On the Intersection Distribution of Degree Three Polynomials and Related Topics

Gohar Kyureghyan

Institute of Mathematics
University of Rostock
18057 Rostock, Germany

gohar.kyureghyan@uni-rostock.de

Shuxing Li*

Department of Mathematics
Simon Fraser University
8888 University Drive, Burnaby BC V5A 1S6, Canada

shuxingl@sfu.ca

Alexander Pott

Institute of Algebra and Geometry, Faculty of Mathematics
Otto von Guericke University Magdeburg
39106 Magdeburg, Germany

alexander.pott@ovgu.de

Submitted: Mar 22, 2020; Accepted: Apr 13, 2021; Published: Jun 18, 2021

Abstract

The intersection distribution of a polynomial f over a finite field $\mathbb{F}_q$ was recently proposed by Li and Pott [*Finite Fields and Their Applications, 66 (2020)*], which concerns the collective behaviour of a collection of polynomials $\{f(x) + cx \mid c \in \mathbb{F}_q\}$. The intersection distribution has an underlying geometric interpretation, which indicates the intersection pattern between the graph of f and the lines in the affine plane $AG(2, q)$. When q is even, the long-standing open problem of classifying o-polynomials can be rephrased in a simple way, namely, classifying all polynomials which have the same intersection distribution as x^2. Inspired by this connection, we proceed to consider the next simplest case and derive the intersection distribution for all degree three polynomials over $\mathbb{F}_q$ with q both odd and even. Moreover, we

*Research supported by the Alexander von Humboldt Foundation and the Pacific Institute for the Mathematical Sciences.

initiate to classify all monomials having the same intersection distribution as x^3, where some characterizations of such monomials are obtained and a conjecture is proposed. In addition, two applications of the intersection distributions of degree three polynomials are presented. The first one is the construction of nonisomorphic Steiner triple systems and the second one produces infinite families of Kakeya sets in affine planes with previously unknown sizes.

Mathematics Subject Classifications: 11T06, 51E15, 51E10, 05B07

1 Introduction

Throughout this paper, let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be a finite field with characteristic p and f a polynomial over $\mathbb{F}_q$. The intersection distribution of f originates from an elementary problem concerning the interaction between the graph $\{(x, f(x)) \mid x \in \mathbb{F}_q\}$ of f and the lines in the classical affine plane $AG(2, q)$. More precisely, for $0 \leqslant i \leqslant q$, we ask about the number of affine lines intersecting the graph of f in exactly i points. Note that there are q vertical affine lines of the form $\{(x, y) \mid y \in \mathbb{F}_q\}$, where x ranges over $\mathbb{F}_q$. Since each of these vertical lines intersects G_f in exactly one point, we shall omit them and restrict to the remaining q^2 non-vertical lines. As an attempt to answer this question, the following concept of intersection distribution was proposed in [22, Definition 1.1(1)].

Definition 1.1 (Intersection distribution)**.** For $0 \leqslant i \leqslant q$, define

$$v_i(f) = |\{(b, c) \in \mathbb{F}_q^2 \mid f(x) - bx - c = 0 \text{ has } i \text{ solutions in } \mathbb{F}_q\}|.$$

The sequence $(v_i(f))_{i=0}^q$ is the intersection distribution of f. The integer $v_0(f)$ is the non-hitting index of f.

We remark that for $0 \leqslant i \leqslant q$, there are exactly $v_i(f)$ non-vertical lines, which intersect the graph $\{(x, f(x)) \mid x \in \mathbb{F}_q\}$ in exactly i points. In particular, the non-hitting index $v_0(f)$ is the number of affine lines which does not hit the graph of f. The intersection distribution of a polynomial f conveys considerable information of f. For instance, the non-hitting index $v_0(f)$ measures the distance from f to linear functions, and to the so called o-polynomial (when q is even) or to x^2 (when q is odd) [22, Result 1.7]. Thus, intersection distribution serves as a new viewpoint to distinguish polynomials, which is different from the usual extended-affine equivalence ([5, p. 1142]) and the Carlet-Charpin-Zinoviev equivalence [5, Definition 1], [6, Proposition 3]. Moreover, the aforementioned geometric interpretation indicates that for the point set in the classical projective plane $PG(2, q)$ arising from a polynomial f, detailed information follows from the intersection distribution f (see for instance [22, Proposition 3.2]).

Having explained the reason why the intersection distribution is interesting, we proceed to consider its computation. First, we have the following basic equations, which essentially have been stated in [22, Proposition 2.1] (see also [18, Lemma 12.1]).

Proposition 1.2. *Let f be a polynomial over $\mathbb{F}_q$. The following equations hold.*

$$\sum_{i=0}^{q} v_i(f) = q^2,$$
$$\sum_{i=1}^{q} i v_i(f) = q^2,$$
$$\sum_{i=2}^{q} i(i-1) v_i(f) = q(q-1).$$

Secondly, to facilitate the computation of the intersection distribution, the following definition was proposed in [22, Definition 1.1(2)].

Definition 1.3 (Multiplicity distribution)**.** Let f be a polynomial over $\mathbb{F}_q$. For $b \in \mathbb{F}_q$ and $0 \leqslant i \leqslant q$, define

$$M_i(f,b) = |\{c \in \mathbb{F}_q \mid f(x) - bx - c = 0 \text{ has } i \text{ solutions in } \mathbb{F}_q\}|.$$

The sequence $(M_i(f,b))_{i=0}^{q}$ is the multiplicity distribution of f at b. The multiset of sequences $\{(M_i(f,b))_{i=0}^{q} \mid b \in \mathbb{F}_q\}$ is the multiplicity distribution of f.

By definition, for $0 \leqslant i \leqslant q$, there are exactly $M_i(f,b)$ lines among the parallel class of q affine lines $\{y = bx + c \mid c \in \mathbb{F}_q\}$, which intersect the graph of f in i points. From now on, we use $\mathbb{F}_q^*$ to denote the set of nonzero elements in $\mathbb{F}_q$.

Remark 1.4.

(1) By definition, for a polynomial f over $\mathbb{F}_q$ and $0 \leqslant i \leqslant q$, we have

$$v_i(f) = \sum_{b \in \mathbb{F}_q} M_i(f,b).$$

Hence, the multiplicity distribution of f implies its intersection distribution.

(2) Let $f(x) = \sum_{i=0}^{n} a_i x^i$, where $n \geqslant 2$ and $a_n \neq 0$. Note that for each $0 \leqslant i \leqslant q$, we have $M_i(f,b) = M_i(a_n^{-1}(f - a_1 x - a_0), a_n^{-1}(b - a_1))$. Hence, in order to compute the intersection distribution of f, one can assume without generality that $a_1 = a_0 = 0$ and $a_n = 1$.

(3) Let f be a permutation polynomial and f^{-1} be its inverse. Clearly, $M_1(f,0) = M_1(f^{-1},0) = q$. Moreover, note that for $b \in \mathbb{F}_q^*$, the two equations $f(x) - bx - c = 0$ and $f^{-1}(x) - \frac{1}{b}x + \frac{c}{b} = 0$ have the same number of solutions. Hence, f and f^{-1} have the same multiplicity distribution and therefore, the same intersection distribution.

We remark that in general, computing the intersection and multiplicity distributions is a nontrivial problem. In [22, Appendix B], the multiplicity distributions of monomials x^d over $\mathbb{F}_q$, where $d \in \{p^i, p^i + 1, \frac{q-1}{2}, \frac{q+1}{2}, q-2, q-1\}$, have been determined. Indeed,

combining [22, Propositions B.1, B.9] and Remark 1.4(1)(2), we have the following proposition. For the sake of simplicity, from now on, we only list the first few values of the intersection distribution $v_i(f)$ and multiplicity distribution $M_i(f,b)$ with i at most 4, and the unmentioned values are all zeros.

Proposition 1.5. *Let x^2 be a monomial over $\mathbb{F}_q$.*

(1) If $p=2$, then

$$\begin{cases} M_0(x^2,0)=0, & M_1(x^2,0)=q, \quad M_2(x^2,0)=0, \\ M_0(x^2,b)=\frac{q}{2}, & M_1(x^2,b)=0, \quad M_2(x^2,b)=\frac{q}{2}, \quad \text{if } b\neq 0. \end{cases}$$

(2) If p is odd, then for each $b\in\mathbb{F}_q$,

$$M_0(x^2,b)=\frac{q-1}{2}, \quad M_1(x^2,b)=1, \quad M_2(x^2,b)=\frac{q-1}{2}.$$

In particular, for each polynomial f over $\mathbb{F}_q$ with degree two, we have

$$v_0(f)=\frac{q(q-1)}{2}, \quad v_1(f)=q, \quad v_2(f)=\frac{q(q-1)}{2}. \tag{1.1}$$

Consequently, the intersection distribution of polynomials with degree two is clear. We remark that f having degree two forces $v_i(f)=0$ for each $i>2$, so that the intersection distribution (1.1) follows from Proposition 1.2. A natural question is, if we drop the degree two condition, is there any other polynomial which has intersection distribution (1.1)? Historically, this problem has been intensively studied in terms of classifying ovals or hyperovals in the classical projective planes (see [18, Chapter 8] for instance). When q is odd, a famous result due to Segre [25] indicates each polynomial f satisfying (1.1) is in some sense equivalent to x^2. On the other hand, when q is even, the situation is much more subtle. In this case, a polynomial f with the same intersection distribution as x^2 is called an *o-polynomial*. The classification of o-polynomials, especially o-monomials, is a long-standing problem which has attracted much attention (see [7, 8, 18, 27] and the references therein).

In this paper, we pursue a result analogous to the one stated above. More precisely, we take one step forward to consider the intersection distribution of degree three polynomials. This is the next simplest case as the degree three condition ensures that $v_i(f)=0$ for each $i>3$. Together with Proposition 1.2, the intersection distribution of each degree three polynomial f can be determined by exactly one of $v_i(f)$, $0\leqslant i\leqslant 3$. By Remark 1.4(2), it suffices to determine the intersection distribution of x^3-ax^2 for each $a\in\mathbb{F}_q$, and we have the following complete description.

