INFINITE FAMILIES OF 3-DESIGNS FROM O-POLYNOMIALS

CUNSHENG DING
Department of Computer Science and Engineering
The Hong Kong University of Science and Technology
Clear Water Bay, Kowloon, Hong Kong

CHUNMING TANG*
School of Mathematics and Information
China West Normal University, Sichuan Nanchong, 637002, China

(Communicated by Sihem Mesnager)

Abstract. A classical approach to constructing combinatorial designs is the
group action of a $t$-transitive or $t$-homogeneous permutation group on a base
block, which yields a $t$-design in general. It is open how to use a $t$-transitive
or $t$-homogeneous permutation group to construct a $(t+1)$-design in general.
It is known that the general affine group $GA_1(GF(q))$ is doubly transitive
on $GF(q)$. The classical theorem says that the group action by $GA_1(GF(q))$
yields 2-designs in general. The main objective of this paper is to construct
3-designs with $GA_1(GF(q))$ and o-polynomials. O-polynomials (equivalently,
hyperovals) were used to construct only 2-designs in the literature. This pa-
per presents for the first time infinite families of 3-designs from o-polynomials
(equivalently, hyperovals).

1. Introduction

Let $P$ be a set of $v \geq 1$ elements, and let $B$ be a set of $k$-subsets of $P$, where $k$
is a positive integer with $1 \leq k \leq v$. Let $t$ be a positive integer with $t \leq k$. The
pair $\mathcal{D} = (P,B)$ is called a $t$-$(v,k,\lambda)$ design, or simply $t$-design, if every $t$-subset
of $P$ is contained in exactly $\lambda$ elements of $B$. The elements of $P$ are called points,
and those of $B$ are referred to as blocks. We usually use $b$ to denote the number
of blocks in $B$. A $t$-design is called simple if $B$ does not contain repeated blocks.
In this paper, we consider only simple $t$-designs. A $t$-design is called symmetric if
$\lambda = 1$, and is denoted by $S(t,k,v)$. A classical method of constructing $t$-designs by group action is described in the
following theorem [2, p. 175].

2010 Mathematics Subject Classification: Primary: 51E21, 05B05, 12E10.
Key words and phrases: Hyperoval, o-polynomial, polynomial, projective plane, $t$-design.

C. Ding’s research was supported by the Hong Kong Research Grants Council, Proj. No.
16300415. C. Tang was supported by National Natural Science Foundation of China (Grant No.
11871058) and China West Normal University (14E013, CXTD2014-4 and the Meritocracy
Research Funds).

* Corresponding author: Chunming Tang.
Theorem 1. Let \( \mathcal{P} \) be a set of \( v \geq 1 \) elements, and let \( G \) be a permutation group on \( \mathcal{P} \). Let \( B \subset \mathcal{P} \) be a subset with at least two elements, which is called the base block. Define

\[
G(B) = \{ g(B) : g \in G \},
\]

where \( g(B) = \{ g(b) : b \in B \} \). If \( G \) is \( t \)-homogeneous on \( \mathcal{P} \) and \( |B| \geq t \), then \( (\mathcal{P}, G(B)) \) is a \( t \-(v, k, \lambda) \) design with

\[
k = |B|, \quad \lambda = b \frac{k}{v}, \quad |G| = \frac{|B|}{|G_B|} \left( \begin{array}{c} k \\ t \end{array} \right),
\]

where \( b = |G|/|G_B| \) and \( G_B = \{ g \in G : g(B) = B \} \) is the setwise stabiliser of \( B \).

Let \( q \) be a prime power. The general affine group \( GA_1(q) \) of degree one consists of all the following permutations of the set \( GF(q) \):

\[
\pi_{(a,b)}(x) = ax + b,
\]

where \( a \in GF(q)^* \) and \( b \in GF(q) \). It is a group under the function composition operation, and is interesting, as it is doubly transitive on \( GF(q) \) and has a small group size. This group is also denoted by \( AGL(1,q) \) in some references, and can be written as

\[
GA_1(q) \sim GF(q) \rtimes GF(q)^*,
\]

which is the external semidirect product of the additive group of \( GF(q) \) and the multiplicative group of \( GF(q) \).

Notice that \( GA_1(q) \) is doubly transitive on \( GF(q) \). If one employs the group \( GA_1(q) \) and Theorem 1, one constructs 2-designs in general. In this paper, we will demonstrate that it is possible to construct 3-designs with the action of \( GA_1(q) \). To this end, we have to choose a special base block \( B \subset GF(q) \). In this paper, we choose the base block \( B \) with \( o \)-polynomials.

A hyperoval in the projective plane \( PG(2, GF(2^m)) \) is a set of \( 2^m + 2 \) points such that no three of them are collinear. \( O \)-polynomials are a special type of polynomials over \( GF(2^m) \) and correspond to hyperovals in the projective space \( PG(2, GF(2^m)) \) (see Theorem 4). Hence, an \( o \)-polynomial can be viewed as a hyperoval, and vice versa. Hyperovals were used to construct two types of 2-designs in the literature (see Theorems 6 and 7). This means that \( o \)-polynomials were used to construct 2-designs indirectly (via their corresponding hyperovals) in the literature.

The main objective of this paper is to construct infinite families of 3-designs from \( o \)-polynomials. This is the first time that 3-designs are constructed from \( o \)-polynomials.

2. A CONSTRUCTION FOR 3-DESIGNS WITH O-MONOMIALS OVER GF(q)

2.1. A GENERAL CONSTRUCTION OF 2-DESIGNS WITH PERMUTATION POLYNOMIALS. Let \( q \) be a prime power, and let \( f \) be a polynomial over \( GF(q) \), which is always viewed as a function from \( GF(q) \) to \( GF(q) \) throughout this paper. For each \( (b, c) \in GF(q)^2 \), define

\[
B_{(f,b,c)} = \{ f(x) + bx + c : x \in GF(q) \}.
\]

Let \( k \) be an integer with \( 2 \leq k \leq q \). Define

\[
B_{(f,k)} = \{ B_{(f,b,c)} : |B_{(f,b,c)}| = k, \ b, \ c \in GF(q) \}.
\]
The incidence structure $\mathcal{D}(f, k) := (\text{GF}(q), \mathcal{B}_{(f,k)})$ may be a $t$-$(q, k, \lambda)$ design for some $\lambda$, where $\text{GF}(q)$ is the point set, and the incidence relation is the set membership. In this case, we say that the polynomial $f$ supports a $t$-$(q, k, \lambda)$ design.

The following is a general result about monomials. It presents an interesting application of monomials in the theory of combinatorial designs.

**Theorem 2.** Let $f(x) = x^e$ be a permutation polynomial of $\text{GF}(q)$, and let $k \geq 2$ be a positive integer such that $|\mathcal{B}_{(f,k)}| \geq 1$. Then the incidence structure $\mathcal{D}(f, k) := (\text{GF}(q), \mathcal{B}_{(f,k)})$ is a 2-$(q, k, \lambda)$ design for some $\lambda$.

**Proof.** The general affine group $\text{GA}_1(\text{GF}(q))$ is defined by

$$\text{GA}_1(\text{GF}(q)) := \{ux + v : (u, v) \in \text{GF}(q)^* \times \text{GF}(q)\}.$$ 

Let $\sigma(x) = ux + v \in \text{GA}_1(\text{GF}(q))$, where $u \in \text{GF}(q)^*$ and $v \in \text{GF}(q)$. Note that $\gcd(e, q - 1) = 1$. Let $1/e$ denote the multiplicative inverse of $e$ modulo $q - 1$. We have then

$$u(f(x) + bx + c) + v = u(x^e + bx + cu + v) = (u^{1/e}x)^e + u^{1/e}b(u^{1/e}x) + cu + v.$$ 

We then deduce that $\sigma(B_{(f,b,c)}) = B_{(f,ux^{1/e}b,cu+v)}$. This means that the general affine group $\text{GA}_1(\text{GF}(q))$ fixes $\mathcal{B}_{(f,k)}$. It is well known that $\text{GA}_1(\text{GF}(q))$ acts on $\text{GF}(q)$ doubly transitively. The desired conclusion then follows. $\square$

Theorem 2 says that $\mathcal{D}(f, k) := (\text{GF}(q), \mathcal{B}_{(x^e,k)})$ is a 2-$(q, k, \lambda)$ design if $x^e$ is a permutation polynomial. In Section 2.2, we will prove that $\mathcal{D}(f, k) := (\text{GF}(q), \mathcal{B}_{(x^e,k)})$ is a 3-$(q, q/2, \lambda)$ design if $x^e$ is an o-polynomial.

