l \text{ is even.}
\end{cases}$

Dillon and Dobbertin showed [15, Theorem A] that $\Delta$ is a difference set with indicated (Singer) parameters.

The fact that $I_1 = 1/\Delta$ was shown in [43, Theorem 1] (see also [16, Theorem 5.13]).

In the next lemma we show that, since $\gcd(2^k - 1, 2^l - 1) = 2^\gcd(k,l) = 1$ and $2^k$, we can easily determine the sets $I_1, I_2$, and $I_3$. The map $\rho$ appears quite frequently when one works with projective polynomials, for instance, in Serre’s proof that $\text{PSL}(2,q)$ is the Galois group of the equation $x^{q+1} - x + b = 0$ for arbitrary prime power $q$ (see [44, pp. 131–132]). The lemma can be found for general $\gcd(k,l)$ and $q = 2^k$ in [43, pp. 175–176]. We provide a simple proof for $\gcd(k,l) = 1$ again in characteristic 2.

**Lemma 14**: Let $q = 2^k, \gcd(k,l) = 1$ and

$\rho : \mathbb{L} \setminus \mathbb{F}_2 \rightarrow \mathbb{L} \setminus \mathbb{F}_2,$

$x \mapsto \frac{x^{q+1}}{(x^q + x)^{q+1}}.$

We have

i) $\rho(x) x \in \mathbb{F}_2 \setminus \mathbb{F}_2 = I_1,$

ii) $\rho(x) x \in \mathbb{H} \setminus \mathbb{F}_2 = I_2,$

iii) $I_2 = \{0\},$

iv) $\rho(x^{q+1} + x x \in \mathbb{L} = I_1 \cup I_2 \cup I_3.$

**Proof**: Let $b \in I_1 \cup I_2 \cup I_3$ and $f = \rho b = x^{q+1} + x + b$.

Let $r \in \mathbb{L}$ be a root of $f$. Then

$f(x + r) = (x + r)^{q+1} + x + r + b$

$= x^{q+1} + r x^q + (r + 1)^q x + r^{q+1} + r + b$

$= x^{q+1} + r x^q + (r + 1)^q x$

$\sim_{\mathbb{L}} (r + 1)^q x^q + r x + 1 = f'(x)$

Then $|Z_f| = 2$ if and only if $|Z_f^r| = 1$ if and only if $r \in \mathbb{F}_2$.

Thus $b = 0$ and Part (iii) follows. Otherwise we have $A \in \mathbb{L}^\times$ such that

$A^{q-1} = \frac{r}{(r + 1)^q},$

since $x \mapsto x^{q-1}$ is bijective on $\mathbb{L}$ by Lemma 6. We have $f \in \Pi_1$ if and only if $\text{tr}(1/Ar) = 1$ and $f \in \Pi_3$ if and only if $\text{tr}(1/Ar) = 0$ by Hilbert’s Theorem 90. Now, let $h \in \mathbb{L}^\times$ satisfy

$\frac{1}{A} = h^q,$

That is to say

$\frac{1}{A} = h^{q-1}$ $\iff$ $\frac{1}{A^{q-1}} = h^{q(q-1)} (r + 1)^{q-1}$ $= \frac{r}{r^{q-1}}.$

Thus, recalling $r \not\in \mathbb{F}_2$,

$h^{q-1} = \frac{r + 1}{r} = 1 + \frac{1}{r}.$

Therefore for each $r \in \mathbb{L} \setminus \mathbb{F}_2$, there is unique $h \in \mathbb{L} \setminus \mathbb{F}_2$, where $h \in \mathbb{H} \setminus \mathbb{F}_2$ if and only if $f \in \Pi_3$ and $h \in \mathbb{H} \setminus \mathbb{F}_2$ if and only if $f \in \Pi_1$. Or, equivalently

$r = \frac{h}{h + h^q}.$
The remaining Parts (i), (ii), (iv) follow after observing
\[ b = x^{q^{r+1}} + r = \left( \frac{h}{h + h^q} \right)^{q^{r+1}} + \frac{h}{h + h^q} \]
\[ = \frac{h^{q^{r+1}} + h(h^{q^r} + h^q)}{(h^q + h)^{q^{r+1}}} \]
\[ = \frac{(h^q + h)^{q^{r+1}+1}}{(h^q + h)^{q^{r+1}}}. \]

The following lemma is key to our classification. It will prove that the Kim function \( \kappa \) exists as a theorem of small cases, using the properties of Dillon-Dobbertin difference sets with Singer parameters.

**Lemma 15:** Let \( l > 3 \), \( q = 2^k \) and \( \gcd(k, l) = 1 \). For all
- \( d \in \mathbb{L}^\times \) if \( l \) is odd, and
- \( d \in \mathbb{L}^\times \setminus (\mathbb{L}^\times)^{q+1} \) if \( l \) is even, we have
\[ dI_3 \cap (I_1 \cup I_2 \cup I_3) \neq \emptyset. \]

**Proof:** By Lemma 14 (iii), \( I_2 = \{0\} \) and therefore \( dI_3 \cap I_2 = \emptyset \). Also the \( d = 1 \) case is clear. Let
\[ M = \frac{I_1 \cup I_3}{I_3^{[3]}}. \]

