ON ALLTOP FUNCTIONS, p-ARY ALLTOP FUNCTIONS, AND ALMOST HADAMARD MATRICES

FERRUH ÖZBUDAK, FUAD HAMIDLI, VLADIMIR N. POTAPOV

Abstract. Alltop presented complex sequences utilizing cubic polynomials over $\mathbb{F}_p$ for prime $p > 3$, designed for spread spectrum radar and communication, nearly meeting the Welch bound. Hall et al. formally defined Alltop functions as functions with planar derivatives at every nonzero point, and discovered Alltop functions over $\mathbb{F}_{q^2}$ apart from x^3, where $q = p^n$, $p > 3$ is an odd prime. In this work, we classify all homogeneous q-cubic Alltop functions over $\mathbb{F}_{q^2}$ up to $\mathbb{F}_q$-EA-equivalence, and all q-cubic Alltop monomials over $\mathbb{F}_{q^3}$. In particular, we find all $u \in \mathbb{F}_{q^2}^*$ such that $x^3 + ux^{2q+1}$ is an Alltop function. The classification uses algebraic function fields and the Hasse–Weil bound. We introduce a new concept of a "p-ary Alltop function" $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ as a function whose difference functions are p-ary bent functions and provide a connection between Alltop functions and p-ary Alltop functions. We construct an infinite family of strict p-ary Alltop functions in characteristic 3. For $q \equiv 2 \pmod 3$, the norm–trace family is strict with respect to all homogeneous q-cubic Alltop functions, without a term restriction. We also obtain binomial-strict families. We generalize Alltop functions and p-ary Alltop functions using higher derivatives. We prove that generalized p-ary Alltop functions of degree k correspond to k-dimensional almost Hadamard matrices. Every 2-dimensional submatrix of an almost Hadamard matrix must be either some Hadamard matrix or all 1s matrix. We construct generalized p-ary Kerdock codes with parameters $\left(p^n, p^{2n+1}, (p-1)(p^{n-1} - p^{\frac{n}{2}-1})\right)_p$ for even n and $\left(p^n, p^{2n+1}, (p-1)p^{n-1} - p^{\frac{n-1}{2}}\right)_p$ for odd n based on either planar or p-ary Alltop functions.

Keywords: Alltop function, almost Hadamard matrix, p-ary Kerdock code, nonlinearity
AMS(2020) Math Sc. Cl. 11T71, 05B20, 94A60, 94B05

1. Introduction

In 1980, W. O. Alltop [1] introduced complex sequences utilizing cubic polynomials over the field $\mathbb{F}_p$ for prime $p > 3$, designed for spread spectrum radar and communication, nearly meeting the Welch bound.

Ferruh Özbudak is with Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul, Türkiye, e-mail: ferruh.ozbudak@sabanciuniv.edu.

Fuad Hamidli is with Department of Computer Science, New Jersey Institute of Technology New Jersey, USA, e-mail: fuad.hamidli@njit.edu.

Vladimir N. Potapov is with Faculty of Engineering and Natural Sciences, Sabancı University, 34956, Istanbul, Türkiye, e-mail: quasigroup349@gmail.com.

In 2012, Hall, Rao, and Donovan formally defined Alltop functions as functions that have planar derivatives at every nonzero point [7]. They demonstrated the non-existence of Alltop functions over $\mathbb{F}_{3^n}$ for any positive integer n.

In 2013, Hall, Rao, and Gagola discovered a new class of Alltop functions, proving their EA-inequivalence to x^3, the only known Alltop function over $\mathbb{F}_{q^2}$, where $q = p^n$, p is an odd prime, and $n \geq 1$ is an integer [8]. Additionally, they showed that using any Alltop function allows one to construct mutually unbiased bases, which is crucial in quantum information theory.

It seems a complete characterization of Alltop functions is difficult. For example, recently Price, Hall and Bartlett obtained computation results and they conjecture that there are no further families of Alltop monomials [21]. The results in Section 3 should be viewed as evidence for this conjectural picture within the restricted family of q-cubic functions considered here. In particular, the monomial and binomial analysis over $\mathbb{F}_{q^2}$ leads to the complete classification of all homogeneous q-cubic Alltop functions in Theorem 3.8. Over $\mathbb{F}_{q^3}$, Theorem 3.2 completely settles the monomial case.

In this paper, we present a detailed and systematic study of large infinite classes of Alltop functions. Our approach uses deep algebraic and arithmetic methods, including estimates for Weil character sums, and it leads to the determination and classification of several rich families of Alltop functions. Motivated by the well-known analogy between planar functions and bent functions, we introduce the notion of a p-ary Alltop function. In particular, we construct an infinite family of strict p-ary Alltop functions in characteristic 3: none is a component of any vectorial Alltop function. For $q \equiv 2 \pmod 3$, the norm–trace family is strict with respect to all homogeneous q-cubic Alltop functions, without a restriction on the number of terms. We also obtain families that are strict with respect to specified q-cubic monomial and binomial classes. Moreover, we derive applications to higher-dimensional Hadamard matrices and Kerdock codes.

In Section 2, we provide an overview of the basic definitions and the existing results on Alltop functions. Section 3 presents the main classification results on Alltop functions in this paper: we obtain a complete classification of all homogeneous q-cubic Alltop functions over $\mathbb{F}_{q^2}$ up to $\mathbb{F}_q$-EA-equivalence, together with a full classification of q-cubic Alltop monomials over $\mathbb{F}_{q^3}$. A central ingredient is an EA-equivalence reduction (supported by explicit linearized permutation polynomials) that organizes all q-cubic binomials into a small number of canonical classes; the most difficult case is then handled via Weil character sums, yielding a strong nonexistence theorem for an entire class, while the remaining exceptional class is settled in Theorem 3.7 by an algebraic function-field argument. In Subsection 3.3, we extend the monomial and binomial classification to all homogeneous q-cubics over $\mathbb{F}_{q^2}$, including those with three or four terms. Theorem 3.8 shows that the $\mathbb{F}_q$-EA-equivalence classes are represented by x^3 and, when $3 \nmid (q+1)$, by x^{q+2}.

In Section 4, we introduce a new notion of a "p-ary Alltop function", namely a map from $\mathbb{F}_{p^n}$ to $\mathbb{F}_p$, and we establish a connection between classical (vectorial) Alltop functions and p-ary Alltop functions over finite fields. A natural source of p-ary Alltop functions is given by component (trace) functions of vectorial Alltop functions. Moreover, there exist other p-ary Alltop functions which do not arise in this way; we call them "strict" p-ary Alltop functions (see Definition 4.2 below), meaning that they cannot be written as a component (trace) function of any vectorial Alltop function. In Subsection 4.2, Theorem 4.4 gives an infinite family of strict p-ary Alltop functions on $\mathbb{F}_{3^{3n}}$ for every $n \geq 1$, and proves strictness with respect to all homogeneous q-cubic Alltop functions for the norm–trace family when $q \equiv 2 \pmod 3$. We also construct families that are strict with respect to specified q-cubic monomial and binomial classes. We conclude the section with further characterization results in Subsection 4.3.

In section 5 we introduce a generalization of Alltop functions using higher derivatives and present some classification results. We develop the concept of generalized Alltop functions of degree k, including planar functions in the case $k = 2$ and Alltop functions in the case $k = 3$. Similarly, we develop the concept of generalized p-ary Alltop functions of degree k, including bent functions in the case $k = 2$ and p-ary Alltop functions in the case $k = 3$.

In section 6 we present an application of generalized p-ary Alltop functions to the construction of multidimensional almost Hadamard matrices. In 1979, Shlichta [22] defined the k-dimensional proper Hadamard matrix. Every 2-dimensional submatrix of a proper Hadamard matrix must be an ordinary Hadamard matrix. In 1981, Hammer and Seberry [9] defined k-dimensional almost Hadamard matrices. Every 2-dimensional submatrix of an almost Hadamard matrix is an ordinary Hadamard matrix or a matrix consisting of all 1s. A survey of the theory of Hadamard matrices, including multidimensional matrices, is contained in [10]. We consider p-ary Butson type almost Hadamard matrices. It means that all elements of such matrix must be complex pth roots of unity. In Theorem 6.1, we establish a correspondence between generalized p-ary Alltop functions of degree k and their associated k-dimensional p-ary Butson type almost Hadamard matrices with an all-ones $(k-1)$-dimensional submatrix in each direction.

In section 7, we propose constructions of p-ary Kerdock codes based on planar and p-ary Alltop functions. The original binary Kerdock code was discovered by Kerdock in 1972 [11]. This code consist of codewords of the Reed–Muller code $RM(1, n)$ along with $2^{n-1} - 1$ cosets of $RM(1, n)$ in the Reed–Muller code $RM_2(2, n)$ such that the Boolean functions associated with these cosets are quadratic bent functions with the property that the sum of every two of them is again a bent function. Binary Kerdock codes with length 2^n exist if and only if n is even. The parameters of these codes are $(2^n, 2^{2n}, 2^{n-1} - 2^{n/2-1})$, where 2^{2n} is the cardinality of the code, and $2^{n-1} - 2^{n/2-1}$ is the

code distance. The original Kerdock codes are neither linear nor additive. However, there exist additive binary codes with the same parameters [5].

The first p-ary generalization of Kerdock codes (for $n = 4$ and $p = 3$) was constructed in [19]. In 2001, van Asch and van Tilborg [3] constructed $\mathbb{Z}_{p^2}$-linear codes with parameters $(p^n, p^{2n}, d(n,p))_p$ for $gcd(n-1,p) = 1$, where the code distance $d(n,p)$ is not less than $(p-1)(p^{n-1} - (p-1)p^{(n-1)/2})$. We proposed linear and nonlinear p-ary Kerdock codes with parameters $\left(p^n, p^{2n+1}, (p-1)(p^{n-1} - p^{\frac{n}{2}-1})\right)_p$ for even n and $\left(p^n, p^{2n+1}, (p-1)p^{n-1} - p^{\frac{n-1}{2}}\right)_p$ for odd n, where $p > 2$ is a prime number.

Throughout the paper we use the following notation. Let p be a prime and $m, n \geq 1$ be positive integers. The (relative) trace Tr_{p^{mn}/p^n} is the onto map from $\mathbb{F}_{p^{mn}}$ to its subfield $\mathbb{F}_{p^n}$ given by

$$\begin{array}{rccl} \mathrm{Tr}_{p^{mn}/p^n} : \mathbb{F}_{p^{mn}} & \to & \mathbb{F}_{p^n} \\ x & \mapsto & x + x^{p^n} + \cdots + x^{p^{(m-1)n}}. \end{array}$$

We use the terms *function* and *map* interchangeably meaning to the same. We also use the terms *derivative* and *difference* interchangeably meaning to the same operation on the functions: $F \mapsto D_a F := F(x+a) - F(x)$.

2. Introduction to Alltop Functions

In this section we present some basic results on Alltop functions. We also fix some notation throughout the paper.

Let p be an odd prime, $q = p^s$, where $s \geq 1$ be an integer. Let $\mathbb{F}_q$ is a finite field with q elements and $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$.

A function $F : \mathbb{F}_q \to \mathbb{F}_q$ is called a *planar function* over $\mathbb{F}_q$ if, for any $a \in \mathbb{F}_q^*$, the discrete derivative (see, for example [20] and the references therein)

$$D_a F(x) = F(x+a) - F(x)$$

is a permutation function.

A function $F : \mathbb{F}_q \to \mathbb{F}_q$ is called an *Alltop function* over $\mathbb{F}_q$ if, for any $a \in \mathbb{F}_q^*$, the discrete derivative $D_a F(x) = F(x+a) - F(x)$ is a planar function. Equivalently, for any $a, b \in \mathbb{F}_q^*$, the expression

$$D_b D_a F(x) = F(x+a+b) - F(x+a) - F(x+b) + F(x)$$

is a permutation function.

Note that linear and quadratic functions over $\mathbb{F}_{p^n}$ cannot be Alltop functions, since their second derivative remains a constant.

Let $F(x) = x^3$ over $\mathbb{F}_{p^n}$, where $p > 3$ is an odd prime. Observe that $D_b D_a F(x) = 6abx + 3ab(a+b)$, which is a permutation in $\mathbb{F}_{p^n}$. The function x^3 is known (see [1]) as the original Alltop function, it used in the construction of sequences in 1980 by Alltop to meet cross and auto-correlation bounds (Welch bound).

It is well known that a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ has a unique representation (called the univariate algebraic normal form) as a univariate polynomial over $\mathbb{F}_{p^n}$ of degree at most $p^n - 1$. Hence we can assume that

$$F(x) = \sum_{i=0}^{p^n-1} c_i x^i,$$

where $c_i \in \mathbb{F}_{p^n}$ are uniquely determined by F. A set of all polynomial over $\mathbb{F}_{p^n}$ is determined by $\mathbb{F}_{p^n}[x]$.

Any integer $d \in \{0, \ldots, p^n - 1\}$ can be uniquely written in base p as $d = \sum_{j=0}^{n-1} b_j p^j$ with $b_j \in \{0, \ldots, p-1\}$.

Defining $w_p(d) = \sum_{j=0}^{n-1} b_j$, the *algebraic degree* of a nonzero function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is defined and denoted as

$$d^o(F) = \max\{w_p(i) : i \in \{0, \ldots, p^n - 1\}, c_i \neq 0\},$$

where $F(x) = \sum_{i=0}^{p^n-1} c_i x^i$ is the univariate polynomial representation of F. The algebraic degree of the zero function is 0 by convention.

Assume that p is a prime, $s \geq 1$ and $q = p^s$.

For $n \geq 2$, we say that $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is *q-affine* if its algebraic normal form is in the form $F(x) = \sum_{i=0}^{q^n-1} c_i x^i$, with

$$x^i \in \{1, x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}\} \text{ for each } c_i \neq 0.$$

For $n \geq 2$, we say that $F : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is (at most) *q-quadratic* if its algebraic normal form is in the form $F(x) = \sum_{i=0}^{q^n-1} c_i x^i$, with

$$x^i \in \{1, x, x^q, x^{q^2}, \ldots, x^{q^{n-1}}\} \cup \{x^2, x^{1+q}, \ldots, x^{1+q^{n-2}}, x^{2q}, x^{q+q^2}, \ldots\}$$
for each $c_i \neq 0$.

Let F and G be functions on $\mathbb{F}_{p^n}$. The functions F and G are called *extended affine equivalent* (EA-equivalent) if there exist an affine map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and affine invertible maps $L_1, L_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that

$$G + \phi = L_1 \circ F \circ L_2$$

.

We call an EA-equivalence on $\mathbb{F}_{q^m}$ an $\mathbb{F}_q$-EA-equivalence when its affine maps are $\mathbb{F}_q$-affine.

Let F and G be functions on $\mathbb{F}_{p^n}$. The functions F and G are said to be *extended quadratic equivalent* (EQA-equivalent) if there exist a (at most) quadratic map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ and affine invertible maps $L_1, L_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that

$$G + \phi = L_1 \circ F \circ L_2$$

.

Remark 2.1. *It is easy to see that the Alltop property is preserved under extended quadratic equivalency. In addition, for any homogeneous cubic functions F and G on $\mathbb{F}_{p^n}$, extended affine equivalency (EA) is the same as extended quadratic equivalency (EQA). Indeed, EA-equivalence clearly implies EQA-equivalence. Conversely, suppose that F and G are homogeneous cubic functions and that they are EQA-equivalent. Then there exist a map ϕ of degree at most two, an affine map L_1, and an invertible affine map L_2 such that*

$$G + \phi = L_1 \circ F \circ L_2.$$

Let A_1 and A_2 denote the linear parts of L_1 and L_2, respectively. Since F is homogeneous cubic, the degree-three homogeneous part of $L_1 \circ F \circ L_2$ is precisely $A_1 \circ F \circ A_2$; the translations in L_1 and L_2 contribute only terms of degree at most two. Since both F and G are homogeneous cubic and ϕ has degree at most two, comparing the degree-three homogeneous parts gives

$$G = A_1 \circ F \circ A_2.$$

Thus F and G are EA-equivalent. Hence, for homogeneous cubic functions, EA-equivalence and EQA-equivalence coincide.

In the literature, there are the following results on the existence of Alltop functions.

Theorem 2.1 ([8])**.** *Let $p \geq 5$ be an odd prime, and n is an integer such that 3 does not divide $p^n + 1$. Then $F(x) = x^{p^n+2}$ is an Alltop polynomial on $\mathbb{F}_{p^{2n}}$.*

Theorem 2.2 ([8])**.** *Let $p \geq 5$ be an odd prime, and n is an integer such that 3 does not divide $p^n + 1$. Then the Alltop functions x^3 and x^{p^n+2} on $\mathbb{F}_{p^{2n}}$ are not EA-equivalent.*

Theorem 2.3. [7] *There are no Alltop functions over $\mathbb{F}_{3^n}$.*

3. Towards Classification of Alltop Functions

Throughout this section, unless otherwise stated, $\mathbb{F}_q$ denotes a finite field of characteristic $p \geq 5$. This assumption is natural in the classical Alltop setting considered here: the original Alltop function x^3 has second derivative

$$D_b D_a(x^3) = 6abx + 3ab(a + b).$$

Thus characteristics 2 and 3 are excluded. Moreover, the non-existence of Alltop functions over $\mathbb{F}_{3^n}$ is recalled in Theorem 2.3, and several computations below involve division by 2 and 3.

In this section, we classify all homogeneous q-cubic Alltop functions over $\mathbb{F}_{q^2}$ up to $\mathbb{F}_q$-EA-equivalence and all q-cubic Alltop monomials over $\mathbb{F}_{q^3}$. Subsection 3.1 treats monomials over both fields, and Subsection 3.2 completes the binomial case over $\mathbb{F}_{q^2}$ in Theorem 3.7. Building on these cases, Subsection 3.3 establishes the full homogeneous q-cubic classification over $\mathbb{F}_{q^2}$ in Theorem 3.8. The proofs, especially in Subsections 3.2 and 3.3, are technically demanding and require deep mathematical tools.