Two designs $\mathcal{D}(\mathcal{P}, \mathcal{B})$ and $\mathcal{D}(\mathcal{P}', \mathcal{B}')$ are said to be isomorphic if there is a 1-to-1 mapping $\sigma$ from $\mathcal{P}$ to $\mathcal{P}'$ such that $\sigma$ sends each block in $\mathcal{B}$ to a block in $\mathcal{B}'$. Such a $\sigma$ is called an isomorphism from $\mathcal{D}(\mathcal{P}, \mathcal{B})$ to $\mathcal{D}(\mathcal{P}', \mathcal{B}')$. An isomorphism from $\mathcal{D}(\mathcal{P}, \mathcal{B})$ to $\mathcal{D}(\mathcal{P}', \mathcal{B}')$ is called an automorphism of $\mathcal{D}(\mathcal{P}, \mathcal{B})$. All automorphisms of $\mathcal{D}(\mathcal{P}, \mathcal{B})$ form a group under the function composition, and is called the automorphism group of $\mathcal{D}(\mathcal{P}, \mathcal{B})$. It is straightforward to prove the following theorem.

**Theorem 3.** Let $f$ and $g$ be two polynomials over $\text{GF}(q)$ such that $\mathcal{D}(f, k)$ and $\mathcal{D}(g, k)$ are $t$-designs. If there are $h \in \text{GF}(q)^*$, $u \in \text{GF}(q)^*$ and $v \in \text{GF}(q)$ such that $g(x) = h.f(ux + v)$ for all $x \in \text{GF}(q)$, then $\mathcal{D}(f, k)$ and $\mathcal{D}(g, k)$ are isomorphic.

#### 2.2. Designs from o-polynomials over $\text{GF}(2^m)$

Throughout this section $q = 2^m$ for some positive integer $m$. The objective of this section is to construct 2-designs and 3-designs from o-polynomials over $\text{GF}(q)$. Since o-polynomials and hyperovals in the Desarguesian plane $\text{PG}(2, \text{GF}(q))$ can be viewed as the same and hyperovals were used to construct two types of 2-designs in the literature, we have to introduce hyperovals and their designs, so that we will be able to compare our newly constructed designs with hyperoval designs in the literature.

#### 2.2.1. Hyperovals and their designs

An arc in the projective plane $\text{PG}(2, \text{GF}(q))$ is a set of at least three points in $\text{PG}(2, \text{GF}(q))$ such that no three of them are collinear (i.e., on the same line). For any arc $\mathcal{A}$ of $\text{PG}(2, \text{GF}(q))$, it is well known that $|\mathcal{A}| \leq q + 2$.

A hyperoval $\mathcal{H}$ in $\text{PG}(2, \text{GF}(q))$ is a set of $q + 2$ points such that no three of them are collinear, i.e., an arc with $q + 2$ points. Hyperovals are maximal arcs, as they have the maximal number of points as arcs. Two hyperovals are said to be equivalent.
if there is a collineation (i.e., an automorphism) of \( \text{PG}(2, \text{GF}(q)) \) that sends one to the other. Note that the automorphism group of \( \text{PG}(2, \text{GF}(q)) \) is the projective general linear group \( \text{PGL}_3(\text{GF}(q)) \). The \textit{automorphism group} of a hyperoval is the set of all collineations of \( \text{PG}(2, \text{GF}(q)) \) that leave the hyperoval invariant.

The next theorem shows that all hyperovals in \( \text{PG}(2, \text{GF}(q)) \) can be constructed with a special type of permutation polynomials of \( \text{GF}(q) \) [13, p. 504].

**Theorem 4** (Segre). Let \( m \geq 2 \). Any hyperoval in \( \text{PG}(2, \text{GF}(q)) \) can be written in the form

\[
\mathcal{H}(f) = \{(f(c), c, 1) : c \in \text{GF}(q)\} \cup \{(1, 0, 0)\} \cup \{(0, 1, 0)\},
\]

where \( f \in \text{GF}(q)[x] \) is such that

1. \( f \) is a permutation polynomial of \( \text{GF}(q) \) with \( \deg(f) < q \) and \( f(0) = 0, f(1) = 1 \);
2. for each \( a \in \text{GF}(q) \), \( g_a(x) = (f(x + a) + f(a))x^{q-2} \) is also a permutation polynomial of \( \text{GF}(q) \).

Conversely, every such set \( \mathcal{H}(f) \) is a hyperoval.

Polynomials satisfying the two conditions of Theorem 4 are called \( o \)-polynomials, i.e., oval-polynomials. For example, \( f(x) = x^2 \) is an \( o \)-polynomial over \( \text{GF}(q) \) for all \( m \geq 2 \). In the next section, we will summarize known \( o \)-polynomials over \( \text{GF}(q) \).

Two \( o \)-monomials \( f \) and \( g \) are said to be equivalent if the two hyperovals \( \mathcal{H}(f) \) and \( \mathcal{H}(g) \) are equivalent. The following result is well-known in the literature.

**Lemma 5.** Let \( q \geq 4 \). Two monomial hyperovals \( \mathcal{H}(x^j) \) and \( \mathcal{H}(x^e) \) in \( \text{PG}(2, \text{GF}(q)) \) are equivalent if and only if \( j \equiv e, 1/e, 1-e, 1/(1-e), e/(e-1) \) or \( (e-1)/e \) (mod \( q-1 \)).

Any hyperoval \( \mathcal{H} \) in \( \text{PG}(2, \text{GF}(q)) \) meets each line either in 0 or 2 points. A line is called an interior line (also called secant) of \( \mathcal{H} \) if it meets the hyperoval in two points, and an exterior line otherwise. Hence, a hyperoval partitions the lines of \( \text{PG}(2, \text{GF}(q)) \) into two classes, i.e., interior and exterior lines. This property allows us to define the so-called hyperoval designs as follows.

Let \( \mathcal{H} \) be any hyperoval in the Desarguesian projective plane \( \text{PG}(2, \text{GF}(q)) \). The \textit{hyperoval design} \( \mathcal{W}(q, \mathcal{H}) \) is the incidence structure with points the lines of \( \text{PG}(2, \text{GF}(q)) \) exterior to \( \mathcal{H} \) and blocks the points of \( \text{PG}(2, \text{GF}(q)) \) not on the hyperoval; incidence is given by the incidence in \( \text{PG}(2, \text{GF}(q)) \). We have then the following conclusion on the incidence structure \( \mathcal{W}(q, \mathcal{H}) \).

**Theorem 6** ([1]). The incidence structure \( \mathcal{W}(q, \mathcal{H}) \) defined by a hyperoval \( \mathcal{H} \) in \( \text{PG}(2, \text{GF}(q)) \) is a 2-{\((q - 1)q/2, q/2, 1)\} design, i.e., a Steiner system.

The second type of 2-designs from hyperovals are constructed as follows. Let \( \mathcal{H} \) be a hyperoval in \( \text{PG}(2, \text{GF}(q)) \). Let \( \mathcal{P} \) be the set of \( q^2 - 1 \) exterior points to \( \mathcal{H} \), i.e., the set of points in \( \text{PG}(2, \text{GF}(q)) \) not on \( \mathcal{H} \). For each point \( x \in \mathcal{P} \), define a block

\[
B_x = \{ y \in \mathcal{P} \setminus \{ x \} : yx \text{ is a secant to } \mathcal{H} \} \cup \{ x \}.
\]

Define further \( \mathcal{B} = \{ B_x : x \in \mathcal{P} \} \). We have then the following conclusion.

**Theorem 7** ([1, 12, 14]). The incidence structure \( \mathcal{S}(q, \mathcal{H}) := (\mathcal{P}, \mathcal{B}) \) is a symmetric 2-\{(q^2 - 1, q/2, 1, q^2 - 1)\} design.