The claim of the lemma is equivalent to the claim that for all \( d \in \mathbb{L} \setminus \mathbb{F}_2 \),
\[ \text{mult}_M(d) > 0. \]

We have
\[ M = \frac{I_1 \cup I_3}{I_3^{[3]}}, \]
and
\[ J = \frac{I_1 \cup I_3^{[3]}}{I_3 \cup I_3^{[3]}} = \frac{M \cup I_1^{[3]} \cup I_1^{[3]} \cup I_1^{[3]}}{I_1}. \]

It is clear by Lemma 14 (iii) and (iv) that
\[ I_1 \cup I_3^{[3]} = \{ x^{q^{r+1}} + x : x \in \mathbb{L} \setminus \mathbb{F}_2 \}. \]

For \( x, y, d \in \mathbb{L} \setminus \mathbb{F}_2 \), we will find the number of solutions of
\[ \frac{x^{q^{r+1}} + x}{y^{q^{r+1}} + y} = d, \]
which is (for \( y, d \in \mathbb{L} \setminus \mathbb{F}_2 \) and \( x \in \mathbb{L}^\times \setminus \{1/y\} \) the same as the number of solutions of
\[ \frac{(xy)^{q^{r+1}} + xy}{y^{q^{r+1}} + y} = \frac{x^{q^{r+1}}y^q + x}{y^q + 1} = d. \]

Or, equivalently
\[ y^q(x^{q^{r+1}} + d) = (x + d). \]

For all \( x \in \mathbb{L} \setminus \mathbb{F}_2 \) such that \( x^{q^{r+1}} \neq d \) or \( x \neq d \), there exists a (unique) \( y \in \mathbb{L} \setminus \mathbb{F}_2 \). The equality holds when \( x = 1/y \) if and only if \( y^q d = d \), that is to say \( x = y = 1 \).

Thus
\[ \mult_J(d) = \begin{cases} 2^l - 4 & \text{if } l \text{ is odd,} \\ 2^l - 6 & \text{if } l \text{ is even and } d \in (\mathbb{L}^\times)^{q+1}, \\ 2^l - 3 & \text{if } l \text{ is even and } d \in \mathbb{L}^\times \setminus (\mathbb{L}^\times)^{q+1}, \end{cases} \]
since \( \gcd(2^k + 1, 2^l - 1) = 3 \) if \( l \) is even and 1 if \( l \) is odd. Since \( I_3 \) is a difference set with Singer parameters, we have by Lemma 13
\[ \mult_{I_3/I_3}(d) = \begin{cases} 2^l - 2 & \text{if } l \text{ is odd,} \\ 2^l - 2 & \text{if } l \text{ is even.} \end{cases} \]

Since for all \( i \in I_3 \) we have at most one \( j \in I_3 \) since \( I_1 \) is a set by Lemma 14 (i), we have the trivial bound \( \mult_{I_3^{[3]}/I_3}(d) \leq |I_3^{[3]}| \). By Lemma 14 (ii), we have,
\[ \mult_{I_3^{[3]}/I_3}(d) \leq \begin{cases} 2^{l-1} - 1 & \text{if } l \text{ is odd,} \\ 2^{l-1} - 2 & \text{if } l \text{ is even.} \end{cases} \]

Note that by the definition of \( J \), we must have,
\[ \mult_J(d) = \mult_M(d) + \mult_{I_3/I_3}(d) + \mult_{I_3^{[3]}/I_3}(d). \]

Now assume \( \mult_M(d) = 0 \). If \( l \) is odd, this means
\[ 2^l - 4 \leq 0 + 2^{l-2} - 1 + 2^{l-1} - 1, \]
\[ 2^{l-2} \leq 2, \]
which means \( l \leq 3 \). Similarly for \( l \) is even and \( d \in \mathbb{L}^\times \setminus (\mathbb{L}^\times)^{q+1}, \)
\[ 2^l - 3 \leq 0 + 2^{l-2} + 2^{l-1} - 2, \]
\[ 2^{l-2} \leq 1, \]
which means \( l \leq 2 \).

The claim also holds for \( d \in (\mathbb{L}^\times)^{q+1} \) similarly but skipped, since it will not be used and requires computerized check for \( l = 4 \).

**B. Results on Fractional Projective Permutations of \( \mathbb{P}^1(\mathbb{L}) \)**

Given two \( q \)-projective polynomials \( f(x, 1) \), \( g(x, 1) \) over \( \mathbb{L} \), we can define a fractional projective map \( x \mapsto f(x, 1)/g(x, 1) \) on \( \mathbb{P}^1(\mathbb{L}) \) whenever \( f \) and \( g \) do not have a common zero. Fractional projective permutations over a finite field \( \mathbb{L} \) of order \( p^h \) have been classified for every parameter \( p, k, l \) [16]. Recall the specific Dembowski-Ostrom polynomials of type (1). The monomial Gold maps \( X \mapsto X^s \) where \( s \in \{q+1, (q+1)r, qr+1, q+r\} \) on \( \mathbb{F}_{p^h} \) with \( q = p^k \) and \( r = p^l \) have been shown to be connected to the fractional projective permutations. Identifying \( \mathbb{F}_{p^h} = \mathbb{L}(\xi) = \mathbb{L} + \mathbb{L} \xi \mathbb{L} \), the above Gold maps can be written as \((q, q)\)-biprojective polynomials \( G_s(x, y) = (f_s(x, y), g_s(x, y)) \) using \( X = x\xi + y \).

