Constructing new families of covering arrays using finite geometry and finite fields

Kianoosh Shokri

Thesis submitted to the University of Ottawa
in partial fulfillment of the requirements for the degree of
Doctorate in Philosophy Mathematics and Statistics*

Department of Mathematics and Statistics
Faculty of Science
University of Ottawa

© Kianoosh Shokri, Ottawa, Canada, 2026

*The Ph.D. program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

Covering arrays are well-studied objects in combinatorial design theory. A strength-t *covering array*, denoted by $\mathrm{CA}(N; t, k, v)$, is an $N \times k$ array over an alphabet with v symbols such that in any t-set of columns, each t-tuple over the alphabet occurs in at least one row. Finite fields and finite geometry have been widely employed in the construction of covering arrays. Let q be a prime power. One of the significant geometric objects arising from $\mathrm{PG}(2, q)$ that has been used to construct strength-3 covering arrays is a pair of *orthogoval* projective planes. Two projective (affine) planes with the same point sets are orthogoval if the intersection of any two lines, one from each plane, has size at most two. The existence of such pairs of orthogoval projective planes has been independently proven and published multiple times.

In this thesis, we extend the concept of a pair of orthogoval projective planes to a key property involving Möbius planes in $\mathrm{PG}(3, q)$. We say that m (truncated) Möbius planes are *anti-cocircular* if the common intersection of any choice of m circles, one from each of the planes, has size at most three. We prove the existence of three anti-cocircular truncated Möbius planes for any odd prime power q. This new geometric object has significant properties that enable the construction of strength-4 covering arrays. The covering arrays obtained through this method significantly improve the upper bounds on the size of the best-known arrays. Moreover, these covering arrays have a rich structure, which can be beneficial to their use as ingredients in recursive constructions. Our results suggest the existence of analogous properties in higher-dimensional projective geometries, with potential applications in the construction of higher strength covering arrays.

Another contribution of this thesis involves strength-3 covering arrays. Strength-3 covering arrays obtained from a pair of orthogoval projective planes have a significant property that makes them suitable for recursive constructions. Each such array is obtained by the vertical concatenation of two strength-2 orthogonal arrays that together form a strength-3 covering array. Taking advantage of this structure, we construct new families of strength-3 covering arrays by first horizontally concatenating multiple copies of this strength-3 array. The coverage is then completed by adding key ingredient arrays, which together are used as part of a general recursive construction. In certain cases, the ingredient arrays are carefully selected to introduce systematic redundancy among rows, allowing redundant rows to be removed to optimize the size of the covering arrays. These new families reduce the size of some of the best-known covering arrays. Such improvements were enabled by exploiting the diverse properties inherited from finite fields and finite geometry.

Dedications

To my parents

Acknowledgements

This thesis could not have been completed without the help and support of many people.

First and foremost, I would like to express my sincere gratitude to my supervisor, Professor Lucia Moura. I consider myself truly fortunate to have had the opportunity to work with her. She has inspired me in many ways throughout my Ph.D. Her insight into our research has been remarkable and has shaped the entire course of my doctoral journey. Her patience, steady guidance, and genuine trust in me gave me the confidence to explore beyond my existing knowledge and to deepen my understanding of mathematics. Her approach to leading research, identifying open problems, pushing boundaries, and tackling challenging questions has become an integral part of my own research methodology.

I am also sincerely thankful to Professor Brett Stevens. Without his vital support, this research would not have reached its current level. His suggestion to reconsider my perspective opened a new direction in our work and allowed me to achieve far more than I had initially imagined. Working with Lucia and Brett has been a truly enriching experience. Through our many discussions and meetings, I learned mathematics more deeply than at any other time in my life. I am profoundly grateful to both of them for their unwavering support throughout my academic journey.

I would also like to thank my thesis examiners, Professors Jonathan Jedwab, Michael Newman, Daniel Panario, and Steven Wang for their valuable time and for their thoughtful and constructive feedback.

I would like to express my sincere gratitude to Dr. Amir Asghari for his continuous support and mentorship from the beginning of my undergraduate studies in pure mathematics to the present. I would also like to acknowledge the late Professor Ebad Mahmoodian for his encouragement and his lasting influence on my academic path.

I am grateful to my friends Masoomeh, Aaron, Lord, Khalil, Prangya, Serine, Cesar, Sophie, and Andrew for their support throughout my Ph.D.

I am deeply thankful to my parents, Giti and Ghodrat, and my sister, Aida, for their love, encouragement, and unwavering support, which have continually motivated me to work harder and pursue my goals. My parents have sacrificed more than I could ever deserve, and I dedicate this work to them.

While I was abroad, far from my family, and working on my Ph.D., my beautiful niece Lyanna was born. Every time I saw her sweet face in the many photographs I received, my heart was filled with love, encouragement, and renewed motivation. Thank you, little Lyanna.

Finally, I wish to thank my wife and best friend, Homa. We have walked together through many journeys, and this one could not have been completed without her unwavering love, patience, and support. I am grateful to have you by my side. Thank you, my beloved Homa.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The combination of different areas in mathematics can expand the frontiers of our knowledge and reveal hidden facts beneath the layers of what we already know. The vital key lies in the connections between these areas, which ignites the fundamental path that leads to novel ideas and discoveries.

This thesis investigates connections between combinatorial design theory and finite geometry that are useful for the construction of covering arrays. These connections have been known for some time, and reviewing the literature emphasizes the fact that one is indeed the complement of the other.

The following discussion serves as the motivation for our research. Then, we explain our accomplishments as the outcome of employing different points of views to provide novel solutions to related problems.

An *orthogonal array* $\mathrm{OA}_\lambda(N; t, k, v)$ is an $N \times k$ array over an alphabet of v symbols, such that in every $N \times t$ subarray, each t-tuple on the v symbols occurs exactly λ times. A *covering array* $\mathrm{CA}_\lambda(N; t, k, v)$ is an $N \times k$ array over an alphabet of v symbols, such that in every $N \times t$ subarray, each t-tuple on the v symbols occurs at least λ times. The parameter t is the *strength*. The covering array number denoted by $\mathrm{CAN}_\lambda(t, k, v)$ is the minimum N for which a $\mathrm{CA}_\lambda(N; t, k, v)$ exists.

The following array is an $\mathrm{OA}_2(8; 2, 7, 2)$:

$$M = \begin{array}{|c|c|c|c|c|c|c|}\hline 0&0&1&0&1&1&1\\\hline 0&1&0&1&1&1&0\\\hline 1&0&1&1&1&0&0\\\hline 0&1&1&1&0&0&1\\\hline 1&1&1&0&0&1&0\\\hline 1&1&0&0&1&0&1\\\hline 1&0&0&1&0&1&1\\\hline 0&0&0&0&0&0&0\\\hline\end{array}.$$

We observe that, in the $\mathrm{OA}_2(8; 2, 7, 2)$ M, the first seven rows are circulant, i.e. an array where one row is the cyclic shift of the previous. A row of zeros is then added to complete

the orthogonal array requirement.

The first row of M is obtained using the linear recurrence $a_n = a_{n-2} + a_{n-3}$ with initial values $(a_0, a_1, a_2) = (0, 0, 1)$, and its characteristic polynomial is $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, which is primitive. This is an example of a linear feedback shift register (LFSR) sequence introduced and studied in Chapter 3. Note that the orthogonal arrays constructed by this method are not circulant when $q > 2$, since in this case the period of the sequence is larger than the array length.

There is another method to construct an $\mathrm{OA}_2(8; 2, 7, 2)$. Let $\alpha \in \mathbb{F}_{2^3}$ be a primitive element. Here, we take α as a root of the polynomial given before. Let G_7^1 be the generator matrix where column i is the tuple representation of α^i, $0 \leq i < 7$, as coefficients in the basis $\{\alpha^0, \alpha^1, \alpha^2\}$ of $\mathbb{F}_2^3$. The explicit general construction is given in Construction 3.1.1. The array consisting of each row in the span of G_7^1 is an 8×7 array, which is denoted by $A(G_7^1)$. These arrays are shown next:

$$G_7^1 = \begin{array}{|c|c|c|c|c|c|c|} \hline \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \hline 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline \end{array},$$

$$A(G_7^1) = \begin{array}{|c|c|c|c|c|c|c|} \hline 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ \hline 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ \hline 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline \end{array}.$$

One important property of the columns of G_7^1 is that no two columns are multiples of each other, consequently, the array $A(G_7^1)$ is an $\mathrm{OA}_2(8; 2, 7, 2)$. Moreover, in Theorem 3.1.3, we generalize the above result, that $A(G_7^1)$ is identical to M up to row permutation over the field $\mathbb{F}_2$, to the field $\mathbb{F}_q$.

If we label the columns of M by the exponents of α in G_7^1, the set of column indices that have zeros in each row, except the all-zero row, corresponds to each block of a 2-$(7, 3, 1)$ design, as shown in Table 1.1.

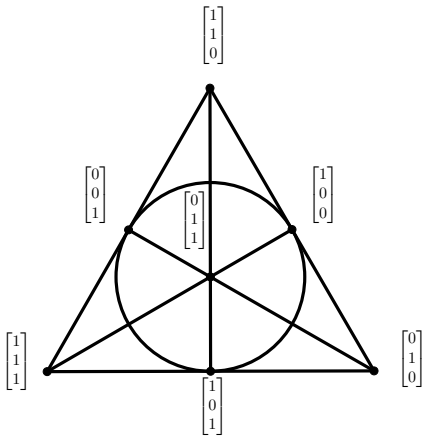
Another fascinating fact is the connection between the matrix G_7^1 and the projective plane $\mathrm{PG}(2, 2)$, or the Fano plane. For q a prime power, an important class of projective planes, $\mathrm{PG}(2, q)$, has as its points the 1-dimensional subspaces of $\mathbb{F}_q^3$ and as its lines the 2-dimensional subspaces of $\mathbb{F}_q^3$. Hence, any three points are collinear if and only if one is equal to a linear combination of the other two. The columns of G_7^1 correspond to the points of the Fano plane, as shown in Fig. 1.1.

A block $S = \{i, j, k\}$ of the 2-$(7, 3, 1)$ design in Table 1.1 corresponds to three collinear points $\alpha^i, \alpha^j, \alpha^k$ in the Fano plane. Let M_S be a 3×3 submatrix of G_7^1 corresponding to

Table 1.1: Positions of zeros in each non-zero row correspond to blocks of a 2-$(7, 3, 1)$ design.

0	1	2	3	4	5	6	Blocks of 2-$(7, 3, 1)$ design
0	0	1	0	1	1	1	$\{0, 1, 3\}$
0	1	0	1	1	1	0	$\{0, 2, 6\}$
1	0	1	1	1	0	0	$\{1, 5, 6\}$
0	1	1	1	0	0	1	$\{0, 4, 5\}$
1	1	1	0	0	1	0	$\{3, 4, 6\}$
1	1	0	0	1	0	1	$\{2, 3, 5\}$
1	0	0	1	0	1	1	$\{1, 2, 4\}$
0	0	0	0	0	0	0	

Figure 1.1: Columns of G_1^7 corresponding to the points of the Fano plane.



columns with labels in the set $S = \{i, j, k\}$, where $0 \leq i < j < k \leq 6$. The set S is a block of the 2-$(7, 3, 1)$ design if and only if $\text{rank}(M_S) = 2$. This follows from the existence of a row with zeros in the columns of M_S in $A(G_7^1)$. Geometrically, the points corresponding to labels from S are collinear. If S is not a block of the 2-$(7, 3, 1)$ design, then $\text{rank}(M_S) = 3$, and the corresponding points in the Fano plane are not collinear. When $\text{rank}(M_S) = 3$, all distinct triples occur as a row of $A(G_1^7)$ for column indices in S. In M, there are exactly seven 3-sets of columns (corresponding to the blocks of the 2-$(7, 3, 1)$ design), where not all distinct 2^3 3-tuples are covered. This shows that M is a strength-2 orthogonal array very close to being a strength-3 orthogonal array, since 28 out of the 35 3-sets of columns have the required coverage.

Munemasa [39] showed the existence of an orthogonal array $\text{OA}_{2^{m-2}}(2^m; 2, n, 2)$ for $m \leq n \leq 2m + 1$, where m is a positive integer, that is close to being an $\text{OA}_{2^{m-3}}(2^m; 3, n, 2)$.

A general method to construct an $\text{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$, where q is a prime power, is described in Section 3.1. The orthogonal array $\text{OA}_q(q^3; 2, q^2 + q + 1, q)$ is very close to being a strength-3 orthogonal array since only $\frac{q-1}{q^2+q-1}$ of the 3-sets of columns are not covered. This suggests using more than one $\text{OA}_q(q^3; 2, q^2 + q + 1, q)$, vertically concatenated, to construct

a strength-3 covering array.

Raaphorst, Moura, and Stevens [48] constructed a CA$(2q^3 - 1; 3, q^2 + q + 1, q)$, which we denote by R_q, where q is a prime power. Since its publication in 2014, the array R_q gives the best upper bound on CAN$(3, q^2 + q + 1, q)$ for $q \geq 4$ [15]. Another advantage of R_q is that it is fast to generate and requires low storage capacity since only a primitive polynomial of degree 3 is sufficient to generate the array. We illustrate their method with an example in $\mathbb{F}_2$. Let $f(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ be the same primitive polynomial with root $\alpha \in \mathbb{F}_{2^3}$ used before.

Let G_7^{-1} be a new generator matrix constructed using α^{-1} in place of α in the construction of G_7^1:

$$G_7^{-1} = \begin{array}{|c|c|c|c|c|c|c|} \hline \alpha^0 & \alpha^{-1} & \alpha^{-2} & \alpha^{-3} & \alpha^{-4} & \alpha^{-5} & \alpha^{-6} \\ \hline 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ \hline 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ \hline \end{array}.$$

Note that $f_r(x) = x^3 f(\frac{1}{x})$ is the reciprocal of f, which is a primitive polynomial. By definition of f_r, α^{-1} is a root.

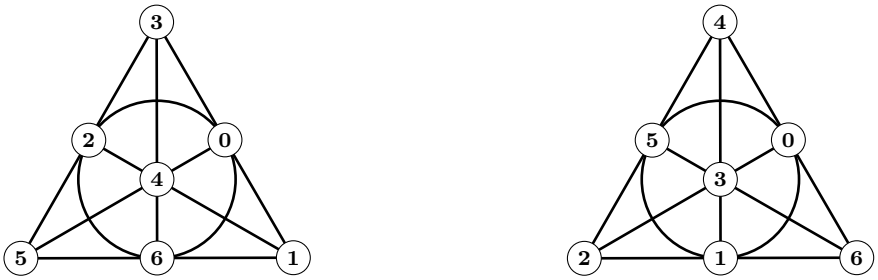
Each generator matrix, G_7^1 and G_7^{-1}corresponds to a row of a covering perfect hash family CPHF$(2; 7, 2, 3)$ (see Definition 3.2.3). The array obtained by the vertical concatenation of $A(G_7^1)$ and $A(G_7^{-1})$, with one copy of the zero row removed, is a CA$(15; 3, 7, 2)$, shown in Fig. 1.2.

Figure 1.2: The CA$(15; 3, 7, 2)$ R_2 obtained by the vertical concatenation of $A(G_7^1)$ and $A(G_7^{-1})$ with one copy of the zero row removed.

0	0	0	0	0	0	0
0	0	1	0	1	1	1
0	1	0	1	1	1	0
0	1	1	1	0	0	1
1	0	0	1	0	1	1
1	0	1	1	1	0	0
1	1	0	0	1	0	1
1	1	1	0	0	1	0
0	1	1	1	0	1	0
0	0	1	1	1	0	1
0	1	0	0	1	1	1
1	1	1	0	1	0	0
1	0	0	1	1	1	0
1	1	0	1	0	0	1
1	0	1	0	0	1	1

The geometric interpretation underlying this construction is quite interesting. The columns of G_7^1 and G_7^{-1} correspond to two projective planes on the same point set such that the

Figure 1.3: A pair of orthogoval PG(2, 2), left: corresponding to G_7^1, right: corresponding to G_7^{-1}.



intersection of any two lines, one from each, has size at most two. A pair of projective (affine) planes on the same point set with this property is called *orthogoval* [17].

Table 1.2: A pair of orthogoval PG(2, 2) corresponding to G_7^1 and G_7^{-1}.

Lines of PG(2, 2) corresponding to G_7^1	Lines of PG(2, 2) corresponding to G_7^{-1}
$\{0, 1, 3\}$	$\{0, 4, 6\}$
$\{0, 2, 6\}$	$\{0, 1, 5\}$
$\{1, 5, 6\}$	$\{0, 2, 3\}$
$\{0, 4, 5\}$	$\{3, 5, 6\}$
$\{3, 4, 6\}$	$\{1, 2, 6\}$
$\{2, 3, 5\}$	$\{2, 4, 5\}$
$\{1, 2, 4\}$	$\{1, 3, 4\}$

The existence of orthogoval projective planes has been widely studied and proved independently several times in [6, 25, 28, 34, 48, 65], and non-independent novel proofs have been published in [2, 17, 45]. The existence of a pair of orthogoval affine planes is proved in [17],

A pair of orthogoval projective planes can be used to construct a strength-3 covering array $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ [48], which is a generalization of the example in Fig. 1.2.

We have given an illustration of the broader picture that forms the foundational framework of our research. Next, we present the thesis contributions and outline our major results.

1.1 Thesis contributions

In this thesis, we explore fascinating properties of the 3-dimensional projective geometry $\mathrm{PG}(3, q)$. Our work extends the concept of a pair of orthogoval projective planes, which has been studied extensively over the past decades.

By combining ideas and techniques from finite geometry, finite fields, and design theory, we present constructive methods that substantially reduce the size of the best-known covering

arrays for certain parameters.

1.1.1 Major contributions

We outline the major results and accomplishments of this thesis, which can be found in Chapter 4 and Chapter 5.

1. In Chapter 4, we extend the definition of orthogoval projective planes to a higher-dimensional projective geometry $\mathrm{PG}(3, q)$. We study the plane sections of an ovoid in $\mathrm{PG}(3, q)$ which give a Möbius plane (see Definition 2.3.9). We then construct three truncated Möbius planes for any odd prime power q, on the same point set, with the property that the common intersection of any choice of three blocks, one from each plane, has size at most three. As a direct result, this construction yields a strength-4 covering array $\mathrm{CA}(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ for any odd prime power q, by vertically concatenating three strength-3 covering arrays, where each corresponds to one of the truncated Möbius planes. This construction significantly improves the best-known upper bounds on $\mathrm{CAN}(4, \frac{q^2+1}{2}, q)$ by almost 25% as q grows. We also employ properties of finite geometry in a recursive construction and obtain larger strength-4 covering arrays $\mathrm{CA}(5q^4 - 4q^3 - q^2 + 2q; 4, q^2 + 1, q)$ for any odd prime power q. The results of this chapter have been included in a paper and submitted to arXiv [56].