It is well known that the Hadamard design \( \mathcal{S}(q, \mathcal{H}) \) defined above can be extended into a 3-\{(q^2, q/2, q^2 - 1)\} design, denoted by \( \mathcal{S}(q, \mathcal{H})^r \) [1].
Infinite families of 3-designs from o-polynomials

2.2.2. Known o-polynomials over GF(2^m). Recall that q = 2^m. To construct 2-designs and 3-designs subsequently, we need o-polynomials over GF(q). The objective of this section is to summarise known constructions of o-polynomials over GF(q) and consequently hyperovals in PG(2, GF(q)).

In the definition of o-polynomials, it is required that f(1) = 1. However, this is not essential, as one can always normalise f(x) by using f(1) − 1 f(x) due to the fact that f(1) ≠ 0. In this section, we do not require that f(1) = 1 for o-polynomials.

For any permutation polynomial f(x) over GF(q), we define 
\[ f(x) = x f(x^{q-2}), \]
and use \( f^{-1} \) to denote the compositional inverse of f, i.e., \( f^{-1}(f(x)) = x \) for all \( x \in GF(q) \).

The following two theorems introduce basic properties of o-polynomials whose proofs can be found in references about hyperovals.

**Theorem 8.** Let f be an o-polynomial over GF(q). Then the following statements hold:
- \( f^{-1} \) is also an o-polynomial;
- \( f(x^{2^j}) \) is also an o-polynomial for any \( 1 \leq j \leq m - 1 \);
- f is also an o-polynomial; and
- \( f(x + 1) + f(1) \) is also an o-polynomial.

**Theorem 9.** Let \( x^e \) be an o-polynomial over GF(q). Then every polynomial in \( \{x^e, x^1, x^{1-e}, x^{1-1/e}, x^{1+1/e} \} \) is also an o-polynomial, where \( 1/e \) denotes the multiplicative inverse of e modulo \( q - 1 \).

**Theorem 10 ([14]).** A polynomial f over GF(q) with f(0) = 0 is an o-polynomial if and only if \( f_u := f(x) + ux \) is 2-to-1 for every \( u \in GF(q)^* \).

Below we summarize some classes of o-polynomials over GF(q). If f is an endomorphism of the additive group of GF(q) and induces an o-polynomial over GF(q), then f is called a translation o-polynomial. All translation o-polynomials over GF(q) are described in the following theorem [16].

**Theorem 11.** Trans(x) = \( x^{2^h} \) is an o-polynomial over GF(q), where \( \gcd(h, m) = 1 \).

The following is a list of known properties of translation o-polynomials.
- \( \text{Trans}^{-1}(x) = x^{2^{m-h}} \) and \( \text{Trans}(x) = xf(x^{q-2}) = x^{4-2^{m-h}} \).

The following theorem describes a class of o-polynomials, which are called Segre o-polynomials [17, 18].

**Theorem 12.** Let m be odd. Then Segre(x) = \( x^6 \) is an o-polynomial over GF(q).

For this o-monomial, we have the following.
1. Segre(x) = \( x^{q-6} \).
2. Segre^{-1}(x) = \( x^{5\times 2^{m-1-3}} \).

Glynn discovered two families of o-polynomials [10]. The first is described as follows.

**Theorem 13.** Let m be odd. Then Glynn_1(x) = \( x^{3\times 2^{(m+1)/2} + 4} \) is an o-polynomial.
The second family of o-polynomials discovered by Glynn is documented in the following theorem.

**Theorem 14.** Let $m$ be odd. Then
\[
\text{Glynn}_2(x) = \begin{cases} 
    x^2(m+1)/2 + 2^{(3m+1)/4} & \text{if } m \equiv 1 \pmod{4}, \\
    x^2(m+1)/2 + 2^{(m+1)/4} & \text{if } m \equiv 3 \pmod{4}
\end{cases}
\]
is an o-polynomial over $GF(q)$.

The following describes another class of o-polynomials discovered by Cherowitzo [3, 4].

**Theorem 15 ([8]).** Let $m$ be odd and $e = (m+1)/2$. Then
\[
\text{Cherowitzo}(x) = x^{2e} + x^{2e+2} + x^{3 \times 2^e+4}
\]
is an o-polynomial over $GF(q)$.

For this o-trinomial, we have the following conclusions.
1. Cherowitzo$^{-1}(x) = x(x^{2e+1} + x^3 + x)^{2^e-1}$.
2. The following documents a family of o-trinomials due to Payne.

**Theorem 16 ([15]).** Let $m$ be odd. Then
\[
\text{Payne}(x) = x^5 + x^3 + x^1
\]
is an o-polynomial over $GF(q)$.

We have the following statements regarding the Payne o-trinomial.
1. Payne$(x) = xD_5(x^1, 1)$, where $D_5(a, x)$ is the Dickson polynomial of order 5.
2. Payne$(x) = Payne(x)$.
3. Note that
\[
\frac{1}{6} = \frac{5 \times 2^{m-1} - 2}{3}.
\]

We have then
\[
\text{Payne}(x) = x^{2^{m-1} + 2} + x^{2^{m-1}} + x^{2^m - 2}.
\]

**Theorem 17 ([8]).** Let $m$ be odd. Then
\[
(3) \quad \text{Payne}^{-1}(x) = \left(D_3 \times 2^{2m-2} (x, 1)\right)^6.
\]

The Subiaco o-polynomials are given in the following theorem [5].

**Theorem 18.** Define
\[
\text{Subiaco}_a(x) = ((a^2(x^4 + x) + a^2(1 + a + a^2)(x^3 + x^2))(x^4 + a^2x^2 + 1)^{q-2} + x^{2m-1},
\]
where $\text{Tr}(1/a) = 1$ and $d \notin GF(4)$ if $m \equiv 2 \pmod{4}$. Then Subiaco$_a(x)$ is an o-polynomial over $GF(q)$.

As a corollary of Theorem 18, we have the following.

**Corollary 19.** Let $m$ be odd. Then
\[
(4) \quad \text{Subiaco}_1(x) = (x + x^2 + x^3 + x^4)(x^4 + x^2 + 1)^{q-2} + x^{2m-1}
\]
is an o-polynomial over $GF(q)$. 

*Advances in Mathematics of Communications Volume X, No. X (200X), X–XX*
2.2.3. Families of 2-designs and 3-designs from o-polynomials. We start with a few auxiliary results. Let $g(x)$ be a polynomial over $\text{GF}(q)$. The value set of $g(x)$ is the image of the induced map $g : \text{GF}(q) \to \text{GF}(q)$. Thus the value set is 

$$V(g) = \{g(x) : x \in \text{GF}(q)\}.$$ 

We denote the cardinality of $V(g)$ by $v(g)$.

**Lemma 20.** Let $f(x) \in \text{GF}(q)[x]$ be an o-polynomial. For any $u_1, u_2, u_3 \in \text{GF}(q)$ with $(u_1 + u_2)(u_2 + u_3)(u_3 + u_1) \neq 0$, define 

$$I(u_1, u_2, u_3) = \{(a, b, c) \in \text{GF}(q)^3 : ab \neq 0, \{u_1, u_2, u_3\} \subseteq V(af(x) + bx + c)\}.$$ 

Then $|I(u_1, u_2, u_3)| = \frac{(q-1)(q-2)}{8}.$

**Proof.** Put 

$$T = \{(a, b, c, x_1, x_2, x_3) \in \text{GF}(q)^6 : af(x_i) + bx_i + c = u_i \ (i = 1, 2, 3)\}.$$ 

Then 

$$|T| = \sum_{(a, b, c) \in \text{GF}(q)^3} J(a, b, c) = \sum_{(x_1, x_2, x_3) \in \text{GF}(q)^3} K(x_1, x_2, x_3),$$ 

where 

$$J(a, b, c) = |\{(x_1, x_2, x_3) \in \text{GF}(q)^3 : af(x_i) + bx_i + c = u_i \ (i = 1, 2, 3)\}|,$$ 

and 

$$K(x_1, x_2, x_3) = |\{(a, b, c) \in \text{GF}(q)^3 : af(x_i) + bx_i + c = u_i \ (i = 1, 2, 3)\}|.$$ 