The following lemma has been proved for general parameters in [16]. Here we include only the results necessary for our treatment.

**Lemma 16:** Let \( p = 2 \), \( q = p^k \), \( r = p^l \) and \( \gcd(k, l) = 1 \).
- If \( l \) is odd, then
\[ x \mapsto \frac{x^{q^{r+1}} + c}{x^q + x + d} \]
permutes \( \mathbb{P}^1(\mathbb{L}) \) if and only if \( c \in \mathbb{F}_2 \) and \( d = 1 \).
If \( l \) is even and \( f(x, 1) = 0 = g(x, 1) \) does not hold for 
\( x \in \mathbb{F}^1(L) \), then the fractional projective map 
\[ x \mapsto f(x, 1)/g(x, 1) \]
permutes \( \mathbb{P}^1(L) \) if and only if 
\( (f, g) \approx_{\mathcal{L}} G_{q+1} \) or 
\( (f, g) \approx_{\mathcal{L}} G_{q+r} \).

Note that in the even case \( G_{q+1} \) and \( G_{q+r} \) are APN, since 
\( \text{gcd}(k, l) = \text{gcd}(k, 2l) = \text{gcd}(k+l, 2l) = 1 \) by [5] which states 
that \( G_{2l+1} \) is APN over \( \mathbb{F}^2q \) if and only if 
\( \text{gcd}(i, n) = 1 \).

V. THE CLASSIFICATION

First we will prove a necessary \( \text{gcd} \)-condition on a \((q, q)\)-
bijective APN function \( F \).

**Proposition 17:** Let \( q = 2^k \) and \( \text{gcd}(k, l) > 1 \). Then \( F \in \mathcal{F}_{q,L} \) is not APN.

**Proof:** Let \( F = (f, g) = ((a_0, b_0, c_0, d_0)_q, (a_1, b_1, c_1, d_1)_q) \). By Lemma 4, if \( F \) is APN, then
\[
\begin{align*}
b_1 x^q + c_1 x &= d_1 (y^q + y), \\
b_0 x^q + c_0 x &= d_0 (y^q + y),
\end{align*}
\]
has two solutions in \( \mathbb{L} \times \mathbb{L} \). Solutions to this equation pair
include \((x, y) \in \{0\} \times \text{Ker}(y^q + y) \). Thus \( \text{gcd}(k, l) = 1 \). \( \square \)

Now we can concentrate on the case \( \text{gcd}(k, l) = 1 \). We can assume 
\( (f, g) \in \mathcal{S}_{q,L} \times \mathcal{V}_{q,L} \) where \( \mathcal{S}_{q,L} \) is found in Lemma 12.
We will first deal with the case \( f \in S \) (see Lemma 12 for the definitions of \( S \) and \( \mathcal{S}_{q,L} \) we use).

A. The Case \( f \in S \)

**Proposition 18:** Let \( q = 2^k, l > 3, \text{gcd}(k, l) = 1 \) and 
\( F : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}, 
\( (x, y) \mapsto (f(x, y), g(x, y)), \)
where \( f \in S \subset \mathcal{S}_{q,L} \) and \( g \in \mathcal{V}_{q,L} \). Then \( F \) is not APN.

**Proof:** We will analyze each function \( f \in S \) case by case.
We let \( g = (a_1, b_1, c_1, d_1)_q \).
\ inappropriate tensor product symbol is used.
\( \cdot \)\ inappropriate tensor product symbol is used.

- \( f \in \{(0, 0, 0, 0)_q, (0, 0, 0, 1)_q \} \).

We have \( D^\infty_f(x,y) = 0 \) for all \( (x, y) \) and \( D^\infty_g(x,y) = 0 \) if and only if
\( a_1 x^q + a_1 x = c_1 y^q + b_1 y. \)

If \( a_1 = 0 \) or \( b_1 = c_1 = 0 \), then the claim easily follows 
since \((x, y) \in \mathbb{L} \times \{0\} \) (or \( \{0\} \times \mathbb{L} \) resp.) satisfy the equality. 
Otherwise \( |\text{Im}(a_1 x^q + a_1 x) \cap \text{Im}(c_1 y^q + b_1 y)| \geq 2^{l-2} \), since both image sets are at least \( l-1 \) dimensional 
\( \mathbb{F}_2 \)-vector spaces which have to intersect at a vector space with dimension at least \( l-2 \).

- \( f = (0, 0, 1, 0)_q \).