Theorem 1.6. *Let $f(x)=x^3-ax^2$ be a polynomial over $\mathbb{F}_q$. If $p\neq 3$, then we have*

$$v_0(f)=\frac{q^2-1}{3}, \quad v_1(f)=\frac{q^2-q+2}{2}, \quad v_2(f)=q-1, \quad v_3(f)=\frac{q^2-3q+2}{6}. \tag{1.2}$$

If $p = 3$ and $a = 0$, then we have

$$v_0(f) = \frac{q(q-1)}{3}, \quad v_1(f) = \frac{q(q+1)}{2}, \quad v_2(f) = 0, \quad v_3(f) = \frac{q(q-1)}{6}. \tag{1.3}$$

If $p = 3$ and $a \neq 0$, then we have

$$v_0(f) = \frac{q^2}{3}, \quad v_1(f) = \frac{q(q-1)}{2}, \quad v_2(f) = q, \quad v_3(f) = \frac{q(q-3)}{6}.$$

In order to derive the above theorem, we present a detailed computation determining the multiplicity distribution of degree three polynomial $x^3 - ax^2$ in Section 2. To achieve this, we consider the number of $\mathbb{F}_q$-solutions to

$$x^3 - \beta x - c = 0, \quad \text{if } p \neq 3, \quad \text{or} \quad x^3 - x^2 - c = 0, \quad \text{if } p = 3,$$

where $c \in \mathbb{F}_q$ and β is either 1 or a primitive element of $\mathbb{F}_q$. When the equation has at least one solution $x_0 \in \mathbb{F}_q$, we give a characterization of the number of $\mathbb{F}_q$-solutions in terms of x_0. In Section 3, we proceed to consider a much more challenging problem, namely, determining all monomials which have the same intersection distribution as x^3. Although a complete answer is by far elusive, we make some detailed analysis and present strong restrictions to these monomials. Moreover, based on the numerical experiment, we propose a conjecture classifying all monomials having the same intersection distribution as x^3. As an application, in Section 4, we observe that polynomials over $\mathbb{F}_{3^m}$ with intersection distribution (1.3) produces Steiner triples systems. Interestingly, some numerical results indicate that certain distinct monomials satisfying (1.3) generate nonisomorphic Steiner triple systems. In Section 5, applying the multiplicity distribution of $x^3 - ax^2$, we construct several infinite families of Kakeya sets in affine planes, whose sizes are different from the known ones. Section 6 concludes the paper and proposes a few open problems.

2 The multiplicity and intersection distributions of degree three polynomials

In this section, we consider the multiplicity distribution of degree three polynomial. In view of Remark 1.4(2), we only need to consider a degree three polynomial of the form $x^3 - ax^2$, where $a \in \mathbb{F}_q$.

From now on, we always denote a primitive element of finite field $\mathbb{F}_q$ by α. Given a finite field $\mathbb{F}_q$ and a positive integer $N \mid q-1$, we use $C_0^{(N,q)}$ to denote the set consisting of nonzero N-th powers in $\mathbb{F}_q$. Suppose α is a primitive element of $\mathbb{F}_q$, then for $0 \leqslant i \leqslant N-1$, define $C_i^{(N,q)} = \alpha^i C_0^{(N,q)} = \{\alpha^i x \mid x \in C_0^{(N,q)}\}$. Hence, when q is odd, we know that $C_0^{(2,q)}$ is the set of nonzero squares and $C_1^{(2,q)}$ is the set of nonsquares in $\mathbb{F}_q$.

The following proposition says, roughly speaking, in order to determine the multiplicity distribution of $x^3 - ax^2$, it suffices to compute $M_i(x^3, 0)$, $M_i(x^3, 1)$, $M_i(x^3, \alpha)$ and when $p = 3$, also $M_i(x^3 - x^2, 0)$.

Lemma 2.1.

(1) When $p = 2$, we have

$$M_i(x^3, b) = \begin{cases} M_i(x^3, 0), & \text{if } b = 0, \\ M_i(x^3, 1), & \text{if } b \neq 0, \end{cases}$$

and

$$M_i(x^3 - ax^2, b) = M_i(x^3, \frac{b}{a^2} + 1) = \begin{cases} M_i(x^3, 0), & \text{if } \frac{b}{a^2} = 1, \\ M_i(x^3, 1), & \text{if } \frac{b}{a^2} \neq 1, \end{cases}$$

where $a \neq 0$ and $b \in \mathbb{F}_q$.

(2) When $p = 3$, we have

$$M_i(x^3, b) = \begin{cases} M_i(x^3, 0), & \text{if } b = 0, \\ M_i(x^3, 1), & \text{if } b \in C_0^{(2,q)}, \\ M_i(x^3, \alpha), & \text{if } b \in C_1^{(2,q)}. \end{cases}$$

For $a \neq 0$ and $b \in \mathbb{F}_q$, we have $M_i(x^3 - ax^2, b) = M_i(x^3 - x^2, 0)$.

(3) When $p > 3$, we have

$$M_i(x^3, b) = \begin{cases} M_i(x^3, 0), & \text{if } b = 0, \\ M_i(x^3, 1), & \text{if } b \in C_0^{(2,q)}, \\ M_i(x^3, \alpha), & \text{if } b \in C_1^{(2,q)}, \end{cases}$$

and

$$M_i(x^3 - ax^2, b) = M_i(x^3, \frac{b}{a^2} + \frac{1}{3}) = \begin{cases} M_i(x^3, 0), & \text{if } \frac{b}{a^2} = -\frac{1}{3}, \\ M_i(x^3, 1), & \text{if } \frac{b}{a^2} + \frac{1}{3} \in C_0^{(2,q)}, \\ M_i(x^3, \alpha), & \text{if } \frac{b}{a^2} + \frac{1}{3} \in C_1^{(2,q)}, \end{cases}$$

where $a \neq 0$ and $b \in \mathbb{F}_q$.

Proof. In all the three cases, the expression of $M_i(x^3, b)$ is clear. So we only need to consider $M_i(x^3 - ax^2, b)$ with $a \neq 0$. For this purpose, we consider the number of solutions in $\mathbb{F}_q$ to the equation $x^3 - ax^2 - bx - c = 0$.

If $p = 2$ or $p > 3$, namely, $\gcd(3, q) = 1$, dividing a^3 on both sides and replacing $\frac{x}{a}$ with x, we have $x^3 - x^2 - \frac{b}{a^2}x - \frac{c}{a^3} = 0$. Replacing x with $x + \frac{1}{3}$ in the latter equation leads to $x^3 - (\frac{b}{a^2} + \frac{1}{3})x - (\frac{c}{a^3} + \frac{b}{3a^2} + \frac{2}{27}) = 0$. Note that fixing a and b, when c ranges over $\mathbb{F}_q$, so does $\frac{c}{a^3} + \frac{b}{3a^2} + \frac{2}{27}$. Hence, $M_i(x^3 - ax^2, b) = M_i(x^3, \frac{b}{a^2} + \frac{1}{3})$. Note that when $p = 2$, $M_i(x^3, \frac{b}{a^2} + 1) = M_i(x^3, \frac{b}{a^2} + \frac{1}{3})$. The rest follows easily.

If $p = 3$, namely, $\gcd(3, q) = 3$, dividing a^3 on both sides and replacing $\frac{x}{a}$ with x, we have $x^3 - x^2 - \frac{b}{a^2}x - \frac{c}{a^3} = 0$. Replacing x with $x - \frac{b}{2a^2}$, we have $x^3 - x^2 - (\frac{c}{a^3} - \frac{b^2}{4a^4} + \frac{b^3}{8a^6}) = 0$. Note that fixing a and b, when c ranges over $\mathbb{F}_q$, so does $\frac{c}{a^3} - \frac{b^2}{4a^4} + \frac{b^3}{8a^6}$. Hence, $M_i(x^3 - ax^2, b) = M_i(x^3 - x^2, 0)$. □

Note that $M_i(x^3,0)$ is easy to compute. Moreover, when $p=3$, $M_i(x^3,1)$ and $M_i(x^3,\alpha)$ are also straightforward.

Lemma 2.2. *(1) When $p\neq 3$, we have*

$$\begin{cases} M_0(x^3,0)=\frac{2(q-1)}{3}, M_1(x^3,0)=1, M_2(x^3,0)=0, M_3(x^3,0)=\frac{q-1}{3}, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } q\equiv 1 \pmod 3, \\ M_0(x^3,0)=0, M_1(x^3,0)=q, M_2(x^3,0)=0, M_3(x^3,0)=0, \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } q\equiv 2 \pmod 3. \end{cases}$$

(2) When $p=3$, we have

$$\begin{aligned} &M_0(x^3,0)=0, \quad M_1(x^3,0)=q, \quad M_2(x^3,0)=0, \quad M_3(x^3,0)=0,\\ &M_0(x^3,1)=\frac{2q}{3}, \quad M_1(x^3,1)=0, \quad M_2(x^3,1)=0, \quad M_3(x^3,1)=\frac{q}{3},\\ &M_0(x^3,\alpha)=0, \quad M_1(x^3,\alpha)=q, \quad M_2(x^3,\alpha)=0, \quad M_3(x^3,\alpha)=0. \end{aligned}$$

Now we introduce the concept of cyclotomic number, which will be used later. For $0\leqslant i,j\leqslant 1$, define the cyclotomic numbers of order 2 as

$$(i,j)_q=|(1+C_i^{(2,q)})\cap C_j^{(2,q)}|.$$

The cyclotomic numbers of order 2 are well known, see for instance [26].

Lemma 2.3. *Let q be an odd prime power. If $q\equiv 1 \pmod 4$, we have*

$$(0,0)_q=\frac{q-5}{4}, \quad (0,1)_q=(1,0)_q=(1,1)_q=\frac{q-1}{4}.$$

If $q\equiv 3 \pmod 4$, we have

$$(0,1)_q=\frac{q+1}{4}, \quad (0,0)_q=(1,0)_q=(1,1)_q=\frac{q-3}{4}.$$

Employing the cyclotomic numbers of order 2, we proceed to prove the following preparatory lemma.

Lemma 2.4. *Let* Tr *be the absolute trace defined on $\mathbb{F}_q$. For the equations $x^3-x-c=0$ or $x^3-\alpha x-c=0$, assume that $x_0\in\mathbb{F}_q$ is a solution.*

(1) When $p=2$, we have

$$|\{x\in\mathbb{F}_q \mid x^3-x-c=0\}|=\begin{cases} 1 & \text{if } \mathrm{Tr}(\frac{1}{x_0})=\mathrm{Tr}(\frac{1}{c})=\mathrm{Tr}(1)+1,\\ 2 & \text{if } x_0\in\{0,1\}, \text{ or equivalently, } c=0,\\ 3 & \text{if } \mathrm{Tr}(\frac{1}{x_0})=\mathrm{Tr}(\frac{1}{c})=\mathrm{Tr}(1),\ x_0\neq 1. \end{cases}$$

Consequently,

$$\begin{cases} M_0(x^3,1)=\frac{q+1}{3}, M_1(x^3,1)=\frac{q}{2}-1, M_2(x^3,1)=1, M_3(x^3,1)=\frac{q-2}{6}, & \text{if } m \text{ odd},\\ M_0(x^3,1)=\frac{q-1}{3}, M_1(x^3,1)=\frac{q}{2}, M_2(x^3,1)=1, M_3(x^3,1)=\frac{q-4}{6}, & \text{if } m \text{ even}. \end{cases}$$

(2) When $p = 3$, we have

$$|\{x \in \mathbb{F}_q \mid x^3 - x^2 - c = 0\}| = \begin{cases} 1 & \text{if } 2x_0 + 1 \in C_1^{(2,q)}, \\ 2 & \text{if } x_0 \in \{0, 1\}, \text{ or equivalently, } c = 0, \\ 3 & \text{if } 2x_0 + 1 \in C_0^{(2,q)} \text{ and } x_0 \neq 0. \end{cases}$$

Consequently, we have

$$M_0(x^3 - x^2, 0) = \frac{q}{3}, \quad M_1(x^3 - x^2, 0) = \frac{q-1}{2},$$
$$M_2(x^3 - x^2, 0) = 1, \quad M_3(x^3 - x^2, 0) = \frac{q-3}{6}.$$