3.1. Cubic Alltop q-Monomials over $\mathbb{F}_{q^2}$ and over $\mathbb{F}_{q^3}$.

In this subsection we classify all q-cubic monomial Alltop functions over $\mathbb{F}_{q^2}$ and over $\mathbb{F}_{q^3}$. It is interesting to note that the results are completely different over $\mathbb{F}_{q^2}$ and over $\mathbb{F}_{q^3}$. Our main result is Theorem 3.2

We start over $\mathbb{F}_{q^2}$. Using Remark 2.1, it is enough to consider monic q-cubic functions. Over the field $\mathbb{F}_{q^2}$, the set of all monic, q-cubic monomial functions consists of the followings:

- $A_1)$ x^3
- $A_2)$ x^{q+2}
- $A_3)$ $x^{2q+1} = (x^{q+2})^q$
- $A_4)$ $x^{3q} = (x^3)^q$

The pairs $A_1)$ and $A_4)$, as well as $A_2)$ and $A_3)$, are equivalent under EA equivalence, as they are q-th powers of each other.

The following theorem classifies q-cubic monomial Alltop functions over $\mathbb{F}_{q^2}$ and is due to Hall, Rao, and Gagola [8]. For the reader's convenience, we include a detailed proof sketch, emphasizing the argument that x^{q+2} is Alltop over $\mathbb{F}_{q^2}$ if and only if $3 \nmid (q+1)$ and $\mathrm{char}(\mathbb{F}_q) \geq 5$. We will reuse several techniques from this sketch later.

Theorem 3.1 ([8]). *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. We have the followings:*

i.) *If $3 \mid (q+1)$, then x^3 is the only monic q-cubic Alltop monomial on $\mathbb{F}_{q^2}$ up to EA-equivalence.*

ii.) *If $3 \nmid (q+1)$, then x^3 and x^{q+2} are the only monic q-cubic Alltop monomials on $\mathbb{F}_{q^2}$ up to EA-equivalence. Moreover they are not extended quadratic equivalent.*

Sketch of the proof. In this sketch of the proof we consider the Alltop property of x^{q+2} over $\mathbb{F}_{q^2}$. Let $a \in \mathbb{F}_{q^2}^*$ and $F(x) = x^{q+2}$. We have

$$\begin{aligned} D_aF(x) &= (x+a)^{q+2} - x^{q+2} \\ &= (x^q + a^q)(x^2 + 2ax + a^2) - x^{q+2} \\ &= 2ax^{q+1} + a^q x^2 + \text{lot}, \end{aligned}$$

where lot refers to lower order terms in their algebraic degrees.

Let $b \in \mathbb{F}_{q^2}^*$, $F_1(x) = x^{q+1}$ and $F_2(x) = x^2$. We also have

$$\begin{aligned} D_bF_1(x) &= x^q b + xb^q + \text{lot}, \\ D_bF_2(x) &= 2bx + \text{lot}. \end{aligned}$$

These imply

$$\begin{aligned} D_aD_bF(x) &= 2a(x^qb + xb^q) + \text{lot} \\ &\quad +a^q(2bx) + \text{lot} \\ &= 2abx^q + (2ab^q + 2a^qb)x + \text{lot}. \end{aligned} \tag{1}$$

Hence F is Alltop if and only if the map

$$x \mapsto x^q + \left(a^{q-1} + b^{q-1}\right) x$$

is a permutation of $\mathbb{F}_{q^2}$ for all $a, b \in \mathbb{F}_{q^2}^*$.

For $\alpha \in \mathbb{F}_{q^2}^*$, the map $x \mapsto x^q + \alpha x$ is $\mathbb{F}_q$-linear and it is a permutation if and only if

$$\alpha^{q+1} \neq 1.$$

Put $\beta = (a/b)^{q-1}$. We have

$$(a^{q-1} + b^{q-1})^{q+1} = 1 \iff (\beta + 1)^{q+1} = 1$$

and

$$(\beta + 1)^{q+1} = 2 + \beta + \frac{1}{\beta}.$$

Here we use the facts that $\beta = (a/b)^{q-1}$, $a, b \in \mathbb{F}_{q^2}^*$ and hence $\beta^{q+1} = 1$.

These arguments imply that F is Alltop if and only if there is no β satisfying both

$$\beta^2 + \beta + 1 = 0 \text{ and } \beta^{q+1} = 1.$$

As the characteristic is at least 5 and $(\beta^2 + \beta + 1)(\beta - 1) = \beta^3 - 1$, we conclude that F is Alltop if and only if $\gcd(3, q + 1) = 1$. □

Next we consider the case of over $\mathbb{F}_{q^3}$. Over the field $\mathbb{F}_{q^3}$, the set of all monic, q-cubic monomial functions consists of the followings:

- $B_1)$ x^3
- $B_2)$ x^{q+2}
- $B_3)$ x^{2q+1}
- $B_4)$ x^{3q}
- $B_5)$ x^{q^2+2}
- $B_6)$ x^{q^2+q+1}
- $B_7)$ x^{q^2+2q}
- $B_8)$ x^{2q^2+1}
- $B_9)$ x^{2q^2+q}
- $B_{10})$ x^{3q^2}

For the functions F and G in the list $B_1 \dots B_{10}$, let $F \sim G$ denote that the relation that there exists a $0 \leq i \leq 2$ such that $F(x) = G(x)^{q^i}$ for each $x \in \mathbb{F}_{q^3}$. Under this relation we have the following orbits

- $x^3 \sim x^{3q} \sim x^{3q^2}$,
- $x^{q+2} \sim x^{q^2+2q} \sim x^{2q^2+1}$,
- $x^{2q+1} \sim x^{2q^2+q} \sim x^{q^2+2}$,
- x^{q^2+q+1}.

The following theorem classifies q-cubic monomial Alltop functions over $\mathbb{F}_{q^3}$. We remark that the results in Theorem 3.1 and the next theorem are completely different, while the only difference is the domains $\mathbb{F}_{q^2}$ and $\mathbb{F}_{q^3}$.

First we need a lemma that we use in the proof of the next theorem.

Lemma 3.1. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. There exists $a \in \mathbb{F}_q^*$ such that the polynomial $f_a(x) \in \mathbb{F}_q[x]$ given by*

$$f_a(x) = x^3 - ax^2 + (-a-3)x - 1$$

is irreducible over $\mathbb{F}_q$.

Proof. Assume the contrary. Then for each $a \in \mathbb{F}_q^*$, there exists $x_0 \in \mathbb{F}_q$ such that $f_a(x_0) = 0$. This implies existence of a function

$$\begin{array}{rcl} \varphi : \mathbb{F}_q^* & \to & \mathbb{F}_q \\ a & \mapsto & x_0, \end{array}$$

where x_0 is a chosen root of $f_a(x)$ in $\mathbb{F}_q$. We will complete the proof by a contradiction to the existence of φ.

Let I be the image of φ, which is a subset of $\mathbb{F}_q$. First note that $0 \notin I$. Indeed, otherwise there exists $a \in \mathbb{F}_q^*$ such that

$$f_a(0) = -1 = 0,$$

which is a contradiction. Similarly $-1 \notin I$. Indeed, otherwise there exists $a \in \mathbb{F}_q^*$ such that

$$f_a(-1) = -1 - a + (a+3) - 1 = 1 = 0,$$

which is a contradiction. Therefore $|I| \leq q-2$.

As $\varphi : \mathbb{F}_q^* \to I$ is a function with image I, we have

$$\mathbb{F}_q^* = \bigsqcup_{x_0 \in I} \varphi^{(-1)}(x_0), \tag{2}$$

where $\varphi^{(-1)}(x_0)$ is the preimage of φ.

Next we show that $|\varphi^{(-1)}(x_0)| = 1$ for each $x_0 \in I$. Indeed if $x_0 \in I$ and $a \in \varphi^{(-1)}(x_0)$, then we have

$$x_0^3 - ax_0^2 + (-a-3)x_0 - 1 = 0.$$

This implies

$$a(x_0^2 + x_0) = x_0^3 - 3x_0 - 1.$$

As $0 \notin I$ and $-1 \notin I$, we have $x_0^2 + x_0 \neq 0$. Hence we obtain

$$a = \frac{x_0^3 - 3x_0 - 1}{x_0^2 + x_0}.$$

This shows that $|\varphi^{(-1)}(x_0)| = 1$ for each $x_0 \in I$.

Using the statements above we conclude that

$$\left| \bigsqcup_{x_0 \in I} \varphi^{(-1)}(x_0) \right| = \sum_{x_0 \in I} |\varphi^{(-1)}(x_0)| = \sum_{x_0 \in I} 1 \leq q - 2.$$

This is a contradiction to (2) as $|\mathbb{F}_q^*| = q - 1$. This completes the proof.

□

Now we are ready for the classification of q-cubic monomial Alltop functions over $\mathbb{F}_{q^3}$. We note that its proof is not straightforward and it uses new ingredients from the arithmetic and combinatorics of finite fields.

Theorem 3.2. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. Then x^3 is the only monic q-cubic Alltop monomial on $\mathbb{F}_{q^3}$ up to EA-equivalence.*

Proof. Using the orbits stated above, it is enough to prove that the functions x^{q+2}, x^{2q+1} and x^{q^2+q+1} are not Alltop.

Let $F(x) = x^{q+2}$ and $a, b \in \mathbb{F}_{q^3}^*$. Using the methods of the proof of Theorem 3.1, we obtain that it is enough to prove the existence of $a, b \in \mathbb{F}_{q^3}$ such that

$$x^q + (a^{q-1} + b^{q-1})x$$

is not a permutation polynomial over $\mathbb{F}_{q^3}$.

For $\alpha \in \mathbb{F}_{q^3}^*$, the map $x \mapsto x^q + \alpha x$ is $\mathbb{F}_q$-linear and it is a permutation if and only if

$$\alpha^{q^2+q+1} \neq -1.$$

Note that $b^{(q-1)(q^2+q+1)} = 1$. Put $\beta = (a/b)^{q-1}$. Hence it is enough to show the existence of $\beta \in \mathbb{F}_{q^3}^*$ such that

$$(1+\beta)^{q^2+q+1} = -1 \text{ and } \beta^{q^2+q+1} = 1. \tag{3}$$

Using Lemma 3.1, we choose $u \in \mathbb{F}_q^*$ such that the polynomial $f_u(x) \in \mathbb{F}_q[x]$ given by

$$f_u(x) = x^3 - ux^2 + (-u-3)x - 1$$

is irreducible over $\mathbb{F}_q$. Let $\beta \in \mathbb{F}_{q^3}$ be a root of $f_u(x)$. Hence we have

$$f_u(x) = (x - \beta)(x - \beta^q)(x - \beta^{q^2}).$$

Using two representation of $f_u(x)$ and comparing the coefficients we obtain

$$\begin{aligned} u &= \beta+\beta^q+\beta^{q^2}, \\ -u-3 &= \beta^{q+1}+\beta^{q^2+1}+\beta^{q^2+q}, \\ 1 &= \beta^{q^2+q+1}. \end{aligned} \tag{4}$$

Hence in order to prove (3) it remains to show that

$$(1+\beta)^{q^2+q+1} = -1.$$

Note that we have

$$\begin{aligned} (1+\beta)^{q^2+q+1} &= 1+(\beta+\beta^q+\beta^{q^2}) \\ &\quad +(\beta^{q+1}+\beta^{q^2+1}+\beta^{q^2+q})+\beta^{q^2+q+1} \\ &= 1+u \\ &\quad +(-u-3)+1 \\ &= -1, \end{aligned}$$

where we use (4). This completes the proof of the statement that x^{q+2} is not Alltop over $\mathbb{F}_{q^3}$.

Let $F(x)=x^{2q+1}$ and $a\in\mathbb{F}_{q^3}^*$. We have

$$\begin{aligned} D_aF(x) &= (x^q+a^q)^2(x+a)-x^{2q+1} \\ &= (2a^qx^q)x+x^{2q}a+\text{lot}, \\ &= 2a^qx^{q+1}+ax^{2q}+\text{lot}. \end{aligned}$$

Let $b\in\mathbb{F}_{q^3}^*$, $F_1(x)=x^{q+1}$ and $F_2(x)=x^{2q}$. We also have

$$\begin{aligned} D_bF_1(x) &= x^qb+xb^q+\text{lot}, \\ D_bF_2(x) &= 2b^qx^q+\text{lot}. \end{aligned}$$

These imply

$$\begin{aligned} D_aD_bF(x) &= 2a^q(x^qb+xb^q)+\text{lot} \\ &\quad +a(2b^qx^q)+\text{lot} \\ &= (2a^qb+2ab^q)x^q+2a^qb^qx+\text{lot}. \end{aligned}$$

Hence F is Alltop if and only if the map

$$x\mapsto \left(1/a^{q-1}+1/b^{q-1}\right)x^q+x$$

is a permutation of $\mathbb{F}_{q^3}$ for all $a,b\in\mathbb{F}_{q^3}^*$.

For $\alpha\in\mathbb{F}_{q^3}^*$, the map $x\mapsto \alpha x^q+x$ is $\mathbb{F}_q$-linear and it is a permutation if and only if

$$\alpha^{q^2+q+1}\neq -1.$$

Put $\beta = (b/a)^{q-1}$. Hence the existence of $\beta \in \mathbb{F}_{q^3}^*$ satisfying the conditions on (3) also implies that F is not Alltop. This completes the proof of the statement that x^{2q+1} is not Alltop over $\mathbb{F}_{q^3}$.

Let $F(x) = x^{q^2+q+1}$ and $a \in \mathbb{F}_{q^3}^*$. We have

$$D_a F(x) = x^{q^2+q}a + x^{q+1}a^{q^2} + x^{q^2+1}a^q + \text{lot}.$$

Let $b \in \mathbb{F}_{q^3}^*$, $F_1(x) = x^{q^2+q}$, $F_2(x) = x^{q+1}$ and $F_3(x) = x^{q^2+1}$. We also have

$$\begin{aligned} D_b F_1(x) &= x^{q^2}b^q + x^q b^{q^2} + \text{lot}, \\ D_b F_2(x) &= x^q b + x b^q + \text{lot}, \\ D_b F_3(x) &= x^{q^2}b + x b^{q^2} + \text{lot}. \end{aligned}$$

These imply

$$D_a D_b F(x) = x^{q^2}(ab^q + a^q b) + x^q(a^{q^2}b + ab^{q^2}) + x(a^{q^2}b^q + a^q b^{q^2}) + \text{lot}. \tag{5}$$

In the special case that $a = b \in \mathbb{F}_{q^3}^*$, it is enough to show that the polynomial

$$x^{q^2}(2a^{q+1}) + x^q(2a^{q^2+1}) + x(2a^{q^2+q})$$

is not a permutation polynomial over $\mathbb{F}_{q^3}$ for some $a \in \mathbb{F}_{q^3}^*$. Indeed dividing by $2a^{q^2+q+1}$ we obtain

$$\left(\frac{x}{a}\right)^{q^2} + \left(\frac{x}{a}\right)^q + \left(\frac{x}{a}\right)$$

whose image over $\mathbb{F}_{q^3}$ is in $\mathbb{F}_q$. This completes the proof. □

3.2. **Cubic Alltop q-Binomials over $\mathbb{F}_{q^2}$.**

In this subsection, we develop a systematic framework for the classification of q-cubic Alltop binomial functions over $\mathbb{F}_{q^2}$, organizing the entire family into a finite collection of explicit classes introduced below. The resulting analysis is technically demanding and draws on deep arithmetic tools—most notably estimates for Weil-type character sums—yielding a classification that is complete by Theorem 3.7.

Using Remark 2.1, it is enough to consider q-cubic binomial functions up to a nonzero constant. Up to multiplication by a nonzero constant, the complete set of all q-cubic binomial functions consists of the followings:

- $C_1)$ $x^3 + ux^{2q+1}$
- $C_2)$ $x^3 + ux^{q+2}$
- $C_3)$ $x^3 + ux^{3q}$
- $C_4)$ $x^{q+2} + ux^{2q+1}$
- $C_5)$ $x^{q+2} + ux^{3q}$
- $C_6)$ $x^{2q+1} + ux^{3q}$

Here u is an arbitrary element of $\mathbb{F}_{q^2}^*$.

If we classify the whole family of q-cubic binomial functions in the class C_1, then we automatically classify the whole family of q-cubic binomial functions in the class C_5. The reason is that for each $u_1 \in \mathbb{F}_{q^2}^*$, there exists $u_2 \in \mathbb{F}_{q^2}^*$ such that the function $x^{q+2} + u_1 x^{3q}$ is EA-equivalent to the function $x^3 + u_2 x^{2q+1}$. Indeed,

$$u_1^{-q}(x^{q+2} + u_1 x^{3q})^q = x^3 + u_1^{-q} x^{2q+1},$$

so $u_2 = u_1^{-q}$.

Similarly for the classes C_2 and C_6.

Therefore it is enough to consider the classes C_1, C_2, C_3, and C_4.

The rest of this subsection is as follows: First we characterize the Alltop functions in the classes C_3, and C_4 in Proposition 3.1 and 3.2 below. These results are not involved.

Then we show that there is no Alltop function in the class C_2 using Weil sums. We refer to Theorems 3.3 and 3.4, whose proofs are rather involved.

Finally, we consider the class C_1, which turns out to be particularly interesting. Unlike the other classes, there exist $u_1, u_2 \in \mathbb{F}_{q^2}^*$ such that $x^3 + u_1 x^{2q+1}$ is EA-equivalent to x^3, whereas $x^3 + u_2 x^{2q+1}$ is EA-equivalent to x^{q+2}; see Theorems 3.5 and 3.6. This phenomenon is reminiscent of a related result for planar functions in [13]. In this subsection, we complete the classification of cubic Alltop q-binomials in Theorem 3.7.