Since \( (f, g) \approx_{\mathcal{L}} (f, rf + sg) \) if and only if \( s \neq 0 \) we can assume 
that \( c_1 = 0 \). The equalities for \( D^\infty_f(x,y) = 0 = 
D^\infty_g(x,y) = 0 \) for \( u \in \{0, \infty\} \) give
\[
\begin{align*}
D^\infty_f(x,y) &= x = 0, \\
D^\infty_g(x,y) &= b_1 x^q + d_1 y^q + d_1 y = 0,
\end{align*}
\]
and
\[
\begin{align*}
D^\infty_f(x,y) &= y^q = 0, \\
D^\infty_g(x,y) &= a_1 x^q + a_1 x + b_1 y.
\end{align*}
\]

imply that \( a_1 \neq 0 \) and \( d_1 \neq 0 \). Thus, setting \( a_1 = 1 \) by the scaling action, we will check the common solutions of 
\[
\begin{align*}
D^\infty_f(x,y) &= x + uy^q = 0, \\
D^\infty_g(x,y) &= (u + b_1)x^q + u^q x + d_1 y^q + (b_1 u^q + d_1)y = 0, 
\end{align*}
\]
for \( u \in \mathbb{L}^\times \). Replacing \( x \) by \( uy^q \) in the second equation
\[
\begin{align*}
D^\infty_g(x,y) &= (u + b_1)(uy^q + u^q (uy^q)) + d_1 y^q + (b_1 u^q + d_1)y = 0, \\
&= (u^q + b_1 u^q)y^q + (b_1 u^q + d_1)y = 0, \\
&= u^q (y^q + y^q) + b_1 u^q (y^q + y) + d_1 (y^q + y) = 0.
\end{align*}
\]
Thus for every \( u \in \mathbb{L}^\times \), all \((uy^q, y)\) for \( y \in \mathbb{F}_2 \) give a solution. To be APN, these should be the only solutions.
We will use the fact that \( y^q + y = h \in \mathcal{H} \setminus \{0\} \) for 
\( y \in \mathbb{L} \setminus \mathbb{F}_2 \) by Hilbert’s Theorem 90. If \( b_1 = 0 \), then
\[
\frac{d_1}{u^q + 1} = \frac{h^q}{h}
\]
has a solution for every \( h \in \mathcal{H} \setminus \{0\} \). Now, applying 
\( u \mapsto ub_1 \) we get, by setting \( d^q = d_1/b_1^q + 1 \),
\[
\begin{align*}
u^q + h^q + h^q + h^q + d^q h = 0, \\
h v^q + v^q + h^q + h^q + d^q h = 0,
\end{align*}
\]
setting \( v = d/u \) and then multiplying the equality by \( v^q + 1/d^q \). Now if \( l \in \mathcal{H} \) (i.e., \( l \) is even) then \( d \not\in \mathbb{L}^\times \) for \( F \) to be APN. For \( h \in \mathcal{H} \setminus \mathbb{F}_2 \), setting \( v = x((h^q + h^q)/h^q) \), we get
\[
\begin{align*}
x^q + x + \frac{d^q + 1}{(h^q + h^q)^q + 1} = 0.
\end{align*}
\]
We have
\[
\begin{align*}
&\|h^q + h^q + h^q + 1\|_h \in \mathcal{H} \setminus \mathbb{F}_2 \\
&\|h^q + h^q + h^q + d^q h\|_h \in \mathcal{H} \setminus \mathbb{F}_2 \\
&= I_3^{[3]},
\end{align*}
\]
by Lemma 14 (ii), since \( h \in \mathcal{H} \) if and only if \( h^q \in \mathcal{H} \).

Now \( F \) is APN if and only if \( d_{l_1} \cap (I_1 \cup I_2 \cup I_3) = \emptyset \).
By Lemma 15 we have \( d_{l_1} \cap (I_1 \cup I_2 \cup I_3) \neq \emptyset \), for 
\( l > 3 \) and we are done.

- \( f = (1, 0, 0, d_1)_q \) for \( d_1 \in \mathbb{L}^\times \).

We can assume \( a_1 = 0 \). We have
\[
\begin{align*}
D^\infty_f(x,y) &= d_0 (y^q + y) = 0, \\
D^\infty_g(x,y) &= b_1 x^q + c_1 x + d_1 y^q + y = 0.
\end{align*}
\]
Thus either \( c_1 = 0 \) or \( b_1 = 0 \) (but not both), and 
since \((0, 0, b_1, d_1)_q \sim_{\mathcal{M}} (0, 0, c_1, d_1)_q \sim_{\mathcal{M}} (0, 0, 1, 0)_q \) we 
are done as we have already handled that case before. \( \square \)
Remark 19: In the proof of the case \( f = (0, 0, 1, 0)_q \) we assumed \( l > 3 \) and we used Lemma 15 to show that \( F \) is not APN. For \( l = 3 \), the necessary and sufficient condition

\[ dI_3 \cap (I_1 \cup I_2 \cup I_3) = \emptyset, \]

holds for \( d \in J = \{ \omega, \omega^2, \omega^4 \} \) where \( \omega \in \mathbb{F}_{2^3} \) satisfying \( \omega^3 + \omega + 1 = 0 \). In this case

\[ I_0 = \{ \omega, \omega^2, \omega^4 \}, \]
\[ I_1 = \{ \omega^3, \omega^5, \omega^6 \}, \]
\[ I_2 = \{ 0 \}, \text{ and} \]
\[ I_3 = \{ 1 \}. \]

It is easy to see the direct product satisfies \( JI_3 = I_0 \). Thus \( F : \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \rightarrow \mathbb{F}_{2^3} \times \mathbb{F}_{2^3} \), with \( F = ((0, 0, 1, 0)_2, (1, b_1, 0, d_2)_2) \) for \( b_1, d_1 \in \mathbb{F}_{2^3} \) is APN if and only if \( \omega^2 = d_1 / b_1^3 \). These are precisely the Kim \( \kappa \) functions (up to \( \sim_{\text{gf}} \) equivalence).