Notice that $g(x) = af(x) + bx + c$ is 2-to-1 when $ab \neq 0$. We have $v(g) = q/2$ if $ab \neq 0$. If $ab = 0$ and $a \neq b$, then $g(x)$ is a permutation. We deduce then 

$$v(af(x) + bx + c) = \begin{cases} 1, & \text{if and only if } a = b = 0, \\ q, & \text{if and only if } ab = 0 \text{ and } a \neq b, \\ q/2, & \text{if and only if } ab \neq 0. \end{cases}$$ 

Since $g(x) = af(x) + bx + c$ is 2-to-1 when $v(g) = q/2$ and is a permutation when $v(g) = q$, we have 

$$J(a, b, c) = \begin{cases} 0, & \text{if } \{u_1, u_2, u_3\} \nsubseteq V(g), \\ 1, & \text{if } \{u_1, u_2, u_3\} \subseteq V(g) \text{ and } v(g) = q, \\ 8, & \text{if } \{u_1, u_2, u_3\} \subseteq V(g) \text{ and } v(g) = q/2. \end{cases}$$ 

It then follows that 

$$|T| = \sum_{(a, b, c) \in \text{GF}(q)^3} J(a, b, c)$$ 

$$= |\{(a, b, c) \in \text{GF}(q)^3 : v(af(x) + bx + c) = q\}| + 8|I(u_1, u_2, u_3)|$$ 

$$= 2(q-1)q + 8|I(u_1, u_2, u_3)|.$$ 

Let $x_1, x_2$ and $x_3$ be three pairwise distinct elements in $\text{GF}(q)$. Then $(f(x_1), x_1, 1)$, $(f(x_2), x_2, 1)$, and $(f(x_3), x_3, 1)$ are three points in the hyperoval defined by the
o-polynomial \( f(x) \), and thus are linearly independent over \( \text{GF}(q) \). We then deduce that

\[
K(x_1, x_2, x_3) = \begin{cases} 0, & |\{x_1, x_2, x_3\}| < 3, \\ 1, & |\{x_1, x_2, x_3\}| = 3. \end{cases}
\]

Thus,

\[
|T| = \sum_{(x_1, x_2, x_3) \in \text{GF}(q)^3} K(x_1, x_2, x_3) = q(q - 1)(q - 2).
\]

Consequently,

\[
I(u_1, u_2, u_3) = \frac{1}{8} (q(q - 1)(q - 2) - 2(q - 1)q) = \frac{q(q - 1)(q - 4)}{8}.
\]

This completes the proof. \( \square \)

**Lemma 21.** Let \( a \in \text{GF}(q)^* \) and \( f(x) = x^d \in \text{GF}(q)[x] \) be an o-monomial. For any \( u_1, u_2, u_3 \in \text{GF}(q) \) with \((u_1 + u_2)(u_2 + u_3)(u_3 + u_1) \neq 0\), define

\[
I_a(u_1, u_2, u_3) = \{(b, c) \in \text{GF}(q)^2 : b \neq 0, \{u_1, u_2, u_3\} \subseteq V(af(x) + bx + c)\}.
\]

Then, \(|I_a(u_1, u_2, u_3)| = \frac{q(q - 4)}{8}\).

**Proof.** Recall that \( f(x) = x^d \) is a permutation of \( \text{GF}(q) \). We have then

\[
V(af(x) + bx + c) = \{(ax^d + bx + c : x \in \text{GF}(q)\}
\]

\[
= \{(a^{-d}x)^d + ba^{-d}x^{-d}x + c : x \in \text{GF}(q)\}
\]

\[
= V(x^d + ba^{-d}x + c),
\]

where \( d^{-1} \) is a positive integer such that \( dd^{-1} \equiv 1 \pmod{q - 1} \). Thus, \((b, c) \mapsto (ba^{-d}, c)\) induces a bijective mapping from \( I_a(u_1, u_2, u_3) \) to \( I_{I}(u_1, u_2, u_3) \). Then, \(|I_a(u_1, u_2, u_3)| = |I_I(u_1, u_2, u_3)|\). We then deduce by Lemma 20 that

\[
|I_a(u_1, u_2, u_3)| = \frac{1}{q - 1} |I(u_1, u_2, u_3)| = \frac{q(q - 4)}{8}.
\]

This completes the proof. \( \square \)

We are now ready to prove the following result, which is one of the main results of this paper.

**Theorem 22.** Let \( f(x) = x^e \) be an o-monomial over \( \text{GF}(q) \). Then \( \mathbb{D}(f, q/2) := (\text{GF}(q), \mathcal{B}_{(f,q/2)}) \) is a \( 3-(q, q/2, q(q - 4)/8\mu) \) design, where

\[
\mu = |\text{Stab}_{\text{AG}_1(\text{GF}(q))}(J_e)| = |\{(u, v) \in \text{GF}(q)^* \times \text{GF}(q) : uJ_e + v = J_e\}|
\]

and

\[
J_e = \{y^e + y : y \in \text{GF}(q)\}.
\]

**Proof.** We follow the notation of Lemmas 20 and 21 and their proofs. By the definition of o-polynomials, we have \( \gcd(e(c - 1), q - 1) = 1 \). Define the following multiset:

\[
\mathcal{B}_{(f,q/2)} = \{\{x^c + bx + c : x \in \text{GF}(q)\} : b \in \text{GF}(q)^*, c \in \text{GF}(q)\}\}
\]

By the proof of Theorem 2,

\[
\mathcal{B}_{(f,q/2)} = \{\{bJ_e + c : b \in \text{GF}(q)^*, c \in \text{GF}(q)\} \}
\]
Let \( \text{Corollary 23.} \)

\( (J_e \text{ the stabiliser of the block } B) \) and \( \mu \) determination of the parameters of the 3-design boils down to that of the size \( |B| \).

Consequently, the multiset \( \{\{V(x^e + bx + c) : (b, c) \in I_1(u_1, u_2, u_3)\}\} \)

is the same as the multiset \( |\text{Stab}_{AG_1(GF(q))}(J_e)|\{\{B_{f(b,c)} \in B_{f(q/2)} : \{u_1, u_2, u_3\} \subset B_{f(b,c)}\}\} \),

where \( \{u_1, u_2, u_3\} \) is a set of three distinct elements in GF\( (q) \), and \( I_1(u_1, u_2, u_3) \) was defined in Lemmas 20 and 21. It then follows that \( (GF(q), B_{f(q/2)}) \) is a \( t-(q, q/2, \lambda) \) design if and only if \( (GF(q), B_{f(q/2)}) \) is a \( t-(q, q/2, \lambda/\mu) \) design, where \( \mu \) was defined earlier.

By Lemma 21, \((GF(q), B_{f(q/2)})\) is a 3-\((q, q/2, q(q - 4)/8)\) design, which may contain repeated blocks. As a result, \((GF(q), B_{f(q/2)})\) is a 3-\((q, q/2, q(q - 4)/8\mu)\) simple design.

Theorem 22 says that every o-monomial \( x^e \) supports a 3-design \( D(x^e, q/2) \). The determination of the parameters of the 3-design boils down to that of the size \( \mu \) of the stabiliser of the block \( J_e \) under the action of \( GA_1(GF(q)) \).

The following is a corollary of Theorem 22. We give a direct proof of it below.

**Corollary 23.** Let \( f(x) = x^e \) be an o-monomial over GF\( (q) \) such that \( |B_{f(q/2)}| = (q - 1)/2 \). Then \( D(f, q/2) := (GF(q), B_{f(q/2)}) \) is a 3-\((q, q/2, q(q - 4)/8)\) design.

**Proof.** It follows from Theorem 10 that \( |B_{f(b,c)}| = q/2 \) for all \( (b, c) \in GF(q)^* \times GF(q) \). By assumption, all blocks \( B_{f(b,c)} \) with \( (b, c) \in GF(q)^* \times GF(q) \) are pairwise distinct. The design property then follows from Lemma 21. \( \square \)

The reader is informed that 3-\((q, q/2, q(q - 4)/8)\) designs with the same parameters as those of Corollary 23 were obtained from special APN functions in [21]. According to Magma experiments, the 3-designs in [21] and those in Corollary 23 are not isomorphic. Hence, there are different ways of constructing 3-\((q, q/2, q(q - 4)/8)\) designs, where \( q \) is a power of 2.