(3) When $p > 3$, for $\beta \in \{1, \alpha\}$ and

$$j = \begin{cases} 1 & \text{if } \beta = 1, \\ -1 & \text{if } \beta = \alpha, \end{cases}$$

we have

$$|\{x \in \mathbb{F}_q \mid x^3 - \beta x - c = 0\}| = \begin{cases} 1 & \text{if } 1 - \frac{3x_0^2}{4\beta} \in \beta C_1^{(2,q)}, \\ 2 & \text{if } 3 \in \beta C_0^{(2,q)} \text{ and } x_0^2 \in \{\frac{\beta}{3}, \frac{4\beta}{3}\}, \\ 3 & \text{if } 1 - \frac{3x_0^2}{4\beta} \in \beta C_0^{(2,q)} \\ & \text{and } x_0^2 \neq \frac{\beta}{3} \text{ whenever } 3 \in \beta C_0^{(2,q)}. \end{cases}$$

Consequently, we have

$$\begin{cases} M_0(x^3, \beta) = \frac{q-1}{3}, M_1(x^3, \beta) = \frac{q-j}{2}, M_2(x^3, \beta) = 1 + j, M_3(x^3, \beta) = \frac{q-4-3j}{6}, \\ \qquad \text{if } p \equiv 1 \pmod{12} \text{ or } m \text{ even}, \\ M_0(x^3, \beta) = \frac{q-1}{3}, M_1(x^3, \beta) = \frac{q+j}{2}, M_2(x^3, \beta) = 1 - j, M_3(x^3, \beta) = \frac{q-4+3j}{6}, \\ \qquad \text{if } p \equiv 7 \pmod{12} \text{ and } m \text{ odd}, \\ M_0(x^3, \beta) = \frac{q+1}{3}, M_1(x^3, \beta) = \frac{q-2+j}{2}, M_2(x^3, \beta) = 1 - j, M_3(x^3, \beta) = \frac{q-2+3j}{6}, \\ \qquad \text{if } p \equiv 5 \pmod{12} \text{ and } m \text{ odd}, \\ M_0(x^3, \beta) = \frac{q+1}{3}, M_1(x^3, \beta) = \frac{q-2-j}{2}, M_2(x^3, \beta) = 1 + j, M_3(x^3, \beta) = \frac{q-2-3j}{6}, \\ \qquad \text{if } p \equiv 11 \pmod{12} \text{ and } m \text{ odd}. \end{cases}$$

Proof. We first prove (1). Suppose $x^3 - x - c = 0$ has exactly two solutions in $\mathbb{F}_q$. Then $x^3 - x - c = (x - x_1)(x - x_2)^2$ for some distinct $x_1, x_2 \in \mathbb{F}_q$. Comparing the coefficients, we have $x_1 = 0$, $x_2 = 1$, and $c = 0$. Therefore, $M_2(x^3, 1) = 1$ as $x^3 - x - c = 0$ has exactly two solutions in $\mathbb{F}_q$ if and only if $c = 0$ and the two solutions are 0 and 1. Next, we proceed to consider when $x^3 - x - c = 0$ has exactly one or three solutions. Suppose $x^3 - x - c = 0$ has one solution $x_0 \in \mathbb{F}_q$, then we can factor $x^3 - x - c = (x - x_0)(x^2 + x_0 x + x_0^2 - 1)$,

where $c = x_0^3 + x_0$. We need to check if $x^2 + x_0x + x_0^2 - 1 = 0$ has solutions in $\mathbb{F}_q$, where $x_0 \notin \{0, 1\}$. Note that $x^2 + x_0x + x_0^2 - 1 = 0$ is equivalent to $1 + \frac{1}{x_0^2} = (\frac{x}{x_0})^2 + \frac{x}{x_0}$. Hence, $x^2 + x_0x + x_0^2 - 1 = 0$ has no solution if and only if $\mathrm{Tr}(\frac{1}{x_0}) = \mathrm{Tr}(1) + 1$, and two solutions if and only if $\mathrm{Tr}(\frac{1}{x_0}) = \mathrm{Tr}(1)$. Note that $\mathrm{Tr}(\frac{1}{c}) = \mathrm{Tr}(\frac{1}{x_0+1}(\frac{1}{x_0} + \frac{1}{x_0+1})) = \mathrm{Tr}(\frac{1}{x_0} + \frac{1}{x_0+1} + \frac{1}{(x_0+1)^2}) = \mathrm{Tr}(\frac{1}{x_0})$. If m is odd, then there are $\frac{q}{2} - 1$ choices of $x_0 \in \mathbb{F}_q \setminus \{0, 1\}$, such that $\mathrm{Tr}(\frac{1}{x_0}) = \mathrm{Tr}(1) + 1 = 0$. Thus, $M_1(x^3, 1) = \frac{q}{2} - 1$. Moreover, there are $\frac{q}{2} - 1$ choices of $x_0 \in \mathbb{F}_q \setminus \{0, 1\}$, such that $\mathrm{Tr}(\frac{1}{x_0}) = \mathrm{Tr}(1) = 1$. Thus, $M_3(x^3, 1) = \frac{1}{3}(\frac{q}{2} - 1) = \frac{q-2}{6}$ and therefore, the value of $M_0(x^3, 1)$ follows immediately. Similar arguments lead to the values of $M_i(x^3, 1)$ when m is even.

The proofs of (2) and (3) are very similar to each other. Below, we only prove (3) with $\beta = \alpha$. Suppose $x^3 - \alpha x - c = 0$ has exactly two solutions in $\mathbb{F}_q$. Then $x^3 - \alpha x - c = (x - x_1)(x - x_2)^2$ for some distinct $x_1, x_2 \in \mathbb{F}_q$. Comparing the coefficients, we have $x_1^2 = \frac{4\alpha}{3}$, $x_2^2 = \frac{\alpha}{3}$, and $x_1 + 2x_2 = 0$. Hence, $x^3 - \alpha x - c = 0$ has two solutions in $\mathbb{F}_q$ if and only if $3 \in \alpha C_0^{(2,q)}$ and $c = \pm\frac{2\alpha}{3}\sqrt{\frac{\alpha}{3}}$. In this case, we have $M_2(x^3, \alpha) = 2$, where $\{2\sqrt{\frac{\alpha}{3}}, -\sqrt{\frac{\alpha}{3}}\}$ and $\{-2\sqrt{\frac{\alpha}{3}}, \sqrt{\frac{\alpha}{3}}\}$ are two sets of solutions. Next, we proceed to consider when $x^3 - \alpha x - c = 0$ has exactly one or three solutions. Since $x^3 - \alpha x - c = 0$ has one solution $x_0 \in \mathbb{F}_q$, we can factor $x^3 - \alpha x - c = (x - x_0)(x^2 + x_0x + x_0^2 - \alpha)$, where $c = x_0^3 - \alpha x_0$. We need to check if $x^2 + x_0x + x_0^2 - \alpha = 0$ has solutions in $\mathbb{F}_q$, where $x_0^2 \notin \{\frac{\alpha}{3}, \frac{4\alpha}{3}\}$. Since $x^2 + x_0x + x_0^2 - \alpha = 0$ is equivalent to $(x + \frac{x_0}{2})^2 = \alpha - \frac{3x_0^2}{4}$, it has zero or two solutions if and only if $1 - \frac{3x_0^2}{4\alpha} \in C_0^{(2,q)}$ or $1 - \frac{3x_0^2}{4\alpha} \in C_1^{(2,q)}$. We first consider the case of $q \equiv 1 \pmod 4$. If $3 \in C_0^{(2,q)}$, then the number of nonzero square $x_0^2 \in C_0^{(2,q)}$, such that $1 - \frac{3x_0^2}{4\alpha} \in C_0^{(2,q)}$, is equal to $(1, 0)_q = \frac{q-1}{4}$. Note that when $x_0 = 0$, we have $1 - \frac{3x_0^2}{4\alpha} = 1 \in C_0^{(2,q)}$. Thus, $M_1(x^3, \alpha) = 2 \cdot \frac{q-1}{4} + 1 = \frac{q+1}{2}$. Similarly, the number of nonzero square $x_0^2 \in C_0^{(2,q)}$, such that $1 - \frac{3x_0^2}{4\alpha} \in C_1^{(2,q)}$, is equal to $(1, 1)_q = \frac{q-1}{4}$. Hence, $M_3(x^3, \alpha) = 2 \cdot \frac{q-1}{4} \cdot \frac{1}{3} = \frac{q-1}{6}$. If $3 \in C_1^{(2,q)}$, then the number of nonzero square $x_0^2 \in C_0^{(2,q)} \setminus \{\frac{\alpha}{3}, \frac{4\alpha}{3}\}$, such that $1 - \frac{3x_0^2}{4\alpha} \in C_0^{(2,q)}$, is equal to $(0, 0)_q = \frac{q-5}{4}$. Note that when $x_0 = 0$, we have $1 - \frac{3x_0^2}{4\alpha} = 1 \in C_0^{(2,q)}$. Thus, $M_1(x^3, \alpha) = 2 \cdot \frac{q-5}{4} + 1 = \frac{q-3}{2}$. Similarly, the number of nonzero square $x_0^2 \in C_0^{(2,q)} \setminus \{\frac{\alpha}{3}, \frac{4\alpha}{3}\}$, such that $1 - \frac{3x_0^2}{4\alpha} \in C_1^{(2,q)}$, is equal to $(0, 1)_q - 1 = \frac{q-5}{4}$. Note that a minus one appears in the previous equation, as $1 - \frac{3x_0^2}{4\alpha} \in C_1^{(2,q)}$ when $x_0^2 = \frac{\alpha}{3}$. Therefore, $M_3(x^3, \alpha) = 2 \cdot \frac{q-5}{4} \cdot \frac{1}{3} = \frac{q-5}{6}$. Note that $3 \in C_0^{(2,q)}$ if and only if $3 \in C_0^{(2,p)}$ or m is even. Consequently, we have

$$3 \in \begin{cases} C_0^{(2,q)} & \text{if } p \equiv 1, 11 \pmod{12} \text{ or } m \text{ even}, \\ C_1^{(2,q)} & \text{if } p \equiv 5, 7 \pmod{12} \text{ and } m \text{ odd}. \end{cases}$$

Hence, $q \equiv 1 \pmod 4$ and $3 \in C_0^{(2,q)}$ is equivalent to $p \equiv 1 \pmod{12}$ or m even. Similarly, $q \equiv 1 \pmod 4$ and $3 \in C_1^{(2,q)}$ is equivalent to $p \equiv 5 \pmod{12}$ and m odd. Therefore, two out of the four cases in (3) with $\beta = \alpha$ have been completed by the above argument. Applying an analogous approach to the $q \equiv 3 \pmod 4$ case, we complete the proof of (3) with $\beta = \alpha$. □

Remark 2.5. We note that for $\mathbb{F}_q = \mathbb{F}_{2^m}$, the value of $M_i(x^3, 1)$ has been computed in [20, Appendix]. Moreover, as a special case, the multiplicity distribution of x^3 follows from the result of Bluher [3, Theorem 5.6], see also [22, Proposition B.9].