2. In Chapter 5, we use the $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ R_q as the main ingredient in a recursive method to construct new families of strength-3 covering arrays. The main idea is to horizontally concatenate several copies of R_q and complete the missing coverage by adding extra rows from carefully chosen ingredient arrays. By exploiting the properties of R_q and various other key ingredients, such as difference covering arrays, we obtain strength-3 covering arrays for larger number of columns. We construct several new families of covering arrays that improve the upper bounds of the best-known arrays with the same parameters. To build new families, we employ x copies of R_q, where $x \in \{2, q, q + 1, q^2, q^2 - q + 1\}$ and obtain

   - $\mathrm{CA}(4q^3 - 5q^2 + 2q; 3, 2(q^2 + q + 1), q)$ for every prime power q,
   - $\mathrm{CA}(5q^3 - 6q^2 + 2q; 3, q(q^2 + q + 1), q)$ for every prime power q,
   - $\mathrm{CA}(6q^3 - \frac{13}{2}q^2 + \frac{5}{2}q - 1; 3, (q + 1)(q^2 + q + 1), q)$ for every odd prime power q.
   - $\mathrm{CA}(8q^3 - 10q^2 + 4q - 1; 3, q^2(q^2 + q + 1), q)$ for every prime power q,
   - $\mathrm{CA}(8q^3 - 10q^2 + 3q; 3, q^2(q^2 + q + 1), q)$ for every even prime power q,
   - $\mathrm{CA}(8q^3 - 10q^2 + 3q; 3, (q^2 - q + 1)(q^2 + q + 1), q)$ for every prime power q.

   The key property that is exploited to reduce the number of rows in these new families of strength-3 covering arrays comes from the fascinating structure of R_q. The array R_q is obtained by vertically concatenating two strength-2 orthogonal arrays, resulting in a strength-3 covering array. This provides patterns and connections among the other ingredients, which enable us to identify redundancy in the coverage, allowing the

removal of corresponding rows and resulting in improved upper bounds for the size of the best-known arrays. A generalization of this idea is provided in Theorem 5.2.6, which gives a new recursive framework to construct strength-3 covering arrays. It employs covering perfect hash families of strength 3, in which each row corresponds to a covering perfect hash family of strength 2, and incorporates additional key ingredients to complete the missing coverage. The results of this chapter are published in the *Journal of Combinatorial Designs* [55].

1.2 Thesis structure

In Chapter 2, we outline the necessary mathematical background used throughout this thesis. In Section 2.1, covering arrays and their key aspects are reviewed. In Section 2.2, we provide an overview of the algebraic concepts leading to the construction of finite fields and study linear feedback shift register sequences. In Section 2.3, finite geometry and several geometric structures, such as ovoids, Möbius planes, and hypersurfaces, are examined.

In Chapter 3, we review key results used in this thesis. We study strength-2 orthogonal arrays derived from LFSR sequences and projective geometry. We then employ these arrays to construct the array R_q. In Section 3.1, two methods for constructing an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$ are presented, and the resulting arrays are shown to be identical up to row permutations. In Section 3.2, we study the construction of $\mathrm{CA}(2q^3-1; 3, q^2+q+1, q)$ and its relationship to covering perfect hash families. Finally, in Section 3.3, we overview results about orthogoval projective (affine) planes and examine their connection to $\mathrm{CA}(2q^3-1; 3, q^2+q+1, q)$ and other covering arrays.

Chapter 4 presents the main contribution of this thesis, extending the concept of orthogoval projective planes to a higher dimensional projective space $\mathrm{PG}(3, q)$. In Section 4.2, we study the circles of Möbius planes and give several properties of them. Then, we prove the existence of a set of 3 anti-cocircular truncated Möbius planes for any odd prime power q. In Section 4.3 and Section 4.4, we construct strength-4 covering arrays $\mathrm{CA}(3q^4-2; 4, \frac{q^2+1}{2}, q)$, and $\mathrm{CA}(3q^4+(q-2)(2q^3-q); 4, q^2+1, q)$ for any odd prime power q. These arrays improve the size of the best-known arrays (see Table 4.6, Table 4.8).

In Chapter 5, we give a general recursive construction for strength-3 covering arrays. The main ingredient is a covering perfect hash family of strength 3, in which each row forms a covering perfect hash family of strength 2. The array R_q is extensively used to obtain new families of strength-3 covering arrays. In Section 5.1, we review auxiliary arrays such as orthogonal arrays using Bush's construction, partition covering arrays, and difference covering arrays. These arrays serve as key ingredients in the general construction described in Theorem 5.2.6. New families of strength-3 covering arrays are presented in Section 5.2. In Section 5.3, we demonstrate improvements in the size of several best-known arrays (see Table 5.6).

In Chapter 6, we give a conclusion and discuss future directions.

Chapter 2

Preliminaries

This chapter provides the necessary background for the material used throughout this thesis. Covering arrays, finite fields, and finite geometry constitute the mathematical basis of this work. In Section 2.1, we present a general introduction to covering arrays and examine some of their key aspects. In Section 2.2, we review essential concepts of finite fields and LFSR sequences. In Section 2.3, we study finite projective spaces, in particular $\mathrm{PG}(2, q)$ and $\mathrm{PG}(3, q)$.

2.1 Covering arrays

Covering arrays are well studied objects in combinatorial design theory [12, 62] that are used in applications to software testing [43]. Colbourn [12] and Torres-Jimenez et al. [62] provided general surveys about covering arrays, where bounds, constructions, and applications of covering arrays are discussed.

Definition 2.1.1. An *orthogonal array*, denoted by $\mathrm{OA}_\lambda(N; t, k, v)$, is an $N \times k$ array over an alphabet with v symbols, with the property that for any $N \times t$ subarray, each t-tuple over the alphabet occurs exactly $\lambda = \frac{N}{v^t}$ times as a row. Here, λ is the *index*, and t is the *strength* of the orthogonal array. If $\lambda = 1$, we remove λ from the notation and denote it by $\mathrm{OA}(N; t, k, v)$.

In an array over an alphabet of v symbols, a t-set of column indices $\{c_1, \ldots, c_t\}$ is λ-*covered* if each t-tuple over the alphabet occurs at least λ times as a row of the sub-array indexed by $c_1, \ldots, c_t$.

Definition 2.1.2. A *covering array*, denoted by $\mathrm{CA}_\lambda(N; t, k, v)$, is an $N \times k$ array over an alphabet with v symbols, with the property that any t-set of columns is λ-covered. Here, N is the *size*, and t is the *strength* of the covering array. If $\lambda = 1$, we remove λ from the notation and denote it by $\mathrm{CA}(N; t, k, v)$. The covering array number, denoted by $\mathrm{CAN}(t, k, v)$, is the minimum N for which a $\mathrm{CA}(N; t, k, v)$ exists.

Determining bounds on $\mathrm{CAN}(t, k, v)$ is widely studied [12, 13, 62]. Best-known upper bounds for $\mathrm{CAN}(t, k, v)$ for $2 \leq t \leq 6$, $1 \leq k \leq 10000$, and $2 \leq v \leq 25$ are provided in the covering array tables maintained by Colbourn [15].

Example 2.1.3. This example shows a $\mathrm{CA}(5; 2, 4, 2)$. By picking any two columns, each 2-tuple $(0, 0)$, $(1, 1)$, $(0, 1)$, and $(1, 0)$ occurs at least once as a row.

0	0	0	1
1	1	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Two major approaches to constructing covering arrays are: (1) algebraic and combinatorial methods, including those based on finite fields and recursive constructions; and (2) algorithmic methods for generating covering arrays, such as greedy, metaheuristic, and exhaustive approaches. Different methods in these two categories are surveyed in [12, 62].

Next, we review known upper and lower bounds for a strength-t covering array with k columns and v symbols. An obvious lower bound is $v^t \leq \mathrm{CAN}(t, k, v)$. Three general lower bounds are developed by Stevens, Moura, and Mendelsohn [58].

Gargano, Körner, and Vaccaro [24] show that for fixed $v \geq 2$, $\mathrm{CAN}(2, k, v) = \frac{v}{2} \log(k)(1 + o(1))$. In [1, 40, 41], it is established that $\mathrm{CAN}(t, k, 2) \leq 2^t t^{O(\log t)} \log(k)$.

Godbole, Skipper, and Sunley [26] examine a random process to construct a covering array, and show that such a random array exists with nonzero probability for sufficiently large N depending on t, k, and v. By using the probabilistic method, they obtain the following upper bound, for fixed $v, t \geq 2$:

$$\mathrm{CAN}(t, k, v) \leq \frac{(t-1)}{\log(\frac{v^t}{v^t-1})} \log(k)(1 + o(1)).$$

Francetić and Stevens [23], give improvements on this bound. Bryce and Colbourn [7] give an algorithm based on the method of conditional expectations, that runs in polynomial time for fixed t and v, which yields a $\mathrm{CA}(N; t, k, v)$ with $N = O(\log(k))$.

A major application of covering arrays is to generate software test suites to cover all t-way interactions between k factors, where each factor has v possible values. The number of tests required to exhaustively detect all faults in such a system is equal to v^k. However, strength-t covering arrays reduce the number of tests dramatically by testing all possible v^t combinations of values for every t-set of factors using $O(\log k)$ tests for fixed v and t. Table 2.1, adapted from [12], illustrates a system with four factors, each having two values. In this case, $2^4 = 16$ tests are required for exhaustive testing, whereas testing pairwise interactions of factors using a $\mathrm{CA}(5; 2, 4, 2)$ reduces this number to just five tests.

Experimentally, Raunak et al. [52] observed that the number of detected faults in different systems increases as the strength of covering arrays grows from 1 to 6. As shown in Fig. 2.1,

Table 2.1: Testing a system with $k = 4$ factors each having $v = 2$ values.

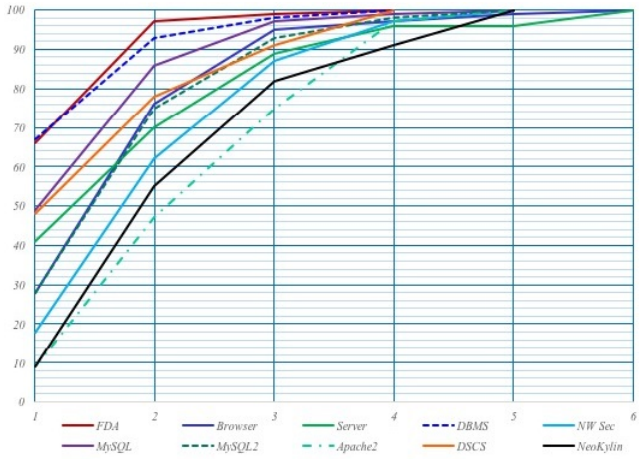
	Factors			
	Web Browser	OS	Connection Type	Printer Config
Config:	Firefox(0) Chrome(1)	Windows(0) Mac(1)	LAN(0) PPP(1)	Local(0) Networked(1)

Table 2.2: Using the CA$(5; 2, 4, 2)$ given in Example 2.1.3 for pairwise interaction.

Test case	Web Browser	OS	Connection Type	Printer Config
1	Firefox	Windows	LAN	Networked
2	Chrome	Mac	LAN	Local
3	Firefox	Mac	PPP	Local
4	Chrome	Windows	PPP	Local
5	Chrome	Mac	PPP	Networked

the number of detected faults for a fixed strength varies across systems under testing. Using strength-2 covering arrays, between 45% and 97% of faults can be detected depending on the system. This percentage increases with higher strength, and covering arrays of strength 6 detect around 98% of the faults in the systems studied (see Fig. 2.1, adapted from [52]). This is evidence that most faults arise from the interaction of up to six factors even though the number of factors may be very large. For more information about combinatorial testing, see [43]. Hardware testing, advanced materials testing, and the study of interactions regulating gene expression are other applications of covering arrays [12].

Figure 2.1: Proportion of faults by using covering arrays of strength $t = 1, \ldots, 6$, for various systems studied in [52].



2.2 Finite fields

In this section, we give a concise overview of algebraic structures leading to the definition of finite fields. In Section 2.2.1, we study LFSR sequences and some of their properties. For further details on finite fields, see [35]. Here, we follow [3].

Definition 2.2.1. A *group* $(G, \circ)$ is a set together with a binary operation $G \times G \to G$ that assigns to each pair $(a, b) \in G \times G$ a unique element $a \circ b \in G$ that satisfies the following axioms:

1. The binary operation is *associative*. That is for $a, b, c \in G$, $(a \circ b) \circ c = a \circ (b \circ c)$.
2. There exists an element $e \in G$ such that for any element $a \in G$, $e \circ a = a \circ e = a$. The element e is the *identity element*.
3. For each element $a \in G$, there exist an *inverse element* in G, denoted by a^{-1}, such that $a \circ a^{-1} = e$.

A group $(G, \circ)$ is *commutative* if for any $a, b \in G$, $a \circ b = b \circ a$. Groups not satisfying this property are said to be *noncommutative*.

Let n be a positive integer. If a is an element of a group G, we denote $a \circ a \circ \cdots \circ a$ for n factors a by a^n. We let a^0 be the identity element, and denote $a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}$ for n factors by a^{-n}.

Definition 2.2.2. If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a subgroup of G.

Theorem 2.2.3 ([42])**.** Let G be a group and a be any element in G. Then the set $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ is a subgroup of G. Furthermore, $\langle a \rangle$ is the smallest subgroup of G that contains a.

For $a \in G$, we call $\langle a \rangle$ the cyclic subgroup generated by a. If G contains some element a such that $G = \langle a \rangle$, then G is a cyclic group. In this case, a is a generator of G. If a is an element of a group G, we define the order of a to be the smallest positive integer n such that $a^n = e$, and we write $ord(a) = n$. If there is no such integer n, we say that the order of a is infinite and write $ord(a) = \infty$ to denote the order of a.

Definition 2.2.4 ([22])**.** Let X be a set and $(G, \circ)$ a group.

1. An *action of G on X* is a map $* : G \times X \longrightarrow X$ such that
   - $e * x = x$ for all $x \in X$,
   - $(g_1 \circ g_2) * (x) = g_1 * (g_2 * x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

   Under these conditions, X is a *G-set*.

2. A group G acts *faithfully* on X if $g * x = x$ for all $x \in X$ implies that $g = e$.

3. A group G is *transitive* on a G-set X if for each $x_1, x_2 \in X$, there exists $g \in G$ such that $g * x_1 = x_2$.

4. The orbit of any $x \in X$ is $Gx = \{g * x : g \in G\}$.

A group G acts *regularly* on X if it acts faithfully and is transitive on X. It is easy to see that if G acts regularly on X, then for any $x_1, x_2 \in X$, there exist a unique $g \in G$ such that $g * x_1 = x_2$.

Definition 2.2.5. A *commutative ring* R is a set with two binary operations, addition and multiplication, such that it is a commutative group with respect to addition with identity element 0, and the multiplication is commutative, associative and distributive ($a(b + c) = ab + ac$) and has an identity element 1. An *ideal* I of a ring R is an additive subgroup with the property that $ra \in I$ for all $r \in R$ and $a \in I$.

A *coset* of I is a set $r + I = \{r + a \mid a \in I\}$, where $r \in R$. The set of cosets, denoted R/I forms a ring called the *quotient ring*, where addition and multiplication are defined by $r + I + s + I = r + s + I$, $(r + I)(s + I) = rs + I$, respectively. An ideal of R is *maximal* if it is not contained in a larger ideal other than R.

Definition 2.2.6. A *field* is a commutative ring in which every non-zero element has a multiplicative inverse. In other words, for all $a \neq 0$, there is a a^{-1} such that $aa^{-1} = 1$. For example, $\mathbb{F}_p = \mathbb{Z}_p$ for any prime number p is a field with modular arithmetic.

Theorem 2.2.7 ([42])**.** An ideal I is maximal if and only if R/I is a field.

Let R be a commutative ring and let $R[x]$ be the set of all polynomials in x with coefficients in R. Then $R[x]$ is a commutative ring with usual addition and multiplication of polynomials.

An *irreducible* polynomial f over a field F is a non-constant polynomial that cannot be expressed as a product of two polynomials g and h over F, where the degrees of g and h are both smaller than the degree of f.

Let f be an irreducible polynomial with degree m over a field $\mathbb{F}_p$ for a prime number p. Let $\langle f \rangle = \{kf : k \in \mathbb{Z}\}$ be the cyclic subgroup of $\mathbb{F}_p[x]$ with respect to addition. Then $\langle f \rangle$ is a maximal ideal of $\mathbb{F}_p[x]$, and by Theorem 2.2.7, $\mathbb{F}_p[x]/\langle f \rangle$ is a field , which has p^m elements.

Theorem 2.2.8. The unique field with $q = p^m$ elements is isomorphic to $\mathbb{F}_p[x]/\langle f \rangle$, where f is an irreducible polynomial of $\mathbb{F}_p[x]$ of degree m.

Theorem 2.2.9. If $\mathbb{F}$ is a finite field with q elements then $a^q = a$, for all $a \in \mathbb{F}$.

The *characteristic* $char(\mathbb{F})$ of a field $\mathbb{F}$ is the smallest integer n such that $1 + \cdots + 1 = 0$, where the sum has n terms. If no such n exists then we define $char(\mathbb{F})$ to be zero.

Theorem 2.2.10. If $char(\mathbb{F}) \neq 0$ then $char(\mathbb{F}) = p$ for some prime p.

Theorem 2.2.11. A field $\mathbb{F}$ with q elements has characteristic p for some prime p and $q = p^m$ for some positive integer m.

Theorem 2.2.12 ([3])**.** The nonzero elements of $\mathbb{F}_q$, denoted by $\mathbb{F}_q^*$, form a multiplicative cyclic group.

Definition 2.2.13. An element $\alpha \in \mathbb{F}_q$ is *primitive* if α generates the multiplicative group $\mathbb{F}_q^*$ of nonzero elements in $\mathbb{F}_q$.

Remark 2.2.14. Let α be a primitive element in $\mathbb{F}_{q^m}$. Then $\alpha^{\frac{q^m-1}{q-1}}$ is a primitive element in $\mathbb{F}_q$.

Definition 2.2.15. A polynomial $f \in \mathbb{F}_p[x]$ of degree m is *primitive* if f is monic, and has a root $\alpha \in \mathbb{F}_{p^m}$ that is primitive. Equivalently, a monic irreducible polynomial f of degree m is a primitive polynomial if $k = q^m - 1$ is the smallest positive integer such that $x^k - 1$ is divisible by f.

Definition 2.2.16. The *reciprocal* f_r of a polynomial f of degree m is defined by $f_r(x) = x^m f(\frac{1}{x})$.

Remark 2.2.17. The reciprocal polynomial of an irreducible polynomial f , $f(x) \neq x$, over $\mathbb{F}_q$ is again irreducible over $\mathbb{F}_q$. In addition, the *monic* reciprocal polynomial defined by $f(x)/f(0)$, where $f(x)$ is a primitive polynomial, is also primitive.

Next, we define trace function, which is widely used throughout the thesis.

Definition 2.2.18. The *trace function* is defined as follows:

$$\begin{gathered}\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q, \\ \mathrm{Tr}(a) = a + a^q + a^{q^2} + \cdots + a^{q^{m-1}}.\end{gathered}$$

The trace function is $\mathbb{F}_q$-linear which means that for all $s, t \in \mathbb{F}_q$ and all $a, b \in \mathbb{F}_{q^m}$, $\mathrm{Tr}(sa + tb) = s\,\mathrm{Tr}(a) + t\,\mathrm{Tr}(b)$.

2.2.1 Linear feedback shift register sequences

Definition 2.2.19. Let $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_1 x + c_0 \in \mathbb{F}_q[x]$ be a polynomial of degree m. A *linear feedback shift register* (LFSR) sequence with characteristic polynomial f and initial values $T = (a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_q^m$ is a sequence $S(f, T) = (a_0, a_1, \ldots)$ over $\mathbb{F}_q$ defined as

$$a_i = \begin{cases} a_i, & 0 \leq i < m, \\ -c_{m-1}a_{i-1} - \cdots - c_0 a_{i-m}, & i \geq m. \end{cases}$$

A sequence $(a_0, a_1, \ldots)$ is periodic if there exists a positive integer n such that $a_{n+i} = a_i$ for all $i \geq 0$. The smallest such n, if one exists, is the period of the sequence. The period of an LFSR sequence with a characteristic polynomial of degree m over $\mathbb{F}_q$ divides $q^m - 1$. The LFSR sequence is an *M-sequence* (maximum period sequence) if the period is $q^m - 1$. The LFSR sequence $S(f, T)$ is an M-sequence if and only if f is primitive [27].