Only o-monomials support 3-designs with respect to this construction defined above. O-polynomials do not support 3-designs in general, but do support 2-designs with respect to this construction. Below we prove this general result. To this end, we need prove the next two auxiliary results.

**Lemma 24.** Let \( f(x) \in GF(q)[x] \) be an o-polynomial. For any \( u_1, u_2 \in GF(q) \) with \( u_1 \neq u_2 \), define

\[
I(u_1, u_2) = \{(b, c) \in GF(q)^2 : b \neq 0, \{u_1, u_2\} \subseteq V(f(x) + bx + c)\}.
\]

Then, \( |I(u_1, u_2)| = \frac{q(q-2)}{4} \).
Proof. Set
\[ T = \{(b, c, x_1, x_2) \in \mathbb{GF}(q)^4 : f(x_i) + bx_i + c = u_i \ (i = 1, 2)\}. \]
Then
\[ |T| = \sum_{(b, c) \in \mathbb{GF}(q)^2} J(b, c) = \sum_{(x_1, x_2) \in \mathbb{GF}(q)^2} K(x_1, x_2), \]
where
\[ J(b, c) = |\{(x_1, x_2) \in \mathbb{GF}(q)^2 : f(x_i) + bx_i + c = u_i \ (i = 1, 2)\}|, \]
and
\[ K(x_1, x_2) = |\{(b, c) \in \mathbb{GF}(q)^2 : f(x_i) + bx_i + c = u_i \ (i = 1, 2)\}|. \]
For \( J(b, c) \), we have
\[ J(b, c) = \begin{cases} 
0, & \{u_1, u_2\} \not\subseteq V(g), \\
1, & \{u_1, u_2\} \subseteq V(g) \text{ and } v(g) = q, \\
4, & \{u_1, u_2\} \subseteq V(g) \text{ and } v(g) = q/2,
\end{cases} \]
where \( g = f(x) + bx + c \).

Note that
\[ v(f(x) + bx + c) = \begin{cases} 
q, & b = 0, \\
q/2, & b \neq 0.
\end{cases} \]
We have
\[ |T| = \sum_{(b, c) \in \mathbb{GF}(q)^2} J(b, c) = |\{(b, c) \in \mathbb{GF}(q)^2 : v(f(x) + bx + c) = q\}| + 4|I(u_1, u_2)| = q + 4|I(u_1, u_2)|. \]
For \( K(x_1, x_2) \), we have
\[ K(x_1, x_2) = \begin{cases} 
0, & x_1 = x_2, \\
1, & x_1 \neq x_2.
\end{cases} \]
Thus,
\[ |T| = \sum_{(x_1, x_2) \in \mathbb{GF}(q)^2} K(x_1, x_2) = q(q - 1). \]
Finally,
\[ I(u_1, u_2) = \frac{1}{4} (q(q - 1) - q) = \frac{q(q - 2)}{4}. \]
This completes the proof. \( \square \)

Another major result of this paper is the following.

**Theorem 25.** Let \( f(x) \) be an \( o \)-polynomial over \( \mathbb{GF}(q) \) such that \( |B_{(f, q/2)}| = (q - 1)q \). Then \( D(f, q/2) := (\mathbb{GF}(q), B_{(f, q/2)}) \) is a 2-\((q, q/2, q(q - 2)/4)\) design.

**Proof.** It follows from Theorem 10 that \( |B_{(f, b, c)}| = q/2 \) for all \( (b, c) \in \mathbb{GF}(q)^* \times \mathbb{GF}(q) \). By assumption, all blocks \( B_{(f, b, c)} \) with \( (b, c) \in \mathbb{GF}(q)^* \times \mathbb{GF}(q) \) are pairwise distinct. The design property then follows from Lemma 24. \( \square \)
Regarding Theorem 25, one basic question is which of the known o-polynomials satisfy $|\mathcal{B}(f,q/2)| = q(q-1)/2$. It will be shown later that $|\mathcal{B}(f,q/2)| = 2(q-1)$ for translation o-monomials $x^h$ and their variants $(ax)^h$. For other o-polynomials, we have the following conjecture, which is strongly supported by experimental data.

**Conjecture 1.** Let $f(x)$ be any o-polynomial over $\text{GF}(q)$ such that $f(x) \neq (ax)^h$ for all $a \in \text{GF}(q)^*$ and all $h$ with $1 \leq h < m$ and $\gcd(h,m) = 1$. Then $|\mathcal{B}(f,q/2)| = q(q-1)$.

As pointed out earlier, o-polynomials do not support 3-designs in general with respect to the construction of Section 2. However, if an o-polynomial $g(x)$ can be expressed as $(ux + v)^e + c$, where $x^e$ is an o-monomial, then $g(x)$ does support a 3-design. For example, $q(x) = x^6 + x^4 + x^2 = (x+1)^6 + 1$. Since $x^6$ is an o-monomial over $\text{GF}(2^m)$, where $m$ is odd, $g(x)$ supports a 3-design.

We would make the following comments on 2-designs $\mathcal{D}(f,q/2)$ supported by o-polynomials $f(x)$ such that $f(x) \neq (ax + b)^e + b^e$ for all o-monomials $y^e$.

1. They are not 3-designs in general. For example, when $m = 5$ and $m = 7$, the Cherowitzo o-polynomial, Payne o-polynomial, and Subiaco o-polynomial support only 2-designs.
2. The 2-designs $\mathcal{D}(f,q/2)$ from these o-polynomials are not affine-invariant, as their automorphism groups are smaller than the group $AG_1(\text{GF}(q))$.

   For example, when $m = 5$, the sizes of the automorphism groups of the 2-designs supported by the Cherowitzo o-polynomial, Payne o-polynomial and Subiaco o-polynomial are 160, while $|AG_1(\text{GF}(q))| = 993$.

3. These 2-designs $\mathcal{D}(f,q/2)$ cannot be isomorphic to the hyperoval 2-designs documented in Theorems 6 and 7, as their parameters do not match.

For the 3-designs $\mathcal{D}(f,q/2)$ supported by o-monomials, we have the following remarks.

1. They are not 4-designs according to Magma experiments.
2. They are affine-invariant, i.e., $AG_1(\text{GF}(q))$ is a subgroup of their automorphism groups. Experimental data indicates that their automorphism groups are larger than $AG_1(\text{GF}(q))$.

   For example, when $m = 5$ and $m = 7$, the automorphism groups of the 3-designs supported by the first Glynn o-monomial, second Glynn o-monomial, and the Segre o-monomial have size $q(q-1)m$, while $|AG_1(\text{GF}(q))| = q(q-1)$.

   In these two cases, the automorphism groups of these designs are
   \[ \Gamma A_1(\text{GF}(q)) = \left\{ ux^2 + v : (u,v) \in \text{GF}(q)^* \times \text{GF}(q), \ 0 \leq i \leq m - 1 \right\}. \]

   The degree of transitivity of the group $\Gamma A_1(\text{GF}(q))$ acting on $\text{GF}(q)$ is only 2, and cannot be used to prove the 3-design property of these designs.

   When $m = 5$, the automorphism group of the design supported by the translation o-monomial $x^2$ has size 319979520, while $|AG_1(\text{GF}(q))| = 992$.

   This is a special and degenerated case, and will be treated shortly.

3. They are not symmetric designs, as only trivial symmetric 3-designs exist.

   Only the designs supported by the translation o-monomials $x^h$ are quasi-symmetric. Other 3-designs have many block intersection numbers according to experimental data.

**Open Problem 1.** Find the automorphism groups of the designs $\mathcal{D}(f,q/2)$ supported by the known o-polynomials $f(x)$. 
2.2.4. The parameters of the 3-designs from the translation o-monomial $x^{2^h}$. Let \( \gcd(h, m) = 1 \). Recall that

\[
J_{2^h} = \{y^{2^h} + y : y \in \text{GF}(q)\}.
\]

Obviously, \( J_{2^h} \) is an additive subgroup of \( \text{GF}(q), + \) with order \( q/2 \).