Combining Lemmas 2.1, 2.2 and 2.4, we can completely determine the multiplicity distribution of degree three polynomials.

Theorem 2.6. *The multiplicity distribution of $f(x) = x^3 - ax^2$ over $\mathbb{F}_q = \mathbb{F}_{p^m}$ is as follows.*

(1) When $p = 2$, if m odd, then we have

$$\begin{cases} M_0(f,b) = 0, M_1(f,b) = q, M_2(f,b) = 0, M_3(f,b) = 0, \\ \qquad\qquad\qquad\qquad \text{if } a = b = 0, \text{ or } a \neq 0, \ \frac{b}{a^2} = 1, \\ M_0(f,b) = \frac{q+1}{3}, M_1(f,b) = \frac{q}{2} - 1, M_2(f,b) = 1, M_3(f,b) = \frac{q-2}{6}, \\ \qquad\qquad\qquad\qquad \text{if } a = 0, \ b \neq 0, \text{ or } a \neq 0, \ \frac{b}{a^2} \neq 1, \end{cases}$$

and if m even, then we have

$$\begin{cases} M_0(f,b) = \frac{2(q-1)}{3}, M_1(f,b) = 1, M_2(f,b) = 0, M_3(f,b) = \frac{q-1}{3}, \\ \qquad\qquad\qquad\qquad \text{if } a = b = 0, \text{ or } a \neq 0, \ \frac{b}{a^2} = 1, \\ M_0(f,b) = \frac{q-1}{3}, M_1(f,b) = \frac{q}{2}, M_2(f,b) = 1, M_3(f,b) = \frac{q-4}{6}, \\ \qquad\qquad\qquad\qquad \text{if } a = 0, \ b \neq 0, \text{ or } a \neq 0, \ \frac{b}{a^2} \neq 1. \end{cases}$$

(2) When $p = 3$, we have

$$\begin{cases} M_0(x^3,0) = 0, M_1(x^3,0) = q, M_2(x^3,0) = 0, M_3(x^3,0) = 0, & \text{if } b \in \{0\} \cup C_1^{(2,q)}, \\ M_0(x^3,b) = \frac{2q}{3}, M_1(x^3,b) = 0, M_2(x^3,b) = 0, M_3(x^3,b) = \frac{q}{3}, & \text{if } b \in C_0^{(2,q)}. \end{cases}$$

Moreover,

$$M_0(f,b) = \frac{q}{3}, \quad M_1(f,b) = \frac{q-1}{2}, \quad M_2(f,b) = 1, \quad M_3(f,b) = \frac{q-3}{6},$$

where $a \neq 0$ and $b \in \mathbb{F}_q$.

(3) When $p > 3$, if $p \equiv 1 \pmod{12}$ or m even, or $p \equiv 7 \pmod{12}$ and m odd, set

$$j = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12} \text{ or } m \text{ even}, \\ -1 & \text{if } p \equiv 7 \pmod{12} \text{ and } m \text{ odd}. \end{cases}$$

Then we have

$$\begin{cases} M_0(f,b) = \frac{2(q-1)}{3}, M_1(f,b) = 1, M_2(f,b) = 0, M_3(f,b) = \frac{q-1}{3}, \\ \qquad\qquad\qquad\qquad \text{if } a = b = 0, \text{ or } a \neq 0, \ \frac{b}{a^2} = -\frac{1}{3}, \\ M_0(f,b) = \frac{q-1}{3}, M_1(f,b) = \frac{q-j}{2}, M_2(f,b) = 1 + j, M_3(f,b) = \frac{q-4-3j}{6}, \\ \qquad\qquad\qquad\qquad \text{if } a = 0, \ b \in C_0^{(2,q)}, \text{ or } a \neq 0, \ \frac{b}{a^2} + \frac{1}{3} \in C_0^{(2,q)}, \\ M_0(f,b) = \frac{q-1}{3}, M_1(f,b) = \frac{q+j}{2}, M_2(f,b) = 1 - j, M_3(f,b) = \frac{q-4+3j}{6}, \\ \qquad\qquad\qquad\qquad \text{if } a = 0, \ b \in C_1^{(2,q)}, \text{ or } a \neq 0, \ \frac{b}{a^2} + \frac{1}{3} \in C_1^{(2,q)}. \end{cases}$$

If $p \equiv 5 \pmod{12}$ *and* m *odd, or* $p \equiv 11 \pmod{12}$ *and* m *odd, set*

$$k = \begin{cases} 1 & \text{if } p \equiv 5 \pmod{12} \text{ and } m \text{ odd,} \\ -1 & \text{if } p \equiv 11 \pmod{12} \text{ and } m \text{ odd.} \end{cases}$$

Then we have

$$\begin{cases} M_0(f,b) = 0, M_1(f,b) = q, M_2(f,b) = 0, M_3(f,b) = 0, \\ \qquad\qquad \text{if } a = b = 0, \text{ or } a \neq 0, \ \frac{b}{a^2} = -\frac{1}{3}, \\ M_0(f,b) = \frac{q+1}{3}, M_1(f,b) = \frac{q-2+k}{2}, M_2(f,b) = 1-k, M_3(f,b) = \frac{q-2+3k}{6}, \\ \qquad\qquad \text{if } a = 0, \ b \in C_0^{(2,q)}, \text{ or } a \neq 0, \ \frac{b}{a^2} + \frac{1}{3} \in C_0^{(2,q)}, \\ M_0(f,b) = \frac{q+1}{3}, M_1(f,b) = \frac{q-2-k}{2}, M_2(f,b) = 1+k, M_3(f,b) = \frac{q-2-3k}{6}, \\ \qquad\qquad \text{if } a = 0, \ b \in C_1^{(2,q)}, \text{ or } a \neq 0, \ \frac{b}{a^2} + \frac{1}{3} \in C_1^{(2,q)}. \end{cases}$$

According to Remark 1.4(1), Theorem 1.6 immediately follows from Theorem 2.6.

Remark 2.7. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree $2 \leqslant d \leqslant q-1$. Define

$$N_f = \{c \in \mathbb{F}_q \mid f(x) + cx \text{ is a permutation over } \mathbb{F}_q\}.$$

Lower and upper bounds on the non-hitting index $v_0(f)$ involving q, d and $|N_f|$ were derived in [22, Proposition 3.4]. More precisely, we have

$$\lceil \frac{q-1}{d} \rceil (q - |N_f|) \leqslant v_0(f) \leqslant (q - \lceil \frac{q}{d} \rceil)(q - |N_f|). \tag{2.1}$$

Since the size of N_f is in general difficult to compute, the tightness of the bounds in (2.1) remains unclear. On the other hand, Theorem 1.6 provides some instances where the bounds are actually tight, which can be achieved by polynomials of the form $x^3 - ax^2$. In fact, the lower bound in (2.1) is tight, when $p = 2$, m odd, or $p \equiv 5, 11 \pmod{12}$, m odd, or $p = 3$, $a \neq 0$. The upper bound in (2.1) is tight, when $p = 3$ and $a = 0$.

Let f be a polynomial over $\mathbb{F}_q$. For $b \in \mathbb{F}_q$ and $0 \leqslant i \leqslant q$, define

$$M_i^*(f,b) = |\{c \in \mathbb{F}_q \mid f(x) - bx - c = 0 \text{ has } i \text{ nonzero solutions in } \mathbb{F}_q\}|.$$

Employing Theorem 2.6, we can derive the intersection distribution of some other monomials closely related to degree three polynomials.

Theorem 2.8. *Let* $f(x) = x^d$ *be a polynomial over* $\mathbb{F}_q$. *Then the following holds.*

(1) If $p = 2$, m *odd and* $d \in \{\frac{q+1}{3}, q-3\}$, *then*

$$v_0(f) = \frac{q^2-1}{3}, \quad v_1(f) = \frac{q^2-q+2}{2},$$
$$v_2(f) = q-1, \quad v_3(f) = \frac{(q-1)(q-2)}{6}.$$

(2) If $p = 2$, m even and $d = q - 3$, then

$$v_0(f) = \frac{(q-1)^2}{3}, \quad v_1(f) = \frac{3q^2+7q-4}{6}, \quad v_2(f) = 0,$$
$$v_3(f) = \frac{(q-1)(q-4)}{6}, \quad v_4(f) = \frac{q-1}{3}.$$

(3) If $p = 3$ and $d \in \{\frac{2q}{3}, q-3\}$, then

$$v_0(f) = \frac{(2q+3)(q-1)}{6}, \quad v_1(f) = \frac{q^2-2q+3}{2},$$
$$v_2(f) = \frac{3(q-1)}{2}, \quad v_3(f) = \frac{(q-1)(q-3)}{6}.$$

(4) If $p > 3$, $q \equiv 1 \pmod 3$ and $d = q - 3$, then

$$v_0(f) = \frac{(2q+1)(q-1)}{6}, \quad v_1(f) = \frac{3q^2-2q+5}{6}, \quad v_2(f) = \frac{3(q-1)}{2},$$
$$v_3(f) = \frac{(q-1)(q-7)}{6}, \quad v_4(f) = \frac{q-1}{3}.$$

(5) If $p > 3$, $q \equiv 2 \pmod 3$ and $d \in \{\frac{q+1}{3}, q-3\}$, then

$$v_0(f) = \frac{(2q+5)(q-1)}{6}, \quad v_1(f) = \frac{q^2-4q+5}{2},$$
$$v_2(f) = \frac{5(q-1)}{2}, \quad v_3(f) = \frac{(q-1)(q-5)}{6}.$$

Proof. We only prove (4), since the other cases are similar. For $b, c \in \mathbb{F}_q$, consider the number of solutions to the equation $x^{q-3} - bx - c = 0$. Note that 0 is a solution if and only if $c = 0$. Clearly,

$$|\{x \in \mathbb{F}_q \mid x^{q-3} - bx = 0\}| = \begin{cases} 1 & \text{if } b \notin C_0^{(3,q)}, \\ 4 & \text{if } b \in C_0^{(3,q)}. \end{cases}$$

If $c \neq 0$, then it is easy to see that every nonzero solution to $x^{q-3} - bx - c = 0$ is also a nonzero solution to $(\frac{1}{x})^3 - \frac{c}{x} - b = 0$. Hence, we need to count the number of nonzero solution to $x^3 - cx - b = 0$, where $b \in \mathbb{F}_q$ and $c \neq 0$. Note that $x^3 - cx - b = 0$ has a zero solution if and only if $b = 0$. Moreover, $x^3 - cx = 0$ has 3 solutions and 2 nonzero solutions if and only if $c \in C_0^{(2,q)}$, and has 1 solution and no nonzero solution if and only if $c \in C_1^{(2,q)}$. Thus, it remains to compute $M_i^*(x^3, c)$, for each $c \in \mathbb{F}_q^*$. Employing Theorem 2.6(3), we have

$$\begin{cases} M_0^*(x^3,c) = \frac{q-1}{3}, M_1^*(x^3,c) = \frac{q-j}{2}, M_2^*(x^3,c) = 2+j, M_3^*(x^3,c) = \frac{q-10-3j}{6}, & \text{if } c \in C_0^{(2,q)}, \\ M_0^*(x^3,c) = \frac{q+2}{3}, M_1^*(x^3,c) = \frac{q+j-2}{2}, M_2^*(x^3,c) = 1-j, M_3^*(x^3,c) = \frac{q-4+3j}{6}, & \text{if } c \in C_1^{(2,q)}, \end{cases}$$

where

$$j = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{12} \text{ or } m \text{ even}, \\ -1 & \text{if } p \equiv 7 \pmod{12} \text{ and } m \text{ odd}. \end{cases}$$

Combining the above observations, we derive the intersection distribution. □

So far, not much is known about the non-hitting index of monomials. Employing Theorems 1.6 and 2.8, in Table 2.1, we give an update of [22, Table 3.2], where an entry with superscript ■ represents the non-hitting index derived from Theorems 1.6 and 2.8, an entry with superscript ★ represents the non-hitting index which has not yet been understood, an entry without superscript represents the non-hitting index known before. Note that in the table, when $(d, q-1) = 1$, we group d and its inverse modulo $q-1$ together. As we shall see, when $q \leqslant 11$, the non-hitting index of each monomial has been explained.