First we consider the class C_3.

Proposition 3.1. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^3 + ux^{3q}$. Then F is Alltop if and only if u is not a $(q-1)$-power in $\mathbb{F}_{q^2}^*$. Moreover, if $F(x)$ is Alltop, then $F(x)$ is EA-equivalent to x^3.*

Proof. We observe that $F = L \circ G$, where L is the $\mathbb{F}_q$-linear map $L(x) = x + ux^q$ and $G(x) = x^3$. We complete the proof as L is invertible if and only if u is not a $(q-1)$-power in $\mathbb{F}_{q^2}^*$. □

Next we consider the class C_4.

Proposition 3.2. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^{q+2} + ux^{2q+1}$. Then F is Alltop if and only if u is not a $(q-1)$-power in $\mathbb{F}_{q^2}^*$ and 3 does not divide $q+1$. Moreover, if $F(x)$ is Alltop, then $F(x)$ is EA-equivalent to x^{q+2}.*

Proof. We observe that $F = L \circ G$, where L is the $\mathbb{F}_q$-linear map $L(x) = x + ux^q$ and $G(x) = x^{q+2}$. Again we note that L is invertible if and only if u is not a $(q-1)$-power in $\mathbb{F}_{q^2}^*$. Moreover G is Alltop if and only if 3 does not divide $q+1$. This completes the proof. □

Now we start considering class C_2. We need to prove the next theorem, that we will use in the consideration of class C_2 in Theorem 3.4 below. The following theorem, whose proof is quite involved, would also be interesting in itself.

Theorem 3.3. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. Let H be the subgroup of $\mathbb{F}_{q^2}^*$ such that $|H| = q+1$. For any $u \in \mathbb{F}_{q^2}^*$, there exist $h_1, h_2 \in H$ such that*

$$(h_1 + h_2 + u)^{q+1} = 1.$$

Proof. Let $\ell \geq 1$ be the smallest positive integer such that

$$q \equiv 2^\ell - 1 \mod \left(2^{\ell+1}\right).$$

Let G be the subgroup of $\mathbb{F}_{q^2}^*$ with $|G| = 2^\ell(q-1)$. We observe that the compositum GH is $\mathbb{F}_{q^2}^*$. Therefore if $u \in \mathbb{F}_{q^2}^*$, then there exists $v \in G$ and $h \in H$ such that $u = vh$. This implies that we can assume $u \in G$ without loss of generality.

Let g be a primitive element of $\mathbb{F}_{q^2}^*$. Put $\theta = g^{\frac{q^2-1}{2^\ell}}$. For $0 \leq i \leq 2^\ell - 1$, let G_i be the subset of G given by $G_i = \{x \in \mathbb{F}_{q^2}^* : x^q = \theta^i x\}$. We obtain that

$$G = \bigsqcup_{i=0}^{2^\ell-1} G_i$$

is a disjoint partition of G.

Let $0 \leq i \leq 2^\ell - 1$. Let $w_{i,1} = g^{\frac{q+1}{2^\ell} i}$ and $w_{i,2} = w_{i,1} g^{\frac{q+1}{2}}$. We observe that $\{w_{i,1}, w_{i,2}\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Assume that $u \in G_i$. Put $\alpha = u/w_{i,1}$. We obtain that $\alpha \in \mathbb{F}_q^*$. Let $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ such that

$$\begin{aligned} h_1 &= x_1 w_{i,1} + y_1 w_{i,2}, \\ h_2 &= x_2 w_{i,1} + y_2 w_{i,2}. \end{aligned}$$

Therefore the following statements are equivalent:

- **Statement 1:** For a given $u \in G_i$, there exist $h_1, h_2 \in H$ such that the following equation

  $$(h_1 + h_2 + u)^{q+1} = 1$$

  holds.

- **Statement 2:** For a given $\alpha \in \mathbb{F}_q^*$, there exist $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ such that the following system of equations

$$\begin{aligned} (x_1 w_{i,1} + y_1 w_{i,2})^{q+1} &= 1, \\ (x_2 w_{i,1} + y_2 w_{i,2})^{q+1} &= 1, \\ ((x_1 + x_2 + \alpha) w_{i,1} + (y_1 + y_2) w_{i,2})^{q+1} &= 1 \end{aligned} \tag{6}$$

holds.

Put $D_{i,1} = w_{i,1}^{q+1}$ and $D_{i,2} = w_{i,2}^{q+1}$. Note that $D_{i,1}, D_{i,2} \in \mathbb{F}_q^*$. By the choice of the basis $\{w_{i,1}, w_{i,2}\}$, using a direct calculation we obtain that the system in (6) is equivalent to the system

$$\begin{aligned} D_{i,1}x_1^2 + D_{i,2}y_1^2 &= 1, \\ D_{i,1}x_2^2 + D_{i,2}y_2^2 &= 1, \\ D_{i,1}(x_1 + x_2 + \alpha)^2 + D_{i,2}(y_1 + y_2)^2 &= 1. \end{aligned} \tag{7}$$

Using the first 2 equations for simplification in the last equation of the system in (7) we obtain

$$D_{i,2}y_1y_2 = -D_{i,1}x_1x_2 - D_{i,1}\alpha(x_1 + x_2) - \left(\frac{D_{i,1}\alpha^2 + 1}{2}\right). \tag{8}$$

Taking the square of the both sides and using the first 2 equations of the system in (7) we get

$$\left(1 - D_{i,1}x_1^2\right)\left(1 - D_{i,1}x_2^2\right) - \left(D_{i,1}x_1x_2 + D_{i,1}\alpha(x_1 + x_2) + \left(\frac{D_{i,1}\alpha^2 + 1}{2}\right)\right)^2 = 0.$$

The last equation is equivalent to

$$a(x_1)x_2^2 + b(x_1)x_2 + c(x_1) = 0, \tag{9}$$

where $a(x), b(x), c(x)$ are the polynomials in $\mathbb{F}_q[x]$ given by

$$\begin{aligned} a(x) &= 2D_{i,1}^2\alpha x_1 + D_{i,1}^2\alpha^2 + D_{i,1}, \\ b(x) &= 2D_{i,1}^2\alpha x_1^2 + (3D_{i,1}^2\alpha^2 + D_{i,1})x_1 + D_{i,1}^2\alpha^3 + D_{i,1}\alpha, \\ c(x) &= (D_{i,1}^2\alpha^2 + D_{i,1})x_1^2 + (D_{i,1}^2\alpha^3 + D_{i,1}\alpha)x_1 + 1/4D_{i,1}^2\alpha^4 + 1/2D_{i,1}\alpha^2 - 3/4. \end{aligned}$$

Let $\Delta(x) = b(x)^2 - 4a(x)c(x)$, which is a polynomial in $\mathbb{F}_q[x]$. The leading coefficient of $\Delta(x)$ is $4D_{i,1}^4\alpha^2$. Put $\Delta_1(x) = \frac{\Delta(x)}{4D_{i,1}^4\alpha^2}$, which is a monic polynomial of degree 4 over $\mathbb{F}_q$. Let $A_3, A_2, A_1, A_0 \in \mathbb{F}_q$ be the coefficients so that

$$\Delta_1(x) = x^4 + A_3x^3 + A_2x^2 + A_1x + A_0.$$

Assume that $D_{i,1} \neq \frac{1}{\alpha^2}$. Let $\overline{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. We observe that there is no $f(x) \in \overline{\mathbb{F}_q}[x]$ such that

$$\Delta(x) = \left(f(x)\right)^2. \tag{10}$$

Indeed, otherwise there exists $c_1, c_0 \in \overline{\mathbb{F}_q}$ such that

$$x^4 + A_3x^3 + A_2x^2 + A_1x + A_0 = \left(x^2 + c_1x + c_0\right)^2.$$

The last polynomial identity implies the following identity on the coefficients:

$$A_2 - \left(\left(\frac{A_3}{2} \right)^2 + 2\frac{A_1}{A_3} \right) = 0. \tag{11}$$

However, using a direct computation and the definitions of these coefficients above, we obtain

$$A_2 - \left(\left(\frac{A_3}{2} \right)^2 + 2\frac{A_1}{A_3} \right) = \frac{D_{i,1}\alpha^2 - 1}{D_{i,1}^2\alpha^2}.$$

As $D_{i,1} \neq \frac{1}{\alpha^2}$ by assumption, we get a contradiction. Hence there is no $f(x) \in \overline{\mathbb{F}_q}[x]$ such that (10) holds.

Let $T = \{x \in \mathbb{F}_q : \Delta(x) = 0, \text{ or } a(x) = 0, \text{ or } 1 = D_{i,1}x^2\}$. It is clear that $|T| \leq 7$. Let η be the quadratic character on $\mathbb{F}_q$ given by

$$\begin{aligned} \eta : \mathbb{F}_q &\rightarrow \{0, 1, -1\} \\ x &\mapsto \begin{cases} 0 & \text{if } x = 0, \\ 1 & \text{if } x \in \mathbb{F}_q^* \text{ and } x \text{ is a square}, \\ -1 & \text{if } x \in \mathbb{F}_q^* \text{ and } x \text{ is a non-square}. \end{cases} \end{aligned}$$

Let $N_1^{(1)}$ be the integer defined as

$$N_1^{(1)} = \sum_{x \in \mathbb{F}_q \setminus T} \left(1 + \eta(1 - D_{i,1}x^2)\right) \left(1 + \eta(\Delta(x))\right).$$

Let $N_1^{(2)}$ be the integer defined as

$$N_1^{(2)} = \sum_{x \in \mathbb{F}_q \setminus T} \left(1 - \eta(1 - D_{i,1}x^2)\right) \left(1 + \eta(\Delta(x))\right).$$

Note that $\Delta(x)$, $N_1^{(1)}$ and $N_1^{(2)}$ depend on the index $0 \leq i \leq 2^\ell - 1$. For the sake of simplicity by do not show this dependency in these notation.

Assume that $D_{i,2}$ is a square in $\mathbb{F}_q^*$. If $N_1^{(1)} > 0$, then there exists $x_1 \in \mathbb{F}_q$ such that $1 - D_{i,1}x_1^2$ is a square in $\mathbb{F}_q^*$, $\Delta(x_1)$ is a square in $\mathbb{F}_q^*$ and $a(x_1) \neq 0$. We choose and fix such $x_1 \in \mathbb{F}_q$. Let $y_1 \in \mathbb{F}_q^*$ be a solution of the first equation in (7). Let $x_2 \in \mathbb{F}_q$ be a solution of (9). Now $x_1, x_2 \in \mathbb{F}_q$ and $y_1 \in \mathbb{F}_q^*$ are already determined. Let $y_2 \in \mathbb{F}_q$ given by (8). The arguments above show that Statement 1 holds for the given $u = \alpha w_{i,1}$, provided that $N_1^{(1)} > 0$, $D_{i,2}$ is a square in $\mathbb{F}_q^*$ and $D_{i,1} \neq \frac{1}{\alpha^2}$.

Assume that $D_{i,2}$ is a non-square in $\mathbb{F}_q^*$. If $N_1^{(2)} > 0$, then using similar arguments as in the previous paragraph we obtain that Statement 1 holds for the given $u = \alpha w_{i,1}$, provided that $D_{i,1} \neq \frac{1}{\alpha^2}$.

Let $E^{(1)}$ and $E^{(2)}$ be the integers defined as

$$E^{(1)} = \sum_{x \in T} \left(1 + \eta(1 - D_{i,1}x^2)\right) \left(1 + \eta(\Delta(x))\right),$$

and

$$E^{(2)} = \sum_{x \in T} \left(1 - \eta(1 - D_{i,1}x^2)\right)\left(1 + \eta(\Delta(x))\right).$$

It is not difficult to observe that $E^{(1)} \leq 16$ and $E^{(2)} \leq 16$.

Let $N^{(1)}$ and $N^{(2)}$ be the integers defined as

$$N^{(1)} = \sum_{x \in \mathbb{F}_q} \left(1 + \eta(1 - D_{i,1}x^2)\right)\left(1 + \eta(\Delta(x))\right),$$

and

$$N^{(2)} = \sum_{x \in \mathbb{F}_q} \left(1 - \eta(1 - D_{i,1}x^2)\right)\left(1 + \eta(\Delta(x))\right).$$

Note that

$$N^{(1)} = \sum_{x \in \mathbb{F}_q} 1 + \sum_{x \in \mathbb{F}_q} \eta(1 - D_{i,1}x^2) + \sum_{x \in \mathbb{F}_q} \eta(\Delta(x)) + \sum_{x \in \mathbb{F}_q} \eta\left((1 - D_{i,1}x^2)\Delta(x)\right).$$

Put $D = D_{i,1}$. The identity

$$\Delta(x) = D(Dx^2 - 1)(D\alpha^2 + 2D\alpha x - 3)(D\alpha^2 + 2D\alpha x + 1)$$

shows that $(1 - Dx^2)\Delta(x)$ is not a square in $\overline{\mathbb{F}_q}[x]$, since the last two linear factors are distinct. Together with (10), this justifies applying Weil's sum ([14, Theorem 5.41]) to both polynomials. We have

$$\left|\sum_{x \in \mathbb{F}_q} \eta(\Delta(x))\right| \leq 3q^{1/2},$$

and

$$\left|\sum_{x \in \mathbb{F}_q} \eta\left((1 - D_{i,1}x^2)\Delta(x)\right)\right| \leq 5q^{1/2},$$

We also have

$$\left|\sum_{x \in \mathbb{F}_q} \eta(1 - D_{i,1}x^2)\right| \leq 1.$$

These arguments imply that

$$N^{(1)} \geq q - 1 - 8q^{1/2}.$$

Similarly we have

$$N^{(2)} = \sum_{x \in \mathbb{F}_q} 1 - \sum_{x \in \mathbb{F}_q} \eta(1 - D_{i,1}x^2) + \sum_{x \in \mathbb{F}_q} \eta(\Delta(x)) - \sum_{x \in \mathbb{F}_q} \eta\left((1 - D_{i,1}x^2)\Delta(x)\right).$$

The same arguments also imply that

$$N^{(2)} \geq q - 1 - 8q^{1/2}.$$

Therefore both $N_1^{(1)}$ and $N_1^{(2)}$ are positive if

$$q - 1 - 8q^{1/2} > 16. \tag{12}$$

If $q > 94$, then (12) holds. The set of cardinalities q such that $\mathbb{F}_q$ is a finite field of characteristic at least 5 and $q \leq 94$ is the set

$$\begin{aligned} S = \{&5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, 43, 47, \\ &49, 53, 59, 61, 67, 71, 73, 79, 83, 89\}. \end{aligned}$$

For each $q \in S$, we use Magma and a direct search method showing that Statement 1 holds for all $u \in G$. This completes the proof provided Statement 2 holds for $\alpha \in \mathbb{F}_q^*$ such that $\alpha^2 D_{i,1} = 1$.

Assume that $0 \leq i \leq 2^\ell - 1$ and $\alpha \in \mathbb{F}_q^*$ such that $\alpha^2 D_{i,1} = 1$. By the change of variables $x_1 \mapsto \frac{x_1}{\alpha}$, $x_2 \mapsto \frac{x_2}{\alpha}$, $y_1 \mapsto y_1$ and $y_2 \mapsto y_2$, the system in (7) is equivalent to the system

$$\begin{aligned} x_1^2 + D_{i,2} y_1^2 &= 1, \\ x_2^2 + D_{i,2} y_2^2 &= 1, \\ (x_1 + x_2 + 1)^2 + D_{i,2}(y_1 + y_2)^2 &= 1. \end{aligned}$$

Note that $(x_1, x_2, y_1, y_2) = (1, -1, 0, 0)$ is a solution of the last system. This completes the proof. □

Now we are ready to consider class C_2.

Theorem 3.4. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^3 + ux^{q+2}$. Then F is not Alltop.*

Proof. Let $a \in \mathbb{F}_{q^2}^*$ and $F(x) = x^3 + ux^{q+2}$. We have

$$D_a F(x) = 2aux^{q+1} + (a^q u + 3a)\, x^2 + \text{lot},$$

where lot refers to lower order terms in their algebraic degrees.

Let $b \in \mathbb{F}_{q^2}^*$. We obtain

$$D_a D_b F(x) = x^q\,(2uab) + x\,(2uab^q + 2ua^q b + 6ab) + \text{lot}.$$

Hence F is Alltop if and only if the map

$$x \mapsto x^q + \left(a^{q-1} + b^{q-1} \ + \frac{3}{u}\right) x$$

is a permutation of $\mathbb{F}_{q^2}$ for all $a, b \in \mathbb{F}_{q^2}^*$. Let H be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ such that $|H| = q + 1$. Note that $a^{q-1} \in H$ and $b^{q-1} \in H$ if $a, b \in \mathbb{F}_{q^2}^*$. Hence using Theorem 3.3 we obtain that there is no $u \in \mathbb{F}_{q^2}^*$ such that F is Alltop. □

Now we start considering class C_1. Put

$$H = \{h \in \mathbb{F}_{q^2}^* : h^{q+1} = 1\}, \qquad T = H^2,$$

and define

$$N = \{\alpha^{q-1} : \alpha \in \mathbb{F}_{q^2}^*,\ \alpha^{q+1} = -1\}. \tag{13}$$

Lemma 3.2. *The set N is a coset of T in H and $|N| = (q+1)/2$. More precisely,*

$$N = \begin{cases} T, & q \equiv 1 \pmod 4, \\ H \setminus T, & q \equiv 3 \pmod 4. \end{cases}$$

Proof. Let ω be a primitive element of $\mathbb{F}_{q^2}^*$ and put $\alpha_0 = \omega^{(q-1)/2}$. Then $\alpha_0^{q+1} = -1$, and every solution of $\alpha^{q+1} = -1$ is of the form $\alpha_0 h$ with $h \in H$. Since $h^{q-1} = h^{-2}$ on H, the image of this coset under $\alpha \mapsto \alpha^{q-1}$ is $\alpha_0^{q-1}T$. This proves that N is a coset of T and has size $(q+1)/2$. If $g = \omega^{q-1}$ generates H, then $\alpha_0^{q-1} = g^{(q-1)/2}$, which belongs to T precisely when $q \equiv 1 \pmod 4$. □

The following theorem classifies all functions in C_1 which are $\mathbb{F}_q$-EA-equivalent to x^3 completely.