Example 2.2.20. Let $f(x) = x^3 + 2x^2 + x + 1 \in \mathbb{F}_3[x]$ and consider the characteristic polynomial of the LFSR sequence whose recurrence relation is $a_n = 2a_{n-3} + 2a_{n-2} + a_{n-1}$, with initial values $(0, 1, 2)$. Since f is primitive, then the LFSR sequence is an M-sequence with period 26 as given next:

$$01211120011010212221002202.$$

We list some important properties of LFSR sequences.

Theorem 2.2.21 ([27, Theorem 4.11])**.** Let f be a degree-m primitive polynomial over $\mathbb{F}_q$ with root α. Then, for any initial values $T = (a_0, \ldots, a_{m-1})$, there exists a unique element $\beta \in \mathbb{F}_{q^m}$ such that $a_i = \mathrm{Tr}(\beta\alpha^i)$ for all $0 \leq i \leq m - 1$. Furthermore, since the trace is $\mathbb{F}_q$-linear, it follows that the LFSR $S(f, T) = (a_i)$ has the property that for all $i \geq 0$, $a_i = \mathrm{Tr}(\beta\alpha^i)$.

Theorem 2.2.22 ([27, Corollary 4.6])**.** Let a be a sequence over $\mathbb{F}_q$. Then a is an M-sequence (i.e. an LFSR sequence with period $q^m - 1$) if and only if the elements of a can be represented by $a_i = \mathrm{Tr}(\beta\alpha^i)$ for all $i \geq 0$, where α is a primitive element in $\mathbb{F}_{q^m}$ and $0 \neq \beta \in \mathbb{F}_{q^m}$.

If f is primitive, then by Theorem 2.2.21 and Theorem 2.2.22, $S(f, T)$ has period $q^m - 1$.

Let $a = (a_i)$ be a sequence over $\mathbb{F}_q$ of period $q^m - 1$, and let $k = \frac{q^m-1}{q-1}$. For $v, w \in \mathbb{F}_q$ and $0 \leq d < q^m - 1$, define:

$$N_{v,w}(d) = |\{i : (a_i, a_{i+d}) = (v, w), 0 \leq i < q^m - 1\}|.$$

Then a has the 2-tuple balance property if a satisfies the following conditions:

1. If $d \not\equiv 0 \pmod{k}$, then for all $(v, w) \neq (0, 0)$, $N_{v,w}(d) = q^{m-2}$, and $N_{0,0}(d) = q^{m-2} - 1$.
2. If $d \equiv 0 \pmod{k}$, then there exists some $\lambda \in \mathbb{F}_q$ ($\lambda = 1$ if and only if $d = 0$) such that $(a_i, a_{i+d}) = (a_i, \lambda a_i)$ for all $0 \leq i < q^m - 1$, and additionally, for $v \neq 0$, $N_{v,\lambda v}(d) = q^{m-1}$, and $N_{0,0}(d) = q^{m-1} - 1$. For $w \neq \lambda v$, $N_{v,w}(d) = 0$.

Theorem 2.2.23 ([27])**.** Let $m \geq 2$. If f is a degree-m primitive polynomial over $\mathbb{F}_q$, then the LFSR sequence defined by f for any initial values $T \neq (0, \ldots, 0)$ has the 2-tuple balance property.

Let $S(f, T) = (a_i)$ be an LFSR sequence. Then, for a positive integer n, $C_i^n(S(f, T)) = (a_i, a_{i+1}, \ldots, a_{i+n-1})$ denotes the sub-interval of $S(f, T)$ starting at a_i with length n.

Proposition 2.2.24 ([27, Property 5.1])**.** Let f be a degree-m primitive polynomial over $\mathbb{F}_q$, and let $S(f,T)$ be the M-sequence with $T \neq (0,0,\ldots,0)$. Each nonzero m-tuple of $\mathbb{F}_q^m$ occurs once per period as a sub-interval $(a_i, a_{i+1}, \ldots, a_{i+m-1})$ of length m.

Proposition 2.2.25 ([48, Corollary 1])**.** If f is a degree-m primitive polynomial over $\mathbb{F}_q$ and $T \in \mathbb{F}_q^m$, $T \neq (0,\ldots,0)$, then the LFSR $S(f,T) = (a_i)$ has the following properties, letting $k = \frac{q^m-1}{q-1}$:

1. For any $i \geq 0$, $C_i^k(S(f,T))$ contains exactly $\frac{q^{m-1}-1}{q-1}$ zeros.
2. For any $i \geq 0$, $j \geq 0$, the positions of zeros in $C_i^k(S(f,T))$ and $C_{i+jk}^k(S(f,T))$ are identical.

Proposition 2.2.26. Let $\alpha \in \mathbb{F}_{q^m}$ be a primitive element, and let f be a degree-m primitive polynomial over $\mathbb{F}_q$ with root α. Let $\alpha^j = c_{m-1,j}\alpha^{m-1} + \cdots + c_{0,j}\alpha^0$ be an element of $\mathbb{F}_{q^m}$ for $0 \leq j \leq q^m - 1$ where $\alpha^0, \ldots, \alpha^{m-1}$ is a basis for $\mathbb{F}_q^m$. Let b_j be the jth element of sequence $S(f,T)$ where $T = (b_0, b_1, \ldots, b_{m-1}) \neq (0,0,\ldots,0)$. Then $b_j = c_{m-1,j}b_{m-1} + \cdots + c_{0,j}b_0$.

Proof. By Theorem 2.2.21, there exists a unique element $\beta \in \mathbb{F}_{q^m}$ such that $b_j = \mathrm{Tr}(\beta\alpha^j)$ for all $j \geq 0$. So,

$$\begin{aligned} b_j &= \mathrm{Tr}(\beta\alpha^j) = \mathrm{Tr}(\beta(c_{m-1,j}\alpha^{m-1} + \cdots + c_{0,j}\alpha^0)) \\ &= c_{m-1,j}\,\mathrm{Tr}(\beta\alpha^{m-1}) + \cdots + c_{0,j}\,\mathrm{Tr}(\beta\alpha^0) \\ &= c_{m-1,j}b_{m-1} + \cdots + c_{0,j}b_0 \end{aligned}$$

∎

2.3 Finite geometry

This section provides an overview of projective spaces, in particular $\mathrm{PG}(2,q)$ and $\mathrm{PG}(3,q)$, and key geometric structures such as ovoids, Möbius planes, and hypersurfaces.

Definition 2.3.1. A *finite projective space* (or finite projective geometry) P is a finite set of *points* together with subsets of points called *lines* satisfying the following properties:

1. any two distinct points are on exactly one line;
2. let A, B, C, D be four distinct points of which no three are colinear. If the lines AB and CD intersect each other, then the lines AD and BC also intersect each other;
3. any line has at least three points.

Definition 2.3.2. A finite projective plane is a finite incidence structure such that:

1. any two distinct points are incident with exactly one line;

2. any two distinct lines are incident with exactly one point;

3. there exists a quadrangle, i.e. four points no three of which are collinear.

Definition 2.3.3. An affine plane is a finite incidence structure such that:

1. any two distinct points are on exactly one line;

2. for any point P outside a line l, there is exactly one line through P that has no point in common with l;

3. there exist three points not on a common line.

An important class of projective planes, $\mathrm{PG}(2,q)$, has its points the 1-dimensional subspaces of $\mathbb{F}_q^3$ and its lines the 2-dimensional subspaces of $\mathbb{F}_q^3$. An affine plane $\mathrm{AG}(2,q)$ can be obtained from $\mathrm{PG}(2,q)$ by removing one line and all of its points. Since $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ are exactly the finite planes satisfying a theorem of Desargues, they are called Desarguesian. For more information about this theorem of Desargues, see [59, VII, Chapter 2].

Let V be a vector space of dimension m over the finite field $\mathbb{F}_q$ for a prime power q. The geometry $\mathrm{PG}(m-1,q)$ that has its points the 1-dimensional subspaces of V and as its lines the 2-dimensional subspaces of V is a finite projective space of dimension $m-1$. There are $\frac{q^m-1}{q-1}$ points, and $\frac{q^{m-1}}{q-1}$ lines, with $\frac{q^{m-2}-1}{q-1}$ points each, in $\mathrm{PG}(m-1,q)$. We present a point in $\mathrm{PG}(m-1,q)$ in *homogeneous coordinates* $(a_0 : a_1 : \cdots : a_{m-1}) = \{(ba_0, ba_1, \ldots, ba_{m-1}) : b \in \mathbb{F}_q\}$.

Definition 2.3.4. Let P be a projective space of dimension at least two. A *collineation* of P is a bijective map α on the point set of P that preserves collinearity; that is, p, q, r collinear implies $\alpha(p)$, $\alpha(q)$, $\alpha(r)$ collinear.

Definition 2.3.5. A k-cap of $\mathrm{PG}(m-1,q)$ is a set of k points of $\mathrm{PG}(m-1,q)$, no three of which are collinear. A k-cap in $\mathrm{PG}(2,q)$ is called a k-arc. In $\mathrm{PG}(2,q)$, a $(q+1)$-arc is an *oval*. In $\mathrm{PG}(3,q)$, an *ovoid* is a k-cap with maximum size.

Since no three points of a k-cap $\mathcal{K}$ of $\mathrm{PG}(n,q)$ are collinear, the lines of $\mathrm{PG}(n,q)$ fall into three classes with respect to $\mathcal{K}$. An *external line* contains no point of $\mathcal{K}$, a *tangent line* contains exactly one point of $\mathcal{K}$, and a *secant line* contains exactly two points of $\mathcal{K}$.

Bose [5], Seiden [54], and Qvist [47] for odd $q > 2$, $q = 4$, and for all even $q > 2$, respectively, showed that the maximum value of k such that there exist a k-cap (ovoid) in $\mathrm{PG}(3,q)$ is q^2+1.

Theorem 2.3.6 ([5, 47, 54])**.** If $q > 2$, the size of an ovoid in $\mathrm{PG}(3,q)$ is q^2+1.

Theorem 2.3.7 ([4, 46])**.** For an ovoid $\mathcal{K}$ in $\mathrm{PG}(3,q)$ with $q > 2$:

1. at each point P of $\mathcal{K}$, the $q+1$ tangent lines to $\mathcal{K}$ lie in a plane, called the tangent plane to $\mathcal{K}$ at P. Thus $\mathcal{K}$ admits q^2+1 *tangent planes*;

2. every plane of PG$(3, q)$ is either a tangent plane or else meets $\mathcal{K}$ in a $(q+1)$-arc, in which case it is called a *secant plane* of $\mathcal{K}$.

Definition 2.3.8. A t-(v, k, λ) *design* is a pair $(X, \mathcal{B})$ where X is a v-set of points and $\mathcal{B}$ is a collection of k-subsets (blocks) of X with the property that every t-subset of X is contained in exactly λ blocks. The parameter λ is the index of the design.

The points and hyperplanes of PG$(m-1, q)$ form a 2-$(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1})$ design.

Definition 2.3.9 ([44])**.** A *Möbius plane* of order q is a 3-$(q^2+1, q+1, 1)$ design.

Remark 2.3.10. Given an ovoid $\mathcal{K}$ in PG$(3, q)$, the incidence structure with *points* the points of the ovoid, *blocks* or *circles* the secant plane sections of the ovoid, and the incidence that of PG$(3, q)$ is a Möbius plane of order q.

O'Keefe [44] provided a survey about ovoids in PG$(3, q)$, where classifications and characterization of ovoids are presented.

In the rest of this section, we review geometric objects and some of their properties in projective geometry. The reviewed materials can be found in [9].

Definition 2.3.11. Let n be a positive integer.

1. A *homogeneous* polynomial ϕ of degree n in the variables $x_0, x_1, \ldots, x_r$ over a field F is the sum of terms of type $ax_0^{n_0}x_1^{n_1}\ldots x_r^{n_r}$ where $a \in F$, each n_i is a non-negative integer, and $n_0+\cdots+n_r = n$. Each term $ax_0^{n_0}x_1^{n_1}\ldots x_r^{n_r}$ of a homogeneous polynomial of degree n is said to be of *degree* n, and a is called its *coefficient*.

2. A *hypersurface* H of *order* n, in PG(r, F), is a set of points $(x_0, x_1, \ldots, x_r)$ satisfying $\phi(x_0, x_1, \ldots, x_r) = 0$, where ϕ is a non-zero homogeneous polynomial of degree n.

3. When $n = 2$, the hypersurface is called a *quadric*, and when $n = 4$, the hypersurface is called a *quartic*. In PG$(2, F)$, a hypersurface is referred to as a *curve*, and when $n = 2$, the plane curve is called a *conic*.

4. If ϕ is irreducible over any extension of F, then the hypersurface $\phi = 0$ is said to be *irreducible*; otherwise the hypersurface is *reducible*.

Notation 2.3.12. Let S be the set of points in PG(r, F) that satisfy the equation $\phi = 0$. We denote $S \hookrightarrow \phi = 0$.

Definition 2.3.13. Let $Q \hookrightarrow \phi = 0$ be a quadric in PG(r, F) with $\phi = \sum_{j \geq i} a_{ij}x_ix_j$, $(0 \leq i \leq j \leq r)$ in $x_0, x_1, \ldots, x_r$. The quadric Q is *singular* if it contains at least one point p such that every line through p intersects Q doubly at p; in other words, the equation of the quadric corresponding to the intersection of Q and the line has a root with multiplicity equal to 2. Such a point p is called a *singular point*.

Theorem 2.3.14. A point p in a quadric Q in PG(r, F) with equation $\phi = 0$ is singular if and only if p satisfies $\frac{\partial \phi}{\partial x_i} = 0$, for $i = 0, 1, \ldots, r$.

The equations $\frac{\partial \phi}{\partial x_i} = 0$, $i = 0, 1, \ldots, r$ can be written in matrix form as $Mx = 0$, where $M = [m_{ij}]$; $m_{ii} = 2a_{ii}$, $m_{ij} = m_{ji} = a_{ij}$. The $(r+1) \times (r+1)$ matrix M is the *matrix associated with the quadric* defined by $\phi = 0$. Note that ϕ can be displayed using M: $\phi(x) = \frac{1}{2} x^T M x$ where $x^T = [x_0, x_1, \ldots, x_r]$. It is clear that $\text{rank}(M) = r + 1$ if and only if $Mx = 0$ has only a trivial solution. Then $\text{rank}(M) = r + 1$ if and only if Q is non-singular.

Some important properties of quadrics are listed in the following:

1. A conic C in $\text{PG}(2, F)$ is reducible if and only if C is singular.
2. For a prime power q, if a non-singular conic has one point in $\text{PG}(2, q)$, then it has precisely $q + 1$ points in $\text{PG}(2, q)$.
3. Any five distinct points, no three collinear, in $\text{PG}(2, q)$ determine a unique conic.
4. If Q is a non-singular quadric in $\text{PG}(3, q)$, then it is irreducible. We prove the contrapositive. Let $Q \hookrightarrow \phi = 0$ be a reducible quadric. Then $\phi = \phi_1 \phi_2$ where ϕ_1 and ϕ_2 are equations of planes. If the two planes are distinct ($\phi_1 \neq \phi_2$), they intersect in a line, and all points on that line are singular. If two planes coincide ($\phi_1 = \phi_2$), then all points on the plane are singular. Therefore, Q is singular.
5. For $r \geq 3$, there are singular quadrics in $\text{PG}(r, F)$ which are irreducible.
6. Let E be a field extension of F. Let $K : \text{PG}(r, F) \longrightarrow \text{PG}(r, E)$ be a linear transformation that induces a collineation of $\text{PG}(r, F)$, i.e. $K(\text{PG}(r, F)) \cong \text{PG}(r, F)$. We represent the linear transformation K by a matrix $K \in E^{(r+1)\times(r+1)}$. Let $\bar{x} = Kx$ denote the new coordinates after transformation K. Let $Q \hookrightarrow \phi = 0$ be a quadric in $\text{PG}(r, F)$ with associated matrix M, and $Q' \hookrightarrow \phi' = 0$ be a quadric in $\text{PG}(r, E)$ with associated matrix M' after transforming ϕ using K. So, $\phi = \frac{1}{2} x^T M x$, and $\phi' = \frac{1}{2} \bar{x}^T M' \bar{x}$. It is clear that $M = K^T M' K$. Since $\det(M) = \det(K^T) \det(M') \det(K)$ and $\det(K) = \det(K^T) \neq 0$, then $\det(M) = 0$ if and only if $\det(M') = 0$. Therefore, Q is singular if and only if Q' is singular.

Definition 2.3.15. Let $Q_1 \hookrightarrow \phi_1 = 0$ and $Q_2 \hookrightarrow \phi_2 = 0$ be two quadrics in $\text{PG}(r, F)$. Let $F' = F \cup \{\infty\}$. Then the set of quadrics $Q_1 + \lambda Q_2 \hookrightarrow \phi_1 + \lambda \phi_2 = 0$, $\lambda \in F'$, where $\lambda = \infty$ corresponds to $Q_2 \hookrightarrow \phi_2 = 0$, is called a *pencil of quadrics*.

Any point of $Q_1 \cap Q_2$ satisfies both $\phi_1 = 0$ and $\phi_2 = 0$ and therefore lies on every quadric of the pencil $Q_1 + \lambda Q_2$. These points are the only points that lie on every quadric of the pencil. Let C be a conic in $\text{PG}(2, q)$ with equation $\phi(x, y, z) = ax^2 + by^2 + cz^2 + dyz + exz + fxy = 0$. Let p_1, p_2, p_3, and p_4 be four distinct points satisfying this equation, no three collinear. We can always define a linear transformation T such that $T(p_1) = (1 : 0 : 0)$, $T(p_2) = (0 : 1 : 0)$, $T(p_3) = (0 : 0 : 1)$, and $T(p_4) = (1 : 1 : 1)$. Then, the new equation of C with respect to the new coordinates is $\phi'(x', y', z') = d'y'z' + e'x'z' + f'x'y' = 0$, since $\phi'(1, 0, 0) = \phi'(0, 1, 0) = \phi'(0, 0, 1) = 0$ force the coefficients of x'^2, y'^2, and z'^2 to be equal to zero, and $d' + e' + f' = 0$.

The next proposition is an easy conclusion from the previous discussion, but we provide the proof since this result is necessary in Chapter 4.

Proposition 2.3.16. The only conics through four distinct points in $\mathrm{PG}(2, q)$ (no three collinear) are the members of a pencil of conics.