Table 2.1: The non-hitting index of all power mappings in $\mathbb{F}_q$, $q \leqslant 16$

q	$(d, v_0(x^d))$
2	$(1,1)$
3	$(1,2)$, $(2,3)$
4	$(1,3)$, $(2,6)$, $(3,5)$
5	$(1,4)$, $(2,10)$, $(3,8)$, $(4,7)$
7	$(1,6)$, $(2,21)$, $(3,16)$, $(4,15)$, $(5,18)$, $(6,11)$
8	$(1,7)$, $(\{2,4\},28)$, $(\{3,5\},21)$, $(6,28)$, $(7,13)$
9	$(1,8)$, $(2,36)$, $(3,24)$, $(4,30)$, $(5,24)$, $(6,28)^{\blacksquare}$, $(7,32)$, $(8,15)$
11	$(1,10)$, $(2,55)$, $(\{3,7\},40)^{\blacksquare}$, $(4,45)^{\blacksquare}$, $(5,38)$, $(6,35)$, $(8,45)^{\blacksquare}$, $(9,50)$, $(10,19)$
13	$(1,12)$, $(2,78)$, $(3,56)^{\blacksquare}$, $(4,57)^{\bigstar}$, $(5,60)^{\bigstar}$, $(6,58)$, $(7,48)$, $(8,69)^{\bigstar}$, $(9,56)^{\bigstar}$, $(10,54)^{\blacksquare}$, $(11,72)$, $(12,23)$
16	$(1,15)$, $(\{2,8\},120)$, $(3,85)$, $(4,60)$, $(5,102)$, $(6,85)^{\bigstar}$, $(\{7,13\},75)^{\blacksquare}$, $(9,85)$, $(10,87)^{\bigstar}$, $(11,90)^{\bigstar}$, $(12,70)^{\bigstar}$, $(14,120)$, $(15,29)$

3 Monomials having the same intersection distribution as x^3

A polynomial $f \in \mathbb{F}_q[x]$ is called *x^3-like*, if it has the same intersection distribution as x^3 over $\mathbb{F}_q$. In this section, inspired by the open problem of classifying o-monomials, which is equivalent to finding all monomials over $\mathbb{F}_q = \mathbb{F}_{2^m}$ with the same intersection distribution as x^2, we consider x^3-like monomials. First of all, we display several classes of x^3-like monomials.

Theorem 3.1. *(1) When $p = 2$ and $1 \leqslant d \leqslant q-1$, the monomial x^d is x^3-like in the following cases:*

(1a) $d = 2^i + 1$, $\gcd(i, m) = 1$,

(1b) $d \equiv (2^i+1)^{-1} \pmod{q-1}$, $\gcd(i, m) = 1$, m odd,

(1c) $d \equiv -2^i \pmod{q-1}$, $\gcd(i,m)=1$, *m odd.*

(2) When $p=3$, the monomial x^d is x^3-like in the following case:

(2a) $d=3^i$, $\gcd(i,m)=1$.

(3) When $p>3$, the monomial x^d is x^3-like in the following cases:

(3a) $d=3$,

(3b) $d=\frac{2q-1}{3}$, $p\equiv 5 \pmod 6$, *m odd, where $\frac{2q-1}{3}$ is the inverse of 3 modulo $q-1$.*

The proof of the above theorem follows from Remark 3.3 below. As we shall see, Theorem 3.1 contains the obvious x^3-like monomials. Besides, there are more monomials which are conjectured to be x^3-like. Below, we propose two conjectures based on a numerical experiment done for all monomials over $\mathbb{F}_q$ in the following ranges:

- $p=2$ and $1 \leqslant m \leqslant 21$,
- $p=3$ and $1 \leqslant m \leqslant 13$,
- $p>3$ and $q \leqslant 10^5$.

Conjecture 3.2. (1) The following two families of monomials x^d over $\mathbb{F}_q=\mathbb{F}_{3^m}$ are x^3-like [1]:

- $d=3^{(m+1)/2}+2$ and d^{-1}, m odd,
- $d=2\cdot 3^{m-1}+1$ and d^{-1}, m odd.

(2) The two families in Part (1), plus those in Theorem 3.1, are all the x^3-like monomials.

Remark 3.3.

(1) When $p=2$, Family (1a) in Theorem 3.1 contains quadratic monomials, whose intersection distribution follows from [3, Theorem 5.6] (see also [22, Proposition B.9]). The monomials in (1a) are permutations whenever m is odd. Their inverses are exactly those in Family (1b). The monomials in Family (1c) are closely related to quadratic monomials, since for each $b,c\in\mathbb{F}_q$, the equations $x^{-2^i}-bx-c=0$ and $bx^{2^i+1}-cx^{2^i}-1=0$ have the same nonzero solutions, and replace x by $\frac{1}{y}$ in the latter one, we have $y^{2^i+1}-cy-b=0$, which goes back to the quadratic monomials case. Each monomial in Family (1c) has an inverse belonging to the same family.

(2) When $p>3$, the monomial in Family (3a) of Theorem 3.1 is a permutation if and only if $p\equiv 5 \pmod 6$ and m being odd. Hence, Family (3b) consists of the inverses of Family (3a) whenever they exist.

[1] This conjecture has been stated in a preprint version of this paper. Based on the knowledge of the preprint, Li, Li, and Qu proved Conjecture 3.2(1) [23].

(3) According to Parts (1) and (2), when $p \neq 3$, all x^3-like monomials are the obvious ones. In contrast, the $p = 3$ case is more interesting since some less obvious monomials occur. On one hand, the Family (2a) contains linearized monomials, whose proof is easy (see for instance [22, Table 3.1]). Moreover, each monomial in Family (2a) has an inverse belonging to the same family. On the other hand, the two more families in Conjecture 3.2(1) are still mysterious.

(4) It is worthy to note that the exponents in Conjecture 3.2(1) are all three-valued decimations in regard to the cross-correlation distribution of ternary m-sequences (see [11, Theorem 6(A)] and [17, Theorem 4.9]). We note that for $1 \leqslant i \leqslant m-1$, the decimations d and $3^i d$ have the same cross-correlation distribution. On the other hand, we think the intersection distribution is a more subtle property, since for $1 \leqslant i \leqslant m-1$, x^d and $x^{3^i d}$ over $\mathbb{F}_{3^m}$ have different intersection distributions in general.

Next, we make some progress towards Conjecture 3.2(2), by providing some restrictions on the monomials satisfying (1.2) or (1.3). Recall that an affine line is an i-secant line to G_f, if it intersects G_f in exactly i points. Since every pair of distinct points in G_f could determine a 2-secant line, the largest value of $v_2(f)$ is $\frac{q(q-1)}{2}$. In this sense, we observe that $v_2(f) = q-1$ in (1.2) and $v_2(f) = 0$ in (1.3) are both very small, which means there are very few 2-secant lines to G_f. Next, we are going to show that this unusual geometric property can be interpreted in an algebraic way, which gives strong restrictions on the monomials satisfying (1.2) or (1.3).

Considering monomials with intersection distribution (1.2), we need to understand under what conditions, there are exactly $q-1$ distinct 2-secant lines to G_f. As a preparation, we have the following two lemmas. We write $g_d(x) = \frac{x^d-1}{x-1}$ and use $H_{q,d} = \{g_d(x) \mid x \in \mathbb{F}_q \setminus \{1\}\}$ to denote the image set of $g_d(x)$ over $\mathbb{F}_q \setminus \{1\}$. The following lemma is easy to see.

Lemma 3.4. *Let f be a polynomial over $\mathbb{F}_q$. For distinct $x_1, x_2 \in \mathbb{F}_q$ with $x_1 \neq 0$, write $y = \frac{x_2}{x_1} \in \mathbb{F}_q \setminus \{1\}$. Then we have the following.*

(1) Two points $(x_1, f(x_1)), (x_2, f(x_2)) \in G_f$ determine a 2-secant line to G_f if and only if the equation $\frac{f(x)-f(x_1)}{x-x_1} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$ has exactly one solution $x = x_2$. In particular, if $f(x) = x^d$, then the two points $(x_1, x_1^d), (x_2, x_2^d) \in G_f$ determine a 2-secant line to G_f if and only if $\frac{y^d-1}{y-1} \in H_{q,d}$ has exactly one preimage y under g_d. Furthermore, if $x_2 \neq 0$ or equivalently $y \neq 0$, by interchanging the roles of x_1 and x_2, the two points $(x_1, x_1^d), (x_2, x_2^d) \in G_f$ determine a 2-secant line to G_f if and only if $\frac{(1/y)^d-1}{1/y-1} \in H_{q,d}$ has exactly one preimage $1/y$ under g_d.

(2) For $f(x) = x^d$ and each $y \in \mathbb{F}_q \setminus \{1\}$ such that $\frac{y^d-1}{y-1}$ has exactly one preimage y under g_d, the $q-1$ pairs of distinct points $\{\{(x_1, x_1^d), (x_2, x_2^d)\} \mid x_1, x_2 \in \mathbb{F}_q^*, \frac{x_2}{x_1} = y\}$

determine $q-1$ distinct 2-secant lines to G_f. Moreover, suppose that

$$\begin{aligned}&\{y \in \mathbb{F}_q \setminus \{1\} \mid \tfrac{y^d-1}{y-1} \text{ has exactly one preimage } y \text{ under } g_d\}\\ =&\{y_1, y_1^{-1}, y_2, y_2^{-1}, \cdots, y_s, y_s^{-1}, y'_1, y'_2, \cdots, y'_t\},\end{aligned}$$

where no element in $\{y'_1, y'_2, \cdots, y'_t\}$ is the inverse of any other element. Then there are exactly $(s+t)(q-1)$ distinct 2-secant lines to G_f.

(3) The two points $(x_1, f(x_1)), (x_2, f(x_2)) \in G_f$ determine a 3-secant line to G_f if and only if the equation $\frac{f(x)-f(x_1)}{x-x_1} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$ has exactly two solutions. In particular, if $f(x) = x^d$, then the two points $(x_1, x_1^d), (x_2, x_2^d) \in G_f$ determine a 3-secant line to G_f if and only if $\frac{y^d-1}{y-1} \in H_{q,d}$ has exactly two preimages under g_d.