Theorem 3.5. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^3 + ux^{2q+1}$. Then F is $\mathbb{F}_q$-EA-equivalent to x^3 over $\mathbb{F}_{q^2}$ if and only if $-u/3 \in N$. In particular, if $-u/3 \in N$, then F is Alltop.*

Proof. By comparing homogeneous cubic parts as in Remark 2.1, it suffices to consider invertible $\mathbb{F}_q$-linear maps. Let $L_1(x) = ax + bx^q \in \mathbb{F}_{q^2}[x]$ and $L_2(x) = cx + dx^q \in \mathbb{F}_{q^2}[x]$ be invertible $\mathbb{F}_q$-additive polynomials in $\mathbb{F}_{q^2}[x]$ such that

$$L_1 \circ x^3 \circ L_2 = F(x)$$

holds for all $x \in \mathbb{F}_{q^2}$. Utilizing $x^{q^2} = x$ for $x \in \mathbb{F}_{q^2}$ and substituting, we derive the following set of nonlinear equations in a, b, c, d, and u:

$$ac^3 + bd^{3q} = 1, \tag{14}$$

$$3cd^2a + 3c^{2q}d^qb = u, \tag{15}$$

$$3c^2da + 3bc^qd^{2q} = 0, \tag{16}$$

$$ad^3 + bc^{3q} = 0. \tag{17}$$

From (15) and the non-vanishing of u, we conclude $c \neq 0$ and $d \neq 0$. We proceed to show $a \neq 0$ and $b \neq 0$. Assuming the contrary, i.e., $a = 0$ or $b = 0$, and using (17) and the fact that $cd \neq 0$, we deduce $a = b = 0$, leading to a contradiction as the left-hand side of (14) becomes 0.

Further, (16) implies

$$a = -bc^{q-2}d^{2q-1}. \tag{18}$$

Combining (17) and (18), we obtain

$$-bc^{q-2}d^{2q+2} + bc^{3q} = -bc^{q-2}(d^{q+1} + c^{q+1})(d^{q+1} - c^{q+1}) = 0. \tag{19}$$

Combining (14) and (18), we get

$$-bc^{q+1}d^{2q-1} + bd^{3q} = bd^{2q-1}(d^{q+1} - c^{q+1}) = 1. \tag{20}$$

From (19) and (20), we immediately deduce

$$c^{q+1} = -d^{q+1}. \tag{21}$$

Using (21) we conclude that

$$c = \alpha d, \tag{22}$$

where $\alpha \in \mathbb{F}_{q^2}^*$ satisfies $\alpha^{q+1} = -1$.

Combining (18) and (22) we obtain

$$a = -b\alpha^{q-2}d^{3q-3}. \tag{23}$$

Using (14), (22), (23) and using the fact $\alpha^{q+1} = -1$, we get

$$b = \frac{1}{2d^{3q}}. \tag{24}$$

Using (23) and (24) we have

$$a = \frac{-\alpha^{q-2}}{2d^3}. \tag{25}$$

Combining (15), (22), (24) and (25), we obtain

$$\alpha^{q-1} = \frac{-u}{3}. \tag{26}$$

Thus $-u/3 \in N$, proving necessity.

Conversely, suppose $-u/3 \in N$ and choose $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^{q+1} = -1$ and $\alpha^{q-1} = -u/3$. For any $d \in \mathbb{F}_{q^2}^*$, put

$$c = \alpha d, \qquad b = \frac{1}{2d^{3q}}, \qquad a = -\frac{\alpha^{q-2}}{2d^3}.$$

These values satisfy (14)–(17). Moreover, $(c/d)^{q+1} = (a/b)^{q+1} = -1$, so both L_1 and L_2 are invertible. This proves the required equivalence. Since x^3 is Alltop, so is F. $\square$

The following theorem classifies all functions in C_1 which are $\mathbb{F}_q$-EA-equivalent to x^{q+2} completely.

Theorem 3.6. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^3 + ux^{2q+1}$. Then F is $\mathbb{F}_q$-EA-equivalent to x^{q+2} over $\mathbb{F}_{q^2}$ if and only if $u \in N$. In particular, if $u \in N$ and $3 \nmid (q+1)$, then F is Alltop.*

Proof. The proof is similar to the proof of Theorem 3.5. Let $L_1(x)$ and $L_2(x)$ be $\mathbb{F}_q$-additive polynomials in $\mathbb{F}_{q^2}[x]$ such that

$$L_1 \circ x^{q+2} \circ L_2 = F(x)$$

holds for all $x \in \mathbb{F}_{q^2}$. This is equivalent to the set of nonlinear equations:

$$ac^2d^q + bcd^{2q} = 1, \tag{27}$$

$$ac^{q+2} + 2cd^{q+1}a + 2c^{q+1}d^qb + d^{2q+1}b = 0, \tag{28}$$

$$2c^{q+1}da + d^{q+2}a + c^{2q+1}b + 2c^qd^{q+1}b = u, \tag{29}$$

$$ac^qd^2 + bdc^{2q} = 0. \tag{30}$$

Again, we observe that $a \neq 0$, $b \neq 0$, $c \neq 0$, and $d \neq 0$ using arguments as in the proof of Theorem 3.5.

Equation (30) leads to

$$a = \frac{-bc^q}{d}. \tag{31}$$

Combining (31) and (28), we get

$$(d^{q+1} - c^{q+1})(d^{q+1} + c^{q+1}) = 0. \tag{32}$$

Combining (31) and (27), we get

$$-bc^{q+2}d^{q-1} + bcd^{2q} = d^{q-1}bc(d^{q+1} - c^{q+1}) = 1. \tag{33}$$

From (32) and (33), we immediately obtain that

$$c^{q+1} = -d^{q+1}.$$

Then, by (29) and (31), we have

$$\begin{aligned} u &= 2c^{q+1}d\left(-\frac{bc^q}{d}\right) + d^{q+2}\left(-\frac{bc^q}{d}\right) + bc^{2q+1} + 2bc^qd^{q+1} \\ &= -2bc^{2q+1} - bc^qd^{q+1} + bc^{2q+1} + 2bc^qd^{q+1} \\ &= -bc^{2q+1} + bc^qd^{q+1} \\ &= bc^q(d^{q+1} - c^{q+1}) \\ &= c^{q-1}bc(d^{q+1} - c^{q+1}). \end{aligned}$$

Now, using (33), namely

$$d^{q-1}bc(d^{q+1} - c^{q+1}) = 1,$$

we obtain

$$bc(d^{q+1} - c^{q+1}) = \frac{1}{d^{q-1}}.$$

Therefore

$$u = c^{q-1}bc(d^{q+1} - c^{q+1}) = \frac{c^{q-1}}{d^{q-1}}.$$

Put $\alpha = \frac{c}{d} \in \mathbb{F}_{q^2}^*$. Since $c^{q+1} = -d^{q+1}$, we have

$$\alpha^{q+1} = \frac{c^{q+1}}{d^{q+1}} = -1.$$

Moreover,

$$u = \frac{c^{q-1}}{d^{q-1}} = \alpha^{q-1}.$$

Thus $u \in N$, proving necessity.

Conversely, choose $\alpha \in \mathbb{F}_{q^2}^*$ with $\alpha^{q+1} = -1$ and $\alpha^{q-1} = u$. For arbitrary $d \in \mathbb{F}_{q^2}^*$, put

$$c = \alpha d, \qquad b = \frac{1}{2\alpha d^{2q+1}}, \qquad a = -\frac{\alpha^{q-1}}{2d^{q+2}}.$$

These values satisfy (27)–(30). Also, $(c/d)^{q+1} = (a/b)^{q+1} = -1$, so both maps are invertible. This proves the equivalence. The last assertion follows from Theorem 3.1. □

We next consider a set of parameters for which F is not Alltop.

Proposition 3.3. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5. For $u \in \mathbb{F}_{q^2}^*$, let $F(x)$ be the q-cubic binomial over $\mathbb{F}_{q^2}$ given by $F(x) = x^3 + ux^{2q+1}$. Let T be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ such that $|T| = \frac{q+1}{2}$. If $u \in 3T$, then F is not Alltop.*

Proof. For $a \in \mathbb{F}_{q^2}^*$ we have

$$D_aF(x) = 3ax^2 + u\left(ax^{2q} + 2a^q x^{q+1}\right) + \text{lot}.$$

For $b \in \mathbb{F}_{q^2}^*$, we further have

$$D_bD_aF(x) = x^q\left(2uab^q + 2ua^q b\right) + x\left(6ab + 2ua^q b^q\right) + \text{lot}.$$

Dividing the terms of $D_bD_aF(x)$ by $2uab$ and $2ab$, respectively, we observe that F is not Alltop if the system

$$\begin{aligned} a^{q-1} + b^{q-1} &= 0, \\ 3 + ua^{q-1}b^{q-1} &= 0 \end{aligned} \tag{34}$$

is solvable with $a, b \in \mathbb{F}_{q^2}^*$. Let H be the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q+1$. There exists $h \in H$ such that $h_1 = h$, $h_2 = -h$, $a^{q-1} = h_1$, $b^{q-1} = h_2$ and the system in (34) is solvable if and only if

$$3 - uh^2 = 0 \iff \frac{u}{3} \in H^2 = T.$$

This completes the proof. □

The following lemma gives the remaining restriction on u.

Lemma 3.3. *Let $p \geq 5$, let q be a power of p, and let $u \in \mathbb{F}_{q^2}^*$. If $F_u(x) = x^3 + ux^{2q+1}$ is Alltop, then*

$$u^{q+1} \in \{1, 9\}.$$

Proof. Put $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^2}$, $v = u^q$ and $r = uv \in k^*$. For $a, b \in K$, half the linear part of $D_a D_b F_u$ is

$$B_u(a, b)(x) = (3ab + ua^q b^q)x + u(ab^q + a^q b)x^q.$$

Its determinant over k is

$$\mathrm{Norm}_{K/k}(3ab + ua^q b^q) - \mathrm{Norm}_{K/k}\big(u(ab^q + a^q b)\big).$$

Thus F_u is Alltop only if this determinant is nonzero for all $a, b \in K^*$.

Choose $\omega \in K$ with $\omega^q = -\omega$ and ω^2 a nonsquare in k. Write $a = a_0 + a_1\omega$, $b = b_0 + b_1\omega$. The determinant gives a polynomial $\Phi_u(a_0, a_1; b_0, b_1)$ over k, homogeneous of degree two in each pair. Put $\phi_u(S, T) = \Phi_u(S, 1; T, 1) \in k[S, T]$. In computing this polynomial, conjugation acts on coefficients in K and fixes the indeterminates S, T.

Assume that $r \notin \{1, 9\}$. Over $\overline{k}$, make the invertible fractional linear changes

$$Z = \frac{S - \omega}{S + \omega}, \qquad W = \frac{T - \omega}{T + \omega}.$$

A direct computation gives $\phi_u(S, T) = (S + \omega)^2 (T + \omega)^2 P(Z, W)$, where

$$P(Z, W) = (3 + uZW)(3ZW + v) - r(Z + W)^2. \tag{35}$$

As a polynomial in W, this is

$$u(3Z^2 - v)W^2 + (9 - r)ZW + v(3 - uZ^2).$$

Its coefficients have no common factor: such a factor would divide Z, whereas the first and last coefficients are nonzero at $Z = 0$. The discriminant is

$$D(Z) = 3\big(4urZ^4 + (27 - 18r - r^2)Z^2 + 4vr\big). \tag{36}$$

Moreover,

$$(27 - 18r - r^2)^2 - 64r^3 = (r - 1)(r - 9)^3.$$

Since the leading and constant coefficients are nonzero, $D(Z)$ has four distinct roots $\zeta_1, \ldots, \zeta_4$ in $\overline{k}$. It is therefore not a square in $\overline{k}(Z)$, and P is irreducible over $\overline{k}$. Clearing the denominators introduces no factor: for example,

$$\phi_u(-\omega, T) = 4u\omega^2\big(3(T - \omega)^2 - v(T + \omega)^2\big)$$

is not the zero polynomial, and the same holds with S, T interchanged. Hence ϕ_u is absolutely irreducible.

Let $E = k(s,t)$ be the algebraic function field defined by $\phi_u(s,t) = 0$. Its full constant field is k. After extending constants to $\overline{k}$, it has the quadratic presentation

$$\overline{k}E = \overline{k}(Z,y), \qquad y^2 = D(Z), \qquad y = 2u(3Z^2 - v)W + (9-r)Z.$$

Let P_i be the place of $\overline{k}(Z)$ defined by $Z - \zeta_i$, and let P_∞ be its pole place. Their normalized valuations satisfy

$$v_{P_i}(D) = 1 \quad (1 \le i \le 4), \qquad v_{P_\infty}(D) = -4;$$

at every other place the valuation of D is zero. By the ramification criterion for a quadratic Kummer extension, precisely the four places P_i ramify. Each has ramification index two and different exponent one; P_∞ is unramified. The Hurwitz genus formula therefore gives

$$2g(E) - 2 = 2(-2) + 4 = 0;$$

here the genus is unchanged by extension of constants. We use the function-field results in [23, Chapter 3].

Thus $g(E) = 1$. By the Hasse–Weil bound [23, Chapter 5], the number $N_1(E)$ of places of degree one satisfies

$$N_1(E) \ge q + 1 - 2\sqrt{q} > 0.$$

Choose such a place Q. If $v_Q(s) \ge 0$, put $(a_0, a_1) = (s(Q), 1)$; if $v_Q(s) < 0$, put $(a_0, a_1) = (1, 0)$. Define (b_0, b_1) in the same way using t. These pairs lie in $k^2 \setminus \{(0,0)\}$. To evaluate the defining relation at a pole of s, use $(1, s^{-1})$ instead of $(s, 1)$, and similarly for t. Bihomogeneity and reduction at Q then give

$$\Phi_u(a_0, a_1; b_0, b_1) = 0.$$

Since $\{1, \omega\}$ is a k-basis of K, the elements $a = a_0 + a_1\omega$ and $b = b_0 + b_1\omega$ are both nonzero. Their second derivative has determinant zero, a contradiction. This proves $u^{q+1} \in \{1, 9\}$. □

The next theorem completes the classification of the class C_1.

Theorem 3.7. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5, and put*

$$\mathcal{A}(q) = \{u \in \mathbb{F}_{q^2}^* : x^3 + ux^{2q+1} \text{ is Alltop}\}.$$

Then

$$\mathcal{A}(q) = \begin{cases} -3N, & 3 \mid (q+1), \\ (-3N) \sqcup N, & 3 \nmid (q+1). \end{cases}$$

Here $\sqcup$ denotes disjoint union. In particular, $|\mathcal{A}(q)| = (q+1)/2$ in the first case and $|\mathcal{A}(q)| = q + 1$ in the second case. Every Alltop member of C_1 is $\mathbb{F}_q$-EA-equivalent to x^3 or, when $3 \nmid (q+1)$, to x^{q+2}.

Proof. The inclusion from right to left follows from Theorems 3.5 and 3.6. Let $u \in \mathcal{A}(q)$ and put $F_u(x) = x^3 + ux^{2q+1}$. By Lemma 3.3, $u^{q+1} \in \{1, 9\}$. Lemma 3.2 also gives

$$N = H \setminus (-T), \qquad -N = H \setminus T.$$

Indeed, if $q \equiv 1 \pmod 4$, then $N = T$ and $-1 \notin T$; if $q \equiv 3 \pmod 4$, then $N = H \setminus T$ and $-1 \in T$.

If $u^{q+1} = 9$, then $u \in 3H$. Proposition 3.3 excludes $u \in 3T$. Thus $u \in 3(H \setminus T) = -3N$.

Suppose $u^{q+1} = 1$, so $u \in H$. If $u \in -T$, choose $h \in H$ with $uh^2 = -1$, and choose $a, b \in \mathbb{F}_{q^2}^*$ with $a^{q-1} = b^{q-1} = h$. The linear part of $D_a D_b F_u$ is

$$4ab(uhx^q + x).$$

Since $(uh)^{q+1} = 1$, this linearized polynomial is not a permutation, a contradiction. Therefore $u \in H \setminus (-T) = N$. By Theorems 3.6 and 3.1, this gives an Alltop function precisely when $3 \nmid (q + 1)$.

Finally, $-3N$ and N are disjoint: otherwise $-3 \in NN^{-1} = T$, whereas the norm of -3 is $9 \neq 1$. The cardinalities follow from $|N| = (q + 1)/2$. □

Together with the results for C_2, C_3, C_4 and the reductions for C_5, C_6, this completes the classification of q-cubic Alltop binomials over $\mathbb{F}_{q^2}$. We next show that allowing three or four terms gives no further $\mathbb{F}_q$-EA-equivalence classes.

3.3. Homogeneous q-Cubic Alltop Functions over $\mathbb{F}_{q^2}$.

The monomial and binomial classifications in Subsections 3.1 and 3.2 extend to arbitrary homogeneous q-cubics as follows.

Theorem 3.8. *Let $p \geq 5$, let q be a power of p, and put $K = \mathbb{F}_{q^2}$. A homogeneous q-cubic map*

$$F(x) = A_1x^3 + A_2x^{q+2} + A_3x^{2q+1} + A_4x^{3q}, \qquad A_i \in K,$$

is Alltop if and only if $F = M \circ G \circ L$ for invertible $\mathbb{F}_q$-linear maps L, M, where $G = x^3$ or, when $3 \nmid (q + 1)$, $G = x^{q+2}$. Thus three and four terms yield no new $\mathbb{F}_q$-EA-equivalence classes.