Proof. Without loss of generality, let $C_1 \hookrightarrow \phi_1 = 0$, $C_2 \hookrightarrow \phi_2 = 0$, and $C_3 \hookrightarrow \phi_3 = 0$ be three conics sharing $(1:0:0)$, $(0:1:0)$, $(0:0:1)$, and $(1:1:1)$. Let the equations of ϕ_1, ϕ_2, and ϕ_3 be

$$\begin{aligned}
\phi_1 &= ayz + bxz + cxy = 0,\\
\phi_2 &= a'yz + b'xz + c'xy = 0,\\
\phi_3 &= a''yz + b''xz + c''xy = 0.
\end{aligned}$$

Assume, for the sake of contradiction, that ϕ_i is not in the pencil of ϕ_j and ϕ_k, for some distinct $i, j, k \in \{1, 2, 3\}$. Then the matrix in the following system of equations has rank 3:

$$\begin{bmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{bmatrix} \begin{bmatrix} yz \\ xz \\ xy \end{bmatrix} = 0.$$

Hence, the system has only the trivial solution: $yz = 0$, $xz = 0$, $xy = 0$. Therefore, at least two of x, y, and z must be zero which contradicts the fact that $(1:1:1)$ is on ϕ_1, ϕ_2, and ϕ_3. ∎

Chapter 3

Orthogonal and covering arrays constructed from finite fields and finite geometry

In this chapter, we review known orthogonal and covering arrays constructed using finite fields and finite geometry. We describe two equivalent approaches for building an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$ given by Raaphorst et al. [48] and Panario et al. [45]. In Section 3.1, these two arrays are defined and proven to be identical up to row permutation. In Section 3.2, we review the construction of a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ obtained by the vertical concatenation of two $\mathrm{OA}_q(q^3; 2, q^2 + q + 1, q)$, and we discuss its relation to a special covering perfect hash family. In Section 3.3, we review orthogoval (affine) projective planes and their connection with $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ and covering perfect hash families.

3.1 Two identical $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$

Rao [49] first constructed an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$, where q is a prime power, and gave an alternative and simpler construction in [50, 51]. An equivalent approach to construct an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$ is proposed by Raaphorst et al. [48], and it uses a primitive polynomial f as the characteristic polynomial of a linear feedback shift register (LFSR) sequence. Panario et al. [45] introduced a generator matrix using powers of a primitive root α of f and stated that the space spanned by the rows of that generator matrix yields an equivalent $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$. Orthogonal arrays constructed from LFSR sequences were first studied by Munemasa [39] for $q = 2$ and for general q in [45, 48]. In Theorem 3.1.3, we show that these arrays are identical up to row permutation; this fact was already stated in [45] without a detailed proof.

In the following, we show the construction of arrays $M(f)$ and $A(G_k^1)$ for $k = \frac{q^m-1}{q-1}$.

Let q be a prime power, and $f \in \mathbb{F}_q[x]$ be a degree-m primitive polynomial where α is a primitive root of f. Let $S(f, T) = (a_i)$ be the associated LFSR sequence, which is an M-

sequence since f is primitive. By using the sub-intervals of this M-sequence with length $k = \frac{q^m-1}{q-1}$, the sub-interval array of f, is given below:

$$M(f) := \begin{bmatrix} C_0^k(S(f,T)) \\ C_1^k(S(f,T)) \\ \vdots \\ C_{q^m-2}^k(S(f,T)) \\ 0\ 0\ \ldots\ 0 \end{bmatrix}.$$

Construction 3.1.1. Let $\mathbb{F}_{q^m}$ be a finite field for a prime power q and α a primitive element of $\mathbb{F}_{q^m}$. Let $L(\alpha^j)$ denote the tuple representation of α^j for the basis $\{\alpha^0, \alpha^1, \ldots, \alpha^{m-1}\}$ of $\mathbb{F}_q^m \cong \mathbb{F}_{q^m}$ a vector space over $\mathbb{F}_q$, i.e. the vector $[c_0, c_1, \ldots, c_{m-1}]^T$ where $\alpha^j = \sum_{n=0}^{m-1} c_n \alpha^n$.

Let G_c^l be the matrix where the ith column is $L(\alpha^{li})$ for $0 \leq i < c$, where $0 < c \leq \frac{q^m-1}{q-1}$, and l is a positive integer,

$$G_c^l := \begin{bmatrix} L(\alpha^0) & L(\alpha^l) & L(\alpha^{2l}) & \ldots & L(\alpha^{(c-1)l}) \end{bmatrix}. \tag{3.1.1}$$

The array $A(G_c^l)$ consisting of each row in the span of G_c^l is a $q^m \times c$ matrix, i.e. the array generated by the linear combination of rows of G_c^l over the elements of $\mathbb{F}_q$.

Let $c = \frac{q^m-1}{q-1}$. As observed in [45], the array G_c^1 has the maximum number of columns that are not multiples of each other, since the power $\frac{q^m-1}{q-1}$ is the smallest nonzero power such that $\alpha^{\frac{q^m-1}{q-1}} \in \mathbb{F}_q$. It is easy to see that G_c^1 has rank m and no two columns of G_c^1 are multiples of each other.

First, we give a lemma, and then prove that $M(f)$ and $G^1_{\frac{q^m-1}{q-1}}$ give identical arrays up to row permutations.

Lemma 3.1.2. Let $m \geq 2$, q be a prime power and $k = \frac{q^m-1}{q-1}$. Let f be a degree-m primitive polynomial over $\mathbb{F}_q$ with root α, a primitive element of $\mathbb{F}_{q^m}$. For each $0 \leq i \leq m-1$, let $I_m^i \in \mathbb{F}_q$ be the m-tuple corresponding to the ith row of the identity matrix I_m of dimension m. Then,

$$G^1_{\frac{q^m-1}{q-1}} := \begin{bmatrix} L(\alpha^0) & L(\alpha^1) & L(\alpha^2) & \ldots & L(\alpha^{\frac{q^m-1}{q-1}-1}) \end{bmatrix} = \begin{bmatrix} C_0^k(S(f,I_m^0)) \\ C_0^k(S(f,I_m^1)) \\ \vdots \\ C_0^k(S(f,I_m^{m-1})) \end{bmatrix}.$$

Proof. Let m_{ij} be the jth element of $C_0^k(S(f,I_m^i))$, $0 \leq j \leq k-1$. Let $c_{0,j}, c_{1,j}, \ldots, c_{m-1,j}$ be the coefficients of α^j in basis $\{\alpha^0, \alpha^1, \ldots, \alpha^{m-1}\}$, i.e. $\alpha^j = \sum_{i=0}^{m-1} c_{i,j}\alpha^i$. We claim $m_{i,j} = c_{i,j}$. For each $0 \leq i \leq m-1$, since $I_m^i = [a_0^i, a_1^i, \ldots, a_s^i, \ldots, a_{m-1}^i]$ where $a_i^i = 1$ and $a_j^i = 0$, for all $j \neq i$, by Proposition 2.2.26, we obtain $m_{i,j} = c_{m-1,j}a_{m-1}^i + \cdots + c_{i,j}a_i^i + \cdots + c_{0,j}a_0^i = c_{i,j}$. Since α^j corresponds to the column j of $G^1_{\frac{q^m-1}{q-1}}$ and $\alpha^j = c_{m-1,j}\alpha^{m-1} + c_{m-2,j}\alpha^{m-2} + \cdots + c_{0,j}\alpha^0$, then the row i in column j of $G^1_{\frac{q^m-1}{q-1}}$ is equal to $c_{i,j}$ which completes the proof. ∎

Theorem 3.1.3. The arrays $M(f)$ and $A(G^1_{\frac{q^m-1}{q-1}})$ are identical up to row permutation, which we denote $M(f) \simeq A(G^1_{\frac{q^m-1}{q-1}})$.

Proof. Let f be a degree-m primitive polynomial over $\mathbb{F}_q$ with root α, a primitive element of $\mathbb{F}_{q^m}$. Let $c_{0,j}, c_{1,j}, \ldots, c_{m-1,j}$ be the coefficients of α^j in basis $\{\alpha^0, \alpha^1, \ldots, \alpha^{m-1}\}$, i.e. $\alpha^j = \sum_{i=0}^{m-1} c_{i,j}\alpha^i$, where $k = \frac{q^m-1}{q-1}$, $0 \le j \le k-1$ and $0 \le i \le m-1$. Let $R_{A(G^1_k)}$ be the set of rows of the array $A(G^1_k)$. By Lemma 3.1.2, $R_{A(G^1_k)} = \{r_0C^k_0(S(f, I^0_m)) + \cdots + r_{m-1}C^k_0(S(f, I^{m-1}_m)) : r_0, \ldots, r_{m-1} \in \mathbb{F}_q\}$. Let $R_{M(f)}$ be the set of rows of $M(f)$. By Proposition 2.2.24, $R_{M(f)} = \{C^k_0(S(f, v)) : v \in \mathbb{F}^m_q\}$. It suffices to show that $R_{A(G^1_k)} = R_{M(f)}$. Let b^v_j be the jth element of $C^k_0(S(f, v))$ where v is an arbitrary vector in $\mathbb{F}^m_q$. So, each $v = r_0I^0_m + \cdots + r_{m-1}I^{m-1}_m = (r_0, r_1, \ldots, r_{m-1})$ for $r_0, \ldots, r_{m-1} \in \mathbb{F}_q$. By Proposition 2.2.26, $b^v_j = c_{m-1,j}r_{m-1} + \cdots + c_{i,j}r_i + \cdots + c_{0,j}r_0$. We claim that the jth element of $r_0C^k_0(S(f, I^0_m)) + \cdots + r_{m-1}C^k_0(S(f, I^{m-1}_m)) \in R_{A(G^1_k)}$ is equal to b^v_j. In the proof of Lemma 3.1.2, we see that the jth element of $C^k_0(S(f, I^i_m))$ for $0 \le i \le m-1$ is $c_{i,j}$. Therefore, the jth element of $r_0C^k_0(S(f, I^0_m)) + \cdots + r_{m-1}C^k_0(S(f, I^{m-1}_m))$ is $r_0c_{0,j} + \cdots + r_ic_{i,j} + \cdots + r_{m-1}c_{m-1,j}$ which is equal to b^v_j. So, $R_{A(G^1_k)} = R_{M(f)}$. ∎

In Fig. 3.1, the array $A(G^1_{q^2+q+1})$ and $M(f)$ for $q = 3$ are presented. On top of array $A(G^1_{q^2+q+1})$, we display the generator matrix $G^1_{q^2+q+1}$. Each row of $A(G^1_{q^2+q+1})$ is obtained by the linear combination of rows of $G^1_{q^2+q+1}$ with coefficients $v = (r_0, r_1, r_2) \in \mathbb{F}^3_3$. In the proof of Theorem 3.1.3, it is shown that $r_0C^k_0(S(f, I^0_3)) + r_1C^k_0(S(f, I^1_3)) + r_2C^k_0(S(f, I^2_3)) = C^k_0(S(f, (r_0, r_1, r_2)))$, where $k = q^2 + q + 1$. This is exactly the row i of $M(f)$, where $(a_i, a_{i+1}, a_{i+2}) = (r_0, r_1, r_2)$, which always exists in an M-sequence (Proposition 2.2.24).

Proposition 3.1.4 ([38, Proposition 2])**.** Let q be a prime power and f be a degree-m primitive polynomial over $\mathbb{F}_q$. Then $M(f)$ is an $\mathrm{OA}_{q^{m-2}}(q^m; 2, \frac{q^m-1}{q-1}, q)$.

The next theorem connects coverage of sets of columns in $M(f)$ with linear independence in G^1_k for $k = \frac{q^m-1}{q-1}$.

Theorem 3.1.5 (Raaphorst et al., [48, Theorem 2])**.** Let f be a primitive polynomial of degree $m \ge 3$ over a finite field $\mathbb{F}_q$ with root α in the extension field $\mathbb{F}_{q^m}$, and write $k = \frac{q^m-1}{q-1}$. Let $M = M(f) = [M_0\ M_1\ \ldots\ M_{k-1}]$ be the $q^m \times k$ subinterval array of f, where M_i is the ith column of M. Then, the following are equivalent:

1. A set of s columns $C = \{M_{i_0}, M_{i_1}, \ldots, M_{i_{s-1}}\}$ is not covered in M.
2. The set of vectors $\{\alpha^{i_0}, \ldots, \alpha^{i_{s-1}}\}$ is linearly dependent over $\mathbb{F}_q$.

Furthermore, if $s = m$, the following statement is also equivalent to (1) and (2):

3. There is a row r other than the all-zero row of M such that $r_{i_0} = \cdots = r_{i_{m-1}} = 0$.

Figure 3.1: The array $A(G^1_{q^2+q+1})$ and array $M(f)$ for $q = 3$ and a primitive polynomial $f(x) = x^3 + 2x^2 + x + 1$.

j	0	1	2	3	4	5	6	7	8	9	10	11	12	
$c_{0,j}$	1	0	0	2	2	0	2	0	1	2	1	1	1	$C_0^k(S(f, I_3^0))$
$c_{1,j}$	0	1	0	2	1	2	2	2	1	0	0	2	2	$C_0^k(S(f, I_3^1))$
$c_{2,j}$	0	0	1	1	0	1	0	2	1	2	2	2	1	$C_0^k(S(f, I_3^2))$
$v = (r_0, r_1, r_2)$														
(0, 0, 0)	0	0	0	0	0	0	0	0	0	0	0	0	0	
(0, 0, 1)	0	0	1	1	0	1	0	2	1	2	2	2	1	
(0, 0, 2)	0	0	2	2	0	2	0	1	2	1	1	1	2	
(0, 1, 0)	0	1	0	2	1	2	2	2	1	0	0	2	2	
(0, 1, 1)	0	1	1	0	1	0	2	1	2	2	2	1	0	
(0, 1, 2)	0	1	2	1	1	1	2	0	0	1	1	0	1	
(0, 2, 0)	0	2	0	1	2	1	1	1	2	0	0	1	1	
(0, 2, 1)	0	2	1	2	2	2	1	0	0	2	2	0	2	
(0, 2, 2)	0	2	2	0	2	0	1	2	1	1	1	2	0	
(1, 0, 0)	1	0	0	2	2	0	2	0	1	2	1	1	1	
(1, 0, 1)	1	0	1	0	2	1	2	2	2	1	0	0	2	
(1, 0, 2)	1	0	2	1	2	2	2	1	0	0	2	2	0	
(1, 1, 0)	1	1	0	1	0	2	1	2	2	2	1	0	0	
(1, 1, 1)	1	1	1	2	0	0	1	1	0	1	0	2	1	
(1, 1, 2)	1	1	2	0	0	1	1	0	1	0	2	1	2	
(1, 2, 0)	1	2	0	0	1	1	0	1	0	2	1	2	2	
(1, 2, 1)	1	2	1	1	1	2	0	0	1	1	0	1	0	
(1, 2, 2)	1	2	2	2	1	0	0	2	2	0	2	0	1	
(2, 0, 0)	2	0	0	1	1	0	1	0	2	1	2	2	2	
(2, 0, 1)	2	0	1	2	1	1	1	2	0	0	1	1	0	
(2, 0, 2)	2	0	2	0	1	2	1	1	1	2	0	0	1	
(2, 1, 0)	2	1	0	0	2	2	0	2	0	1	2	1	1	$C_0^k(S(f, (2, 1, 0)))$
(2, 1, 1)	2	1	1	1	2	0	0	1	1	0	1	0	2	
(2, 1, 2)	2	1	2	2	2	1	0	0	2	2	0	2	0	
(2, 2, 0)	2	2	0	2	0	1	2	1	1	1	2	0	0	
(2, 2, 1)	2	2	1	0	0	2	2	0	2	0	1	2	1	
(2, 2, 2)	2	2	2	1	0	0	2	2	0	2	0	1	2	

i	a_i	a_{i+1}	a_{i+2}											$C_0^k(S(f, (a_i, a_{i+1}, a_{i+2})))$
0	0	1	2	1	1	1	2	0	0	1	1	0	1	
1	1	2	1	1	1	2	0	0	1	1	0	1	0	
2	2	1	1	1	2	0	0	1	1	0	1	0	2	
3	1	1	1	2	0	0	1	1	0	1	0	2	1	
4	1	1	2	0	0	1	1	0	1	0	2	1	2	
5	1	2	0	0	1	1	0	1	0	2	1	2	2	
6	2	0	0	1	1	0	1	0	2	1	2	2	2	
7	0	0	1	1	0	1	0	2	1	2	2	2	1	
8	0	1	1	0	1	0	2	1	2	2	2	1	0	
9	1	1	0	1	0	2	1	2	2	2	1	0	0	
10	1	0	1	0	2	1	2	2	2	1	0	0	2	
11	0	1	0	2	1	2	2	2	1	0	0	2	2	
12	1	0	2	1	2	2	2	1	0	0	2	2	0	
13	0	2	1	2	2	2	1	0	0	2	2	0	2	
14	2	1	2	2	2	1	0	0	2	2	0	2	0	
15	1	2	2	2	1	0	0	2	2	0	2	0	1	
16	2	2	2	1	0	0	2	2	0	2	0	1	2	
17	2	2	1	0	0	2	2	0	2	0	1	2	1	
18	2	1	0	0	2	2	0	2	0	1	2	1	1	$C_0^k(S(f, (2, 1, 0)))$
19	1	0	0	2	2	0	2	0	1	2	1	1	1	
20	0	0	2	2	0	2	0	1	2	1	1	1	2	
21	0	2	2	0	2	0	1	2	1	1	1	2	0	
22	2	2	0	2	0	1	2	1	1	1	2	0	0	
23	2	0	2	0	1	2	1	1	1	2	0	0	1	
24	0	2	0	1	2	1	1	1	2	0	0	1	1	
25	2	0	1	2	1	1	1	2	0	0	1	1	0	
26	0	0	0	0	0	0	0	0	0	0	0	0	0	

Definition 3.1.6. A set $D = \{d_1, d_2, \ldots, d_k\}$ of $k \geq 2$ distinct residues modulo v is called a (v, k, λ)-*difference set* if for every $d \not\equiv 0 \pmod{v}$ there are exactly λ ordered pairs (d_i, d_j) with $d_i, d_j \in D$ such that $d_i - d_j \equiv d \pmod{v}$.

Developing a difference set in $\mathbb{Z}_v$, by taking the translates $D + a = \{d + a : d \in D\}$ for all $a \in \mathbb{Z}_v$, yields a 2-(v, k, λ) design.

Theorem 3.1.7 (Raaphorst et al., [48, Theorem 3])**.** Let $k = \frac{q^m-1}{q-1}, z = \frac{q^{m-1}-1}{q-1}, \lambda = \frac{q^{m-2}-1}{q-1}$. Let M be $A(G_k^1)$ with the all-zero row removed. Then each row of M has exactly z zeros, and the set:

$$\mathcal{B} = \{\{a_1, \ldots, a_{z-1}\} : M_{i,a_1} = \cdots = M_{i,a_{z-1}} = 0,\ 0 \leq i < q^m - 2\} \tag{3.1.2}$$

is the set of blocks of a 2-(k, z, λ) design. Moreover, any block in $\mathcal{B}$ is a (k, z, λ)-difference set.

By Theorem 3.1.5 and Theorem 3.1.7, each block of the 2-$(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1})$ design $(\mathbb{Z}_{\frac{q^m-1}{q-1}}, \mathcal{B})$ corresponds to a hyperplane in $\mathrm{PG}(m-1, q)$.

Let S be an $m \times t$ sub-matrix S of G_k^1 for $1 \leq t \leq m$, and $k = \frac{q^m-1}{q-1}$. Suppose $\mathrm{rank}(S) = r$, for $1 \leq r \leq t$. If $r \neq t$, then only q^r distinct t-tuples are covered in $A(S)$. Otherwise, all distinct t-tuples in $\mathbb{F}_q^t$ are covered by some row in $A(S)$. If $t = m$ and $\mathrm{rank}(S) \neq t$ then, by Theorem 3.1.5, the column indices of S are contained in a block of the 2-$(\frac{q^m-1}{q-1}, \frac{q^{m-1}-1}{q-1}, \frac{q^{m-2}-1}{q-1})$ design and the corresponding points in $\mathrm{PG}(m-1, q)$ are in the hyperplane associated with the block.