Remark 20: Note that the case \( (f, g) \in \{(1, 0, 0, 1)_0 \} \times \Pi_1 \) proved as a subcase in Proposition 18 generalizes the results in [12] and [13] that show that the class of functions satisfying the (generalized) butterfly structure are not APN when \( l > 3 \) is odd. These functions are by definition [12],

\[ B_{q,L} = \{ ((x + ay)^q + (by)^q, (x + a)^q + (bx)^q) : a, b \in \mathbb{L}^x \}. \]

It is easy to see via \( x \mapsto x + ay \) and then \( y \mapsto y/b \) for the left component (and similarly \( y \mapsto y + ax \) and \( x \mapsto x/b \) for the right component) that \( (f, g) \in B_{q,L} \subset \Pi_1 \times \Pi_1 \).

Note that \( \Pi_1 \times \Pi_1 \) contains functions (CCZ-equivalent to permutations) that are not contained directly in \( B_{q,L} \) and whether the CCZ-equivalence class (or \( \approx_L \) class) of \( B_{q,L} \) covers all such functions is not covered in [12] and [13] and seems to be difficult to solve. The question is easy to answer for the right action of GL(2, \( \mathbb{L} \)) together with scaling on both components (the natural subgroup action \( \mathbb{L}^x \times \mathbb{L}^x \times \text{GL}(2, \mathbb{L}) \) that preserves inclusion in \( \Pi_1 \)). After the transformations \( (x \mapsto x + ay \) and then \( y \mapsto y/b \) on the left part and applying all GL(2, \( \mathbb{L} \)) transformations stabilizing the left part \( (1, 0, 0, 1)_q \) (generated by \( (x, y) \mapsto (y, x) \)) and scaling on the right side, we see

\[ B'_{q,L} = \{ (1, 0, 0, 1)_q \times \{(a,b,c,x,y) : a, b, c \in \mathbb{L}^x \} \cup \{a,b,c,x,y) : a, b, c \in \mathbb{L}^x \}, \]

where

\[ h_{a,b,c}(x,y) = c((a + 1)y/b + ax)^q + (bx + ay)^q + 1. \]

The cardinality of this set is \( |B'_{q,L}| \leq 2^{2l+1} \) whereas \( |\Pi_1| = (2^{2l} - 1)(2^{2l} - 2^l)/2 \approx 2^{4l-1} \). Thus \( B'_{q,L} \) is strictly included in \( \{ (1, 0, 0, 1)_q \} \times \Pi_1 \).

Note also that the butterfly structure is defined only for odd \( l \) whereas Proposition 18 covers the even case as well. We also note that \( \Pi_1 \times \Pi_1 \) and, in particular, the functions from the generalized butterfly construction seems to be a good source for cryptographically interesting functions. The engineering aspects of the butterflies were explained in [11].

B. The Even \( l \) Case

By Lemma 12 we can assume \( f \in \Pi_1 \) when \( l \) is even.

Proposition 21: Let \( q = 2^k, l > 3 \) even, \( r = 2^l \), \( \text{gcd}(k, l) = 1 \) and

\[ F : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}, \]
\[ (x, y) \mapsto (f(x, y), g(x, y)), \]

where \( f \in \Pi_1 \) and \( g \in \mathbb{V}_q \). Then \( F \) is APN if and only if \( F \approx_L G_{q+1} \) or \( F \approx_L G_{q+r} \).

Proof: By Lemma 12 and Proposition 18, we must have \( g \in \Pi_1 \). Assume \( f(x_0, 1) = 0 = g(x_0, 1) \) for some \( x_0 \in \mathbb{P}^1(\mathbb{L}) \), then since both \( f, g \) have only one \( \mathbb{P}^1(\mathbb{L}) \)-zero, there exists \( x_1 \in \mathbb{L} \) such that \( f(x_1, 1)g(x_1, 1) \neq 0 \). Now \( f(x, 1) + rg(x, 1) = 0 \) has at least two \( \mathbb{P}^1(\mathbb{L}) \)-zeros \( \{ x_0, x_1 \} \) where the nonzero \( r \) is chosen to satisfy \( r = \frac{f(x_1, 1)}{g(x_1, 1)} \). Thus \( (f, f + rg) \approx_L (f, g) \) is not APN by Proposition 18.

Therefore we can assume that \( f \) and \( g \) do not have a common zero. We must have \( rf(x, 1) + sg(x, 1) \in \Pi_1 \) for every \( (r, s) \in \mathbb{L} \times \mathbb{L} \setminus \{(0, 0)\} \). That is to say

\[ \pi(x) = \frac{f(x, 1)}{g(x, 1)} = s/r \]

has a unique solution \( x \in \mathbb{P}^1(\mathbb{L}) \) for every \( s/r \in \mathbb{P}^1(\mathbb{L}) \), i.e., \( x \mapsto \pi(x) \) is bijective. That is to say

\[ F \approx_L G_{q+1} \text{ or } F \approx_L G_{q+r}, \]

by Lemma 16. \( \square \)

C. The Odd \( l \) Case

By Lemma 12, we can assume that \( f \in \{(0, 1, 1, 0)_q \} \cup \Pi_0 \) when \( l \) is odd.