Proof. Put $k = \mathbb{F}_q$ and $T(a, b, c) = D_aD_bD_cF(0)/6$. Alltopness means that $T(a, b, \cdot)$ is invertible for $a, b \neq 0$. Fix $e \neq 0$ and set $A = T(e, e, \cdot)$. The product $x \circ y = A^{-1}T(e, x, y)$ is a commutative bilinear division algebra with identity e. Being two-dimensional, it is generated by one element and is associative, hence isomorphic to K. An invertible k-linear change on the input and output therefore normalizes T to $T(1, x, y) = xy$.

Choose $\theta^q = -\theta$ and put $d = \theta^2 \in k$, a nonsquare. Write $T(\theta,\theta,\theta) = d\theta + u + v\theta$ with $u, v \in k$. For $a = r + \theta$, $b = s + \theta$, the determinant of $T(a, b, \cdot)$ is

$$P(r,s) = (r^2 - d)(s^2 - d) + v(rs + d) - u(r + s).$$

Directions in k^* already give invertible multiplication maps. Thus P has no zero in k^2, and its discriminant in s,

$$\Delta(r) = (vr - u)^2 + 4(r^2 - d)\big(d(r^2 - d) - vd + ur\big),$$

is a nonzero nonsquare for every $r \in k$.

We use the same quadratic-function-field argument as in Lemma 3.3. Write $\Delta = 4dS^2R$ with S, R monic and R squarefree. If R is nonconstant, its degree is 2 or 4, so $y^2 = 4dR(x)$ has full constant field k and genus at most one. Every rational place of $k(x)$ is inert: at finite places this follows from the values of Δ, and at infinity from the nonsquare $4d$. This contradicts the Hasse–Weil bound $N_1 \geq q + 1 - 2\sqrt{q} > 0$. Consequently $\Delta = 4d(r^2 + \rho r + \sigma)^2$. Coefficient comparison gives

$$\rho = u/(2d), \qquad u(v + 2d + 2\sigma) = 0.$$

If $u \neq 0$, the remaining coefficients give $u^2 = dv^2$, impossible. For $u = 0$, putting $t = \sigma/d$ gives $t^2 = 1 + v/d$ and $(t - 3)(t + 1)^3 = 0$. Hence $v = 0$ or $v = 8d$.

The first case gives $F(x) = x^3$. In the second, $\Delta(r) = 4d(r^2 + 3d)^2$, so -3 must be a square in k. Choose $t^2 = -3$ and put $S_c(X + \theta Y) = X + c\theta Y$ for $c \in k^*$. The normalized map satisfies

$$F(X + \theta Y) = X^3 + 3dXY^2 + \theta(3X^2Y + 9dY^3) = S_{3/t}\big((S_t(X + \theta Y))^{q+2}\big).$$

The representatives have therefore reduced to those of Subsection 3.1, which also represent all the binomials by Theorem 3.7. Theorem 3.1 gives their stated Alltop conditions and the converse. □

4. p-ary Alltop Functions

Throughout this section, unless otherwise stated, $\mathbb{F}_q$ denotes a finite field of characteristic p with $q = p^n$, where p is an odd prime and $n \geq 1$. We consider finite fields of arbitrary odd characteristic in this section. It turns out that the structures considered here cannot exist in characteristic 2. Moreover, there exist interesting examples in all odd characteristics, for example in characteristic 3, and their complete study seems difficult (see Remark 4.1, Definition 4.2 and Subsection 4.2 below). This is very different from the case of classical Alltop functions, see Section 2.

Recall that any map $F : \mathbb{F}_q \to \mathbb{F}_q$ is uniquely written as the evaluation map of a polynomial in $\mathbb{F}_q[x]$ of the form

$$x \mapsto a_0 + a_1 x + \cdots + a_{q-1}x^{q-1},$$

where $a_0, a_1, \ldots, a_{q-1} \in \mathbb{F}_q$.

With this convention, a *p-ary map on* $\mathbb{F}_q$ is a map $f : \mathbb{F}_q \to \mathbb{F}_p$, in particular the image of f is in the prime field $\mathbb{F}_p$. There exists $F \in \mathbb{F}_q[x]$ such that f can be considered in its *trace representation* as the evaluation map

$$x \mapsto \mathrm{Tr}_{q/p}(F(x)),$$

and $\deg F \leq q-1$. In this representation we have $f(x) = \mathrm{Tr}(F(x)) = \mathrm{Tr}(F^p(x))$, and F is not unique if $n \geq 2$.

In this section we introduce *p-ary Alltop functions* defined on $\mathbb{F}_{p^n}$, where $n \geq 1$. The rest of the section is organized as follows. In Subsection 4.1 we recall basic facts and tools. In Subsection 4.2, Theorem 4.4 gives an infinite family of strict p-ary Alltop functions on $\mathbb{F}_{3^{3n}}$ for every $n \geq 1$, and proves strictness with respect to all homogeneous q-cubic Alltop functions for the norm–trace family when $q \equiv 2 \pmod 3$. We also construct families that are strict with respect to specified q-cubic monomial and binomial classes. We conclude the section with further characterization results in Subsection 4.3.

4.1. **Some Fundamental Results on p-ary Alltop Functions.**

Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary function. Note that if $a \in \mathbb{F}_q^*$, then its derivative $D_a f$ is also a p-ary map given by

$$x \mapsto f(x+a) - f(x),$$

where $x \in \mathbb{F}_q$.

Let $g : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary map. We say that g is *balanced* if

$$|g^{-1}(b)| = p^{n-1},$$

for all $b \in \mathbb{F}_p$. Here $g^{-1}(b)$ is the preimage of b under g, which is a subset of $\mathbb{F}_q$.

We start with a formal definition.

Definition 4.1. Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary function. We call f is *p-ary Alltop* if for each $a, b \in \mathbb{F}_q^*$, the second derivative $D_a D_b f : \mathbb{F}_q \to \mathbb{F}_p$ is balanced.

The following is a rather direct characterization.

Proposition 4.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary function. We have that f is p-ary Alltop if and only if*

$$\sum_{x \in \mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p} D_a D_b f(x)} = 0 \tag{37}$$

for all $a, b \in \mathbb{F}_{p^n}^*$. Here the values of term $D_a D_b f(x) \in \mathbb{F}_p$ in the exponent is identified with the set $\{0, \ldots, p-1\}$ so that we have an equation over the complex numbers.

Proof. Let $\theta = e^{\frac{2\pi\sqrt{-1}}{p}} \in \mathbb{C}$. It is well known that the minimal polynomial of θ over $\mathbb{Q}$ is

$$x^{p-1} + \cdots + x + 1 \in \mathbb{Q}[x].$$

For $0 \leq i \leq p-1$, let N_i be the nonnegative integer given by

$$N_i = |\{x \in \mathbb{F}_{p^n} : D_a D_b f(x) = i\}|,$$

where we consider $i \in \mathbb{F}_p$ as well. The equation in (37) is equivalent to the equation

$$N_0 + N_1\theta + \cdots + N_{p-1}\theta^{p-1} = 0. \tag{38}$$

Using the identity $1 + \theta + \cdots + \theta^{p-1} = 0$ and (38) we obtain nonnegative integers $0 \leq N_0' \leq N_0$, $0 \leq N_1' \leq N_1, \cdots, 0 \leq N_{p-1}' \leq N_{p-1}$ such that $0 \in \{N_0', \ldots, N_{p-1}'\}$ and

$$N_0' + N_1'\theta + \cdots + N_{p-1}'\theta^{p-1} = 0. \tag{39}$$

Here we assume that $\max\{N_0', \ldots, N_{p-1}'\}$ is as small as possible. Moreover one of the identities $N_0 = N_1 = \ldots = N_{p-1}$ does not hold if and only if there exists a nonzero element in $\{N_0', \ldots, N_{p-1}'\}$. If one of the identities $N_0 = N_1 = \ldots = N_{p-1}$ does not hold, then using the fact $1 + \theta + \cdots + \theta^{p-1} = 0$ and (39) we obtain a monic polynomial $g(x) \in \mathbb{Q}[x]$ of degree at most $p-2$ such that $g(\theta) = 0$. This is a contradiction to the degree of the minimal polynomial of θ over $\mathbb{Q}$. This implies that the set of identities $N_0 = N_1 = \ldots = N_{p-1}$ is equivalent to (37), which completes the proof. □

Remark 4.1. *Let $p = 2$ and $n \geq 1$ be an integer. Let $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ be a 2-ary function. For $a = b \in \mathbb{F}_{2^n}^*$ we have*

$$D_a D_a f(x) = 0$$

for all $x \in \mathbb{F}_{2^n}$. This implies that there is no 2-ary Alltop map. However, for each odd prime p, including $p = 3$, there are infinitely many p-ary Alltop functions.

Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an arbitrary map on $\mathbb{F}_{p^n}$. For $\alpha \in \mathbb{F}_{p^n}^*$, the map $\mathrm{Tr}_{p^n/p}(\alpha F(x))$ is the p-ary map given by

$$x \mapsto \mathrm{Tr}_{p^n/p}(\alpha F(x)) \tag{40}$$

for $x \in \mathbb{F}_{p^n}$, which is called *the component map of F at the component α*.

The following proposition is a motivation for the notion *p-ary Alltop*. But the class of p-ary Alltop functions is much more general than the one given by the following proposition. In particular we refer to the notion of **strict** *p-ary Alltop* functions in Definition 4.2, and their examples consisting of infinite classes presented in Subsection 4.2 below.

Proposition 4.2. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Let $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be an arbitrary map on $\mathbb{F}_{p^n}$. We have that F is Alltop on $\mathbb{F}_{p^n}$ if and only if the p-ary function $\mathrm{Tr}_{p^n/p}(\alpha F(x))$ in (40) is p-ary Alltop for each $\alpha \in \mathbb{F}_{p^n}^*$.*

Proof. Let $\alpha \in \mathbb{F}_{p^n}^*$. For $a, b \in \mathbb{F}_{p^n}^*$, let $G_{a,b}(x) : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the map on $\mathbb{F}_{p^n}$ obtained by the second derivative given by $G_{a,b}(x) = D_a D_b F(x)$. Using ([14, Theorem 7.7]) we obtain that $G_{a,b}$ is one-to-one if and only if

$$\sum_{x \in \mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p} \mathrm{Tr}_{p^n/p}(\alpha G_{a,b}(x))} = 0 \tag{41}$$

for all $\alpha \in \mathbb{F}_{p^n}^*$. Using Proposition 4.1 and (41) we complete the proof. □

The following definition is important.

Definition 4.2. Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that p is odd. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary Alltop function. We call f *strict* p-ary Alltop if there is no vectorial Alltop map $F : \mathbb{F}_q \to \mathbb{F}_q$ such that f is the component function of F given by $f(x) = \mathrm{Tr}_{q/p}(F(x))$.

More generally, for a specified class $\mathcal{C}$ of vectorial Alltop maps on a field K, we call $f : K \to \mathbb{F}_p$ *strict with respect to* $\mathcal{C}$ if $f \neq \mathrm{Tr}_{K/\mathbb{F}_p}(\alpha F)$ for every $F \in \mathcal{C}$ and $\alpha \in K^*$. On $K = \mathbb{F}_{q^m}$, let $\mathcal{C}_r$ consist of the homogeneous q-cubic Alltop maps with coefficients in K and at most r nonzero terms $x^{q^i+q^j+q^\ell}$, $0 \leq i \leq j \leq \ell < m$, in the fixed field coordinate. We use *monomial-strict*, *binomial-strict* and *trinomial-strict* for strictness with respect to $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$, respectively. These term restrictions concern the displayed maps, not their equivalence classes.

In Subsection 4.2, we construct an infinite family of strict p-ary Alltop functions in characteristic 3, a family strict with respect to all homogeneous q-cubic Alltop functions when $q \equiv 2 \pmod 3$, and binomial-strict families in every odd characteristic.

The following notion of equivalences are suitable for p-ary functions in terms of Alltop property.

Definition 4.3. Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that p is odd. Let $f, g : \mathbb{F}_q \to \mathbb{F}_p$ be p-ary functions. We say that f *and g are extended affine equivalent (EA-equivalent)* if there exist an affine map $\phi : \mathbb{F}_q \to \mathbb{F}_p$ and an invertible affine map $L : \mathbb{F}_q \to \mathbb{F}_q$ such that

$$g + \phi = f \circ L.$$

Moreover we say that f *and g are extended quadratic equivalent (EQA-equivalent)* if there exist an (at most) quadratic map $\phi : \mathbb{F}_q \to \mathbb{F}_p$ and an invertible affine map $L : \mathbb{F}_q \to \mathbb{F}_q$ such that

$$g + \phi = f \circ L.$$

Remark 4.2. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that p is odd. Let $f, g : \mathbb{F}_q \to \mathbb{F}_p$ be p-ary functions. If f and g are extended affine equivalent, then they are extended quadratic equivalent. However the converse does not hold. For example the p-ary functions $f(x) = \mathrm{Tr}_{p^n/p}(x^{p+1})$ and $g(x) = \mathrm{Tr}_{p^n/p}(x)$ are extended quadratic equivalent, but they are not extended affine equivalent.*

The following proposition follows immediately from the definition. We leave its proof to the reader.

Proposition 4.3. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that p is odd. Let $f, g : \mathbb{F}_q \to \mathbb{F}_p$ be p-ary functions. Assume that f and g are extended quadratic equivalent. We have that f is p-ary Alltop if and only if g is p-ary Alltop.*

If $n = 1$, then the notions of Alltop and p-ary Alltop coincide. Moreover we have a full classification of p-ary Alltop (and hence Alltop) functions if $n = 1$ upto extended quadratic equivalence.

Proposition 4.4. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that $n = 1$ and $p > 3$. Then $F : \mathbb{F}_p \to \mathbb{F}_p$ is Alltop if and only if F is extended quadratic equivalent to the map $G : \mathbb{F}_p \to \mathbb{F}_p$ given by $G(x) = x^3$.*

Proof. It is well known that if $F : \mathbb{F}_p \to \mathbb{F}_p$ is planar, then $p > 2$ and F is extended affine equivalent to the map x^2 on $\mathbb{F}_p$.

Assume that $F : \mathbb{F}_p \to \mathbb{F}_p$ is Alltop. We assume that F is monic without loss of generality upto extended affine equivalence. Let d be the degree of F so that we have

$$F(x) = x^d + \text{lot}.$$

If $d = 3$, then this completes the proof as the terms in lot are extended quadratic equivalent to the zero map on $\mathbb{F}_q$.

If $d \leq 2$, then we get a contradiction as the zero map is not p-ary Alltop.

Assume that $d > 3$. Then there exists $a \in \mathbb{F}_p^*$ such that the degree of D_aF is at least 3. However D_aF is planar and its degree cannot be different than 2. This completes the proof.

□

4.2. **Strict p-ary Alltop Functions and Related Families.**

Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that p is odd. In this subsection we first construct an infinite family of strict p-ary Alltop functions over $\mathbb{F}_{3^{3n}}$. For $q \equiv 2 \pmod 3$, the norm–trace construction is strict with respect to all homogeneous q-cubic Alltop functions, without a term restriction. It is binomial-strict over $\mathbb{F}_{q^3}$ in every odd characteristic. We then show that it is impossible to obtain any

strict p-ary Alltop function from a related and natural monomial class over $\mathbb{F}_{q^2}$. Finally we construct a second infinite family of binomial-strict p-ary Alltop functions over $\mathbb{F}_{q^2}$.

First we consider our first class.

Theorem 4.4. *Let p be an odd prime and $n \geq 1$ be an integer. Put $q = p^n$. For $A \in \mathbb{F}_{q^3}^*$, let $f : \mathbb{F}_{q^3} \to \mathbb{F}_p$ be the p-ary map on $\mathbb{F}_{q^3}$ given by*

$$f(x) = \mathrm{Tr}_{q^3/p}(Ax^{q^2+q+1}). \tag{42}$$

Then f is p-ary Alltop if and only if

$$\mathrm{Tr}_{q^3/q}(A) = A^{q^2} + A^q + A \neq 0.$$

If $p = 3$ and $\mathrm{Tr}_{q^3/q}(A) \neq 0$, then f is strict p-ary Alltop. Thus this construction gives an infinite family of strict p-ary Alltop functions on $\mathbb{F}_{3^{3n}}$, $n \geq 1$. If $q \equiv 2 \pmod 3$, every nonzero function in this class is strict with respect to all homogeneous q-cubic Alltop functions, with any number of terms; in fact, it has no vectorial Alltop lift of algebraic degree at most three. For every odd p, the nonzero functions in this class are binomial-strict. There are exactly $q-1$ distinct nonzero functions, each represented by q^2 values of A.

Proof. Put $c = \mathrm{Tr}_{q^3/q}(A)$. By transitivity of the trace,

$$f(x) = \mathrm{Tr}_{q/p}\big(c\mathrm{Norm}_{q^3/q}(x)\big).$$

Thus $c = 0$ gives $f = 0$. For $c \neq 0$ and $a, b \in \mathbb{F}_{q^3}^*$, the identity in (5) gives

$$D_aD_bf(x) = \mathrm{Tr}_{q^3/p}\big(cx(a^{q^2}b^q + a^qb^{q^2})\big) + \text{constant}.$$

Here

$$a^{q^2}b^q + a^qb^{q^2} \neq 0. \tag{43}$$

Otherwise $(a/b)^{q-1} = -1$, whose norm to $\mathbb{F}_q$ would be both 1 and -1. Hence every D_aD_bf is a nonconstant affine function and is balanced, so f is p-ary Alltop. Surjectivity of the norm and nondegeneracy of the trace pairing show that distinct $c \in \mathbb{F}_q^*$ give distinct functions; each c has q^2 preimages A.