In the case that $z \in H_{q,d}$ has exactly one preimage under g_d, we have the following lemma providing crucial information about the images and the preimages of g_d.

Lemma 3.5. *Let $f(x) = x^d$ be over $\mathbb{F}_q$. Suppose $z \in H_{q,d}$ has exactly one preimage $y \in \mathbb{F}_q \setminus \{1\}$ under g_d. Then we have the following:*

(1) If $z = 0$, then q is odd, d is even and $y = -1$.

(2) If $y \notin \{0, -1\}$, then $z \notin \{0, 1\}$, and $y^{-d+1}z \notin \{0, 1, z\}$ also has exactly one preimage $\frac{1}{y} \in \mathbb{F}_q \setminus \{0, \pm 1\}$.

(3) If q is even and $H_{q,d}$ has exactly one element z with exactly one preiamge y under g_d, then $(y, z) = (0, 1)$.

(4) If q is odd and $H_{q,d}$ has exactly two elements z, z' with exactly one preimage under g_d, say y, y' respectively, then either $(y, z) = (0, 1)$ and $(y', z') = (-1, 0)$, or $y \notin \{0, -1\}$, $y' = \frac{1}{y}$ and $z' = y^{-d+1}z$.

Proof. (1) If $0 \in H_{q,d}$ has exactly one preimage y under g_d, then $(d, q-1) = 2$. Thus q is odd and d is even, which implies $y = -1$.

(2) Since $y \neq -1$, by Part (1), $z \neq 0$ and $\frac{1}{y} \neq -1$. Since $y \neq 0$, then $z \neq 1$ and $y^{-d+1} \neq 1$, which implies $y^{-d+1}z \neq z$ and $y \neq 1$. Since $z = \frac{y^d-1}{y-1}$, we have $y^{-d+1}z = \frac{(1/y)^d-1}{(1/y)-1}$. By Lemma 3.4(1), $y^{-d+1}z = \frac{(1/y)^d-1}{(1/y)-1}$ has exactly one preimage $\frac{1}{y} \in \mathbb{F}_q \setminus \{0, \pm 1\}$ under g_d. As the image of $\frac{1}{y} \notin \{0, \pm 1\}$ under g_d, the element $y^{-d+1}z \notin \{0, 1\}$.

(3) Since $H_{q,d}$ has exactly one element z with exactly one preimage y under g_d, by Part (2), $y \in \{0, -1\}$. Note that q being even forces $y = 0$. Consequently, $(y, z) = (0, 1)$.

(4) If $y \notin \{0, -1\}$, then by Part (2), we have $y' = \frac{1}{y}$ and $z' = y^{-d+1}z$. If $y \in \{0, -1\}$, first, assume $y = 0$ and therefore $z = 1$. Suppose $y' \notin \{0, -1\}$, then by Part (2), $z = 1, z', y'^{-d+1}z'$ are distinct and all have exactly one preimage under g_d, which is impossible. Hence, $y' = -1$ and $z' \in \{0, 1\}$. Note that $z = 1$ has exactly one preimage, then $z' \neq 1$ and $(y', z') = (-1, 0)$. □

Now we are ready to derive some restrictions on monomials satisfying (1.2).

Theorem 3.6. *Let $f(x) = x^d$ be over $\mathbb{F}_q$ satisfying* (1.2)*. Then*

(1) Each element in $H_{q,d}$ has either one or two preimages under g_d. Furthermore, the number of elements in $H_{q,d}$ having exactly one preimage under g_d is either one or two.

(2) If q is even, then there exists exactly one element $z \in H_{q,d}$ with exactly one preimage y under g_d, where $(y, z) = (0, 1)$.

(3) If q is odd, then there exist exactly two elements $z, z' \in H_{q,d}$ with exactly one preimage under g_d, say y, y' respectively, where $y \notin \{0, -1\}$, $y' = \frac{1}{y}$ and $z' = y^{-d+1}z$.

(4)

$$(d, q-1) = \begin{cases} 1 & \text{if } 0 \notin H_{q,d}, \\ 3 & \text{if } 0 \in H_{q,d}. \end{cases}$$

Proof. (1) Since $v_i(f) = 0$ for each $i > 3$, then by Lemma 3.4, each element in $H_{q,d}$ has either one or two preimages. Consider the number of elements in $H_{q,d}$, which has exactly one preimage. By Lemmas 3.4(2), if this number is either zero or at least three, then $v_2(f) = 0$ or $v_2(f) \geqslant 2(q-1)$, which contradicts (1.2). Hence, the number is either one or two.

(2) If q is even, then the preimage set $\mathbb{F}_q \setminus \{1\}$ has odd size $q-1$. Combining Part (1) and the parity, there exists exactly one element z in $H_{q,d}$, which has exactly one preimage y under g_d. By Lemma 3.5(3), we have $(y, z) = (0, 1)$.

(3) If q is odd, then the preimage set $\mathbb{F}_q \setminus \{1\}$ has even size $q-1$. Combining Part (1) and the parity, there exists two elements $z, z' \in H_{q,d}$ with exactly one preimage under g_d. Suppose $z = g_d(y)$ and $z' = g_d(y')$. By Lemma 3.5(4), we have either $(y, z) = (0, 1)$ and $(y', z') = (-1, 0)$, or $y \notin \{0, -1\}$, $y' = \frac{1}{y}$ and $z' = y^{-d+1}z$. According to Lemma 3.4(2), the former case implies $v_2(f) \geqslant 2(q-1)$, which contradicts (1.2).

(4) If $0 \notin H_{q,d}$, then clearly $(d, q-1) = 1$. If $0 \in H_{q,d}$, then 0 has exactly either one or two preimages under g_d. If 0 has exactly one preimage under g_d, then by Lemma 3.5(1), we have q being odd and the preimage is -1. This contradicts Part (3). Hence, 0 has exactly two preimages under g_d and therefore $(d, q-1) = 3$. □

Consequently, we have the following necessary and sufficient condition characterizing monomials over $\mathbb{F}_q$ satisfying (1.2), when q is not divisible by 3.

Theorem 3.7. *Let $f(x) = x^d$ be over $\mathbb{F}_q$ where $(3, q) = 1$. Then f satisfies* (1.2) *if and only if one of the following holds.*

(1) If q is even, then 0 is the only preimage of $1 \in H_{q,d}$ under g_d and $g_d|_{\mathbb{F}_q \setminus \{0,1\}}$ is 2-to-1.

(2) If q is odd, then there exist exactly two elements $z, z' \in H_{q,d}$ with exactly one preimage under g_d, say y, y' respectively, where $y \notin \{0, -1\}$, $y' = \frac{1}{y}$ and $z' = y^{-d+1}z$, and $g_d|_{\mathbb{F}_q \setminus \{1, y, y'\}}$ is 2-to-1.

In both q even and odd cases, we have

$$(d, q-1) = \begin{cases} 1 & \text{if } 0 \notin H_{q,d}, \\ 3 & \text{if } 0 \in H_{q,d}. \end{cases}$$

Proof. The necessity follows from Theorem 3.6 and we only need to consider the sufficiency. For Part (1), by employing Lemma 3.4 and Theorem 3.6(2), we have $v_2(f) = q-1$ and $v_i(f) = 0$ for each $i > 3$. For Part (2), by employing Lemma 3.4 and Theorem 3.6(3), we have $v_2(f) = q-1$ and $v_i(f) = 0$ for each $i > 3$. Together with Proposition 1.2, we conclude that f satisfies (1.2). The greatest common divisor $(d, q-1)$ follows from the 2-to-1 property. □

Similarly, we have the following necessary and sufficient condition characterizing monomials over $\mathbb{F}_q$ satisfying (1.3), when q is a power of 3.

Theorem 3.8. *Let $f(x)$ be over $\mathbb{F}_q = \mathbb{F}_{3^m}$. Then f satisfies* (1.3) *if and only if for each $y \in \mathbb{F}_q$, the function $\frac{f(x+y)-f(y)}{x}\Big|_{\mathbb{F}_q^*}$ is 2-to-1. In particular, $f(x) = x^d$ satisfies* (1.3) *if and only if the following holds:*

(1) $\gcd(d-1, q-1) = 2$,

(2) $g_d|_{\mathbb{F}_q \setminus \{1\}}$ *is 2-to-1, which implies*

$$(d, q-1) = \begin{cases} 1 & \text{if } 0 \notin H_{q,d}, \\ 3 & \text{if } 0 \in H_{q,d}. \end{cases}$$

Proof. A polynomial f has intersection distribution (1.3) if and only if every two distinct points in G_f lead to a unique third point in G_f, which lies on the line determined by these two points. Hence, for two distinct $x_1, x_2 \in \mathbb{F}_q$, the equation $\frac{f(x)-f(x_1)}{x-x_1} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$ has a unique solution $x \in \mathbb{F}_q \setminus \{x_1, x_2\}$. Equivalently, for each $y \in \mathbb{F}_q$, we have $\frac{f(x)-f(y)}{x-y}\Big|_{\mathbb{F}_q \setminus \{y\}}$ is 2-to-1. Therefore, f has intersection distribution (1.3) if and only if the function $\frac{f(x+y)-f(y)}{x}\Big|_{\mathbb{F}_q^*}$ is 2-to-1 for each $y \in \mathbb{F}_q$. Consider $f(x) = x^d$. For $y = 0$, the mapping $\frac{f(x)}{x} = x^{d-1}\Big|_{\mathbb{F}_q^*}$ is 2-to-1 if and only if $(d-1, q-1) = 2$. For $y \in \mathbb{F}_q^*$, the mapping $\frac{f(x)-f(y)}{x-y} = \frac{x^d-y^d}{x-y}\Big|_{\mathbb{F}_q \setminus \{y\}}$ is 2-to-1 if and only if $g_d|_{\mathbb{F}_q \setminus \{1\}}$ is 2-to-1. The greatest common divisor $(d, q-1)$ follows from the 2-to-1 property. □

Theorems 3.7 and 3.8 can be viewed as analogies of [18, Theorem 8.22, Corollary 8.24], which give characterizations of o-polynomials and o-monomials. The strict restrictions in these theorems indicate that monomials with intersection distribution (1.2) or (1.3) are very rare. Actually, these two theorems help to significantly reduce the computational complexity of verifying whether a monomial has intersection distribution (1.2) or (1.3), which leads to Conjecture 3.2.

4 Nonisomorphic Steiner triple systems arising from monomials

In this section, we shall observe that a polynomial over $\mathbb{F}_{3^m}$ with intersection distribution (1.3) produces a Steiner triple system. More interestingly, some nonisomorphic Steiner triple systems are obtained by employing distinct polynomials over $\mathbb{F}_{3^m}$.