Since no two columns of G_k^l are multiples of each other, the array $A(G_k^l)$ is an $\mathrm{OA}_{q^{m-2}}(q^m; 2, k, q)$ which is also a $\mathrm{CA}_{q^{m-2}}(q^m; 2, k, q)$.

3.2 Covering arrays of strength 3 constructed from LFSR sequence and generator matrix

The main goal of this section is to review the construction of $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ and its connection with covering perfect hash families.

Let f be a degree-3 primitive polynomial over $\mathbb{F}_q$ and f_r be the reciprocal of f. Raaphorst et al. [48] used LFSR sequence with respect to f and f_r and built a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$.

Note that since f_r is primitive and α^{-1} is a root of f_r, then $M(f_r) \simeq A(G^{-1}_{q^2+q+1})$.

The next two theorems show the main connection between $M(f)$ and $M(f_r)$, that leads to construct a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$.

Theorem 3.2.1 (Raaphorst et al., [48, Lemma 3])**.** Let f be a degree-3 primitive polynomial over $\mathbb{F}_q$ and let f_r be the reciprocal polynomial of f. If a triple of columns $D = \{a, b, c\}$ with $0 \leq a < b < c < q^2 + q + 1$ is not covered in $M(f)$, then D is covered in $M(f_r)$.

Theorem 3.2.2 (Raaphorst et al., [48, Theorem 6])**.** Let q be a prime power and f be a degree-3 primitive polynomial over $\mathbb{F}_q$. Then, the vertical concatenation of $A = M(f) \simeq A(G^1_{q^2+q+1})$ and $A_r = M(f_r) \simeq A(G^{-1}_{q^2+q+1})$ with one copy of the all-zero row removed is a $CA(2q^3 - 1; 3, q^2 + q + 1, q)$.

We present a connection between Theorem 3.2.2 and covering perfect hash families.

Definition 3.2.3. A *covering perfect hash family* denoted by $\text{CPHF}_\lambda(n; k, q, t)$ is an $n \times k$ array of elements from $\mathbb{F}_q^t \setminus \vec{0}$ (equivalently the points of $PG(t-1, q)$) such that, for each set T of t columns, there exist at least λ rows whose entries in the columns of T are linearly independent. If the vector entries all have a non-zero last coordinate then the CPHF is a Sherwood covering perfect hash family $\text{SCPHF}_\lambda(n; k, q, t)$. If $\lambda = 1$, we remove λ from notation.

Theorem 3.2.4. Let q be a prime power. Then, a $\text{CPHF}(2; q^2 + q + 1, q, 3)$ with rows corresponding to $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ exists.

Proof. Let f be a degree-3 primitive polynomial over $\mathbb{F}_q$ and let f_r be the reciprocal of f. Let $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ be the generator matrices with respect to f and f_r, respectively. Since α^{-1} is a root of f_r, $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ are as follows:

$$\begin{aligned} G^1_{q^2+q+1} &= \left[L(\alpha^0)\ L(\alpha^1)\ L(\alpha^2)\ \cdots\ L(\alpha^j)\ \cdots\ L(\alpha^{q^2+q}) \right], \\ G^{-1}_{q^2+q+1} &= \left[L(\alpha^0)\ L(\alpha^{-1})\ L(\alpha^{-2})\ \cdots\ L(\alpha^{-j})\ \cdots L(\alpha^{-(q^2+q)}) \right]. \end{aligned}$$

Let $C = (c_{i,j})$ be a $2 \times (q^2+q+1)$ array with $c_{1,j} = L(\alpha^j)$ and $c_{2,j} = L(\alpha^{-j})$. By Theorem 3.2.1 and Theorem 3.1.5, for any j_1, j_2, and j_3, there exists at least one row $r \in \{1, 2\}$ in C where the 3×3 sub-matrix constructed by $c_{r,j_1}, c_{r,j_2}, c_{r,j_3}$ has rank 3. This proves that C is a $\text{CPHF}(2; q^2 + q + 1, q, 3)$. ∎

In the following theorem, a connection between covering perfect hash family and covering array is given.

Theorem 3.2.5 ([18])**.** If there exists a $\text{CPHF}(n; k, q, t)$, then there exists a $\text{CA}(n(q^t - 1) + 1; t, k, q)$; and if there exists a $\text{SCPHF}(n; k, q, t)$, then there exists a $\text{CA}(n(q^t - q) + q; t, k, q)$.

By Theorem 3.2.4 and Theorem 3.2.5, we obtain that a $\text{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ can be constructed by using a covering perfect hash family.

3.3 Covering arrays of strength 3 from finite geometry

In Theorem 3.2.2, we have seen that the vertical concatenation of $A(G^1_{q^2+q+1})$ and $A(G^{-1}_{q^2+q+1})$ gives a $\text{CA}(2q^3-1; 3, q^2+q+1, q)$. In this section, we investigate its connection with projective geometry $\text{PG}(2, q)$.

Definition 3.3.1 ([17])**.** Two planes, both projective or both affine, of the same order and on the same pointset are *orthogoval* if a line of one plane intersects any line in the other plane in at most two points. A set of planes is called a *set of mutually orthogoval planes* if the planes are pairwise orthogoval.

Since any two columns of $G^1_{q^2+q+1}$ (or of $G^{-1}_{q^2+q+1}$) are linearly independent, and there are $\frac{q^3-1}{q-1}$ columns in total, these columns correspond to the points of $\mathrm{PG}(2,q)$. Using the connection between $\mathrm{CPHF}(2;q^2+q+1,q,3)$ in Theorem 3.2.4 and projective (affine) planes constructed over finite fields, we observe that any 3×3 submatrix corresponding to a 3-set of column indices has rank 3 in either $G^1_{q^2+q+1}$ or $G^{-1}_{q^2+q+1}$. This implies that any three collinear points in one plane are non-collinear in the other, and hence the two projective planes are orthogoval.

We review orthogoval planes $\mathrm{PG}(2,q)$ and $\mathrm{AG}(2,q)$ in the literature and review the corresponding constructed covering arrays. The existence of orthogoval projective planes is proved independently in [6, 25, 28, 34, 48, 65], and non-independent novel proofs are published in [2, 17, 45]. The common idea in these works was to show that for a pair of projective planes with the same pointset, any line in one is an oval in another. They have used different methods using combinatorial design theory and finite geometry. They consider D a $(q^2+q+1,q+1,1)$-difference set whose translates are the lines in $\mathrm{PG}(2,q)$, and show that there exists D' obtained from D, which corresponds to an oval in $\mathrm{PG}(2,q)$. For instance, Hall [28] determined that $\frac{1}{2}D=\{x:2x\in D\}$ is an oval. Bruck [6] showed $-D$ is an oval and noted that this gives a pair of planes where lines in one are ovals in other. Baker et al. [2] unified $-D$, $\frac{1}{2}D$ into a single framework and proved that rD and $\frac{1}{r}D$ are ovals. Raaphorst et al. [48] used a primitive polynomial and its reciprocal to construct strength-3 covering arrays and their construction relied on the property that the two projective planes are orthogoval. Panario et al. [45] provide a new proof of the existence of a pair of orthogoval planes. They used $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ for α not necessarily primitive to represent two projective planes. Colbourn et al. [17] define the term "orthogoval" projective (affine) plane, and provide a new proof for the existence of a pair of orthogoval planes using a Cremona transformation. They extended this to an affine plane and showed the existence of a pair of orthogoval affine planes. They also considered sets (of more than two) mutually orthogoval projective (affine) planes.

Theorem 3.3.2 ([17, Theorem 4.4])**.** Suppose that a set of s mutually orthogoval Desarguesian projective (affine) planes exist. Then there exists a $\mathrm{CPHF}_{s-1}(s;q^2+q+1,q,3)$ ($\mathrm{SCPHF}_{s-1}(s;q^2,q,3)$).

The results by Raaphorst et al. [48](Theorem 3.1.5) and equivalently Theorem 3.2.4 show that there are two orthogoval planes $\mathrm{PG}(2,q)$ for every prime power q.

Colbourn et al. [17] show that for even prime power q and $q=3$, a $\mathrm{SCPHF}(2;q^2,q,3)$ exists by using the properties of mutually orthogoval Desarguesian affine planes.

Proposition 3.3.3 ([17, Corollary 3.9])**.** There exists a pair of Desarguesian orthogoval affine planes of order $q=2^n$, for any n.

Proposition 3.3.4. There exists a pair of Desarguesian orthogoval affine planes of order $q=3$.

Proof. Represent the points of $\mathrm{AG}(2,q)$ as a set V of length-3 vectors in homogeneous coordinates over $\mathbb{F}_q$ with first entry 1. Any two Desarguesian affine planes on the same point set $P = \{p_1, p_2, \ldots, p_{q^2}\}$ are isomorphic to $\mathrm{AG}(2,q)$; let $\phi_1, \phi_2 : P \to V$ be the corresponding isomorphisms. Fig. 3.2 represents a pair of orthogoval affine planes, where $\phi_1(p_i)$ is listed in column i of A_1 and $\phi_2(p_i)$ is listed in column i of A_2. One can check that any three points collinear in one plane are non-collinear in the other plane. ∎

Figure 3.2: Points of two Desarguesian orthogoval affine planes $\mathrm{AG}(2,3)$ given as columns $p_1, p_2, \ldots, p_9$ of A_1 and A_2.

$$A_1 = \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline 1&1&1&1&1&1&1&1&1\\\hline 0&1&2&0&1&2&0&1&2\\\hline 0&0&0&1&1&1&2&2&2\\\hline\end{array}$$

$$A_2 = \begin{array}{|c|c|c|c|c|c|c|c|c|}\hline 1&1&1&1&1&1&1&1&1\\\hline 2&1&1&1&2&0&2&0&0\\\hline 1&0&1&2&0&0&2&1&2\\\hline\end{array}$$

Corollary 3.3.5 ([17])**.** For even prime power q and $q = 3$, a $\mathrm{SCPHF}(2; q^2, q, 3)$ and $\mathrm{CA}(2q^3 - q; 3, q^2, q)$ exist.

Proof. Use Proposition 3.3.3, Proposition 3.3.4, and Theorem 3.3.2. ∎

Two additional columns can be added for the covering arrays obtained by s mutually orthogoval Desarguesian affine planes.

Theorem 3.3.6 ([17])**.** Suppose that a set of s mutually orthogoval Desarguesian affine planes exists. Then there exists a $\mathrm{CA}_{s-1}(sq^3 - q; 3, q^2 + 2, q)$.

The existence of a pair of orthogoval projective (affine) planes gives Theorem 3.3.7.

Theorem 3.3.7 ([17])**.** There exist a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ for any prime power q, and a $\mathrm{CA}(2q^3 - q; 3, q^2 + 2, q)$ for even prime power q and $q = 3$.

The $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ in Theorem 3.2.2 is obtained by the vertical concatenation of $A(G^1_{q^2+q+1})$ and $A(G^{-1}_{q^2+q+1})$. It is possible to remove $2(q-1)$ columns of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ carefully and create new generators G_1 and G_2 respectively, such that q similar rows can be obtained in $A(G_1)$ and $A(G_2)$. By removing q redundant rows, we have Theorem 3.3.8. This is equivalent to removing $2(q-1)$ points from a pair of orthogoval projective planes for any prime power q to obtain truncated orthogoval affine planes [61].

Theorem 3.3.8 ([61])**.** There exist a $\mathrm{CA}(2q^3 - q; 3, q^2 - q + 3, q)$ for any prime power q.

Chapter 4

Existence of three anti-cocircular truncated Möbius planes and constructions of strength-4 covering arrays

The main goal of this chapter is to extend the concept of orthogoval projective planes to a higher-dimensional projective geometry $\mathrm{PG}(3, q)$, and use it to construct strength-4 covering arrays. In Chapter 3, we have seen that a pair of orthogoval projective planes can be used to construct a strength-3 covering array $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$ [48]. The possibility of generalizing or extending the definition of orthogoval planes to other geometric objects in higher dimensions, such as Möbius planes, is mentioned in [17]. A strength-4 covering array $\mathrm{CA}(511; 4, 17, 4)$ obtained in [64] suggests a connection with ovoids in $\mathrm{PG}(3, q)$ for $q = 4$. Using an exhaustive computational search over two copies of $\mathrm{PG}(3, 4)$ to find strength-4 covering arrays, Tzanakis et al. [64] found that the maximum number of columns was achieved by the points of an ovoid. Definition 4.0.1 can be considered a generalization of a pair of orthogoval projective planes, to the case of Möbius planes.

Let $(\mathcal{X}, \mathcal{B})$ be a t-(v, k, λ) design. A *truncated* design is obtained from $(\mathcal{X}, \mathcal{B})$ by removing some of its points, $\mathcal{P} \subseteq \mathcal{X}$, and getting $(\mathcal{X}' = \mathcal{X} \setminus \mathcal{P}, \mathcal{B}' = \{B \cap \mathcal{X}' : B \in \mathcal{B}\})$.

Definition 4.0.1. A set of m (truncated) Möbius planes on the same point set is *anti-cocircular* if the common intersection of any choice of m blocks one from each of the planes has at most size three. In other words, any four points cannot be simultaneously contained in m circles, one in each of the Möbius planes.

The $\mathrm{CA}(511; 4, 17, 4)$ is constructed from 2 anti-cocircular Möbius planes.

In this chapter, we have two objectives. First, we show the existence of 3 anti-cocircular truncated Möbius planes; and second, we build a $\mathrm{CA}(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ for any odd prime power q by vertically concatenating three strength-3 covering arrays. Each strength-3 covering array is obtained by a generator matrix whose columns correspond to one of the three truncated

Möbius planes. For $q \geq 11$, this covering array improves the size of the best-known covering arrays with the same parameters by almost 25 percent, as q grows (see Table 4.6). We summarize in Table 4.1 how various geometric objects give rise to covering arrays, including the new ones presented here.

Table 4.1: Different geometric objects and corresponding constructed covering arrays.

q	Geometric object	Corresponding CA	References
All prime powers	Pair of orthogoval PG$(2,q)$	CA$(2q^3-1;3,q^2+q+1,q)$	[6, 25, 28, 34, 48, 65]
Even prime powers	Pair of orthogoval AG$(2,q)$	CA$(2q^3-q;3,q^2+2,q)$	[17]
All prime powers	Pair of orthogoval truncated AG$(2,q)$	CA$(2q^3-q;3,q^2-q+3,q)$	[61]
$q=3$	Set of 4 mutually orthogoval PG$(2,3)$	CA$_\lambda(27\lambda+26;3,13,3)$, $\lambda<4$	[17]
$q=3$	Set of 7 mutually orthogoval AG$(2,3)$	CA$_\lambda(27\lambda+24;3,11,3)$, $\lambda<7$	[17]
$q=2^n$, gcd$(n,6)=1$	Triple of mutually orthogoval AG$(2,q)$	CA$_\lambda(\lambda q^3+q^3-q;3,q^2+2,q)$, $\lambda<3$	[17]
$q=4$	Set of 7 mutually orthogoval AG$(2,4)$	CA$_\lambda(64\lambda+60;3,18,4)$, $\lambda<7$	[17]
$q=8$	Set of 7 mutually orthogoval AG$(2,8)$	CA$_\lambda(512\lambda+504;3,66,8)$, $\lambda<7$	[17]
$q=4$	2 anti-cocircular Möbius planes	CA$(511;4,17,4)$	[64]
Odd prime powers	3 anti-cocircular truncated Möbius planes	CA$(3q^4-2;4,\frac{q^2+1}{2},q)$	Theorem 4.2.31, Theorem 4.3.1

In the construction of the CA$(3q^4-2;4,\frac{q^2+1}{2},q)$, we use $\frac{q^2+1}{2}$ points of the ovoid (half of the points of the ovoid). We observe that half ovoids have been used in other contexts, such as the construction of a family of projective two-weight codes (strongly regular Cayley graphs) in an unpublished work [67].

Extending our construction to employ all q^2+1 points of the ovoid is feasible using additional geometric properties and recursive constructions. Using these, we construct a CA$(5q^4-4q^3-q^2+2q;4,q^2+1,q)$ for any odd prime power q. These covering arrays improve the size of many covering arrays with the same parameters.

The structure of this chapter is as follows. In Section 4.1, we use the generator matrix $G^{q+1}_{q^2+1}$, whose columns correspond to the points of an ovoid, and establish its connection with the Möbius plane. In Section 4.2, we give results connecting blocks of truncated Möbius planes with hypersurfaces in PG$(3,q)$. We prove the existence of 3 anti-cocircular truncated Möbius planes. In Section 4.3, we prove the existence of a CA$(3q^4-2;4,\frac{q^2+1}{2},q)$ obtained by the vertical concatenation of three strength-3 covering arrays obtained by 3 anti-cocircular truncated Möbius planes. In Section 4.4, we prove the existence of a CA$(5q^4-4q^3-q^2+2q;4,q^2+1,q)$ using a recursive method with the CA$(3q^4-2;4,\frac{q^2+1}{2},q)$ as the main ingredient.

These results have been prepared as a paper and submitted to arXiv [56].

4.1 Generator matrix for $\mathbb{F}_{q^4}$ and Möbius planes

Recall the generator matrix G^l_c given in Construction 3.1.1. Let $c=\frac{q^m-1}{q-1}$. Since any two columns of G^1_c are linearly independent and there are $\frac{q^m-1}{q-1}$ columns, then the columns are in correspondence with the points of PG$(m-1,q)$.

Let $z=\frac{q^{m-1}-1}{q-1}$ and $S=\{i_1,i_2,\dots i_z\}$ be a set of column indices of $A=A(G^1_c)$ with $A_{r,i_1}=\cdots=A_{r,i_z}=0$ for some non-zero row r of $A(G^1_c)$. The points of PG$(m-1,q)$ corresponding to S consist of the z points contained in a hyperplane of PG$(m-1,q)$. In

the main results of this chapter, we use $G^{q+1}_{q^2+1}$ in Construction 3.1.1 for $m = 4$. We are interested in $G^{q+1}_{q^2+1}$, since the columns of $G^{q+1}_{q^2+1}$ correspond to points of an ovoid in PG$(3, q)$ (Proposition 4.1.1) and its plane sections corresponds to a Möbius plane.

Proposition 4.1.1 ([21, Theorem 3])**.** Let q be a prime power and $m = 4$. Let $O = \{L(\alpha^{x(q+1)}) : 0 \le x \le q^2+1\}$ be the set of the columns of $G^{q+1}_{q^2+1}$. Then, the set O is an ovoid in PG$(3, q)$.

By Proposition 4.1.1, the rank of any 4×3 sub-matrix of $G^{q+1}_{q^2+1}$ is 3. The rank of any 4×4 sub-matrix of $G^{q+1}_{q^2+1}$ is either 3 or 4, depending on whether the corresponding 4 points are coplanar or not, respectively.

Remark 4.1.2. Let q be a prime power and $m = 4$. Let $\mathcal{M} = \{i : 0 \le i < q^2+1\}$ be the set of column indices of $G^{q+1}_{q^2+1}$. The columns of $G^{q+1}_{q^2+1}$ correspond to an ovoid O in PG$(3, q)$. Its plane sections correspond to the blocks of a 3-$(q^2+1, q+1, 1)$ design or a Möbius plane. Each block (circle) B of the 3-$(q^2+1, q+1, 1)$ design (Möbius plane) corresponds to the column indices $\{i_1, \ldots, i_{q+1}\}$ with $A_{r,i_1} = \cdots = A_{r,i_{q+1}} = 0$ for some non-zero row $0 \le r \le q^4 - 1$ of $A = A(G^{q+1}_{q^2+1})$. Therefore, the set:

$$\mathcal{C} = \{\{i_1, \ldots, i_{q+1}\} : A_{r,i_1} = \cdots = A_{r,i_{q+1}} = 0,\ 0 \le r \le q^4 - 1\}$$

is the set of blocks of a 3-$(q^2+1, q+1, 1)$ design or Möbius plane $(\mathcal{M}, \mathcal{C})$.