If $p = 3$, there is no vectorial Alltop function on $\mathbb{F}_{q^3}$ by Theorem 2.3. Hence f cannot be a component of any vectorial Alltop function and is strict p-ary Alltop. Since this holds for every $n \geq 1$, it gives the stated infinite family.

For $p \geq 5$, the ten homogeneous q-cubic monomials on $\mathbb{F}_{q^3}$ belong to four distinct p-cyclotomic cosets modulo $q^3 - 1$, represented by $3, q + 2, 2q + 1, q^2 + q + 1$. Their base-$p$ digit patterns show that the first three cosets have length $3n$, and the norm coset has length n. Suppose $f = \mathrm{Tr}_{q^3/p}(\alpha G)$ with $\alpha \neq 0$ and a q-cubic Alltop map G having at most two terms. Since the reduced trace of f contains only the nonzero norm term, that monomial must occur in G. Any second term would give a nonzero reduced

coefficient in one of the other three cosets, a contradiction. Thus G is a multiple of x^{q^2+q+1}, which is not Alltop by Theorem 3.2. This proves binomial-strictness.

Finally assume $q \equiv 2 \pmod 3$, so that $p \equiv 2 \pmod 3$ and n is odd. We first show that a homogeneous cubic Alltop map C on an odd-dimensional $\mathbb{F}_p$-space is a permutation. For $a \neq 0$, put

$$Q_a(x) = D_a C(x - a/2) - C(a)/4.$$

Then Q_a is homogeneous quadratic and planar. By polarization, $Q_a(x) = Q_a(z)$ forces $x = z$ or $x = -z$; in particular, $Q_a^{-1}(0) = \{0\}$ and $Q_a(a) = 3C(a) \neq 0$. For $\nu_a(y) = |Q_a^{-1}(y)|$ and $s \in \mathbb{F}_p^*$, we have

$$\nu_a(sy) - 1 = \eta(s)\big(\nu_a(y) - 1\big),$$

where η is the quadratic character of $\mathbb{F}_p$. Indeed, for $b \neq 0$ the linear part of $D_b Q_a$ is invertible, so every nonzero component of Q_a is a nondegenerate quadratic form in an odd number of variables. Scaling this form by s multiplies its quadratic Gauss sum by $\eta(s)$, and character orthogonality gives the identity. Also $\nu_a(y) \in \{0, 2\}$ for $y \neq 0$. Since $-1/12$ is a nonsquare in $\mathbb{F}_p$ and $\nu_a(3C(a)) = 2$, we obtain $\nu_a(-C(a)/4) = 0$. Thus $D_a C$ has no zero for any $a \neq 0$, proving that C is a permutation.

Suppose now that a vectorial Alltop map G of algebraic degree at most three has component $f \neq 0$. Its homogeneous cubic part C is still Alltop, since removing terms of degree at most two only changes second derivatives by constants. As f is homogeneous cubic, it is also the same component of C. The preceding argument applies in dimension $3n$, so C is a permutation and every nonzero component is balanced. On the other hand, writing $c = \mathrm{Tr}_{q^3/q}(A) \neq 0$, surjectivity of the norm gives

$$|f^{-1}(0)| = 1 + (q/p - 1)(q^2 + q + 1) = \frac{q^3}{p} - \frac{(p-1)(q^2+q)}{p} < \frac{q^3}{p},$$

a contradiction. □

Next we study another monomial q-cubic class having infinitely many p-ary Alltop functions. However, we will show this class does not include any strict p-ary Alltop function in the next corollary.

Theorem 4.5. *Let p be an odd prime and $n \geq 1$ be an integer. Put $q = p^n$. For $A \in \mathbb{F}_{q^2}^*$, let $f : \mathbb{F}_{q^2} \to \mathbb{F}_p$ be the p-ary map on $\mathbb{F}_{q^2}$ given by*

$$f(x) = \mathrm{Tr}_{q^2/p}(Ax^{q+2}).$$

Let $g : \mathbb{F}_{q^2} \to \mathbb{F}_p$ be the p-ary map on $\mathbb{F}_{q^2}$ given by

$$g(x) = \mathrm{Tr}_{q^2/p}(x^{q+2}).$$

Then f is p-ary Alltop if and only if g is a p-ary Alltop. Moreover g is a p-ary Alltop or not as determined as follows:

- **Case** $p = 3$**:** *g is not p-ary Alltop.*
- **Case** $p > 3$ **and** $p \equiv 3 \mod 4$**:** *We have two subcases:*
  - **Subcase** n**: even:** *g is p-ary Alltop.*
  - **Subcase** n**: odd:** *g is p-ary Alltop $\iff$ 3 is a non-square modulo p.*
- **Case** $p > 3$ **and** $p \equiv 1 \mod 4$**:** *We have two subcases:*
  - **Subcase** n**: even:** *g is p-ary Alltop.*
  - **Subcase** n**: odd:** *g is p-ary Alltop $\iff$ 3 is a square modulo p.*

Proof. Put $F(x) = x^{q+2}$. Let $a, b \in \mathbb{F}_{q^2}^*$. Using the methods in the sketch of a proof of Theorem 3.1, in particular the identity in (1) we have

$$D_a D_b F(x) = 2abx^q + (2ab^q + 2a^q b)x + \text{lot}.$$

This implies

$$\begin{aligned}
&D_a D_b f(x) \\
&= \text{Tr}_{q^2/p}\left(2Aabx^q + (2Aab^q + 2Aa^q b)x\right) + \text{lot} \\
&= \text{Tr}_{q/p} \circ \text{Tr}_{q^2/q}\left(2Aabx^q + (2Aab^q + 2Aa^q b)x\right) + \text{lot} \\
&= \text{Tr}_{q/p} \circ \text{Tr}_{q^2/q}\left((2A^q a^q b^q + 2Aab^q + 2Aa^q b)x\right) + \text{lot} \\
&= \text{Tr}_{q^2/p}\left((2A^q a^q b^q + 2Aab^q + 2Aa^q b)x\right) + \text{lot}
\end{aligned}$$

Dividing by $2A^q a^q b^q$ we obtain that f is p-ary Alltop if and only if

$$1 + \left(\frac{1}{aA}\right)^{q-1} + \left(\frac{1}{bA}\right)^{q-1} \neq 0 \tag{44}$$

for all $a, b \in \mathbb{F}_{q^2}^*$.

Let H be the subgroup of $\mathbb{F}_{q^2}^*$ with $|H| = q + 1$. For any $A \in \mathbb{F}_{q^2}^*$ we have

$$H = \left\{ \frac{1}{hA^{q-1}} : h \in H \right\}.$$

These arguments imply that $f(x)$ is p-ary Alltop if and only if $g(x)$ is p-ary Alltop. Moreover $g(x)$ is not p-ary Alltop if and only if there exist $h_1, h_2 \in H$ such that the equation

$$1 + h_1 + h_2 = 0 \tag{45}$$

is solvable with $h_1, h_2 \in H$.

Let θ be a generator of $\mathbb{F}_{q^2}^*$. Put $\theta_1 = \theta^{q+1}$ and $w = \theta^{(q+1)/2}$. Note that θ_1 is a generator of $\mathbb{F}_q^*$ and

$$w + w^q = w(1 + w^{q-1}) = w(1 + \theta^{(q^2-1)/2}) = w(1 - 1) = 0. \tag{46}$$

Put also $D = w^{q+1}$. We observe that

$$D = \theta^{\frac{(q+1)(q+1)}{2}} = \theta_1^{(q+1)/2}.$$

In particular D is in $\mathbb{F}_q^*$. Furthermore we have

$$D \text{ is a square in } \mathbb{F}_q^* \iff (q+1)/2 \text{ is even } \iff q \equiv 3 \mod 4, \tag{47}$$

and

$$D \text{ is a non-square in } \mathbb{F}_q^* \iff (q+1)/2 \text{ is odd } \iff q \equiv 1 \mod 4. \tag{48}$$

Note that $\{1, w\}$ is a basis of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. Let $h_1 = x_1 + y_1 w$ and $h_2 = x_2 + y_2 w$ with $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$. We obtain that there exist $h_1, h_2 \in H$ such that (45) is solvable if and only if there exist $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ such that the following system is solvable:

$$\begin{aligned} x_1 + x_2 + 1 &= 0, \\ y_1 + y_2 &= 0, \\ x_1^2 + D y_1^2 &= 1, \\ x_2^2 + D y_2^2 &= 1. \end{aligned} \tag{49}$$

Here we use the fact that for $x_1, y_1 \in \mathbb{F}_q$ we have

$$\begin{aligned} x_1 + y_1 w \in H &\iff (x_1 + y_1 w)^{q+1} = 1 \\ &\iff (x_1 + y_1 w)(x_1 + y_1 w)^q = 1 \\ &\iff x_1^2 + D y_1^2 + x_1 y_1 (w + w^q) = 1 \\ &\iff x_1^2 + D y_1^2 = 1, \end{aligned}$$

where we use (46).

Putting $x_2 = -1 - x_1$, $y_2 = -y_1$ and $x_1^2 + D y_1^2 = 1$, the last equation in (49) becomes

$$1 + x_1^2 + 2x_1 + D y_1^2 = 1 \iff 1 + 2x_1 + 1 = 1 \iff x_1 = \frac{-1}{2}.$$

Hence the system in (49) has a solution with $x_1, y_1, x_2, y_2 \in \mathbb{F}_q$ if and only if the equation

$$\frac{1}{4} + D y_1^2 = 1 \iff D y_1^2 = \frac{3}{4} \tag{50}$$

is solvable with $y_1 \in \mathbb{F}_q$.

If $p = 3$, then $y_1 = 0$ is a solution of (50).

Assume that $p > 3$ and $p \equiv 3 \mod 4$. First consider the subcase that n is even. We have $q - 1 \equiv 0 \mod 4$ and hence D is a non-square in $\mathbb{F}_q^*$ by (48). As n is even, 3 is a square in $\mathbb{F}_q^*$. These imply that (50) has no solution.

Next consider the subcase that n is odd. We have $q-1 \equiv 2 \mod 4$ and hence D is a square in $\mathbb{F}_q^*$ by (47). As n is odd, 3 is a square in $\mathbb{F}_q^*$ if and only if 3 is a square modulo p. These imply that (50) has no solution if and only if 3 is a non-square modulo p.

Assume that $p > 3$ and $p \equiv 1 \mod 4$. We have $q - 1 \equiv 0 \mod 4$ and hence D is a non-square in $\mathbb{F}_q^*$ by (48) . First consider the subcase that n is even. As n is even, 3 is a square in $\mathbb{F}_q^*$. These imply that (50) has no solution. Next consider the subcase that n is odd. As n is odd, 3 is a square in $\mathbb{F}_q^*$ if and only if 3 is a square modulo p. These imply that (50) has no solution if and only if 3 is a square modulo p. □

Note that the form of p-ary Alltop functions in Theorems 4.4 and 4.5 are related. In characteristic 3, Theorem 4.4 gives an infinite family of strict p-ary Alltop functions. However, in the following corollary, we prove that there is no strict p-ary Alltop functions in the form of Theorem 4.5.

Corollary 4.1. *Let p be an odd prime, let $q = p^n$, and let $A \in \mathbb{F}_{q^2}^*$. If*

$$f(x) = \mathrm{Tr}_{q^2/p}(Ax^{q+2})$$

is p-ary Alltop, then f is not strict p-ary Alltop.

Proof. For $p = 3$, the hypothesis is impossible by Theorem 4.5. Assume that

$$f(x) = \mathrm{Tr}_{q^2/p}(Ax^{q+2})$$

is p-ary Alltop. By Theorem 4.5, one of the cases listed there holds.

In Case $p > 3$ and n even, we have $q = p^n \equiv 1 \pmod 3$, and therefore $3 \nmid (q+1)$.

Now assume that n is odd. If $p \equiv 3 \pmod 4$ and 3 is a non-square modulo p, then $p \equiv 7 \pmod{12}$. Hence $p \equiv 1 \pmod 3$, and so $q \equiv 1 \pmod 3$. Thus $3 \nmid (q+1)$.

Similarly, if $p \equiv 1 \pmod 4$ and 3 is a square modulo p, then $p \equiv 1 \pmod{12}$. Hence again $p \equiv 1 \pmod 3$, and so $q \equiv 1 \pmod 3$. Thus $3 \nmid (q+1)$.

Therefore, whenever f is p-ary Alltop, we have $3 \nmid (q+1)$. By Theorem 3.1, the vectorial monomial x^{q+2} is Alltop over $\mathbb{F}_{q^2}$. Hence Ax^{q+2} is also Alltop, and

$$f(x) = \mathrm{Tr}_{q^2/p}(Ax^{q+2})$$

is a component of a vectorial Alltop function. Therefore f is not strict. □

Next we present our second infinite class of binomial-strict p-ary Alltop functions. This second class is a q-binomial trace class over $\mathbb{F}_{q^2}$.

We will use the following lemma in the proof of the following theorem below.

Lemma 4.1. *Let $\mathbb{F}_q$ be a finite field of characteristic at least 5, and let*

$$H = \{h \in \mathbb{F}_{q^2}^* : h^{q+1} = 1\}.$$

Then

$$-2 \notin (1+H)(1+H)$$

if and only if 3 is a square in $\mathbb{F}_q$.

Proof. We first show that $-2 \in (1+H)(1+H)$ if and only if 3 is a non-square in $\mathbb{F}_q$. Assume

$$-2 = (1+h_1)(1+h_2)$$

for some $h_1, h_2 \in H$. Since $-2 \neq 0$, we have $h_1 \neq -1$, and hence

$$h_2 = \frac{-2}{1+h_1} - 1 = \frac{-3-h_1}{1+h_1}.$$

The condition $h_2 \in H$ is equivalent to $h_2^{q+1} = 1$. Since $h_1 \in H$, we have $h_1^q = h_1^{-1}$. Thus this condition is equivalent to

$$\left(\frac{-3-h_1}{1+h_1}\right)\left(\frac{-3-h_1^{-1}}{1+h_1^{-1}}\right) = 1.$$

After simplification this gives

$$h_1 + h_1^{-1} = -4,$$

or equivalently

$$h_1^2 + 4h_1 + 1 = 0.$$

The discriminant is $12 = 4 \cdot 3$.

If 3 is a square in $\mathbb{F}_q$, then the roots of $X^2 + 4X + 1$ lie in $\mathbb{F}_q$. But an element of $\mathbb{F}_q \cap H$ has square 1, and neither 1 nor -1 is a root of $X^2 + 4X + 1$ in characteristic at least 5. Hence no such h_1 exists.

If 3 is a non-square in $\mathbb{F}_q$, then the two roots of $X^2 + 4X + 1$ lie in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ and are conjugate over $\mathbb{F}_q$. Since their product is 1, each root h satisfies $h^q = h^{-1}$, hence belongs to H. Therefore a solution exists. This proves the claim, and the lemma follows. □

Now we are ready for the second infinite class of binomial-strict p-ary Alltop functions.

Theorem 4.6. *Let p be a prime with $p \geq 5$ and let $n \geq 1$ be an integer. Put $q = p^n$. Assume that 3 is a square in $\mathbb{F}_q$. For each $\lambda \in \mathbb{F}_q^*$, define*

$$f_\lambda : \mathbb{F}_{q^2} \to \mathbb{F}_p$$

by

$$f_\lambda(x) = \mathrm{Tr}_{q^2/p}\left(\lambda x^3 + \lambda x^{q+2}\right).$$

Then f_λ is a monomial-strict p-ary Alltop function. Moreover, f_λ is binomial-strict if and only if $q \equiv 3 \pmod 4$. It is a component of a four-term homogeneous q-cubic Alltop function.

Proof. Put $H = \{h \in \mathbb{F}_{q^2}^* : h^{q+1} = 1\}$. For $a, b \in \mathbb{F}_{q^2}^*$,

$$D_a D_b f_\lambda(x) = \mathrm{Tr}_{q^2/p}\left(2\lambda ab(3 + a^{q-1} + b^{q-1} + a^{q-1}b^{q-1})x\right) + \text{lot}.$$

This is balanced for all $a, b \neq 0$ if and only if $-2 \notin (1 + H)(1 + H)$, which holds by Lemma 4.1. Thus f_λ is p-ary Alltop.

The exponents 3 and $q + 2$ lie in distinct p-cyclotomic cosets modulo $q^2 - 1$, each of length $2n$: their base-p digit patterns are one 3, and a 2 and a 1 separated by n positions. Consequently the two coefficients in

$$\mathrm{Tr}_{q^2/p}(Ax^3 + Bx^{q+2})$$

are uniquely determined. Hence f_λ is monomial-strict.

If $q \equiv 1 \pmod 4$, then $1 \in N$ by Lemma 3.2. Since 3 is a square, -3 is also a square, so $\mathbb{F}_q$ contains the primitive cube roots of unity and $3 \nmid (q + 1)$. Hence $x^3 + x^{2q+1}$ is Alltop by Theorem 3.7, and

$$\mathrm{Tr}_{q^2/p}\left(\lambda(x^3 + x^{2q+1})\right) = f_\lambda(x).$$

Thus f_λ is not binomial-strict in this case.

Suppose $q \equiv 3 \pmod 4$. The binomial classes C_3, C_4 have only one of the two reduced trace terms, so cannot give f_λ. There are no Alltop maps in C_2, C_6 by Theorem 3.4 and the reduction in Subsection 3.2. A component of C_1 or C_5 has the form, respectively,

$$\mathrm{Tr}_{q^2/p}\left(Ax^3 + (Au)^q x^{q+2}\right), \qquad \mathrm{Tr}_{q^2/p}\left((Au)^q x^3 + Ax^{q+2}\right).$$

Equality with f_λ forces $A = \lambda$ and $(Au)^q = \lambda$, hence $u = 1$. But $1 \notin N$ by Lemma 3.2, and $1 \notin -3N$ because elements of $-3N$ have norm $9 \neq 1$. Theorem 3.7 excludes C_1 with parameter 1. The explicit map $u \mapsto u^{-q}$ in Subsection 3.2 excludes C_5 with parameter 1 as well. This proves the stated binomial-strictness criterion.