Recall that a Steiner triple system STS(v) is a set system $(\mathcal{V}, \mathcal{B})$, where $\mathcal{V}$ is a point set of v elements, and $\mathcal{B}$ is a block set consisting of distinct 3-subsets, such that every two points are contained in exactly one block. Two Steiner triple systems $(\mathcal{V}_1, \mathcal{B}_1)$ and $(\mathcal{V}_2, \mathcal{B}_2)$ are isomorphic, if there exists a bijection between $\mathcal{V}_1$ and $\mathcal{V}_2$, which also induces a bijection between $\mathcal{B}_1$ and $\mathcal{B}_2$. For a comprehensive survey about Steiner triple systems, please refer to [9, Section II.2]. The following is a primary example of Steiner triple systems STS(v) with v being a power of 3.

Example 4.1. ([9, Section II.2, Theorem 2.10]) Let $\mathcal{V} = \mathbb{F}_{3^m}$ and

$$\mathcal{B} = \{\{x_1, x_2, x_3\} \mid x_1, x_2, x_3 \in \mathbb{F}_{3^m} \text{ distinct}, x_1 + x_2 + x_3 = 0\}.$$

Then $(\mathcal{V}, \mathcal{B})$ forms an STS(3^m). In another word, the points and lines in the affine geometry $AG(m, 3)$ generate an STS(3^m), which is therefore named an *affine triple system*.

Next, we propose a construction of STS(3^m) arising from polynomials over $\mathbb{F}_{3^m}$. For a polynomial f over $\mathbb{F}_q$, it is called $\mathbb{F}_p$-*linearized*, if $f(x+y) = f(x)+f(y)$ for each $x, y \in \mathbb{F}_q$ and $f(ax) = af(x)$ for each $x \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$. Note that f is $\mathbb{F}_p$-linearized only if $f(0) = 0$.

Theorem 4.2. *Let f be a polynomial over $\mathbb{F}_{3^m}$ intersection distribution* (1.3)*. Let $\mathcal{V} = \mathbb{F}_{3^m}$ and*

$$\mathcal{B}_f = \{\{x_1, x_2, x_3\} \mid x_1, x_2, x_3 \in \mathbb{F}_{3^m} \text{ distinct}, \tfrac{f(x_3)-f(x_1)}{x_3-x_1} = \tfrac{f(x_2)-f(x_1)}{x_2-x_1}\}.$$

Then $(\mathcal{V}, \mathcal{B}_f)$ is an STS(3^m). Moreover,

(1) if $f'(x) = f(x) + bx + c$, then $(\mathcal{V}, \mathcal{B}_f)$ and $(\mathcal{V}, \mathcal{B}_{f'})$ are the same.

(2) if f is a permutation, then $(\mathcal{V}, \mathcal{B}_f)$ and $(\mathcal{V}, \mathcal{B}_{f^{-1}})$ are isomorphic.

(3) if $f(0) = 0$, then $(\mathcal{V}, \mathcal{B}_f)$ is an affine triple system if and only if f is an $\mathbb{F}_3$-linearized polynomial.

Proof. By Theorem 3.8, for each pair of distinct elements $x_1, x_2 \in \mathbb{F}_{3^m}$, there is a unique $x_3 \in \mathbb{F}_{3^m}$ different from x_1 and x_2, such that $\frac{f(x_3)-f(x_1)}{x_3-x_1} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$. Hence, $\mathcal{B}_f$ is well-defined. Since every pair of distinct elements x_1 and x_2 determines a unique x_3, which form a block $\{x_1, x_2, x_3\}$, then $(\mathcal{V}, \mathcal{B}_f)$ is an STS(3^m) by definition.

Part (1) follows easily from the definition of $\mathcal{B}_f$ and $\mathcal{B}_{f'}$. For Part (2), note that $\{x_1, x_2, x_3\} \in \mathcal{B}_f$ if and only if $\{f(x_1), f(x_2), f(x_3)\} \in \mathcal{B}_{f^{-1}}$. Therefore, f is a bijection of $\mathcal{V}$ and induces a bijection between $\mathcal{B}_f$ and $\mathcal{B}_{f^{-1}}$. Thus, $(\mathcal{V}, \mathcal{B}_f)$ and $(\mathcal{V}, \mathcal{B}_{f^{-1}})$ are isomorphic. For Part (3), we can see that assuming $f(0) = 0$ does not lose any generality by Part (1).

If f is $\mathbb{F}_3$-linearized, then $x_3 = -x_1 - x_2$ is the unique solution to $\frac{f(x)-f(x_1)}{x-x_1} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$, which leads to an affine triple system. Conversely, if $(\mathcal{V}, \mathcal{B}_f)$ is an affine triple system, then the summation of the elements in each block is 0. Hence, for each pair of distinct elements x_1 and x_2, we have $x_3 = -x_1 - x_2$ and $\frac{f(-x_1-x_2)-f(x_1)}{x_1-x_2} = \frac{f(x_2)-f(x_1)}{x_2-x_1}$, which implies $f(-x_1 - x_2) = -f(x_1) - f(x_2)$. Set $x_2 = 0$, we have $f(-x_1) = -f(x_1)$ and therefore, $f(-x_1 - x_2) = f(-x_1) + f(-x_2)$. Hence, f is an $\mathbb{F}_3$-linearized polynomial over $\mathbb{F}_{3^m}$. □

Combining Theorems 3.1(2) and 4.2, the affine triple system STS(3^m) can be derived by using monomial $f(x) = x^{3^i}$ over $\mathbb{F}_{3^m}$, where $(i, m) = 1$. We ask if there are other polynomials over $\mathbb{F}_{3^m}$, which produces Steiner triple system nonisomorphic to the affine ones. In view of Conjecture 3.2(1), we compare the Steiner triple systems derived from the two families in it and the affine triple systems when m is small.

Example 4.3. For m being odd, let $f_1(x) = x^3$, $f_2(x) = x^{3^{(m+1)/2}+2}$ and $f_3(x) = x^{2\cdot 3^{m-1}+1}$ be polynomials over $\mathbb{F}_{3^m}$. According to Conjecture 3.2, f_1, f_2 and f_3 have the same intersection distribution for $1 \leqslant m \leqslant 13$, m odd. Let $\mathcal{V} = \mathbb{F}_{3^m}$. A numerical experiment indicates the following.

(1) When $m = 3$, since the two permutations $f_2(x) = x^{11}$ and $f_3(x) = x^{19}$ are inverses of each other, then by Theorem 4.2(1), $(\mathcal{V}, \mathcal{B}_{f_2})$ and $(\mathcal{V}, \mathcal{B}_{f_3})$ are isomorphic. Moreover, $(\mathcal{V}, \mathcal{B}_{f_1})$ and $(\mathcal{V}, \mathcal{B}_{f_2})$ are nonisomorphic.

(2) When $m = 5$, $(\mathcal{V}, \mathcal{B}_{f_1})$, $(\mathcal{V}, \mathcal{B}_{f_2})$ and $(\mathcal{V}, \mathcal{B}_{f_3})$ are pairwise nonisomorphic.

The isomorphism test was implemented using the build-in function "IsIsomorphic" from the Computational Algebra System MAGMA. Assuming that Conjecture 3.2(1) is true, we believe that f_i, $1 \leqslant i \leqslant 3$, produce three pairwise nonisomorphic STS(3^m) when $m \geqslant 5$.

5 Application to Kakeya sets in affine planes

Let ℓ be the line at infinity in $PG(2, q)$. For each point $P \in \ell$, define ℓ_P to be a line through P other than ℓ. A *Kakeya set* in $PG(2, q)$ is defined to be the point set

$$K = (\bigcup_{P\in\ell} \ell_P) \setminus \ell.$$

If we restrict to the affine plane $AG(2, q) = PG(2, q) \setminus \ell$, then the Kakeya set K contains an affine line in each direction. So far, most papers concerning Kakeya sets in affine planes focus on Kakeya sets whose sizes are close to the lower and upper bounds [1, 2, 4, 12, 13, 14, 16]. Note that the construction of Kakeya sets is easy, since for each point $P \in \ell$, we can choose an arbitrary line ℓ_P through P other than ℓ. On the other hand, computing the size of Kakeya set is difficult. In [13], an exhaustive search determines all possible sizes of Kakeya sets in $PG(2, q)$ where $q \leqslant 9$. Inspired by this work, the authors of [22] proposed explicitly constructions of Kakeya sets with nice underlying algebraic structures, which are derived from monomials over finite fields and have previously unknown sizes.

Along this line, we present infinite families of Kakeya sets from degree three polynomials in this section. As a major advantage of our constructions, the sizes of proposed Kakeya sets follow directly from the multiplicity distribution of degree three polynomials, which have been computed in Section 2. For Kakeya sets in affine spaces with higher dimension, please refer to [15, 19, 21, 24, 28].

First of all, we remark that the concept of intersection distribution can be defined with respect to point sets in classical projective planes $PG(2,q)$ [22, Definition 1.3].

Definition 5.1. Let D be a point set in $PG(2,q)$. For $0 \leqslant i \leqslant q+1$, define $u_i(D)$ to be the number of lines in $PG(2,q)$, which intersect D in exactly i points. The sequence $(u_i(D))_{i=0}^{q+1}$ is the intersection distribution of D. The integer $u_0(D)$ is the non-hitting index of D.

For a $(q+2)$-set D in $PG(2,q)$, a point $P \in D$ is called an *internal nucleus* of D, if each line through P intersects D in exactly one more point. The following is an alternative viewpoint to understand Kakeya sets proposed in [2].

Lemma 5.2. [22, Lemma 4.1] *Let K be a Kakeya set in $PG(2,q)$, where $K = (\bigcup_{P\in\ell} \ell_P)\backslash\ell$. Define the dual Kakeya set DK to be the dual of the $q+2$ lines $\{\ell_P \mid P \in \ell\} \cup \{\ell\}$. Then DK is a $(q+2)$-set in $PG(2,q)$ with an internal nucleus, such that $|K| = q^2 - u_0(DK)$.*

Therefore, computing the size of K amounts to calculating the non-hitting index of the dual Kakeya set DK. Moreover, to construct a Kakeya set, it suffices to construct its dual, which is a $(q+2)$-set in $PG(2,q)$ with an internal nucleus. Actually, given a polynomial f over $\mathbb{F}_q$ and $b \in \mathbb{F}_q$, we construct a dual Kakeya set

$$DK(f,b) := \{\langle (x, f(x), 1)\rangle \mid x \in \mathbb{F}_q\} \cup \{\langle (0,1,0), (1,b,0)\rangle\},$$

which has an internal nucleus $\langle (0,1,0)\rangle$. Indeed, the non-hitting index of $DK(f,b)$ follows from the multiplicity distribution of f [22, Proposition 4.3]. Consequently, we have the following proposition. Note that for a dual Kakeya set $DK(f,b)$, we use $K(f,b)$ to denote the Kakeya set dual to $DK(f,b)$.

Proposition 5.3. *For a polynomial f over $\mathbb{F}_q$ and $b \in \mathbb{F}_q$, we have $u_0(DK(f,b)) = v_0(f) - M_0(f,b)$ and therefore, $|K(f,b)| = q^2 - v_0(f) + M_0(f,b)$.*

Therefore, the non-hitting index $v_0(f)$ and the intersection distribution $M_0(f,b)$ imply the size of $K(f,b)$. Combining Theorems 1.6, 2.6 and Proposition 5.3, we can obtain the size of some Kakeya sets derived from monomials.