Let \( (u, v) \in \text{GF}(q)^* \times \text{GF}(q) \) with \( uJ_{2^h} + v = J_{2^h} \). Note that \( uJ_{2^h} \) is also an additive subgroup of \( \text{GF}(q), + \) with order \( q/2 \). It then follows that \( J_{2^h} + v \) is also an additive subgroup of order \( q/2 \), which forces \( v \in J_{2^h} \). Consequently,

\[
(uJ_{2^h} = J_{2^h}).
\]

Let \( J_{2^h} = J_{2^h} \setminus \{0\} \). It is known that \( J_{2^h} \) is a Singer difference set with parameters \( (q-1, (q-2)/2, (q-4)/4) \) in the group \( \text{GF}(q)^*, \times \) (see Theorem 27). It then follows from (6) that \( u = 1 \). Consequently,

\[
\text{Stab}_{AG_1(\text{GF}(q))}(J_{2^h}) = \{x + v : v \in J_{2^h}\}
\]

and

\[
\mu = |\text{Stab}_{AG_1(\text{GF}(q))}(J_{2^h})| = q/2.
\]

The following then follows from Theorem 22.

**Corollary 26.** Let \( \gcd(h, m) = 1 \) and \( f(x) = x^{2^h} \). Then the incidence structure \( D(f, q/2) := (\text{GF}(q), B(f, q/2)) \) is a 3-(\( q, q/2, (q-4)/4 \)) design.

Note that the number of blocks in the design of Corollary 26 is \( 2(q-1) \). Therefore, it is not a symmetric design. It is also well known that nontrivial symmetric 3-designs do not exist. The foregoing discussions in this section showed that the 3-(\( q, q/2, (q-4)/4 \)) designs from the translation o-monomials \( x^{2^h} \) is a Hadamard 3-design, that is, the extension of a symmetric Hadamard 2-(\( q-1, q/2 - 1, q/4 - 1 \)) design, and therefore, a quasi-symmetric design with intersection numbers 0 and \( q/4 \) [20]. This is true for every Hadamard 3-(\( q, q/2, (q-4)/4 \)) design, where \( q \equiv 0 \text{ (mod 4)} \) does not have to be a power of 2. Anyway, our construction of the quasi-symmetric 3-designs uses the direct approach \( D(f, q/2) \), and relates the designs to translation hyperovals.

2.2.5. Parameters of the 3-designs from other o-monomials. To determine the \( \lambda \) value of the 3-(\( q, q/2, \lambda \)) design \( D(x^e, q/2) \) from an o-monomial other than the translation o-monomials \( x^{2^h} \), we need determine the size of the stabilizer \( \text{Stab}_{AG_1(\text{GF}(q))}(J_e) \) of \( J_e \), both of which were defined in Theorem 22. Experimental data strongly supports the next conjecture.

**Conjecture 2.** Let \( x^e \) be an o-monomial, where \( e \) is not a power of 2. Then

\[
\text{Stab}_{AG_1(\text{GF}(q))}(J_e) = \{x\}.
\]

Consequently, the design \( D(x^e, q/2) \) has parameters 3-(\( q, q/2, q(q-4)/8 \)).

To settle this conjecture, one may need the following result proved by Maschietti [14].

**Theorem 27.** Let \( e \) be a positive integer with \( \gcd(e(e-1), q-1) = 1 \). Then \( x^e \) is an o-monomial if and only if \( J_e^* = J_e \setminus \{0\} \) is a \( (q-1, (q-2)/2, (q-4)/4) \) difference set in \( \text{GF}(q)^*, \times \).
Below we prove Conjecture 2 for several o-monomials. Let $J_e$ be defined in (5). Define the following Boolean function $h(x)$ from $\text{GF}(q)$ to $\text{GF}(2)$:

$$h(x) = \begin{cases} 1, & \text{if } x \in J_e, \\ 0, & \text{otherwise.} \end{cases}$$

To prove Conjecture 2 for several o-monomials, we need the following lemma [23].

**Lemma 28.** Let $m$ be odd and $e = 2^i + 2^j$ with $1 \leq i < j \leq m - 1$. If $f(x) = x^e$ is an o-polynomial over $\text{GF}(2^m)$, then

$$\hat{h}(\beta) = \begin{dcases} 0, & \text{if } \text{Tr}(\beta^e) = 0, \\ \pm 2^{\frac{m+1}{2}}, & \text{if } \text{Tr}(\beta^e) = 1, \end{dcases}$$

where $\hat{h}$ denotes the Walsh transform of $h$ and

$$\ell \equiv \frac{e-1}{e} \pmod{(2^m-1)}.$$ 

By Lemma 5 or 9, $x^e$ is also an o-monomial over $\text{GF}(q)$. We will make use of this fact shortly below. We now prove the following lemma, which settles Conjecture 2 for several o-monomials over $\text{GF}(q)$.

**Lemma 29.** Let $m$ be odd and $e = 2^i + 2^j$ with $1 \leq i < j \leq m - 1$. Let $(b, c) \in \text{GF}(q)^* \times \text{GF}(q)$. If $f(x) = x^e$ is an o-polynomial over $\text{GF}(q)$, then

$$\text{Stab}_{\text{AG}_1(\text{GF}(q))}(J_e) = \{x\},$$

where $J_e$ was defined in (5).

**Proof.** Let $h(x)$ be defined in (7), which is the characteristic function of the set $J_e$. Let $(b, c) \in \text{GF}(q)^* \times \text{GF}(q)$ such that $h(bx + c) = h(x)$. The desired conclusion is the same as that $(b, c) = (1, 0)$.

Let $A = \sum_{x \in \text{GF}(q)} (-1)^{h(x) + h(bx + c)}$. Since $h(bx + c) = h(x)$, we have $A = q$. We now compute $A$ in a different way. Note that

$$\sum_{\beta \in \text{GF}(q)} (-1)^{\text{Tr}(\beta(x+y))} = \begin{dcases} q & \text{if } x = y, \\ 0 & \text{if } x \neq y. \end{dcases}$$

We have then

$$qA = \sum_{x, y \in \text{GF}(q)} (-1)^{h(x) + h(bx + c)} \sum_{\beta \in \text{GF}(q)} (-1)^{\text{Tr}(\beta(x+y))}$$

$$= \sum_{\beta \in \text{GF}(q)} \sum_{x \in \text{GF}(q)} (-1)^{h(x) + \text{Tr}(\beta x)} \sum_{y \in \text{GF}(q)} (-1)^{h(by + c) + \text{Tr}(\beta y)}$$

$$= \sum_{\beta \in \text{GF}(q)} \hat{h}(\beta) \sum_{y \in \text{GF}(q)} (-1)^{h(by + c) + \text{Tr}(\frac{\beta}{q} + \frac{c}{q})}$$

$$= \sum_{\beta \in \text{GF}(q)} \hat{h}(\beta) \hat{h}(\frac{\beta}{q}) (-1)^{\text{Tr}(\frac{c}{q})}.$$

Since $A = q$, we then deduce that

$$q^2 = \sum_{\beta \in \text{GF}(q)} \hat{h}(\beta) \hat{h}(\frac{\beta}{q}) (-1)^{\text{Tr}(\frac{c}{q})}.$$

Using this equation and Lemma 28, below we prove that $(b, c) = (1, 0)$. 