Finally, choose $t \in \mathbb{F}_q$ with $t^2 - 4t + 1 = 0$, which is possible because 3 is a square. Then $t^2 \neq 1$ and $1 + t^3 = 3t(1 + t) \neq 0$. The map $x + tx^q$ is therefore invertible, so

$$G_t(x) = \frac{(x + tx^q)^3}{1 + t^3} \tag{51}$$

is a four-term Alltop function. Expanding the cube and using $\mathrm{Tr}(y) = \mathrm{Tr}(y^q)$ gives

$$\mathrm{Tr}_{q^2/p}(\lambda G_t(x)) = \mathrm{Tr}_{q^2/p}\left(\lambda x^3 + \frac{3\lambda(t + t^2)}{1 + t^3}x^{q+2}\right) = f_\lambda(x).$$

Thus the family is not strict without the term restriction. □

In the next corollary we identify when the required condition on 3 holds and obtain an infinite family of binomial-strict p-ary Alltop functions.

Corollary 4.2. *Let p be a prime with $p \geq 5$ and let $n \geq 1$ be an integer. Put $q = p^n$. Assume that one of the following cases holds:*

- *Case 1: n is even.*
- *Case 2: n is odd and $p \equiv \pm 1 \pmod{12}$.*

For $\lambda \in \mathbb{F}_q^*$, let $f_\lambda : \mathbb{F}_{q^2} \to \mathbb{F}_p$ be the p-ary map on $\mathbb{F}_{q^2}$ given by

$$f_\lambda(x) = \mathrm{Tr}_{q^2/p}\left(\lambda x^3 + \lambda x^{q+2}\right);$$

Then f_λ is a monomial-strict p-ary Alltop function. It is binomial-strict precisely when n is odd and $p \equiv 11 \pmod{12}$.

Proof. By Theorem 4.6, it is enough to determine when 3 is a square in $\mathbb{F}_q$. If n is even, then every element of $\mathbb{F}_p^*$ is a square in $\mathbb{F}_q$; in particular, 3 is a square in $\mathbb{F}_q$.

If n is odd, then 3 is a square in $\mathbb{F}_q$ if and only if 3 is a square in $\mathbb{F}_p$. For primes $p > 3$, by the standard consequence of quadratic reciprocity,

$$3 \in (\mathbb{F}_p^*)^2 \quad \Longleftrightarrow \quad p \equiv \pm 1 \pmod{12}.$$

Finally, $q \equiv 3 \pmod 4$ holds exactly when n is odd and $p \equiv 3 \pmod 4$; among the stated cases this is $p \equiv 11 \pmod{12}$. The binomial-strictness assertion follows from Theorem 4.6. □

4.3. **Characterization Results on p-ary Alltop Functions.**

In Subsection 4.2, we constructed strict p-ary Alltop functions in characteristic 3, proved strictness with respect to all homogeneous q-cubic Alltop functions when $q \equiv 2 \pmod 3$, and obtained families with class-relative strictness for $p \geq 5$. Nevertheless it seems difficult to decide if a given p-ary function on $\mathbb{F}_{p^n}$ is p-ary Alltop or not in general.

In this subsection we present two results providing two different characterization results on p-ary Alltop functions.

First we recall some notation. Let p be an odd prime and $n \geq 1$ be an integer. A polynomial $D(x)$ is called *a Dembowski-Ostrom polynomial* over $\mathbb{F}_{p^n}$ if

$$D(x) = \sum_{0 \leq i \leq j \leq n-1} D_{i,j} x^{p^i + p^j} \in \mathbb{F}_{p^n}[x]. \tag{52}$$

A polynomial $A(x)$ is called *an $\mathbb{F}_p$-additive over $\mathbb{F}_{p^n}$* if

$$A(x) = \sum_{0 \leq i \leq n-1} A_i x^{p^i} \in \mathbb{F}_{p^n}[x]. \tag{53}$$

A p-ary map $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ on $\mathbb{F}_{p^n}$ is called a *p-ary cubic function on $\mathbb{F}_{p^n}$* if there exist a Dembowski-Ostrom polynomial $D(x)$ over $\mathbb{F}_{p^n}$ in the form (52), an $\mathbb{F}_p$-additive polynomial $A(x)$ over $\mathbb{F}_{p^n}$ in the form (53) and an $\mathbb{F}_p$-affine map $\alpha : \mathbb{F}_{p^n} \to \mathbb{F}_p$ in the form

$$\alpha(x) = \mathrm{Tr}_{p^n/p}(\alpha_1 x) + \alpha_0, \qquad \alpha_1 \in \mathbb{F}_{p^n},\ \alpha_0 \in \mathbb{F}_p \tag{54}$$

such that

$$f(x) = \mathrm{Tr}_{p^n/p}(xD(x)) + \mathrm{Tr}_{p^n/p}(xA(x)) + \alpha(x).$$

Let $B : \mathbb{F}_{p^n} \times \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ be the symmetric bilinear form given by

$$B(x, y) = D(x + y) - D(x) - D(y). \tag{55}$$

We fix one such trace representation. It need not determine D and B uniquely, but the map $L_{a,b}^{(f)}$ below is independent of the choice, being the linear part of $D_a D_b f$.

Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be a p-ary cubic function on $\mathbb{F}_{p^n}$. For each $a, b \in \mathbb{F}_{p^n}$ we define the corresponding $\mathbb{F}_p$-linear map $L_{a,b}^{(f)}$ as follows:

$$\begin{array}{rcl} L_{a,b}^{(f)} : \mathbb{F}_{p^n} & \to & \mathbb{F}_p \\ x & \mapsto & \mathrm{Tr}_{p^n/p}(xB(a, b)) + \mathrm{Tr}_{p^n/p}(aB(x, b)) + \mathrm{Tr}_{p^n/p}(bB(a, x)). \end{array}$$

Let $\zeta : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the zero map given by $\zeta(x) = 0$ for all $x \in \mathbb{F}_{p^n}$. It is not difficult to observe that $L_{a,b}^{(f)} = \zeta$ if $a = 0$ or $b = 0$.

Now we are ready to present our first characterization result in this subsection.

Theorem 4.7. *Let p be an odd prime and $n \geq 1$ be an integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an arbitrary cubic p-ary function over $\mathbb{F}_{p^n}$. For each $a, b \in \mathbb{F}_{p^n}$, let $L_{a,b}^{(f)} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be the corresponding $\mathbb{F}_p$-linear map defined in (56). Then f is p-ary Alltop if and only if $L_{a,b}^{(f)} \neq \zeta$ whenever both the conditions $a \neq 0$ and $b \neq 0$ hold, where $\zeta : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is the zero map.*

Proof. Assume that $a, b \in \mathbb{F}_{p^n}^*$. It follows from a direct computation that there exists $c \in \mathbb{F}_p$ such that

$$D_a D_b f(x) = L_{a,b}^{(f)}(x) + c$$

for each $x \in \mathbb{F}_{p^n}$. Here the constant $c \in \mathbb{F}_p$ depends on f, a and b.

This implies that f is p-ary Alltop if and only if the map $L_{a,b}^{(f)} : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is balanced. An arbitrary $\mathbb{F}_p$-linear map $L : \mathbb{F}_{p^n} \to \mathbb{F}_p$ is balanced if and only if $L \neq \zeta$. This completes the proof. □

Let p be an odd prime and $n \geq 1$ be an integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an p-ary function over $\mathbb{F}_{p^n}$. For $\alpha \in \mathbb{F}_{p^n}$, the *Walsh transform of f* is the function $\hat{f} : \mathbb{F}_{p^n} \to \mathbb{C}$, which is defined as (see, for example, [6], [16], or [20]).

$$\begin{array}{rcl} \hat{f}(\alpha) & \to & \mathbb{C} \\ x & \mapsto & \sum_{x\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(f(x)-\mathrm{Tr}_{p^n/p}(\alpha x))}. \end{array} \tag{56}$$

For integer $i \geq 0$, let S_i of $2i$-th moment of the Walsh transform of f given by

$$S_i(f) = \sum_{\alpha\in\mathbb{F}_{p^n}} |\hat{f}(\alpha)|^{2i}. \tag{57}$$

Here we have the convention that $S_0(f) = p^n$. We refer to [15] and [16] for very interesting results on $S_{2i}(f)$ related to bent functions. Note that $S_1 = p^{2n}$ by Parseval's identity [6].

Our second characterization results is a one sided result presented in the following proposition.

Proposition 4.5. *Let p be an odd prime and $n \geq 1$ be an integer. Let $f : \mathbb{F}_{p^n} \to \mathbb{F}_p$ be an arbitrary p-ary function over $\mathbb{F}_{p^n}$. Let $S_2(f)$ be the 4-th moment of the Walsh transform of f, which is defined in (57). If f is a p-ary Alltop function, then*

$$S_2(f) = p^{2n}\left(2p^n - 1\right).$$

Proof. We use some methods from [15] in this proof. Let $\alpha \in \mathbb{F}_{p^n}$. Using the definition of $\hat{f}(\alpha)$ in (56) we obtain

$$\hat{f}(\alpha)\overline{\hat{f}(\alpha)} = \sum_{x\in\mathbb{F}_{p^n}} \sum_{y\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(f(x)-f(y))} e^{\frac{2\pi\sqrt{-1}}{p}(\mathrm{Tr}_{p^n/p}(\alpha(y-x)))}.$$

This implies

$$|\hat{f}(\alpha)|^4 = \sum_{x\in\mathbb{F}_{p^n}} \sum_{y\in\mathbb{F}_{p^n}} \sum_{u\in\mathbb{F}_{p^n}} \sum_{v\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(f(x)-f(y)+f(u)-f(v))} e^{\frac{2\pi\sqrt{-1}}{p}(\mathrm{Tr}_{p^n/p}(\alpha(y-x+v-u)))}.$$

Using the definition of $S_2(f)$ in (57) we obtain

$$\begin{array}{rcl} S_2(f) & = & \sum_{\alpha\in\mathbb{F}_{p^n}} |\hat{f}(\alpha)|^4 \\ & = & \sum_{x\in\mathbb{F}_{p^n}} \sum_{y\in\mathbb{F}_{p^n}} \sum_{u\in\mathbb{F}_{p^n}} \sum_{v\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(f(x)-f(y)+f(u)-f(v))} \\ & & \cdot \sum_{\alpha\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(\mathrm{Tr}_{p^n/p}(\alpha(y-x+v-u)))} \end{array}$$

For $z \in \mathbb{F}_{p^n}$ we have

$$\sum_{\alpha\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(\mathrm{Tr}_{p^n/p}(\alpha z))} = \begin{cases} p^n & \text{if } z = 0, \\ 0 & \text{otherwise.} \end{cases}$$

Using the last two identities and putting $v = u + x - y$ we obtain

$$S_2(f) = p^n \sum_{x\in\mathbb{F}_{p^n}} \sum_{y\in\mathbb{F}_{p^n}} \sum_{u\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(f(x)-f(y)+f(u)-f(u+x-y))}.$$

It is easy to observe that the multisets

$$\{* : f(x) - f(y) + f(u) - f(u + x - y) : x, y, u \in \mathbb{F}_{p^n} *\}$$

and

$$\{*D_a D_b f(x) : a, b, x \in \mathbb{F}_{p^n} *\}$$

are the same. These arguments imply that

$$S_2(f) = p^n \sum_{a\in\mathbb{F}_{p^n}} \sum_{b\in\mathbb{F}_{p^n}} \sum_{x\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(D_a D_b f(x))}.$$

Let $T \subseteq \mathbb{F}_{p^n} \times \mathbb{F}_{p^n}$ be the subset

$$T = \{(a, b) : a = 0 \text{ or } b = 0\}.$$

It is clear that $|T| = p^n + p^n - 1 = 2p^n - 1$ and

$$D_a D_b f(x) = 0 \text{ if } (a, b) \in T \text{ and } x \in \mathbb{F}_{p^n}.$$

Hence we have

$$S_2(f) = p^{2n}(2p^n - 1) + p^n \sum_{a\in\mathbb{F}^*_{p^n}} \sum_{b\in\mathbb{F}^*_{p^n}} \sum_{x\in\mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p}(D_a D_b f(x))}.$$

Using Proposition 4.1 we complete the proof. □

5. Generalization of Alltop Functions Using Higher Derivatives

In this short section, we extend the concept of Alltop functions using higher derivatives. There are different applications of higher derivatives in related areas. We refer, for example, [18], and the references therein.

Recall that $\mathbb{F}_q$ is a finite field, where $q = p^n$, p is a prime. Let $2 \le k \le n(p - 1)$ be an integer.

A function F is called a *generalized Alltop function of degree k* over $\mathbb{F}_q$ if, for any $a_1, \ldots, a_{k-1} \in \mathbb{F}^*_q$, the repeated difference (or equivalently higher derivative)

$$D_{a_1} D_{a_2} \cdots D_{a_{k-1}} F : \mathbb{F}_q \to \mathbb{F}_q$$

is a permutation function on $\mathbb{F}_q$.

If $k = 2$, then they correspond to planar functions. The canonical example is x^2 for $p > 2$.

If $k = 3$, then they correspond to Alltop functions. The canonical example is x^3 for $p > 3$.

Let F and G be functions on $\mathbb{F}_{p^n}$. The functions F and G are said to be *extended degree k equivalent* if there exist a map $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ of algebraic degree at most $k-1$ and affine invertible maps $L_1, L_2 : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ such that

$$G + \phi = L_1 \circ F \circ L_2$$

.

It is easy to see that if F and G are maps on $\mathbb{F}_q$, and they are extended degree k equivalent, then we have that

F is generalized Alltop of degree $k \iff G$ is generalized Alltop of degree k.

This concept generalizes to p-ary functions as well. A p-ary function $f : \mathbb{F}_q \to \mathbb{F}_p$ is called a *generalized p-ary Alltop function of degree k* over $\mathbb{F}_q$ if, for any $a_1, \ldots, a_{k-1} \in \mathbb{F}_q^*$, the iterated difference $D_{a_1} D_{a_2} \cdots D_{a_{k-1}} f(x)$ is a balanced function from $\mathbb{F}_q$ to $\mathbb{F}_p$.

If $k = 2$, then they correspond to p-ary bent functions.

If $k = 3$, then they correspond to p-ary Alltop functions.

Most of the results of Subsection 4.1 have analogs in higher derivatives.

The following is a generalization of Proposition 4.1.

Proposition 5.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Let $f : \mathbb{F}_q \to \mathbb{F}_p$ be a p-ary function. We have that f is generalized p-ary Alltop of degree k if and only if*

$$\sum_{x \in \mathbb{F}_{p^n}} e^{\frac{2\pi\sqrt{-1}}{p} D_{a_1} \ldots D_{a_{k-1}} f(x)} = 0$$

for all $a_1, \ldots, a_{k-1} \in \mathbb{F}_{p^n}^*$.

Proof. The proof is similar to proof of Proposition 4.1. □

Next we present the analog of Proposition 4.4 below.

Proposition 5.2. *Let $\mathbb{F}_q$ be a finite field of characteristic p with $q = p^n$. Assume that $n = 1$ and k is an integer with $2 \leq k \leq p-1$. Then $F : \mathbb{F}_p \to \mathbb{F}_p$ is generalized Alltop of degree k if and only if F is extended degree k equivalent to the map $G : \mathbb{F}_p \to \mathbb{F}_p$ given by $G(x) = x^k$.*

Proof. We argue by induction on k. The case $k = 2$ is the classification of planar maps on $\mathbb{F}_p$, and $k = 3$ is Proposition 4.4. Let $k \geq 4$ and represent F by a polynomial of degree $d \leq p-1$. If $d < k$, its $(k-1)$-fold derivatives are constant, a contradiction. For $a \in \mathbb{F}_p^*$, $D_a F$ is generalized Alltop of degree $k-1$. By induction it has polynomial degree $k-1$. Since $\deg(D_a F) = d - 1$, we obtain $d = k$. Scaling its leading coefficient and removing the lower-degree terms gives the required equivalence. Conversely, the $(k-1)$-fold derivative of x^k in nonzero directions has nonzero linear coefficient $k! a_1 \cdots a_{k-1}$; adding a polynomial of degree at most $k-1$ changes it only by a constant. □

6. Almost Hadamard Matrices

This section gives a structural application of generalized p-ary Alltop functions. The point is not merely to reformulate the definitions, but to produce higher-dimensional Butson-type almost Hadamard matrices from finite-field functions whose higher derivatives have strong balance properties.

A *complex Hadamard matrix* is a matrix H of order n in which the entries are complex numbers with unit absolute value, which satisfies the condition $HH^* = n\mathcal{I}$, where H^* is the conjugate transpose of H and $\mathcal{I}$ is the identity matrix.

A k-dimensional matrix $H(x_1, \ldots, x_k)$ of size $N \times \cdots \times N$ is called a *proper Hadamard matrix* (see [22]) if, for any $i, j \in \{1, \ldots, k\}$ the matrix

$$\mathcal{H}_{a_1,\ldots,a_k}(y, z) = H(a_1, \ldots, y, \ldots, z, \ldots, a_k)$$

is the Hadamard matrix for every fixed values $a_1, \ldots, a_m, \ldots a_k \in [N]$, where $[N] = \{1, \ldots, N\}$ and $m \neq i, j$.

A k-dimensional matrix $H(x_1, \ldots, x_k)$ of size $N \times \cdots \times N$ is called an *almost Hadamard matrix* (see [9]) if, for any $i, j \in \{1, \ldots, k\}$ the matrix

$$\mathcal{H}_{a_1,\ldots,a_k}(y, z) = H(a_1, \ldots, y, \ldots, z, \ldots, a_k)$$

is either the Hadamard matrix or all 1s matrix for every fixed values $a_1, \ldots, a_m, \ldots a_k \in [N]$, where $m \neq i, j$.