Proposition 22: Let \( q = 2^k, l > 3 \) odd, \( r = 2^l \), \( \text{gcd}(k, l) = 1 \) and

\[ F : \mathbb{L} \times \mathbb{L} \rightarrow \mathbb{L} \times \mathbb{L}, \]
\[ (x, y) \mapsto (f(x, y), g(x, y)), \]

where \( f \in \{(0, 1, 1, 0)_q \} \cup \Pi_0 \) and \( g \in \mathbb{V}_q \). Then \( F \) is APN if and only if

- \( F \approx_L G_{q+1} \) if \( k \) is odd, and
- \( F \approx_L G_{q+r} \) if \( k \) is even.

Proof: It is clear by Proposition 18 that \( f, g \in \Pi_1 \cup \Pi_0 \).

Now, the claim that if \( f, g \in \Pi_0 \) then \( rf + sg \in \Pi_0 \) for all \( (r, s) \in \mathbb{L} \times \mathbb{L} \setminus \{(0, 0)\} \) is absurd. Thus, whenever \( rf + sg \) has \( \mathbb{P}^1(\mathbb{L}) \)-solution it must have exactly three \( \mathbb{P}^1(\mathbb{L}) \) solutions again by Proposition 18. Since \( (f, g) \approx_L (rf + sg, g) \), we can assume that \( f = (0, 1, 1, 0)_q \) and \( g \in \Pi_0 \cup \Pi_3 \). Let \( g = (a, b, c, d)_q \). We can assume by the left action of \( \text{GL}(2, \mathbb{L}) \), \( b = 0 \), and by scaling, \( a = 1 \) (note that \( a = 0 \) is impossible since it implies \( g \in \Pi_2 \)). Thus \( g = (1, 0, c, d)_q \). We have

\[ D^\infty_f(x, y) = y^q + y = 0, \]
\[ D^\infty_g(x, y) = (x^q + x) + cy^q = 0, \]
which always have \((x, y) \in \mathbb{F}_2 \times \{0\}\) as solutions. Thus, \(\text{tr}(c) = 1\), so that \(\mathbb{L} \times \{1\}\) do not give more solutions, in particular \(c \neq 0\). Also,
\[
\begin{align*}
D_1'(x, y) &= x^q + x = 0, \\
D_2'(x, y) &= cx + d(y^q + y) = 0
\end{align*}
\]

imply \(d \neq 0\).

Now we will introduce the main argument: If \(F = (f, g)\) is APN then \(rf + g \in \mathbb{P}_0 \cup \mathbb{P}_1\). Let us determine the conditions on \(F\) when \(rf + g \in \mathbb{P}_1\). We will show that this is always the case unless \(F\) is equivalent to a Gold map.

By Lemma 11 (iii), \([(1, 0, 0, 1)]_q \sim_\mathbb{F} = \mathbb{P}_1\). Let
\[
A_{\alpha, \beta, u, v} = \begin{pmatrix}
\alpha \\
\beta
\end{pmatrix}
\begin{pmatrix}
u \\
v
\end{pmatrix}
\]
where \(\alpha, \beta \in \mathbb{L} \setminus \mathbb{F}_2\) and \(u, v \in \mathbb{L}\) with \(u \neq v\) so that \(\det(A_{\alpha, \beta, u, v}) = \alpha(\beta(u + v)) \neq 0\).

Let \(h = (1, 0, 0, 1)_q\) and consider the right action of \(\text{PGL}(2, \mathbb{L})\) (viewing \(h\) as a univariate \(q\)-projective polynomial,
\[
h'(x) = \beta y^{q+1} + x^{q+1} h(\mu_{\alpha, \beta, u, v}(x)),
\]
where
\[
\mu_{\alpha, \beta, u, v}(x) : x \mapsto \frac{\alpha(x + u)}{\beta(x + v)}.
\]

Equating the terms of \(h'\) and \(rf + g\), we get
\[
\begin{align*}
\alpha^{q+1} + \beta^{q+1} &= 1, \\
\alpha^{q+1} u + \beta^{q+1} v &= r, \\
\alpha^{q+1} u^q + \beta^{q+1} v^q &= r + c, \\
\alpha^{q+1} u^{q+1} + \beta^{q+1} v^{q+1} &= d.
\end{align*}
\]

Since \(x \mapsto x^{q+1}\) is bijective and \(r \in \mathbb{L}\), we can rewrite these as
\[
\begin{align*}
\gamma(u^q + u) + (\gamma + 1)(v^q + v) &= c, \\
\gamma u^{q+1} + (\gamma + 1)(v^{q+1} + v) &= d,
\end{align*}
\]
where \(\gamma = \alpha^{q+1} = 1 + \beta^{q+1}\). Since \(\alpha, \beta \in \mathbb{L} \setminus \mathbb{F}_2\), so is \(\gamma\) and for all \(\gamma \in \mathbb{L} \setminus \mathbb{F}_2\), we can find \(\alpha\) and \(\beta\) satisfying the above equalities. Equivalently,
\[
\begin{align*}
\gamma(u^q + u + c) &= \gamma + 1)(v^q + v + c), \\
\gamma(u^{q+1} + d) &= \gamma + 1)(v^{q+1} + d).
\end{align*}
\]

Note that \(\text{tr}(c) = 1\) and \(\gamma \in \mathbb{F}_2\), therefore neither side of (5) vanishes. Thus we can divide (6) by (5) side by side to get
\[
\varphi_{c, d}(u) = \varphi_{c, d}(v),
\]
where
\[
\varphi_{c, d} : x \mapsto \frac{x^{q+1} + d}{x^q + x + c}.
\]
Clearly (5) and (6) hold together if and only if (5) and (7) hold together.