Corollary 4.1.3. Let $(\mathcal{M}, \mathcal{C})$ be the Möbius plane corresponding to $G^{q+1}_{q^2+1}$, defined in Remark 4.1.2. The array $A(G^{q+1}_{q^2+1})$ for $m = 4$ in Construction 3.1.1 is an $\mathrm{OA}_q(q^4; 3, q^2+1, q) = \mathrm{CA}_q(q^4; 3, q^2+1, q)$, and any 4-set of columns not covered corresponds to a 4-set of points that are in a unique block of $\mathcal{C}$.

Proof. Proposition 4.1.1 implies any 3 distinct columns of $G^{q+1}_{q^2+1}$ are linearly independent. Then, Theorem 3.1.5 combined with the definition of $(\mathcal{M}, \mathcal{C})$ yields the result. ∎

For $q = 5$, the generator matrix $G^{q+1}_{q^2+1}$ and Möbius plane of order q are displayed in Fig. 4.1 and Table 4.2. In Table 4.2, the blocks of the Möbius plane containing zero element is shown in bold. Other blocks can be obtained using the translates of those blocks.

Figure 4.1: The generator matrix $G^{q+1}_{q^2+1}$ for $q = 5$. Here $\beta = \alpha^{q+1}$.

$G^6_{26} =$

β^0	β^1	β^2	β^3	β^4	β^5	β^6	β^7	β^8	β^9	β^{10}	β^{11}	β^{12}	β^{13}	β^{14}	β^{15}	β^{16}	β^{17}	β^{18}	β^{19}	β^{20}	β^{21}	β^{22}	β^{23}	β^{24}	β^{25}
1	2	1	2	0	0	4	0	3	2	4	4	2	0	4	0	0	1	1	4	4	1	2	1	4	4
0	2	2	3	3	2	4	2	3	3	4	3	4	3	0	0	1	0	2	3	1	1	3	0	1	0
0	4	0	4	4	0	4	3	3	3	3	2	0	4	4	3	0	1	3	1	2	4	4	0	1	2
0	3	1	3	0	3	4	2	4	1	2	4	0	2	2	2	1	1	4	1	0	4	1	1	0	0

Table 4.2: Blocks of the Möbius plane $(\mathcal{M}, \mathcal{C})$ of order $q = 5$, with point set $\mathcal{M} = \{i : 0 \leq i \leq 25, i \in \mathbb{Z}\}$; blocks containing 0 are in bold.

{0, 2, 4, 9, 15, 21}	$\{3, 5, 6, 20, 21, 23\}$	**{0, 6, 11, 13, 15, 20}**	**{0, 5, 7, 9, 14, 20}**
$\{1, 3, 5, 10, 16, 22\}$	$\{4, 6, 7, 21, 22, 24\}$	$\{1, 7, 12, 14, 16, 21\}$	$\{1, 6, 8, 10, 15, 21\}$
$\{2, 4, 6, 11, 17, 23\}$	$\{5, 7, 8, 22, 23, 25\}$	$\{2, 8, 13, 15, 17, 22\}$	$\{2, 7, 9, 11, 16, 22\}$
$\{3, 5, 7, 12, 18, 24\}$	**{0, 6, 12, 17, 19, 21}**	$\{3, 9, 14, 16, 18, 23\}$	$\{3, 8, 10, 12, 17, 23\}$
$\{4, 6, 8, 13, 19, 25\}$	$\{1, 7, 13, 18, 20, 22\}$	$\{4, 10, 15, 17, 19, 24\}$	$\{4, 9, 11, 13, 18, 24\}$
{0, 1, 10, 19, 20, 23}	$\{2, 8, 14, 19, 21, 23\}$	$\{5, 11, 16, 18, 20, 25\}$	$\{5, 10, 12, 14, 19, 25\}$
$\{1, 2, 11, 20, 21, 24\}$	$\{3, 9, 15, 20, 22, 24\}$	**{0, 3, 5, 8, 15, 19}**	**{0, 3, 10, 14, 21, 24}**
$\{2, 3, 12, 21, 22, 25\}$	$\{4, 10, 16, 21, 23, 25\}$	$\{1, 4, 6, 9, 16, 20\}$	$\{1, 4, 11, 15, 22, 25\}$
{0, 6, 8, 9, 23, 24}	**{0, 1, 15, 16, 18, 24}**	$\{2, 5, 7, 10, 17, 21\}$	**{0, 3, 4, 13, 22, 23}**
$\{1, 7, 9, 10, 24, 25\}$	$\{1, 2, 16, 17, 19, 25\}$	$\{3, 6, 8, 11, 18, 22\}$	$\{1, 4, 5, 14, 23, 24\}$
{0, 9, 18, 19, 22, 25}	**{0, 14, 15, 17, 23, 25}**	$\{4, 7, 9, 12, 19, 23\}$	$\{2, 5, 6, 15, 24, 25\}$
{0, 2, 7, 13, 19, 24}	**{0, 7, 10, 12, 15, 22}**	$\{5, 8, 10, 13, 20, 24\}$	**{0, 1, 3, 9, 11, 12}**
$\{1, 3, 8, 14, 20, 25\}$	$\{1, 8, 11, 13, 16, 23\}$	$\{6, 9, 11, 14, 21, 25\}$	$\{1, 2, 4, 10, 12, 13\}$
{0, 5, 11, 17, 22, 24}	$\{2, 9, 12, 14, 17, 24\}$	**{0, 1, 2, 6, 14, 22}**	$\{2, 3, 5, 11, 13, 14\}$
$\{1, 6, 12, 18, 23, 25\}$	$\{3, 10, 13, 15, 18, 25\}$	$\{1, 2, 3, 7, 15, 23\}$	$\{3, 4, 6, 12, 14, 15\}$
{0, 8, 12, 13, 14, 18}	**{0, 9, 10, 13, 16, 17}**	$\{2, 3, 4, 8, 16, 24\}$	$\{4, 5, 7, 13, 15, 16\}$
$\{1, 9, 13, 14, 15, 19\}$	$\{1, 10, 11, 14, 17, 18\}$	$\{3, 4, 5, 9, 17, 25\}$	$\{5, 6, 8, 14, 16, 17\}$
$\{2, 10, 14, 15, 16, 20\}$	$\{2, 11, 12, 15, 18, 19\}$	**{0, 1, 5, 13, 21, 25}**	$\{6, 7, 9, 15, 17, 18\}$
$\{3, 11, 15, 16, 17, 21\}$	$\{3, 12, 13, 16, 19, 20\}$	**{0, 1, 4, 7, 8, 17}**	$\{7, 8, 10, 16, 18, 19\}$
$\{4, 12, 16, 17, 18, 22\}$	$\{4, 13, 14, 17, 20, 21\}$	$\{1, 2, 5, 8, 9, 18\}$	$\{8, 9, 11, 17, 19, 20\}$
$\{5, 13, 17, 18, 19, 23\}$	$\{5, 14, 15, 18, 21, 22\}$	$\{2, 3, 6, 9, 10, 19\}$	$\{9, 10, 12, 18, 20, 21\}$
$\{6, 14, 18, 19, 20, 24\}$	$\{6, 15, 16, 19, 22, 23\}$	$\{3, 4, 7, 10, 11, 20\}$	$\{10, 11, 13, 19, 21, 22\}$
$\{7, 15, 19, 20, 21, 25\}$	$\{7, 16, 17, 20, 23, 24\}$	$\{4, 5, 8, 11, 12, 21\}$	$\{11, 12, 14, 20, 22, 23\}$
{0, 4, 11, 14, 16, 19}	$\{8, 17, 18, 21, 24, 25\}$	$\{5, 6, 9, 12, 13, 22\}$	$\{12, 13, 15, 21, 23, 24\}$
$\{1, 5, 12, 15, 17, 20\}$	**{0, 4, 5, 6, 10, 18}**	$\{6, 7, 10, 13, 14, 23\}$	$\{13, 14, 16, 22, 24, 25\}$
$\{2, 6, 13, 16, 18, 21\}$	$\{1, 5, 6, 7, 11, 19\}$	$\{7, 8, 11, 14, 15, 24\}$	**{0, 8, 16, 20, 21, 22}**
$\{3, 7, 14, 17, 19, 22\}$	$\{2, 6, 7, 8, 12, 20\}$	$\{8, 9, 12, 15, 16, 25\}$	$\{1, 9, 17, 21, 22, 23\}$
$\{4, 8, 15, 18, 20, 23\}$	$\{3, 7, 8, 9, 13, 21\}$	**{0, 4, 12, 20, 24, 25}**	$\{2, 10, 18, 22, 23, 24\}$
$\{5, 9, 16, 19, 21, 24\}$	$\{4, 8, 9, 10, 14, 22\}$	**{0, 2, 5, 12, 16, 23}**	$\{3, 11, 19, 23, 24, 25\}$
$\{6, 10, 17, 20, 22, 25\}$	$\{5, 9, 10, 11, 15, 23\}$	$\{1, 3, 6, 13, 17, 24\}$	**{0, 2, 8, 10, 11, 25}**
{0, 2, 3, 17, 18, 20}	$\{6, 10, 11, 12, 16, 24\}$	$\{2, 4, 7, 14, 18, 25\}$	**{0, 7, 11, 18, 21, 23}**
$\{1, 3, 4, 18, 19, 21\}$	$\{7, 11, 12, 13, 17, 25\}$	**{0, 3, 6, 7, 16, 25}**	$\{1, 8, 12, 19, 22, 24\}$
$\{2, 4, 5, 19, 20, 22\}$			$\{2, 9, 13, 20, 23, 25\}$

4.2 Existence of 3 anti-cocircular truncated Möbius planes

In this section, we introduce three truncated Möbius planes with the same point set but different circles. Then, we prove they are anti-cocircular.

We are interested in circles of the Möbius plane $(\mathcal{M}, \mathcal{C})$ in Remark 4.1.2, that contain the column index zero. We will present these circles in Proposition 4.2.4 using the elements of the set D that is given in Construction 4.2.1.

For the rest of the chapter, we assume q is an odd prime power and α is a primitive element of $\mathbb{F}_{q^4}$.

Construction 4.2.1 ([33, VI, chapter 18])**.** The set of integers $D = \{i \in \mathbb{Z}_{(q^4-1)/(q-1)} :$

$\mathrm{Tr}(\alpha^i) = 0\}$ is a $(\frac{q^4-1}{q-1}, \frac{q^3-1}{q-1}, \frac{q^2-1}{q-1})$-difference set over $\mathbb{Z}_{(q^4-1)/(q-1)}$. The set D can be constructed from a primitive polynomial $f(x) = x^4 + \sum_{j=1}^{4} b_j x^{4-j}$ over $\mathbb{F}_q$ with root α. Consider the recurrence relation $\gamma_j = -\sum_{j=1}^{4} b_j \gamma_{4-j}$ with the initial values $\gamma_j = \mathrm{Tr}(\alpha^j)$, for $0 \le j \le 3$. Then, $D = \{0 \le j \le \frac{q^4-1}{q-1} : \gamma_j = 0\}$.

The blocks of the 2-$(\frac{q^4-1}{q-1}, \frac{q^3-1}{q-1}, \frac{q^2-1}{q-1})$ design in Theorem 3.1.7 for $m = 4$ are the translates of D given in Construction 4.2.1.

Remark 4.2.2. By Construction 4.2.1 and the definition of trace, it is clear that $\mathrm{Tr}(\alpha^0) = \mathrm{Tr}(1) = m = 4 \neq 0$, because q is odd. Thus, $0 \notin D$.

Proposition 4.2.3. Let D be the difference set in Construction 4.2.1. The equation $\mathrm{Tr}(\alpha^{(q+1)x}) = 0$ has a unique solution $x = \frac{q^2+1}{2}$ for $0 \le x < q^2 + 1$. Thus, $x(q+1) \in D$ if and only if $x = \frac{q^2+1}{2}$.

Proof. Using Definition 2.2.18,

$$\begin{aligned}
\mathrm{Tr}\left(\alpha^{(q+1)x}\right) &= \alpha^{(q+1)x} + \left(\alpha^{(q+1)x}\right)^q + \left(\alpha^{(q+1)x}\right)^{q^2} + \left(\alpha^{(q+1)x}\right)^{q^3} \\
&= \alpha^{(q+1)x}\left(1 + \alpha^{(q-1)(q+1)x} + \alpha^{(q^2-1)(q+1)x} + \alpha^{(q^3-1)(q+1)x}\right) \\
&= \alpha^{(q+1)x}\left(1 + \alpha^{(q-1)(q+1)x} + \alpha^{(q^2-1)(q+1)x} + \alpha^{(q^2-1)qx}\right) \quad \left(\text{ since } \alpha^{q^4} = \alpha\right) \\
&= \alpha^{(q+1)x}\left(1 + \alpha^{q^3x-qx}\right)\left(1 + \alpha^{q^2x-x}\right).
\end{aligned}$$

Since $\alpha^{(q+1)x} \neq 0$, then $\mathrm{Tr}(\alpha^{(q+1)x}) = 0$ if and only if $1+\alpha^{q^3x-qx} = 0$ or $(1+\alpha^{q^2x-x}) = 0$. Note that $\alpha^{\frac{q^4-1}{2}} = -1$. If $(1 + \alpha^{q^3x-qx}) = 0$, then $\alpha^{q^3x-qx} = \alpha^{\frac{q^4-1}{2}}$ and $q^3x - qx = \frac{q^4-1}{2}$ modulo $q^4 - 1$. Thus, for some integer $\lambda \ge 0$, we have $q^3x - qx - (\frac{q^4-1}{2}) = \lambda(q^4 - 1)$ which leads to $2xq - (q^2 + 1) = 2\lambda(q^2 + 1)$. Hence, $2xq = (q^2 + 1)(2\lambda + 1)$. If $\lambda = 0$, then $x = \frac{q^2+1}{2q}$. Since q^2+1 is not divisible by q, there is no possible solution for x. If $\lambda \neq 0$, since $\gcd(q, q^2+1) = 1$, then $q \mid 2\lambda + 1$. By the assumption, $0 \le x < q^2 + 1$, so $(q^2 + 1)(2\lambda + 1) = 2xq < 2(q^2 + 1)q$ that gives $0 < 2\lambda + 1 < 2q$. Since $q \mid 2\lambda + 1$ and $0 < 2\lambda + 1 < 2q$, hence, we conclude that $q = 2\lambda+1$. Therefore, $x = \frac{q^2+1}{2}$. If $(1+\alpha^{q^2x-x}) = 0$, then $\alpha^{q^2x-x} = \alpha^{\frac{q^4-1}{2}}$ and $q^2x - x = \frac{q^4-1}{2}$ modulo $q^4 - 1$. Thus, for some integer $\lambda \ge 0$, we have $q^2x - x - (\frac{q^4-1}{2}) = \lambda(q^4 - 1)$ which leads to $2x - (q^2 + 1) = 2\lambda(q^2 + 1)$. Hence, $x = (q^2 + 1)(\frac{1}{2} + \lambda)$. Since $0 \le x < q^2 + 1$, we must have $\lambda < \frac{1}{2}$ which implies that $\lambda = 0$, and thus $x = \frac{q^2+1}{2}$. Therefore, we conclude that $x = \frac{q^2+1}{2}$ is the unique solution to the equation, which shows that $x(q+1) \in D$ if and only if $x = \frac{q^2+1}{2}$. ∎

Proposition 4.2.4. Let D be the difference set in Construction 4.2.1. For $x \in D$, let

$$C_x = \{i : x + (q+1)i \in D, 0 \le i < q^2 + 1\}. \tag{4.2.1}$$

Let $(\mathcal{M}, \mathcal{C})$ be the Möbius plane in Remark 4.1.2. Let $x_0 = \frac{(q^2+1)(q+1)}{2}$. Then $C_{x_0} = \{0\}$. Moreover, $\{C_x : x \in D \setminus \{x_0\}\} = \{B \in \mathcal{C} : 0 \in B\}$.

Proof. We prove $C_{x_0} = \{0\}$. By Proposition 4.2.3, $x_0 \in D$, so $0 \in C_{x_0}$. Let $a \in C_{x_0}$. Then $x_0 + (q+1)a = (q+1)(\frac{q^2+1}{2} + a) \in D$. This implies that $\mathrm{Tr}(\alpha^{(q+1)(\frac{q^2+1}{2}+a)}) = 0$ with $0 \leq a < q^2+1$. So, $\frac{q^2+1}{2}+a$ is a solution of the equation $\mathrm{Tr}(\alpha^{(q+1)x}) = 0$. By Proposition 4.2.3, $a = 0$. So, $C_{x_0} = \{0\}$.

Note that for any $B \in \mathcal{C}$, $B = \{i_1, i_2, \ldots, i_{q+1}\}$ is a set of column indices of $A = A(G^{q+1}_{q^2+1})$ where $A_{r,i_1} = A_{r,i_2} = \cdots = A_{r,i_{q+1}} = 0$ for a non-zero row r in $A(G^{q+1}_{q^2+1})$. Then, by Theorem 3.1.7, $(q+1)i_j \in D_r$, for all $i_j \in B$, where D_r is a block of the 2-$(\frac{q^4-1}{q-1}, \frac{q^3-1}{q-1}, \frac{q^2-1}{q-1})$ design $(\mathbb{Z}_{(q^4-1)/(q-1)}, \mathcal{B})$ defined in that theorem.

Let $\mathcal{A} = \{C_x : x \in D \setminus \{x_0\}\}$ and $\mathcal{C}^0 = \{B \in \mathcal{C} : 0 \in B\}$. First, we prove that $\mathcal{A} \subseteq \mathcal{C}^0$. By the definition of C_x, it is clear that $0 \in C_x$. For all $i \in C_x$, $(q+1)i \in D - x$ where $D - x \in \mathcal{B}$, which implies that $C_x \in \mathcal{C}^0$. Now, we prove $\mathcal{C}^0 \subseteq \mathcal{A}$. Let $B = \{i_1, i_2, \ldots, i_{q+1}\} \in \mathcal{C}^0$ such that $i_j = 0$ for some $1 \leq j \leq q+1$. Since $A_{r,i_1} = A_{r,i_2} = \cdots = A_{r,i_{q+1}} = 0$ for a non-zero row r in $A(G^{q+1}_{q^2+1})$, $(q+1)i_j \in D_r$ for all $i_j \in B$ where $D_r \in \mathcal{B}$. Since D_r is a translate of D, then there exists $x \in \mathbb{Z}_{(q^4-1)/(q-1)}$ such that $D = D_r + x$. So, $x + (q+1)i_j \in D$. Since $0 \in D_r$, then $x \in D$ which implies that $B = C_x$. ∎

An example of the set D for $q = 5$ and corresponding C_x for each $x \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$ is given in Table 4.3. The blocks in Table 4.2 that are shown in bold are precisely the sets C_x for $x \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$.

In the following, we study some properties of the Möbius plane in Remark 4.1.2 and its circles, especially the circles containing the zero element given by Eq. (4.2.1).

Remark 4.2.5. If $0, i, j, k \in C_x$, then by Theorem 3.1.5, there exist non-zero $a, b, c \in \mathbb{F}_q$ such that $1 + a\alpha^{i(q+1)} + b\alpha^{j(q+1)} + c\alpha^{k(q+1)} = 0$. By multiplying $\alpha^{d(q+1)}$ to both sides, we obtain a block B which is a translate of C_x such that $d, i+d, j+d, k+d \in B$ for $1 \leq d$.