A Hadamard (proper Hadamard or almost Hadamard) matrix is called a *p-ary Butson type matrix* if it consists of elements ϵ^x, $x \in \mathbb{F}_p$. Here $\epsilon = e^{\frac{2\pi\sqrt{-1}}{p}}$ is a primitive p-th root of 1 in $\mathbb{C}$, as usual.

Let $I \subseteq [k] = \{1, \ldots, k\}$ be a subset of variables, $|I|$ is the cardinality of I. By the definition of the discrete differences we have that

$$D_{a_1} \ldots D_{a_{k-1}} D_{a_k} f(x) = D_{a_1} \ldots D_{a_{k-1}} f(x + a_k) - D_{a_1} \ldots D_{a_{k-1}} f(x), \tag{58}$$

where $a_i \in \mathbb{F}_{p^n}^*$. By induction we obtain the following equation:

$$D_{a_1} \ldots D_{a_k} f(x) = \sum_{I \subseteq [k]} (-1)^{|I|+k} f\left(x + \sum_{i \in I} a_i\right). \tag{59}$$

Indeed, by (58) we deduce

$$\begin{aligned} D_{a_1} \ldots D_{a_{k-1}} D_{a_k} f(x) &= D_{a_1} \ldots D_{a_{k-1}} f(x + a_k) - D_{a_1} \ldots D_{a_{k-1}} f(x) \\ &= \sum_{I \subseteq [k-1]} (-1)^{|I|+k-1} \left(f\left(x + a_k + \sum_{i \in I} a_i\right) - f\left(x + \sum_{i \in I} a_i\right)\right) \\ = \sum_{I' = I \cup \{k\}, I \subseteq [k-1]} (-1)^{|I'|+k} f\left(x + \sum_{i \in I'} a_i\right) &+ \sum_{I' \subseteq [k], k \notin I'} (-1)^{|I'|+k} f\left(x + \sum_{i \in I'} a_i\right). \end{aligned}$$

Let $k \geq 3$ be an integer. Define a k-dimensional matrix $H_k[f]$ of size $p^n \times \cdots \times p^n$ by the formula

$$H_k[f](x_1, x_2, \ldots, x_k) = \epsilon^{\sum\limits_{I \subseteq [k]} (-1)^{|I|+k} f(\sum\limits_{i \in I} x_i)}.$$

In particular, for $k = 3$ we have

$$H_3[f](x, y, z) = \epsilon^{f(x+y+z)-f(x+y)-f(y+z)-f(z+x)+f(x)+f(y)+f(z)}.$$

Theorem 6.1. *Let f is a p-ary function, $f(0) = 0$. If f is a generalized p-ary Alltop function of degree k, $k \geq 3$, then $H = H_k[f]$ is a k-dimensional Butson type almost Hadamard matrix whose two-dimensional slices are all ones if a fixed coordinate is zero and are Hadamard otherwise. The converse is also true.*

Proof. It is easy to see that for every f the sum $\sum\limits_{I \subseteq [k]} (-1)^{|I|+k} f(\sum\limits_{i \in I} x_i)$ is equal to zero if one or more arguments are zero. Then the correspondent submatrices of H consist of only ones. Next, we consider an arbitrary 2-dimensional submatrix of H with nonzero fixed coordinates.

Since H is symmetric, we can verify the definition of the almost Hadamard matrices only for one direction of lines (other cases are equivalent). At first, we prove that

$$\sum_{y \in \mathbb{F}_{p^n}} H(x_1, \ldots, x_{k-2}, y, a)\overline{H}(x_1, \ldots, x_{k-2}, y, b) = 0,$$

for $a \neq b, a, b \in \mathbb{F}_{p^n}$.

We see that $H(x_1, \ldots, x_{k-2}, y, a)\overline{H}(x_1, \ldots, x_{k-2}, y, b) = \epsilon^S$, where

$$S = \sum_{I' \subseteq [k-2]} (-1)^{|I'|+k} f\left((\sum_{i \in I'} x_i) + y + a\right) -$$

$$\sum_{I' \subseteq [k-2]} (-1)^{|I'|+k} f\left((\sum_{i \in I'} x_i) + y + b\right) + R(x_1, \ldots, x_{k-2}, a, b),$$

where a function R does not depend on y. Take $y' = y + b$. Then

$$S = \sum_{I' \subseteq [k-2]} (-1)^{|I'|+k-2} f\left((\sum_{i \in I'} x_i) + y' + (a - b)\right) -$$

$$\sum_{I' \subseteq [k-2]} (-1)^{|I'|+k-2} f\left((\sum_{i \in I'} x_i) + y'\right) + R(x_1, \ldots, x_{k-2}, a, b)$$

$$= (D_{x_1} \ldots D_{x_{k-2}} f(y' + (a - b)) - D_{x_1} \ldots D_{x_{k-2}} f(y')) + R(x_1, \ldots, x_{k-2}, a, b)$$

$$= D_{x_1} \ldots D_{x_{k-2}} D_{a-b} f(y') + R(x_1, \ldots, x_{k-2}, a, b),$$

by equations (58) and (59).

By the definition of generalized p-ary Alltop function of degree k, the derivative $D_{x_1} \dots D_{x_{k-2}} D_{a-b} f(y')$ is balanced. Then

$$\sum_{y \in \mathbb{F}_{p^n}} H(x_1, \dots, x_{k-2}, y, a) \overline{H}(x_1, \dots, x_{k-2}, y, b) = \sum_{y \in \mathbb{F}_{p^n}} \epsilon^S$$

$$= \epsilon^{R(x_1,\dots,x_{k-2},a,b)} \sum_{y' \in \mathbb{F}_{p^n}} \epsilon^{D_{x_1} \dots D_{x_{k-2}} D_{a-b} f(y')} = 0.$$

Conversely, assume the stated slice condition. For arbitrary nonzero $x_1, \dots, x_{k-2}, a$, compare the rows indexed by a and $b = 0$. Their orthogonality gives the last character sum equal to zero. Proposition 5.1 implies that $D_{x_1} \cdots D_{x_{k-2}} D_a f$ is balanced, as required. □

7. p-Ary Kerdock Codes

This section gives a coding-theoretic application of the p-ary Alltop viewpoint. The advantage is that the Kerdock-set property is reduced to the bentness of differences, so the finite-field constructions above give a uniform source of nonlinear p-ary codes with explicitly controlled parameters.

A set of p-ary bent functions K is called a *Kerdock set* if for any $f_1, f_2 \in K$, where $f_1 \neq f_2$, the difference $f_1 - f_2$ is a bent function.

At first, we consider Kerdock set based on planar function. Recall that a function $F : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is called planar if $D_a F$ is a permutation of $\mathbb{F}_{p^n}$ for every $a \in \mathbb{F}_{p^n}^*$. It is well known (see, for example, [16] or [20]) that F is planar if and only if $\mathrm{Tr}(bF)$ is a bent function for every $b \in \mathbb{F}_{p^n}^*$. Thus, we see that $\mathcal{K}_F^1 = \{\mathrm{Tr}(bF) : b \in \mathbb{F}_{p^n}^*\}$ is a Kerdock set for any planar function F. Note that, the monomial x^2 is a planar function over any field, which is not of characteristic 2. The original Kerdock set [11] consists of non-degenerate quadratic polynomials over $\mathbb{F}_2$ and it cannot be obtained from a planar function. New results on the description of planar functions over $\mathbb{F}_3$ are contained in [2].

Next, we construct another Kerdock set based on p-ary Alltop functions.

Theorem 7.1. *If f is a p-ary Alltop function, then $\mathcal{K}_f^2 = \{D_a f : a \in \mathbb{F}_{p^n}^*\}$ is a Kerdock set.*

Proof. Each $D_a f$, $a \neq 0$, is bent because all its nonzero derivatives are balanced. We need to verify that $D_a f - D_b f$ is a bent function for any $a, b \in \mathbb{F}_{p^n}^*$, $a \neq b$.

$$D_a f(x) - D_b f(x) = f(x + a) - f(x + b) = f(x' + a - b) - f(x') = D_{a-b} f(x'),$$

where $x' = x + b$. $D_{a-b}f$ is a bent function by the hypothesis of the theorem. Since the class of all bent functions is closed under EA-equivalence, $D_af(x) - D_bf(x)$ is also a bent function. □

We treat the set

$$\mathcal{D}(\mathcal{K}) = \{f(x) + \mathrm{Tr}(bx) + c : f \in \mathcal{K} \cup \{\mathbf{0}\}, b \in \mathbb{F}_{p^n}, c \in \mathbb{F}_p\},$$

where $\mathbf{0}$ is the zero-function and $\mathcal{K}$ is the Kerdock set, as a *generalized p-ary Kerdock code*. Here, the codewords of $\mathcal{D}(\mathcal{K})$ are sequences of the values of the functions from $\mathcal{D}(\mathcal{K})$.

The *code distance* of a code C is the minimum of the Hamming distances between distinct codewords. The weight $wt(f)$ of a codeword f is the Hamming distance between f and the zero function. So, the weight of a function is the cardinality of its support. To estimate the code distance of a p-ary Kerdock code, we need the following results.

Proposition 7.1 ([17] Propositions 3.1 and 3.2)**.** *Let $p > 2$ be a prime number and let f be a bent function in n variables.*
If n is even then the weight $wt(f)$ can meet only four values: $(p-1)(p^{n-1} \pm p^{n/2-1})$, $(p-1)(p^{n-1} - p^{n/2-1}) + p^{n/2}$ and $(p-1)(p^{n-1} + p^{n/2-1}) - p^{n/2}$.
If n is odd then weight $wt(f)$ can meet only three values: $(p-1)p^{n-1}$ and $(p-1)p^{n-1} \pm p^{(n-1)/2}$.

A code C has parameters $(N, |C|, d_C)_p$, where $C \subset \mathbb{F}_p^N$, $|C|$ is the cardinality of C, and d_C is the code distance.

Theorem 7.2. *Let $\mathcal{K}$ be a Kerdock set of type $\mathcal{K}_F^1$ or $\mathcal{K}_f^2$, where F is a planar function and f is a p-ary Alltop function in $\mathbb{F}_p^n$ respectively. Then $\mathcal{D}(\mathcal{K})$ is a generalized p-ary Kerdock code with parameters $\left(p^n, p^{2n+1}, (p-1)(p^{n-1} - p^{\frac{n}{2}-1})\right)_p$ for even n and $\left(p^n, p^{2n+1}, (p-1)p^{n-1} - p^{\frac{n-1}{2}}\right)_p$ for odd n.*

Proof. It is easy to see that elements of $\mathcal{D}(\mathcal{K})$ with different f, b and c are distinct. Indeed, the difference $f_1 - f_2$, where $f_1, f_2 \in \mathcal{K}$, is a bent function, so the algebraic degree of $f_1 - f_2$ is greater than 1. Thus, $|\mathcal{D}(\mathcal{K})| = (|\mathcal{K}| + 1)|A|$, where A is the set of all affine functions. Obviously $|\mathcal{K}| + 1 = p^n$ and $|A| = p^{n+1}$.

It is well known that the sum of arbitrary bent and affine functions is a bent function. Then all differences of elements of $\mathcal{D}(\mathcal{K})$ are bent functions or affine functions by the definition of the Kerdock set. The weight of a nonconstant affine function is equal to $(p-1)p^{n-1}$, and a nonzero constant has weight p^n. Then the code distance of $\mathcal{D}(\mathcal{K})$ is equal to the minimum weight of bent functions by Proposition 7.1. □

Remark 7.1. *If $\mathcal{K} \cup \{\mathbf{0}\}$ is a linear set, then $\mathcal{D}(\mathcal{K})$ is a linear code. Thus, if $\mathcal{K} = \mathcal{K}_F^1$, where F is a planar functions, then $\mathcal{D}(\mathcal{K})$ is linear. The set $\mathcal{K}_f^2$ is not linear in general.*

Remark 7.2. *By Proposition 7.1 a generalized p-ary Kerdock code with length p^n has at most six nonzero distances between codewords if n is even. Indeed, we have four different distances between bent functions and affine functions, another distance $p^n - p^{n-1}$ between any two affine functions and distance p^n between constants. If n is odd then a generalized p-ary Kerdock code with length p^n has only four nonzero distances for $n \geq 3$ (three for $n = 1$). The examples of $\mathbb{Z}_{p^2}$-linear p-ary Kerdock codes constructed by van Asch and van Tilborg have five and seven nonzero distances as $p = 3$, $n = 4$ and $n = 6$ respectively* [3, Tables 3 and 4].

8. Conclusion

We have studied Alltop functions and their p-ary analogues from the viewpoints of finite-field arithmetic, combinatorics and coding theory. In Section 3, we extended the monomial and binomial analysis over $\mathbb{F}_{q^2}$ to a complete classification of all homogeneous q-cubic Alltop functions up to $\mathbb{F}_q$-EA-equivalence in Theorem 3.8. Over $\mathbb{F}_{q^3}$, we classified the q-cubic Alltop monomials. In Section 4, we constructed an infinite family of strict p-ary Alltop functions in characteristic 3. For $q \equiv 2 \pmod 3$, the norm–trace family is strict with respect to all homogeneous q-cubic Alltop functions, without a term restriction. We also obtained families strict with respect to the specified q-cubic monomial and binomial classes for $p \geq 5$. The last sections connected the higher-derivative viewpoint to almost Hadamard matrices and to p-ary Kerdock-type codes.

It would be interesting to obtain further characterizations of strict p-ary Alltop functions and to study the coding-theoretic properties of the associated Kerdock-type constructions.

Declarations

Availability of data and materials Not applicable.

Competing interests Not applicable.

Funding The research of Ferruh Özbudak is supported by Sabancı University Research Grants (F.A.CF-24-02904 and B.A.CF-24-02881).

Authors' contributions Not applicable.

Acknowledgements The authors would like to thank the anonymous referees for helpful comments which have highly improved the quality of the article.

Authors' information Not applicable.

References

[1] W.O.Alltop. Complex sequences with low periodic correlations. IEEE Transactions on Information Theory, 26(3):350-354, 1980.

[2] S. Andreoli, L. Budaghyan, R. Coulter, A. Haukenes, N. Kaleyski, E. Piccione. On a classification of planar functions in characteristic three. Cryptogr. Commun., 17:823–853, 2025.

[3] B. van Asch, H. C. A. van Tilborg. Two "dual" families of nearly-linear codes over Z_p, p odd. Appl. Algebra Engrg. Comm. Comput., 11(4):313-329, 2001.

[4] C. Bey, G. M. Kyureghyan. On Boolean functions with the sum of every two of them being bent. Des. Codes Cryptogr., 49:341-346, 2008. DOI 10.1007/s10623-008-9196-4

[5] A. R. Calderbank, P. J. Cameron, W. M. Kantor, J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. Proc. Lond. Math. Soc., III. Ser. 75, No. 2, 436-480, 1997.

[6] C. Carlet. Boolean Functions for Cryptography and Coding Theory. Cambridge University Press, Cambridge, 2020.

[7] J.L.Hall, A.Rao and D.Donovan. Planar difference functions. Information Theory Proceedings (ISIT), 2012 IEEE International Symposium, pp. 1082–1086, IEEE, 2012.

[8] J.L.Hall, A.Rao and S.M.Gagola III. A family of Alltop functions that are EA-inequivalent to the cubic function. IEEE Transactions on Communications, 61(11), pp. 4722-4727, 2013.

[9] J. Hammer, J.R. Seberry. Higher-dimensional orthogonal designs and applications. IEEE Trans. Inf. Theory, 27(6):772-779, 1981.

[10] K.J. Horadam Hadamard Matrices and Their Applications. Princeton University Press, Princeton, NJ 2007

[11] A. M. Kerdock. A class of low-rate nonlinear binary codes. Inform.and Control, 20:182-187, 1972.

[12] V. Krčadinac, M. O. Pavčević, K. Tabak. Three-dimensional Hadamard matrices of Paley type. Finite Fields Appl., 92, Paper No.102306, 6 pp. 2023.

[13] G.Kyureghyan, F.Özbudak and A.Pott. Some planar maps and related function fields. Contemporary Mathematics 574, Arithmetic, Geometry, Cryptography and Coding Theory, pp. 87-114, 2012.

[14] R. Lidl and H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications, Vol. 20. Cambridge University Press, 2nd edition, 1997.

[15] S.Mesnager. Characterizations of plateaued and bent functions in characteristic p. International Conference on Sequences and Their Applications, pp. 72–82, Springer, 2014.

[16] S. Mesnager, Bent Functions: Fundamentals and Results. Springer International Publishing Switzerland, 2016.

[17] F. Özbudak, R. M. Pelen, Duals of non-weakly regular bent functions are not weakly regular and generalization to plateaued functions. Finite Fields Appl., 64, 101668, 16 pp. 2020.

[18] F. Özbudak, A. Sălăgean. New generalized almost perfect nonlinear functions. Finite Fields Appl., 70 (2021), Paper No. 101796, 32 pp.

[19] N. J. Patterson, A four-dimensional Kerdock set over GF(3). J. Combinatorial Theory Ser. A, 20(3):365-366, 1976.

[20] A. Pott. Almost perfect and planar functions. Des. Codes Cryptogr., 78 (2016), 141–195.

[21] A. Price, J. Hall, H. Bartlett. Refining the search space of Alltop monomials. J. Algebraic Combin., 57 (2023), 709–725.

[22] P. J. Shlichta, Higher dimensional Hadamard matrices. IEEE Trans. Inform. Theory, 25(5):566-572, 1979.

[23] H. Stichtenoth. Algebraic Function Fields and Codes. Graduate Texts in Mathematics, Vol. 254, 2nd edition. Springer, Berlin, Heidelberg, 2009.