---

*Advances in Mathematics of Communications, Volume X, No. X (200X), X–XX*
Recall that $x^\ell$ is a permutation of $\GF(q)$, where $\ell$ was defined in (8). Suppose that $b \neq 1$. Then $b^\ell \neq 1$. Consequently, the total number of $\beta$ in $\GF(q)$ such that $\Tr(\beta^\ell) = 1$ and $\Tr((\beta/b)^\ell) = 1$ is $2^{m-2}$. It then follows from Lemma 28 that

$$
\sum_{\beta \in \GF(q)} \hat{h}(\beta) \hat{h}(\beta/b)(-1)^{\Tr(\beta)} = \sum_{\Tr(\beta^\ell) = 1, \Tr((\beta/b)^\ell) = 1} \hat{h}(\beta) \hat{h}(\beta/b)(-1)^{\Tr(\beta)} 
\leq \sum_{\Tr(\beta^\ell) = 1, \Tr((\beta/b)^\ell) = 1} 2^{m+1} 2^{\frac{m+1}{2}} \times 1 
= 2^{m-2} 2^{\frac{m+1}{2}} 2^{\frac{m+1}{2}} 
= 2^{2m-1} 
< q^2,
$$

which is contrary to (9). Consequently, we must have $b = 1$. Since $b = 1$, by Lemma 28 Equation (9) becomes

$$
q^2 = 2^{m+1} \sum_{\Tr(\beta^\ell) = 1} (-1)^{\Tr(c\beta)}.
$$

This equation forces $\Tr(c\beta) = 0$ for all the $2^{m-1}$ nonzero elements $\beta \in \GF(q)$ such that $\Tr(\beta^\ell) = 1$. Note that $\Tr(c \times 0) = 0$. Thus, $\Tr(cx) = 0$ has at least $2^{m-1} + 1$ solutions, which is possible only if $c = 0$. This completes the proof.

The next result follows directly from Theorem 22 and Lemma 29.

**Corollary 30.** Let notation be the same as before. Then the incidence structure $\mathbb{D}(f, q/2) := (\GF(q), \mathcal{B}_{(f,q/2)})$ is a 3-$(q, q/2, q(q - 4)/8)$ design if $f(x) = \Segre(x)$ or $f(x) = \Glynn_2(x)$.

It can be easily proved that $\mathbb{D}(f, q/2)$ is isomorphic to $\mathbb{D}(f^{-1}, q/2)$ if $f$ is an o-monomial over $\GF(q)$. The conclusion of Corollary 30 is also true for the two designs $\mathbb{D}(\Segre^{-1}(x), q/2)$ and $\mathbb{D}(\Glynn_2^{-1}(x), q/2)$. Note that Conjecture 2 is still open for the o-monomials $\Segre(x)$ and $\Glynn_1(x)$.

It is well known that the development of the difference set $J^*_e$ can be extended into a 3-$(q, q/2, (q - 4)/4)$ design. For any o-monomial $x^e$, where $e$ is not a power of 2, the 3-design $\mathbb{D}(x^e, q/2)$ has parameters 3-$(q, q/2, q(q - 4)/8)$. Therefore, our 3-designs $\mathbb{D}(x^e, q/2)$ supported by such o-monomials $x^e$ cannot be isomorphic to the extended 3-design of the development of the difference set $J^*_e$. Recall that the translation o-monomials are exceptions.

2.2.6. The isomorphism of designs $\mathbb{D}(f, q/2)$ from o-polynomials $f$. First of all, we point out that two equivalent o-polynomials $f$ and $g$ may give two non-isomorphic designs $\mathbb{D}(f, q/2)$ and $\mathbb{D}(g, q/2)$. For example, by Lemma 5 the two o-polynomials $x^2$ and $x^{q-2}$ are equivalent, but $\mathbb{D}(x^2, q/2)$ and $\mathbb{D}(x^{q-2}, q/2)$ are not isomorphic, as $\mathbb{D}(x^2, q/2)$ is a 3-$(q, q/2, (q - 4)/4)$ design and $\mathbb{D}(x^{q-2}, q/2)$ is a 3-$(q, q/2, q(q - 4)/8)$ design. By Lemma 5, the two hyperovals $\mathcal{H}(x^2)$ and $\mathcal{H}(x^{q/2})$ are equivalent, while it can be proved that the two designs $\mathbb{D}(x^2, q/2)$ and $\mathbb{D}(x^{q/2}, q/2)$ are isomorphic. Hence, the equivalence of o-polynomials is different from the isomorphism of designs $\mathbb{D}(f, q/2)$ from o-polynomials.

If $f(x) = x^e$ is an o-polynomial, it is easily seen that $\mathbb{D}(f, q/2)$ and $\mathbb{D}(f^{-1}, q/2)$ are isomorphic. But $\mathbb{D}(f, q/2)$ and $\mathbb{D}(f^{-1}, q/2)$ may not be isomorphic if $f$ is not a monomial. For example, $\mathbb{D}(\Cherowitzo(x), q/2)$ and $\mathbb{D}(\Cherowitzo^{-1}(x), q/2)$ are not isomorphic when $m = 5$. 

*Advances in Mathematics of Communications* Volume X, No. X (200X), X–XX
Since it is hard to do a theoretical isomorphy classification of designs $\mathbb{D}(f,q/2)$ from o-polynomials $f$, we have done an isomorphy classification for the following set of o-polynomials for the case $m = 5$ with Magma:
\[
\{ \text{Segre}(x), \text{Segre}(x), \text{Glynn}_1(x), \text{Glynn}_2(x), \text{Cherowitzo}(x), \text{Cherowitzo}^{-1}(x), \text{Payne}(x), \text{Subiaco}(x) \}. 
\]
Their designs $\mathbb{D}(f,q/2)$ for $m = 5$ are pairwise not isomorphic, except that the two designs $\mathbb{D}(\text{Segre}(x),q/2)$ and $\mathbb{D}(\text{Glynn}_1(x),q/2)$ are isomorphic. But $\mathbb{D}(\text{Segre}(x),q/2)$ and $\mathbb{D}(\text{Glynn}_1(x),q/2)$ are not isomorphic when $m = 7$. Hence, the 3-designs of these o-monomials are pairwise not isomorphic in general.

3. AN EXTENDED CONSTRUCTION OF 3-DESIGNS FROM O-POLYNOMIALS

In the construction of designs introduced in Section 2, not every polynomial $f$ supports a 2-design $\mathbb{D}(f,k)$. Only special polynomials over $\text{GF}(q)$ can support a 2-design. In this section, we outline an extended construction of 2-designs from polynomials over finite fields $\text{GF}(q)$.

Let $f(x)$ be a polynomial over $\text{GF}(q)$. For each $(a,b,c) \in \text{GF}(q)^3$, we define
\[
\hat{B}_{(f,a,b,c)} = \{ afx + bx + c : x \in \text{GF}(q) \}.
\]
Let $k$ be any integer with $2 \leq k \leq q$. Define
\[
\hat{B}_{(f,k)} = \{ \hat{B}_{(f,a,b,c)} : |\hat{B}_{(f,a,b,c)}| = k, (a,b,c) \in \text{GF}(q)^3 \}.
\]
We have then the following result.

**Theorem 31.** Let notation be the same as before. If $|\hat{B}_{(f,k)}| > 1$, then the incidence structure $\hat{\mathbb{D}}(f,k) = (\text{GF}(q),\hat{B}_{(f,k)})$ is a $2$-$(q^m,k,\lambda)$ design for some $\lambda$.

**Proof.** The desired conclusion follows from the facts that the general affine group $\text{GA}_1(\text{GF}(q))$ is a subgroup of the automorphism group of the incidence structure $\hat{\mathbb{D}}(f,k)$, $\text{GA}_1(\text{GF}(q))$ fixes $\hat{B}_{(f,k)}$, and $\text{GA}_1(\text{GF}(q))$ acts on $\text{GF}(q)$ doubly transitively.

**Theorem 31** tells us that almost every polynomial over $\text{GF}(q)$ gives 2-designs under this extended construction $\hat{\mathbb{D}}(f,k)$. This fact makes the extended construction $\hat{\mathbb{D}}(f,k)$ less interesting than the previous one $\mathbb{D}(f,k)$, though many 2-designs with nice parameters may be obtained by choosing special types of polynomials. However, it would be very nice if this extended construction $\hat{\mathbb{D}}(f,k)$ can produce $t$-designs with $t \geq 3$.

It is easily seen that for any o-monomial $x^e$ over $\text{GF}(2^m)$, we have $\hat{\mathbb{D}}(x^e,2^m-1) = \mathbb{D}(x^e,2^m-1)$. Hence, it is indeed a 3-design, but was already covered by the construction $\mathbb{D}(x^e,2^m-1)$.