Proposition 4.2.6. If $0, i, -i, j \in C_x$, $i, j \notin \left\{0, \frac{q^2+1}{2}\right\}$, then $-j \in C_x$.

Proof. Since $0, i, -i, j \in C_x$, by Theorem 3.1.5, then $\{\alpha^x, \alpha^{x+i(q+1)}, \alpha^{x-i(q+1)}, \alpha^{x+j(q+1)}\}$ are linearly dependent, so there exist non-zero $a, b, c \in \mathbb{F}_q$ such that

$$1 + a\alpha^{i(q+1)} + b\alpha^{-i(q+1)} + c\alpha^{j(q+1)} = 0. \tag{4.2.2}$$

Let $\beta = \alpha^{(q+1)(q^2+1)}$, a primitive element in $\mathbb{F}_q$ (See Remark 2.2.14). By raising both sides of the Eq. (4.2.2) to the power of q^2, we have

$$\left(1 + a\alpha^{i(q+1)} + b\alpha^{-i(q+1)} + c\alpha^{j(q+1)}\right)^{q^2} = 1 + a\alpha^{i(q+1)q^2} + b\alpha^{-i(q+1)q^2} + c\alpha^{j(q+1)q^2} = 0.$$

For $0 \leq i < q^2 + 1$, $\alpha^{i(q+1)q^2} = \beta^i \alpha^{-i(q+1)}$ where powers are modulo $q^4 - 1$. So,

$$1 + (a\beta^i)\alpha^{-i(q+1)} + (b\beta^{-i})\alpha^{i(q+1)} + (c\beta^j)\alpha^{-j(q+1)} = 0. \tag{4.2.3}$$

Since $\beta \in \mathbb{F}_q$, Eq. (4.2.3) shows that there exist a block B in 3-$(q^2+1, q+1, 1)$ design such that $0, i, -i, -j \in B$. Since $0, i, -i$ determine a unique block C_x, then $0, i, -i, j, -j \in C_x$. ∎

Table 4.3: List of elements of the set D constructed in Construction 4.2.1 and circles containing zero of $(\mathcal{M}, \mathcal{C})$, $M_{1/2}$, M_1, and M_2, for $q = 5$.

$D = \{1, 5, 8, 11, 13, 25, 39, 40, 44, 55, 56, 62, 64, 65, 78, 87, 91, 106, 111, 117, 119, 123, 124, 125, 127, 136, 143, 146, 147, 152, 154\}$

$x \in D \setminus \{78\}$	C_x	$C_{x,1/2} = 2C_x \cap \mathcal{M}^{(e)}$	$C_{x,1} = C_x \cap \mathcal{M}^{(e)}$	$C_{x,2} = (C_x \cap \mathcal{M}^{(e)})/2$
1	$\{0, 2, 4, 9, 15, 21\}$	$\{0, 4, 8, 18\}$	$\{0, 2, 4\}$	$\{0, 2, 14\}$
5	$\{0, 1, 10, 19, 20, 23\}$	$\{0, 2, 20\}$	$\{0, 10, 20\}$	$\{0, 10, 18\}$
8	$\{0, 6, 8, 9, 23, 24\}$	$\{0, 12, 16, 18\}$	$\{0, 6, 8, 24\}$	$\{0, 4, 12, 16\}$
11	$\{0, 9, 18, 19, 22, 25\}$	$\{0, 18\}$	$\{0, 18, 22\}$	$\{0, 22, 24\}$
13	$\{0, 2, 7, 13, 19, 24\}$	$\{0, 4, 14\}$	$\{0, 2, 24\}$	$\{0, 12, 14\}$
25	$\{0, 5, 11, 17, 22, 24\}$	$\{0, 10, 22\}$	$\{0, 22, 24\}$	$\{0, 12, 24\}$
39	$\{0, 8, 12, 13, 14, 18\}$	$\{0, 16, 24\}$	$\{0, 8, 12, 14, 18\}$	$\{0, 4, 6, 20, 22\}$
40	$\{0, 4, 11, 14, 16, 19\}$	$\{0, 8, 22\}$	$\{0, 4, 14, 16\}$	$\{0, 2, 8, 20\}$
44	$\{0, 2, 3, 17, 18, 20\}$	$\{0, 4, 6\}$	$\{0, 2, 18, 20\}$	$\{0, 10, 14, 22\}$
55	$\{0, 6, 12, 17, 19, 21\}$	$\{0, 12, 24\}$	$\{0, 6, 12\}$	$\{0, 6, 16\}$
56	$\{0, 1, 15, 16, 18, 24\}$	$\{0, 2\}$	$\{0, 16, 18, 24\}$	$\{0, 8, 12, 22\}$
62	$\{0, 14, 15, 17, 23, 25\}$	$\{0\}$	$\{0, 14\}$	$\{0, 20\}$
64	$\{0, 7, 10, 12, 15, 22\}$	$\{0, 14, 20, 24\}$	$\{0, 10, 12, 22\}$	$\{0, 6, 18, 24\}$
65	$\{0, 9, 10, 13, 16, 17\}$	$\{0, 18, 20\}$	$\{0, 10, 16\}$	$\{0, 8, 18\}$
87	$\{0, 4, 5, 6, 10, 18\}$	$\{0, 8, 10, 12, 20\}$	$\{0, 4, 6, 10, 18\}$	$\{0, 2, 16, 18, 22\}$
91	$\{0, 6, 11, 13, 15, 20\}$	$\{0, 12, 22\}$	$\{0, 6, 20\}$	$\{0, 10, 16\}$
106	$\{0, 3, 5, 8, 15, 19\}$	$\{0, 6, 10, 16\}$	$\{0, 8\}$	$\{0, 4\}$
111	$\{0, 1, 2, 6, 14, 22\}$	$\{0, 2, 4, 12\}$	$\{0, 2, 6, 14, 22\}$	$\{0, 14, 16, 20, 24\}$
117	$\{0, 1, 5, 13, 21, 25\}$	$\{0, 2, 10\}$	$\{0\}$	$\{0\}$
119	$\{0, 1, 4, 7, 8, 17\}$	$\{0, 2, 8, 14, 16\}$	$\{0, 4, 8\}$	$\{0, 2, 4\}$
123	$\{0, 4, 12, 20, 24, 25\}$	$\{0, 8, 24\}$	$\{0, 4, 12, 20, 24\}$	$\{0, 2, 6, 10, 12\}$
124	$\{0, 2, 5, 12, 16, 23\}$	$\{0, 4, 10, 24\}$	$\{0, 2, 12, 16\}$	$\{0, 6, 8, 14\}$
125	$\{0, 3, 6, 7, 16, 25\}$	$\{0, 6, 12, 14\}$	$\{0, 6, 16\}$	$\{0, 8, 16\}$
127	$\{0, 5, 7, 9, 14, 20\}$	$\{0, 10, 14, 18\}$	$\{0, 14, 20\}$	$\{0, 10, 20\}$
136	$\{0, 3, 10, 14, 21, 24\}$	$\{0, 6, 20\}$	$\{0, 10, 14, 24\}$	$\{0, 12, 18, 20\}$
143	$\{0, 3, 4, 13, 22, 23\}$	$\{0, 6, 8\}$	$\{0, 4, 22\}$	$\{0, 2, 24\}$
146	$\{0, 1, 3, 9, 11, 12\}$	$\{0, 2, 6, 18, 22, 24\}$	$\{0, 12\}$	$\{0, 6\}$
147	$\{0, 8, 16, 20, 21, 22\}$	$\{0, 16\}$	$\{0, 8, 16, 20, 22\}$	$\{0, 4, 8, 10, 24\}$
152	$\{0, 2, 8, 10, 11, 25\}$	$\{0, 4, 16, 20, 22\}$	$\{0, 2, 8, 10\}$	$\{0, 4, 14, 18\}$
154	$\{0, 7, 11, 18, 21, 23\}$	$\{0, 14, 22\}$	$\{0, 18\}$	$\{0, 22\}$

In Table 4.3, $C_{13} = \{0, 2, 7, 13, 19, 24\}$, $C_{39} = \{0, 8, 12, 13, 14, 18\}$, $C_{65} = \{0, 9, 10, 13, 16, 17\}$, $C_{91} = \{0, 6, 11, 13, 15, 20\}$, $C_{117} = \{0, 1, 5, 13, 21, 25\}$, $C_{143} = \{0, 3, 4, 13, 22, 23\}$ are all the blocks satisfying the hypotheses of Proposition 4.2.6. Each of these blocks contains pairs of points in the form $\{i, -i\}$ module 26.

Proposition 4.2.7. Suppose $0, \frac{q^2+1}{2} \in C_x$, then for any $i \in C_x$, $-i \in C_x$.

Proof. Since $0, \frac{q^2+1}{2} \in C_x$, then $x, x + \frac{q^2+1}{2}(q+1) \in D$. So, $\mathrm{Tr}(\alpha^x) = \mathrm{Tr}\left(\alpha^{x+\frac{q^2+1}{2}(q+1)}\right) = 0$. We have

$$\mathrm{Tr}(\alpha^x) = \alpha^x + \alpha^{xq} + \alpha^{xq^2} + \alpha^{xq^3} = 0. \tag{4.2.4}$$

Since $\alpha^{\frac{q^2+1}{2}(q+1)(q-1)} = \alpha^{\frac{q^4-1}{2}} = -1$ and q is odd, we have $\left(\alpha^{\frac{q^2+1}{2}(q+1)}\right)^q = -\alpha^{\frac{q^2+1}{2}(q+1)}$ and $\left(\alpha^{\frac{q^2+1}{2}(q+1)}\right)^{q^2} = \alpha^{\frac{q^2+1}{2}(q+1)}$, which yields

$$\mathrm{Tr}\left(\alpha^{x+\frac{q^2+1}{2}(q+1)}\right) = \alpha^{\frac{q^2+1}{2}(q+1)}\left(\alpha^x - \alpha^{xq} + \alpha^{xq^2} - \alpha^{xq^3}\right) = 0, \tag{4.2.5}$$

and hence

$$\alpha^x - \alpha^{xq} + \alpha^{xq^2} - \alpha^{xq^3} = 0. \tag{4.2.6}$$

By adding Eq. (4.2.4) and Eq. (4.2.6), we obtain $2(\alpha^x + \alpha^{xq^2}) = 0$. So, we have

$$\alpha^x = -\alpha^{xq^2}, \qquad \alpha^{xq} = -\alpha^{xq^3}. \tag{4.2.7}$$

Let $i \in C_x$. Then $x + i(q+1) \in D$. So,

$$\mathrm{Tr}\left(\alpha^{x+i(q+1)}\right) = \alpha^x\alpha^{i(q+1)} + \alpha^{xq}\alpha^{iq(q+1)} + \alpha^{xq^2}\alpha^{iq^2(q+1)} + \alpha^{xq^3}\alpha^{iq^3(q+1)} = 0. \tag{4.2.8}$$

Let $\beta = \alpha^{(q+1)(q^2+1)} \in \mathbb{F}_q$. We multiply both sides of Eq. (4.2.8) by β^{-i}. For $0 \le i < q^2+1$, we have $\beta^{-i}\alpha^{i(q+1)} = \alpha^{-iq^2(q+1)}$ where powers are modulo $q^4 - 1$. So, we obtain

$$\alpha^x\alpha^{-iq^2(q+1)} + \alpha^{xq}\alpha^{-iq^3(q+1)} + \alpha^{xq^2}\alpha^{-i(q+1)} + \alpha^{xq^3}\alpha^{-iq(q+1)} = 0. \tag{4.2.9}$$

By replacing the coefficients using Eq. (4.2.7), we have

$$-\alpha^{xq^2}\alpha^{-iq^2(q+1)} - \alpha^{xq^3}\alpha^{-iq^3(q+1)} - \alpha^x\alpha^{-i(q+1)} - \alpha^{xq}\alpha^{-iq(q+1)} = 0. \tag{4.2.10}$$

Eq. (4.2.10) shows that $\mathrm{Tr}(\alpha^{x-i(q+1)}) = 0$. This means that $x - i(q+1) \in D$ and $-i \in C_x$. ∎

In Table 4.3, $C_{13} = \{0, 2, 7, 13, 19, 24\}$, $C_{39} = \{0, 8, 12, 13, 14, 18\}$, $C_{65} = \{0, 9, 10, 13, 16, 17\}$, $C_{91} = \{0, 6, 11, 13, 15, 20\}$, $C_{117} = \{0, 1, 5, 13, 21, 25\}$, $C_{143} = \{0, 3, 4, 13, 22, 23\}$ are all the blocks that contain $0, 13$. The other elements come in pairs $\{i, -i\}$, as shown in Proposition 4.2.7.

Proposition 4.2.8. If $0, i, -i \in C_x$, $i \neq 0, \frac{q^2+1}{2}$, then $2i \notin C_x$.

Proof. Let $\beta = \alpha^{(q+1)(q^2+1)} \in \mathbb{F}_q$. By contradiction, suppose $2i \in C_x$. So, $\{\alpha^x, \alpha^{x+i(q+1)}, \alpha^{x-i(q+1)}, \alpha^{x+2i(q+1)}\}$ are linearly dependent, and there exist non-zero $a, b, c \in \mathbb{F}_q$ such that

$$1 + a\alpha^{-i(q+1)} + b\alpha^{i(q+1)} + c\alpha^{2i(q+1)} = 0. \tag{4.2.11}$$

By raising both sides of the Eq. (4.2.11) to the power of q^2, we have

$$1 + a\beta^{-i}\alpha^{i(q+1)} + b\beta^{i}\alpha^{-i(q+1)} + c\beta^{2i}\alpha^{-2i(q+1)} = 0. \tag{4.2.12}$$

By subtracting Eq. (4.2.11) from Eq. (4.2.12), we have

$$\begin{aligned}(b - a\beta^{-i})\left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right) + c\left(\alpha^{2i(q+1)} - \beta^{2i}\alpha^{-2i(q+1)}\right) = \\ (b - a\beta^{-i})\left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right) + c\left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right)\left(\alpha^{i(q+1)} + \beta^{i}\alpha^{-i(q+1)}\right) = \\ \left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right)\left(b - a\beta^{-i} + c\left(\alpha^{i(q+1)} + \beta^{i}\alpha^{-i(q+1)}\right)\right) = 0.\end{aligned}$$

If $\left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right) = 0$, then $\alpha^{2i(q+1)} = \alpha^{i(q^2+1)(q+1)}$, which leads to $\alpha^{i(q+1)(q^2-1)} = 1$. So, $q^4 - 1 \mid i(q^2-1)(q+1)$ and hence $q^2 + 1 \mid i(q+1)$. Since $\gcd(q^2+1, q+1) = 2$, $i = l(\frac{q^2+1}{2})$ for some $l \in \mathbb{Z}$. Since $i \neq 0, \frac{q^2+1}{2}$, and $0 \leq i < \frac{q^2+1}{2}$, then there exists no such l, and $\left(\alpha^{i(q+1)} - \beta^{i}\alpha^{-i(q+1)}\right) \neq 0$. So, $\left(b - a\beta^{-i} + c\left(\alpha^{i(q+1)} + \beta^{i}\alpha^{-i(q+1)}\right)\right) = 0$. Since $b - a\beta^{-i}, c \in \mathbb{F}_q$, then $\alpha^{i(q+1)} + \beta^{i}\alpha^{-i(q+1)} \in \mathbb{F}_q$. Let $f(x) = (x - \alpha^{i(q+1)})(x - \beta^{i}\alpha^{-i(q+1)})$ be a polynomial over $\mathbb{F}_q$. Since $\alpha^{i(q+1)}$ is a root of f, we obtain that $\alpha^{i(q+1)} \in \mathbb{F}_{q^2}$. So, $\alpha^{i(q+1)(q^2-1)} = 1$. Then $q^4 - 1 \mid i(q+1)(q^2-1)$, which implies that $q^2 + 1 \mid i(q+1)$. Since $\gcd(q^2+1, q+1) = 2$ and $0 < i < q^2 + 1$, then $i = \frac{q^2+1}{2}$ which contradicts with $i \neq \frac{q^2+1}{2}$. We obtained that $2i \notin C_x$. ∎

In Table 4.3, $C_{13} = \{0, 2, 7, 13, 19, 24\}$, $C_{39} = \{0, 8, 12, 13, 14, 18\}$, $C_{65} = \{0, 9, 10, 13, 16, 17\}$, $C_{91} = \{0, 6, 11, 13, 15, 20\}$, $C_{117} = \{0, 1, 5, 13, 21, 25\}$, $C_{143} = \{0, 3, 4, 13, 22, 23\}$ are all the blocks that contain $0, i, -i$ for any $i \neq 0, 13$, where $i \in \{0, 1, 2, \ldots, 25\}$. Proposition 4.2.8, guarantees no such block contains $2i$.

Lemma 4.2.9. There exists no $x \in D$ such that $\left\{0, k, \frac{q^2+1}{2}, k + \frac{q^2+1}{2}\right\} \subseteq C_x$ for any $k \neq 0$. Furthermore, there exists no block B in 3-$(q^2+1, q+1, 1)$ design in Remark 4.1.2 such that $\left\{i, j, i + \frac{q^2+1}{2}, j + \frac{q^2+1}{2}\right\} \subseteq B$.

Proof. By contradiction, suppose there exists $x \in D$ such that $\left\{0, k, \frac{q^2+1}{2}, k + \frac{q^2+1}{2}\right\} \subseteq C_x$. Since $0, \frac{q^2+1}{2} \in C_x$, by Proposition 4.2.7, $-k \in C_x$, so $\left\{-k, 0, k, \frac{q^2+1}{2}, k + \frac{q^2+1}{2}\right\} \subseteq C_x$. By picking $d = k$ in Remark 4.2.5, there exists a block B such that $\left\{0, k, 2k, k + \frac{q^2+1}{2}, 2k + \frac{q^2+1}{2}\right\} \subseteq B$. Since any three elements determine a unique block and $\left\{0, k, k + \frac{q^2+1}{2}\right\} \subseteq C_x$ and $\left\{0, k, k + \frac{q^2+1}{2}\right\} \subseteq B$, then $C_x = B$. Therefore, $\{-k, 0, k, 2k\} \subseteq C_x$ which is a contradiction by Proposition 4.2.8. So, there exist no $x \in D$ such that $\left\{0, k, \frac{q^2+1}{2}, k + \frac{q^2+1}{2}\right\} \subseteq C_x$. For the second part, pick $d = -i$ in Remark 4.2.5. So, if there exist $x \in D$ such that $\left\{0, j - i, \frac{q^2+1}{2}, j - i + \frac{q^2+1}{2}\right\} \subseteq C_x$, then by letting $k = j - i$, the contradiction is obtained by the first part. ∎

Lemma 4.2.9 is illustrated by the example in Table 4.3. The blocks C_x that contain $\{0, 13\}$ do not contain any other pair of points whose difference is 13.

Proposition 4.2.10. There exists no $x \in D$ such that $\{0, i, j, 2i, 2j\} \subseteq C_x$, where $|\{0, i, j, 2i, 2j\}| = 5$.