Theorem 5.4.

(1) Suppose $q \equiv 0 \pmod 3$. Then $|K(x^3 - ax^2, b)| = \frac{2q^2+q}{3}$ if $a = 0$, $b \notin C_0^{(2,q)}$, or $a \neq 0$, $b \in \mathbb{F}_q$, and $|K(x^3, b)| = \frac{2q^2+3q}{3}$ if $b \in C_0^{(2,q)}$.

(2) Suppose $q \equiv 1 \pmod 3$. Then $|K(x^3 - ax^2, b)| = \frac{2q^2+2q-1}{3}$ if $a = b = 0$, or $a \neq 0$, $\frac{b}{a^2} = -\frac{1}{3}$, and $|K(x^3 - ax^2, b)| = \frac{2q^2+q}{3}$ if $a = 0$, $b \neq 0$, or $a \neq 0$, $\frac{b}{a^2} \neq -\frac{1}{3}$.

(3) Suppose $q \equiv 2 \pmod 3$. *Then* $|K(x^3 - ax^2, b)| = \frac{2q^2+1}{3}$ *if* $a = b = 0$, *or* $a \neq 0$, $\frac{b}{a^2} = -\frac{1}{3}$, *and* $|K(x^3 - ax^2, b)| = \frac{2q^2+q+2}{3}$ *if* $a = 0$, $b \neq 0$, *or* $a \neq 0$, $\frac{b}{a^2} \neq -\frac{1}{3}$.

In Table 5.1, we list the known sizes of Kakeya sets in $PG(2, q)$, with prime power $q \leqslant 19$. When $q \leqslant 9$, all possible sizes follow from the exhaustive search in [13, Table 1]. When $11 \leqslant q \leqslant 19$, we only list the known sizes realizable by explicit constructions. We note that when the sizes of the Kakeya sets are close to the lower and upper bounds, there have been a series of literature concerning their construction and characterization [1, 2, 4, 12, 13, 14, 16]. In the table, an entry with superscript ■ represents the size of Kakeya sets following from the explicit constructions in Theorem 5.4, which are unknown before. An entry with superscript ★ represents the size of Kakeya sets which do not have explicit constructions so far. An entry without superscript represents the size of Kakeya sets with known explicit constructions before.

Table 5.1: The known sizes of Kekaya set in $PG(2, q)$, for prime power $q \leqslant 19$

q	Sizes of Kekaya sets
2	3, 4
3	7, 9
4	10, 12, 13, 16
5	17, 18, 19, 21, 25
7	31, $32^{\bigstar}$, 33, 34, 35, $36^{\bigstar}$, 37, 39, 43, 49
8	36, 40, 42, 43, $44^{\bigstar}$, $45^{\bigstar}$, 46, $47^{\bigstar}$, 48, 49, 52, 57, 64
9	49, $51^{\bigstar}$, 52, 53, 54, 55, $56^{\bigstar}$, 57, $58^{\bigstar}$, $59^{\bigstar}$, $60^{\bigstar}$, 61, $62^{\bigstar}$, 63, 67, 73, 81
11	71, 75, 77, $81^{\blacksquare}$, 85, 86, 87, 91, 93, 97, 103, 111, 121
13	97, 103, 112, 115, $117^{\blacksquare}$, 121, 127, 129, 133, 139, 147, 157, 169
16	136, 144, 148, 150, 160, 166, 176, 181, 192, 193, 196, 201, 208, 217, 228, 241, 256
17	161, 169, 189, $193^{\blacksquare}$, $199^{\blacksquare}$, 200, 209, 217, 219, 223, 229, 237, 247, 259, 273, 289
19	199, 207, 209, $247^{\blacksquare}$, $253^{\blacksquare}$, 259, 261, 262, 271, 273, 277, 283, 291, 301, 313, 327, 343, 361

6 Conclusion

In this paper, we determined the multiplicity distribution of polynomials with the form $x^3 - ax^2$, which gives the intersection distribution of each degree three polynomial. Inspired by the famous open problem of classifying o-polynomials, we initiated to classify all monomials having the same intersection distribution as x^3 and made some progress along this line. Interestingly, when $p = 3$, numerical experiment indicated that some monomials with the same intersection distribution as x^3 led to nonisomorphic Steiner triple systems.

Finally, the multiplicity distribution of $x^3 - ax^2$ generated several families of Kakeya sets, whose sizes are different comparing with the known ones.

Except Conjecture 3.2, we think the following four problems deserve further investigation.

(1) In Table 2.1, the non-hitting indices of certain monomials have not been well understood. Therefore, it is interesting to give a theoretical explanation for these non-hitting indices.

(2) In Section 3, we only considered x^3-like monomials. On the other hand, the restriction of being monomials is technical and one may further consider x^3-like polynomials. In view of Theorem 1.6, there are plenty of x^3-like binomials when $p \neq 3$. In addition, when $p = 3$, consider binomials of the form $x^{d_1} + ax^{d_2}$, where $a \in \mathbb{F}_{3^m}$ and $2 < d_2 < d_1 < 3^m$. Interestingly, an exhaustive search for $1 \leqslant m \leqslant 5$ shows that all such x^3-like binomials must be linearized. More precisely, we have $(d_1, d_2) \in \{(9, 3)\}$ if $m = 3$, $(d_1, d_2) \in \{(27, 3)\}$ if $m = 4$ and $(d_1, d_2) \in \{(27, 9), (81, 3)\}$ if $m = 5$.

(3) In Example 4.3, the fact that the Steiner triple systems being nonisomorphic follows from a numerical computation. A theoretic proof confirming the nonisomorphism, even only for small values of m, could be very enlightening.

(4) In Table 5.1, there are a few Kakeya sets having no theoretical constructions, whose sizes are only known by numerical experiment. We ask for explicit constructions for these Kakeya sets.

We mention a recent work due to Ding and Tang [10], in which polynomials over finite fields were employed to construct combinatorial t-designs. While determining the parameters of the t-design arising from a polynomial f is difficult in general [10], we note that the multiplicity distribution of f implies the parameters of the associated t-design. Therefore, this design-theoretic application supplies one more motivation to study the multiplicity distribution of polynomials over finite fields. Finally, we note that a recent paper by Li, Li, and Qu [23] has confirmed Conjecture 3.2(1).

Acknowledgement

Shuxing Li is supported by the Pacific Institute for the Mathematical Sciences. This project was initiated during the second and third authors visited the first author at University of Rostock. They wish to thank the Institute of Mathematics for the great hospitality. The second author was then supported the Alexander von Humboldt Foundation. He wishes to thank Christian Kaspers, Otto von Guerick University of Magdeburg, for his kind help with the numerical experiments on Conjecture 3.2.

References

[1] A. Blokhuis, M. De Boeck, F. Mazzocca, and L. Storme. The Kakeya problem: a gap in the spectrum and classification of the smallest examples. *Des. Codes Cryptogr.*, 72(1):21–31, 2014.

[2] A. Blokhuis and F. Mazzocca. The finite field Kakeya problem. In *Building bridges*, volume 19 of *Bolyai Soc. Math. Stud.*, pages 205–218. Springer, Berlin, 2008.

[3] A. W. Bluher. On $x^{q+1} + ax + b$. *Finite Fields Appl.*, 10(3):285–305, 2004.

[4] M. De Boeck and G. Van de Voorde. A note on large Kakeya sets. arXiv:2003.08480v1.

[5] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. *IEEE Trans. Inform. Theory*, 52(3):1141–1152, 2006.

[6] C. Carlet, P. Charpin, and V. Zinoviev. Codes, bent functions and permutations suitable for DES-like cryptosystems. *Des. Codes Cryptogr.*, 15(2):125–156, 1998.

[7] F. Caullery and K.-U. Schmidt. On the classification of hyperovals. *Adv. Math.*, 283:195–203, 2015.

[8] W. Cherowitzo. Hyperovals in desarguesian planes: An update. *Discrete Math.*, 155(1):31–38, 1996.

[9] C. J. Colbourn. *Handbook of combinatorial designs*, chapter Triple systems, pages 58–71. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[10] C. Ding and C. Tang. Infinite families of 3-designs from o-polynomials. To appear in *Adv. Math. Commun.* https://doi.org/10.3934/amc.2020082.

[11] H. Dobbertin, T. Helleseth, P. Vijay Kumar, and H. Martinsen. Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type. *IEEE Trans. Inform. Theory*, 47(4):1473–1481, 2001.

[12] J. M. Dover and K. E. Mellinger. Small Kakeya sets in non-prime order planes. *European J. Combin.*, 47:95–102, 2015.

[13] J. M. Dover and K. E. Mellinger. Some spectral results on Kakeya sets. *Adv. Geom.*, 15(3):333–338, 2015.

[14] J. M. Dover, K. E. Mellinger, and K. E. Scott. Minimal Kakeya sets. *J. Combin. Des.*, 22(2):95–104, 2014.

[15] Z. Dvir. On the size of Kakeya sets in finite fields. *J. Amer. Math. Soc.*, 22(4):1093–1097, 2009.

[16] X. W. C. Faber. On the finite field Kakeya problem in two dimensions. *J. Number Theory*, 124(1):248–257, 2007.

[17] T. Helleseth. Some results about the cross-correlation function between two maximal linear sequences. *Discrete Math.*, 16(3):209–232, 1976.

[18] J. W. P. Hirschfeld. *Projective geometries over finite fields*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, second edition, 1998.

[19] S. Kopparty, V. F. Lev, S. Saraf, and M. Sudan. Kakeya-type sets in finite vector spaces. *J. Algebraic Combin.*, 34(3):337–355, 2011.

[20] P. Vijay Kumar, T. Helleseth, A. R. Calderbank, and Jr. A. R. Hammons. Large families of quaternary sequences with low correlation. *IEEE Trans. Inform. Theory*, 42(2):579–592, 1996.

[21] G. Kyureghyan, P. Müller, and Q. Wang. On the size of Kakeya sets in finite vector spaces. *Electron. J. Combin.*, 20(3):#P36, 2013.

[22] S. Li and A. Pott. Intersection distribution, non-hitting index and Kakeya sets in affine planes. *Finite Fields Appl.*, 66:101691, 38, 2020.

[23] Y. Li, K. Li, and L. Qu. On two conjectures about the intersection distribution. arXiv:2010.00312v1.

[24] A. Maschietti. Kakeya sets in finite affine spaces. *J. Combin. Theory Ser. A*, 118(1):228–230, 2011.

[25] B. Segre. Ovals in a finite projective plane. *Canadian J. Math.*, 7:414–416, 1955.

[26] T. Storer. *Cyclotomy and difference sets*. Lectures in Advanced Mathematics, No. 2. Markham Publishing Co., Chicago, Ill., 1967.

[27] T. L. Vis. *Monomial hyperovals in Desarguesian planes*. ProQuest LLC, Ann Arbor, MI, 2010. Thesis (Ph.D.)–University of Colorado at Denver.

[28] T. Wolff. Recent work connected with the Kakeya problem. In *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162. Amer. Math. Soc., Providence, RI, 1999.