Now assume \(\varphi_{c, d}\) is not bijective on \(\mathbb{L}\). Then there exist \(u, v \in \mathbb{L}\) such that \(\varphi_{c, d}(u) = \varphi_{c, d}(v)\) with \(u + v \notin \mathbb{F}_2\). It is clear that
\[
\varphi_{c, d}(x) + \varphi_{c, d}(x + 1) = \frac{x^{q+1} + d + (x + 1)^{q+1} + d}{x^q + x + c} \neq 0,
\]
since \(\text{tr}(1) = 1\). For such \(u, v\), (5) becomes
\[
\frac{u^q + u + c}{v^q + v + c} = \frac{\gamma + 1}{\gamma} = 1 + \frac{1}{\gamma} \notin \mathbb{F}_2.
\]

Thus, selecting \(\alpha, \beta \in \mathbb{L} \setminus \mathbb{F}_2\) we can produce such \(\gamma\). Hence, \(\varphi_{c, d}\) must be bijective, and by Lemma 16, we must have \(c = d = 1\) and \(g = (1, 0, 1, 1)_q\).

Now let \((\xi) = \mathbb{F}_2^\times\). Any \(X \in \mathbb{F}_2^\times\) can be written as \(X = x + y\xi\) where \(x, y \in \mathbb{L}\). We have
\[
\xi^k = \begin{cases} 
\xi + 1 & \text{if } k \text{ is odd,} \\
\xi & \text{if } k \text{ is even.}
\end{cases}
\]

Now if \(k\) is odd, then
\[
\begin{align*}
(x + y\xi)^{q+1} &= x^{q+1} + x\xi^q + y^{q+1} + \xi(x^q y + x\xi^q) \\
&\approx ((x^{q+1} + x\xi^q + y^{q+1}), x\xi^q + x\xi^q) \\
&\approx (0, 1, 1, 0)_q, (1, 0, 1, 1)_q,
\end{align*}
\]
and if \(k\) is even,
\[
\begin{align*}
(x + y\xi)^{q+r} &= x^{q+r} + x\xi^q + y^{q+r} + \xi(x^q y + x\xi^q) \\
&\approx ((x^{q+r} + x\xi^q + y^{q+r}), x\xi^q + x\xi^q) \\
&\approx (0, 1, 1, 0)_q, (1, 0, 1, 1)_q,
\end{align*}
\]
using \((x, y) \mapsto (y, x)\) in the penultimate line, proving our assertion that \((f, g) \approx (G_{q+r}\) when \(k\) is odd, and \((f, g) \approx (G_{q+r}\) when \(k\) is even. Note that when \(l\) is odd and \(\gcd(k, l) = 1\), we have \(\gcd(k, 2l) = 1\) if \(k\) is odd and \(\gcd(l - k, 2l) = 1\) if \(k\) is even. By [5], these maps are APN since \(q + r = q(1 + r/q) = 2k(1 + 2^{-k}).\)

\(D. \ \text{Proof of Theorem 1}\)

Now, Propositions 17, 18, 21 and 22 together with Lemma 12 proves Theorem 1.

**Acknowledgment**

The author would like to thank Claude Carlet for his comments, and to Lukas Kölsch for many discussions that improved the treatment considerably. He also would like to thank the reviewers for the comments that improved the presentation.

**References**

[1] X.-D. Hou, “Affinity of permutations of \(\mathbb{F}_2^n\),” *Discrete Appl. Math.*, vol. 154, pp. 313–325, Feb. 2006.

[2] K. A. Browning, J. F. Dillon, M. T. McQuistan, and A. J. Wolfe, “An APN permutation in dimension six,” *Finite Fields, Appl., Contemp. Math.*, Amer. Math. Soc., vol. 518, pp. 33–42, Jun. 2010.
C. Carlet, “Open questions on nonlinearity and on APN functions,” in Arithmetic Finite Fields (Lecture Notes in Computer Science), vol. 9061, Cham, Switzerland: Springer, 2015, pp. 83–107, doi: 10.1007/978-3-319-16277-5_5.

F. Göloğlu, “Almost perfect nonlinear trinomials and hexanomials,” Finite Fields Appl., vol. 33, pp. 258–282, May 2015, doi: 10.1016/j.ffa.2014.12.006.

R. Gold, “Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.),” IEEE Trans. Inf. Theory, vol. IT-14, no. 1, pp. 154–156, Jan. 1968.

F. Göloğlu and P. Langevin, “Almost perfect nonlinear families which are not equivalent to permutations,” Finite Fields Appl., vol. 67, Oct. 2020, Art. no. 10170271.

B. Chase and P. Lisoněk, “Kim-type APN functions are affine equivalent to gold functions,” Cryptogr. Commun., vol. 13, no. 6, pp. 981–993, Nov. 2021.

K. Li, C. Li, T. Helleseth, and L. Qu, “A complete characterization of the APN property of a class of quadraticmials,” IEEE Trans. Inf. Theory, vol. 67, no. 11, pp. 7535–7549, Nov. 2021.