Recall that $\mathbb{D}(f,2^m-1)$ is only a 2-design if $f$ is the Cherowitzo or Payne trinomial. What will happen if we plug the Cherowitzo and Payne trinomials into this extended construction? Regarding this question, we have the following.

**Theorem 32.** Let $m \geq 4$ and $q = 2^m$. Then the incidence structure $\hat{\mathbb{D}}(f,q/2) = (\text{GF}(q),\hat{B}_{(f,q/2)})$ is a $3$-$(q,q/2,(q-4)(q-1)q/8)$ design if $f$ is an o-polynomial over $\text{GF}(q)$ with $|\hat{B}_{(f,q/2)}| = q(q-1)^2$.

**Proof.** Lemmas 20 and 21 can be modified into a proof of the desired result. The details are omitted.
Theorem 32 is valuable only when there is an o-polynomial over GF(q) with $|\hat{B}_{f,k}| = q(q - 1)^2$. In fact, we have the following conjecture.

**Conjecture 3.** Let $m \geq 5$ be odd and $q = 2^m$. Let $f(x)$ be an o-polynomial over GF(q) such that $f(x) \neq (ax+b)^e + b^e$ for all o-monomials $y^e$ and all $(a,b) \in GF(q)^2$. Then $|\hat{B}_{f,q/2}| = q(q - 1)^2$.

It might be hard to settle Conjecture 3 in general. But it is possible to prove the conjecture for the Cherowitzo, Payne and Subiaco o-polynomials. The reader is invited to attack this conjecture.

We inform the reader that Conjecture 3 is true for the Cherowitzo trinomial, Payne trinomial and Subiaco polynomials for $m \in \{5, 7, 9\}$ according to Magma experimental data. Hence, 3-designs have been indeed obtained from this extended construction $\hat{D}(f,q/2)$ with o-polynomials introduced in this section. Recall that $\hat{D}(f,q/2)$ is always a 2-design for any o-polynomial $f$ over GF(q) by Theorem 32, and a 3-design for any o-monomial over GF(q), where $q = 2^m$.

4. **Summary and concluding remarks**

The first contribution of this paper is the two general constructions of $t$-designs with general polynomials over finite fields documented in Sections 2 and 3. The second contribution is the two infinite families of 3-designs from o-polynomials. The first infinite family of 3-designs are from o-monomials over GF($2^m$), and the second infinite family 3-designs are from o-polynomials over GF($2^m$).

Notice that only o-monomials produce 3-designs with the first construction. That is why we focused on designs from o-monomials in Section 2.2. Thus, o-monomials and o-polynomials are very different in the first construction of designs in Section 2. The situation is quite different in the construction of designs in Section 3, as both o-monomials and o-polynomials give 3-designs. The topic of this paper is not easy, as solving Conjectures 1, 2 and 3 would be quite difficult. The reader is cordially invited to settle the three conjectures.

It is very easy to use $GA_1(q)$ to construct 2-designs due to Theorem 1 (see, for example, [6] and [9]). But it is difficult to use $GA_1(q)$ to construct 3-designs, as the transitivity level of the permutation group $GA_1(q)$ is only 2. This is the first time that o-polynomials are used to produce infinite families of 3-designs. It would be nice if o-polynomials could be used to construct an infinite family of 4-designs.

The row vectors of the incidence matrix of a design $\hat{D}$ generate a binary linear code $C_2(\hat{D})$ [22]. Experimental data indicates that the linear codes of most of the designs presented in this paper are interesting. In a future project we will study the parameters and properties of the codes of these designs.

The set of row vectors of the incidence matrix of a design $\hat{D}$ generate a binary linear code $C_2(\hat{D})$ [22]. Experimental data indicates that the linear codes of most of the designs presented in this paper are interesting. In a future project we will study the parameters and properties of the codes of these designs.

The set of row vectors of the incidence matrix of a design with $v$ points is a constant weight binary code of length $v$ [19, 22]. The Hamming distance between two distinct rows is equal to $2v - h$, where the $h$ is the block intersection number of the two blocks corresponding to the two rows in the incidence matrix. The designs presented in this paper give interesting constant weight binary codes according to our Magma experiments. It would be worthy to study the constant weight codes from the designs presented in this paper.

**Acknowledgments**

The authors are grateful to the reviewers for their comments that improved the presentation of this paper.
References

[1] E. F. Assmus, Jr. and J. D. Key, Designs and Their Codes, Cambridge Tracts in Mathematics, 103. Cambridge University Press, Cambridge, 1992.
[2] T. Beth, D. Jungnickel and H. Lenz, Design Theory, Cambridge University Press, Cambridge, 1986, 688 pp.
[3] W. Cherowitzo, Hyperovals in Desarguesian planes of even order, Combinatorics '86 (Trento, 1986), Annals of Discrete Math., North-Holland, Amsterdam, 37 (1988), 87–94.
[4] W. Cherowitzo, Hyperovals in Desarguesian planes: An update, Disc. Math., 155 (1996), 31–38.
[5] W. Cherowitzo, T. Penttila, I. Pinneri and G. F. Royle, Flocks and ovals, Geometriae Dedicata, 60 (1996), 17–37.
[6] C. S. Ding and C. J. Li, Infinite families of 2-designs and 3-designs from linear codes, Discrete Math., 340 (2017), 2415–2431.
[7] C. S. Ding and J. Yuan, A family of skew Hadamard difference sets, J. Combinatorial Theory Ser. A, 113 (2006), 1526–1535.
[8] C. Ding and P. Yuan, Five constructions of permutation polynomials over GF(q^2), unpublished manuscript, (2015). http://arxiv.org/abs/1511.00322.
[9] C. S. Ding and Z. C. Zhou, Parameters of 2-designs from some BCH codes, Codes, Cryptography and Information Security, Lecture Notes in Computer Science, Springer, Cham, 10194 (2017), 110–127.
[10] D. G. Glynn, Two new sequences of ovals in finite Desarguesian planes of even order, Combinatorial Mathematics X, Lecture Notes in Mathematics, Heidelberg, Springer Verlag, 1983 (1983), 217–229.
[11] D. G. Glynn, A condition for the existence of ovals in PG(2,q), q even, Geometriae Dedicata, 32 (1989), 247–252.
[12] W.-A. Jackson, A characterisation of Hadamard designs with SL(2,q) acting transitively, Geom. Dedicata, 46 (1993), 197–206.
[13] R. Lidl and H. Niederreiter, Finite Fields, Second edition, Encyclopedia of Mathematics and its Applications, 20. Cambridge University Press, Cambridge, 1997.
[14] A. Maschietti, Difference set and hyperovals, Des. Codes Cryptg., 14 (1998), 89–98.
[15] S. E. Payne, A new infinite family of generalized quadrangles, Congressus Numerantium, 49 (1985), 115–128.
[16] B. Segre, Sui k-archi nei piani finiti di caratteristica 2, Revue de Math. Pures Appl., 2 (1957), 289–300.
[17] B. Segre, Ovali e curve nei piani di Galois di caratteristica due, Atti Accad. Naz. Lincei Rend., 32 (1962), 785–790.
[18] B. Segre and U. Bartocci, Ovali ed alte curve nei piani di Galois di caratteristica due, Acta Arith., 18 (1971), 423–449.
[19] N. V. Semakov and V. A. Zinov’ev, Balanced codes and tactical configurations, Problemy Peredachi Informatsii, 5 (1969), 22–28.
[20] M. S. Shrikhande, Quasi-symmetric designs, Handbook of Combinatorial Designs, 2nd Edition, CRC Press, New York, (2007), 578–582.
[21] C. M. Tang, Infinite families of 3-designs from APN functions, J. Combinatorial Designs, 28 (2020), 97–117.
[22] V. D. Tonchev Codes and designs, Handbook of coding theory, North-Holland, Amsterdam, 1,2 (1998), 1229–1267.
[23] Q. Xiang, On balanced binary sequences with two-level autocorrelation functions, IEEE Trans. Inf. Theory, 44 (1998), 3153–3156.

Received November 2019; revised February 2020.
E-mail address: cding@ust.hk
E-mail address: tangchunningmath@163.com