D. Krasanayova, “Constructions of APN permutations,” M.S. thesis, Dept. Algebra, Charles Univ., Prague, Czech Republic, 2016.

F. Göloğlu, D. Krasanayova, and P. Lisoněk, “Generalized Kim APN functions are not equivalent to permutations,” Tech. Rep., 2020.

L. Perrin, A. Udovenko, and A. Biryukov, “Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem,” in Advances in Cryptology—CRYPTO II, vol. 9815, M. Robshaw and J. Katz, Eds. Cham, Switzerland: Springer, 2016, pp. 133–154, doi: 10.1007/978-3-662-53008-5_4.

C. Kaspers and Y. Zhou, “The number of almost perfect nonlinear functions,” Des., Codes Cryptogr., vol. 86, no. 3, pp. 611–621, Mar. 2018.

F. Göloğlu and L. Kölsch, “Autotopism groups of Knuth semifields,” Tech. Rep., 2022.

C. Kaspers and Y. Zhou, “The number of almost perfect nonlinear functions grows exponentially,” J. Cryptol., vol. 34, no. 1, p. 4, Jan. 2021.

H. Taniguchi, “On some quadratic APN functions,” Des., Codes Cryptogr., vol. 87, no. 9, pp. 1973–1983, Sep. 2019.

D. Bartoli, J. Bierbrauer, G. Kyureghyan, M. Giulietti, S.Marcugini, and F. Pambianco, “A family of semifields in characteristic 2,” J. Algebra. Combinatorics, vol. 45, no. 2, pp. 455–473, Mar. 2017.

J. Bierbrauer, D. Bartoli, G. Faina, S. Marcugini, and F. Pambianco, “A family of semifields in odd characteristic,” Des., Codes Cryptogr., vol. 86, no. 3, pp. 611–621, Mar. 2019.

L. E. Dickson, “Linear algebras with associativity not assumed,” Duke Math. J., vol. 1, no. 2, pp. 113–125, Jun. 1935.

D. R. Hughes and E. Kleinfeld, “Seminuclear extensions of Galois fields,” Amer. J. Math., vol. 82, pp. 389–392, 1960, doi: 10.2307/2372965.

D. E. Knuth, “Finite semifields and projective planes,” J. Algebra, vol. 2, pp. 182–217, Jun. 1965, doi: 10.1016/0021-8693(65)90018-9.

C. Carlet, “Relating three linearity parameters of vectorial functions and building APN functions from bent functions,” Des., Codes Cryptogr., vol. 59, nos. 1–3, pp. 89–109, 2011.

L. Kölsch, B. Kriepke, and G. M. Kyureghyan, “Image sets of perfectly nonlinear functions (Corresp.),” Rad Hrvatske Akademije Znanosti i Umjetnosti. Matematiˇckie Znanosti, vol. 86, no. 3, pp. 611–621, Mar. 2018.

C. Carlet, “More constructions of APN and differentially 4-uniform functions by concatenation,” Sci. China Math., vol. 56, pp. 1373–1384, Jul. 2013.

K. Li, Y. Zhou, C. Li, and L. Qu, “Two new families of quadratic APN functions,” IEEE Trans. Inf. Theory, vol. 68, no. 7, pp. 4761–4769, Jul. 2022.

M. Calderini, K. Li, and I. Villa, “Two new families of bivariate APN functions,” 2022, arXiv:2204.07462.

C. Kaspers and Y. Zhou, “A lower bound on the number of inequivalent APN functions,” J. Combinat. Theory A, vol. 186, Feb. 2022, Art. no. 105554. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0097316521001539

L. Kölsch, B. Kriepke, and G. M. Kyureghyan, “Image sets of perfectly nonlinear maps,” 2020, arXiv:2012.00870.

C. Kaspers, “Equivalence problems of almost perfect nonlinear functions and disjoint difference families,” Ph.D. dissertation, Inst. Algebra Geometry, Otto-Von-Guericke-Universität Magdeburg, Fakultät Für Mathematik, Magdeburg, Germany, 2021, doi: 10.25673/36521.

C. Carlet, P. Charpin, and V. Zinoviev, “Codes, bent functions and permutations suitable for DES-like cryptosystems,” Des., Codes Cryptogr., vol. 15, no. 2, pp. 125–156, 1998.

S. Yoshiara, “Equivalences of quadratic APN functions,” J. Algebra. Combinatorics, vol. 35, no. 3, pp. 461–475, May 2012.

C. Bracken, C. H. Tan, and Y. Tan, “On a class of quadratic polynomials with no zeros and its application to APN functions,” Finite Fields Their Appl., vol. 25, pp. 26–36, Jan. 2014, doi: 10.1016/j.ffa.2013.08.006.

T. Helleseth and A. Kholosha, “On the equation $x^{2^k+1} + x + a$ over GF($2^k$),” Finite Fields Appl., vol. 14, no. 1, pp. 159–176, Jan. 2008.

S. S. Abhyankar, “Galois theory on the line in nonzero characteristic,” Bull. Amer. Math. Soc., vol. 27, no. 1, pp. 68–133, Jul. 1992.

**Faruk Göloğlu** received the Ph.D. degree from Otto-Von-Guericke University Magdeburg in 2009. He is currently with Charles University, Prague.