Proof. By contradiction, suppose there exists x such that $\{0, i, j, 2i, 2j\} \subseteq C_x$. Then by picking $d = -i$ in Remark 4.2.5, there exists a block B such that $\{-i, 0, j - i, i\} \subseteq B$. By Proposition 4.2.6, $i - j \in B$, which implies $2i - j \in C_x$. This implies that by picking $d = -j$ in Remark 4.2.5, there exists a block B' such that $\{-j, i - j, 0, j, 2(i - j)\} \subseteq B'$. By Proposition 4.2.6, $j - i \in B'$. Therefore, $\{i - j, 0, j - i, 2(i - j)\} \subseteq B'$, which is impossible by Proposition 4.2.8. ∎

The example in Table 4.3 can be inspected to verify Proposition 4.2.10. For each $i \in \{1, 2, \ldots, 25\}$, the unique block containing $0, i, 2i$ does not contain $j, 2j$ for any other j where $j, 2j \notin \{0, i, 2i\}$.

Construction 4.2.11. Let $\mathcal{M}^{(e)} = \{i : i \equiv 0 \pmod 2, 0 \leq i < q^2 + 1\}$. The set $\mathcal{M}^{(e)}$ is a subset of $\mathcal{M}$ associated to the Möbius plane $(\mathcal{M}, \mathcal{C})$ given in Remark 4.1.2. Let D be the associated difference set given in Construction 4.2.1. We define three truncated Möbius planes on the same set of points $\mathcal{M}^{(e)}$. The truncation removes odd points from $\mathcal{M}$ and corresponding blocks. Denote for any $C \in \mathcal{C}$, $2C = \{2i : i \in C\}$, and $(C \cap \mathcal{M}^{(e)})/2 = \{i/2 : i \in C \cap \mathcal{M}^{(e)}, i \equiv 0 \pmod 4\} \cup \{(i + q^2 + 1)/2 : i \in C \cap \mathcal{M}^{(e)}, i \equiv 2 \pmod 4\}$.

1. $M_1 = (\mathcal{M}^{(e)}, \{C \cap \mathcal{M}^{(e)} : C \in \mathcal{C}\})$. Circles containing zero can be expressed as follows: for any $x \in D$, $C_{x,1} = C_x \cap \mathcal{M}^{(e)} = \{i : x + (q+1)i \in D, i \equiv 0 \pmod 2, 0 \leq i < q^2 + 1\}$.
2. $M_2 = (\mathcal{M}^{(e)}, \{(C \cap \mathcal{M}^{(e)})/2 : C \in \mathcal{C}\})$. Circles containing zero can be expressed as follows: for any $x \in D$, $C_{x,2} = (C_x \cap \mathcal{M}^{(e)})/2 = \{i : x + 2(q+1)i \in D, i \equiv 0 \pmod 2, 0 \leq i < q^2 + 1\}$.
3. $M_{1/2} = (\mathcal{M}^{(e)}, \{2C \cap \mathcal{M}^{(e)} : C \in \mathcal{C}\})$. Circles containing zero can be expressed as follows: for any $x \in D$, $C_{x,1/2} = 2C_x \cap \mathcal{M}^{(e)} = \{i : x + \frac{1}{2}(q+1)i \in D, i \equiv 0 \pmod 2, 0 \leq i < q^2 + 1\}$.

Remark 4.2.12. It is important to note that $G^{q+1}_{q^2+1}$ is in correspondence to $(\mathcal{M}, \mathcal{C})$ and $G^{q+1}_{\frac{q^2+1}{2}}$, $G^{2(q+1)}_{\frac{q^2+1}{2}}$, and $G^{4(q+1)}_{\frac{q^2+1}{2}}$ with columns labeled with even integers $0, 2, \ldots, q^2 - 1$ are in correspondence with $M_{1/2}$, M_1, and M_2, respectively. Since each of $G^{q+1}_{\frac{q^2+1}{2}}$, $G^{2(q+1)}_{\frac{q^2+1}{2}}$, and $G^{4(q+1)}_{\frac{q^2+1}{2}}$ is a subarray of $G^{q+1}_{q^2+1}$, having half of its columns, $M_{1/2}$, M_1, and M_2 are each a truncated Möbius plane. See Fig. 4.2 and Table 4.3 for an example for $q = 5$. Table 4.3 displays $C_{x,1}$, $C_{x,2}$, and $C_{x,1/2}$ for $q = 5$.

Each block of the 2-$(q^3 + q^2 + q + 1, q^2 + q + 1, q + 1)$ design in Theorem 3.1.7 for $m = 4$ corresponds to a plane in $\mathrm{PG}(3, q)$, and each C_x for $x \in D$ corresponds to the intersection

Figure 4.2: Generator matrices for truncated Möbius planes for $q = 5$ ($\beta = \alpha^{q+1}$)

	0	2	4	6	8	10	12	14	16	18	20	22	24	
$G^{q+1}_{\frac{q^2+1}{2}} =$	β^0	β^1	β^2	β^3	β^4	β^5	β^6	β^7	β^8	β^9	β^{10}	β^{11}	β^{12}	$M_{1/2}$
$G^{2(q+1)}_{\frac{q^2+1}{2}} =$	β^0	β^2	β^4	β^6	β^8	β^{10}	β^{12}	β^{14}	β^{16}	β^{18}	β^{20}	β^{22}	β^{24}	M_1
$G^{4(q+1)}_{\frac{q^2+1}{2}} =$	β^0	β^4	β^8	β^{12}	β^{16}	β^{20}	β^{24}	β^2	β^6	β^{10}	β^{14}	β^{18}	β^{22}	M_2

of a plane in $\mathrm{PG}(3, q)$ and the ovoid O in Proposition 4.1.1. Our goal is to connect C_x with a hypersurface in $\mathrm{PG}(3, q)$ and show that M_1, M_2, and $M_{1/2}$ are 3 truncated Möbius planes with the same point sets where the common intersection of any choice of blocks, one from each plane, has at most size three.

We start by introducing a linear transformation Ω that changes the coordinates of any $L(\alpha^i) \in \mathbb{F}_q^4$ to new coordinates in $\mathbb{F}_{q^4}^4$.

A *Singer cycle* of a finite projective space $\mathrm{PG}(m-1, q)$ is a collineation δ such that the group $\langle\delta\rangle$ acts regularly on the points (and hyperplanes) of $\mathrm{PG}(m-1, q)$. The group $G = \langle\delta\rangle$ is then called a *Singer group*.

Let $f(x) = x^4 - ax^3 - bx^2 - cx - d$ be a degree-4 primitive polynomial over $\mathbb{F}_q$ with root α. Let $\delta : \mathbb{F}_{q^4} \to \mathbb{F}_{q^4}$ be the map where $\delta(\alpha^l) = \alpha^{l+1}$ for $0 \le l < (q^2+1)(q+1)$. The Singer group $G = \langle\delta\rangle$ is of order $(q^2+1)(q+1)$ and acts regularly on the points of $\mathrm{PG}(3, q)$. The matrix corresponding to δ is

$$A = \begin{bmatrix} 0 & 0 & 0 & d \\ 1 & 0 & 0 & c \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & a \end{bmatrix}. \tag{4.2.13}$$

Let

$$\Omega = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^q & \alpha^{2q} & \alpha^{3q} \\ 1 & \alpha^{q^2} & \alpha^{2q^2} & \alpha^{3q^2} \\ 1 & \alpha^{q^3} & \alpha^{2q^3} & \alpha^{3q^3} \end{bmatrix}. \tag{4.2.14}$$

Then, Ω is a linear transformation that diagonalizes the map $\delta(\alpha^i) = \alpha^{i+1}$, i.e.,

$$S = \begin{bmatrix} \alpha & 0 & 0 & 0 \\ 0 & \alpha^q & 0 & 0 \\ 0 & 0 & \alpha^{q^2} & 0 \\ 0 & 0 & 0 & \alpha^{q^3} \end{bmatrix} = \Omega A \Omega^{-1}, \tag{4.2.15}$$

where each column of Ω corresponds to each left eigenvector of A. It is clear that $\Omega(L(\alpha^i)) = \left[\alpha^i, \alpha^{iq}, \alpha^{iq^2}, \alpha^{iq^3}\right]^T \in \mathbb{F}_{q^4}^4$. Since Ω is a linear transformation, it preserves the linear dependence relations after transformation, so Ω induces a collineation of $\mathrm{PG}(3, q)$.

Proposition 4.2.13 can be considered an extension of [2, Theorem 3.2] from $\mathrm{PG}(2,q)$ to $\mathrm{PG}(3,q)$.

Proposition 4.2.13. Let $\frac{m}{n} \in \mathbb{Q}$ in lowest terms ($\gcd(m,n)=1$). Suppose $0, i', j', k' \in C_s$ for some $s \in D$, and $i, j, k \in \mathbb{Z}_{(q^2+1)(q+1)}$ such that $mi = ni'$, $mj = nj'$, and $mk = nk'$. Then $\Omega(L(\alpha^0))$, $\Omega(L(\alpha^{i(q+1)}))$, $\Omega(L(\alpha^{j(q+1)}))$, and $\Omega(L(\alpha^{k(q+1)}))$ satisfy the equation $\alpha^s x^{\frac{m}{n}} + \alpha^{sq} y^{\frac{m}{n}} + \alpha^{sq^2} z^{\frac{m}{n}} + \alpha^{sq^3} t^{\frac{m}{n}} = 0$.

Proof. Let $\pi_0 = \mathrm{PG}(3,q)$ and $\pi = \mathrm{PG}(3,q^4)$. The Singer group G induces a collineation that fixes π_0. We introduce new coordinates such that

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} \to \begin{bmatrix}1\\1\\1\\1\end{bmatrix}, \begin{bmatrix}0\\1\\0\\0\end{bmatrix} \to \begin{bmatrix}\alpha\\\alpha^q\\\alpha^{q^2}\\\alpha^{q^3}\end{bmatrix}, \begin{bmatrix}0\\0\\1\\0\end{bmatrix} \to \begin{bmatrix}\alpha^2\\\alpha^{2q}\\\alpha^{2q^2}\\\alpha^{2q^3}\end{bmatrix}, \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \to \begin{bmatrix}\alpha^3\\\alpha^{3q}\\\alpha^{3q^2}\\\alpha^{3q^3}\end{bmatrix}. \tag{4.2.16}$$

We consider $v = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}^T$ which is not on any plane, through any choice of three points from $\begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}^T$, $\begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}^T$, $\begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix}^T$, and $\begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix}^T$. The set of points of $\pi_0 = \mathrm{PG}(3,q)$ is the orbit of v under successive powers of S. Hence, $\Omega(L(\alpha^l)) = S^l(v) = (\alpha^l : \alpha^{lq} : \alpha^{lq^2} : \alpha^{lq^3})$ for $0 \le l < (q^2+1)(q+1)$. Thus, Ω is a linear transformation that changes the coordinate of $L(\alpha^l)$ to $(\alpha^l : \alpha^{lq} : \alpha^{lq^2} : \alpha^{lq^3})$.

Suppose $0, i'(q+1), j'(q+1), k'(q+1) \in B$ where B is a block of the 2-$(q^3+q^2+q+1, q^2+q+1, q+1)$ design in Theorem 3.1.7 for $m=4$. Since each block of this 2-$(q^3+q^2+q+1, q^2+q+1, q+1)$ design corresponds to the points of a plane in $\mathrm{PG}(3,q)$, and $\Omega(L(\alpha^l)) = (\alpha^l : \alpha^{lq} : \alpha^{lq^2} : \alpha^{lq^3})$ for $0 \le l < (q^2+1)(q+1)$ is a linear transformation that changes the coordinates of $L(\alpha^l)$ to $(\alpha^l : \alpha^{lq} : \alpha^{lq^2} : \alpha^{lq^3})$, then $\Omega(L(\alpha^0)), \Omega(L(\alpha^{i'(q+1)})), \Omega(L(\alpha^{j'(q+1)})), \Omega(L(\alpha^{k'(q+1)}))$, satisfy the equation of some plane $a_0x+a_1y+a_2z+a_3t=0$ where $a_0, a_1, a_2, a_3 \in \mathbb{F}_{q^4}$, that gives a system of linear equations where M is the coefficient matrix and $X = \begin{bmatrix}a_0 & a_1 & a_2 & a_3\end{bmatrix}^T$:

$$MX = \begin{bmatrix} 1 & 1 & 1 & 1 \\ \alpha^{i'(q+1)} & \alpha^{i'q(q+1)} & \alpha^{i'q^2(q+1)} & \alpha^{i'q^3(q+1)} \\ \alpha^{j'(q+1)} & \alpha^{j'q(q+1)} & \alpha^{j'q^2(q+1)} & \alpha^{j'q^3(q+1)} \\ \alpha^{k'(q+1)} & \alpha^{k'q(q+1)} & \alpha^{k'q^2(q+1)} & \alpha^{k'q^3(q+1)} \end{bmatrix} \begin{bmatrix}a_0\\a_1\\a_2\\a_3\end{bmatrix} = 0. \tag{4.2.17}$$

Since $L(\alpha^0)$, $L(\alpha^{i'(q+1)})$, $L(\alpha^{j'(q+1)})$, $L(\alpha^{k'(q+1)})$ are coplanar no three are collinear, and the transformation Ω maintains these properties, then $\mathrm{rank}(M) = 3$. Hence, $MX = 0$ has a unique solution in $\mathrm{PG}(3,q^4)$. We claim that the unique solution is $(a_0 : a_1 : a_2 : a_3) = (\alpha^s : \alpha^{sq} : \alpha^{sq^2} : \alpha^{sq^3})$. Let D be the difference set given in Construction 4.2.1. Since $0, i', j', k' \in C_s$, then $s, s+i'(q+1), s+j'(q+1), s+k'(q+1) \in D$. So, $\mathrm{Tr}(\alpha^s) = \mathrm{Tr}(\alpha^{s+i'(q+1)}) = \mathrm{Tr}(\alpha^{s+j'(q+1)}) = \mathrm{Tr}(\alpha^{s+k'(q+1)}) = 0$, thus $X = \begin{bmatrix}\alpha^s & \alpha^{sq} & \alpha^{sq^2} & \alpha^{sq^3}\end{bmatrix}^T$ is the solution of Eq. (4.2.17). So, a plane containing $\Omega(L(\alpha^0))$, $\Omega(L(\alpha^{i'(q+1)}))$, $\Omega(L(\alpha^{j'(q+1)}))$, $\Omega(L(\alpha^{k'(q+1)}))$ is $\alpha^s x + \alpha^{sq} y + \alpha^{sq^2} z + \alpha^{sq^3} t = 0$. Since $i' = \frac{m}{n} i$, $j' = \frac{m}{n} j$, and $k' = \frac{m}{n} k$, the points $\Omega(L(\alpha^0))$, $\Omega(L(\alpha^{i(q+1)}))$, $\Omega(L(\alpha^{j(q+1)}))$, $\Omega(L(\alpha^{k(q+1)}))$ satisfy $\alpha^s x^{\frac{m}{n}} + \alpha^{sq} y^{\frac{m}{n}} + \alpha^{sq^2} z^{\frac{m}{n}} + \alpha^{sq^3} t^{\frac{m}{n}} = 0$. ∎

Proposition 4.2.14. Let O be the ovoid constructed in Proposition 4.1.1 and let $O' = \{\Omega(p) : p \in O\}$. Then, $O' \hookrightarrow xz - yt = 0$.

Proof. First we prove that for any point $p \in O$, $\Omega(p)$ satisfies $xz - yt = 0$. If $p \in O$, then $p = \alpha^{i(q+1)}$ for $0 \leq i < q^2 + 1$. Then $\Omega(L(\alpha^{i(q+1)})) = (\alpha^{i(q+1)} : \alpha^{iq(q+1)} : \alpha^{iq^2(q+1)} : \alpha^{iq^3(q+1)})$. Hence, $\alpha^{i(q+1)}\alpha^{iq^2(q+1)} - \alpha^{iq(q+1)}\alpha^{iq^3(q+1)} = \alpha^{i(q+1)(q^2+1)} - (\alpha^{i(q+1)(q^2+1)})^q = \alpha^{i(q+1)(q^2+1)} - \alpha^{i(q+1)(q^2+1)} = 0$, where the last simplification is because $\alpha^{(q+1)(q^2+1)}$ is a primitive element of $\mathbb{F}_q$ and has order equal to q, and so $(\alpha^{i(q+1)(q^2+1)})^q = \alpha^{i(q+1)(q^2+1)}$. Now we prove that if a point $\Omega(p)$ satisfies $xz - yt = 0$, then, $p \in O$. Suppose $\Omega(L(\alpha^s)) = (\alpha^s : \alpha^{sq} : \alpha^{sq^2} : \alpha^{sq^3})$ for $0 \leq s < (q^2 + 1)(q + 1)$ satisfies $xz - yt = 0$. So, $\alpha^s\alpha^{sq^2} - \alpha^{sq}\alpha^{sq^3} = 0$. Then we have $\alpha^{s(q^2+1)} = \alpha^{sq(q^2+1)}$ which leads to $\alpha^{s(q^2+1)(q-1)} = 1$. Since the order of α is $q^4 - 1$, then $(q^4 - 1) \mid s(q^2 + 1)(q - 1)$. Therefore, $s = l(q + 1)$ for $0 \leq l < q^2 + 1$. This shows that $p = \alpha^s = \alpha^{l(q+1)}$ which belongs to O. ∎

Proposition 4.2.15. Let $b = \alpha^u$ for some $u \in D$. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$ in $\mathrm{PG}(3, q^4)$. Then the conic $O_c = O \cap P$ on P has the form

$$O_c \hookrightarrow b^q y^2 + b^{q^2} yz + b^{q^3} xz + bxy = 0, \tag{4.2.18}$$

1. O_c is non-singular if and only if $u \neq \frac{(q^2+1)(q+1)}{2}$.
2. if $u = \frac{(q^2+1)(q+1)}{2} \in D$, then $|P \cap O| = 1$.

Proof.

(1) Substitute $t = \frac{xz}{y}$ in the equation for P to get equation Eq. (4.2.18) for O_c with M the associated matrix. Then,

$$\det(M) = \begin{vmatrix} 0 & b & b^{q^3} \\ b & 2b^q & b^{q^2} \\ b^{q^3} & b^{q^2} & 0 \end{vmatrix} = -2\left(b^{q^3+q} - b^{q^2+1}\right)b^{q^3}. \tag{4.2.19}$$

It is clear that $\det(M) = 0$ (the rank of M is not 3) if and only if $b^{q^2+1} - b^{q^3+q} = 0$. Suppose $b^{q^2+1} = b^{q^3+q}$, then $b^{(q-1)(q^2+1)} = 1$ and we have $q^4 - 1 \mid u(q^2 + 1)(q - 1)$ which leads to $q + 1 \mid u$. Hence $u = k(q + 1)$ for some integer k. Since $u \in D$, the only element in D which is multiple of $q + 1$ is $\frac{(q^2+1)(q+1)}{2}$.

(2) If $u = \frac{(q^2+1)(q+1)}{2}$, let $(\alpha^{x(q+1)} : \alpha^{xq(q+1)} : \alpha^{xq^2(q+1)} : \alpha^{x^3(q+1)}) \in P \cap O$. Thus

$$b\alpha^{x(q+1)} + b^q\alpha^{xq(q+1)} + b^{q^2}\alpha^{xq^2(q+1)} + b^{q^3}\alpha^{xq^3(q+1)} = \mathrm{Tr}\left(\alpha^{\left(x+\frac{q^2+1}{2}\right)(q+1)}\right) = 0 \tag{4.2.20}$$

By Proposition 4.2.3, the only solution of Eq. (4.2.20) is $x = 0$ that corresponds to $(1 : 1 : 1 : 1)$. ∎

Proposition 4.2.16. Let $P \hookrightarrow \alpha^u x + \alpha^{uq} y + \alpha^{uq^2} z + \alpha^{uq^3} t = 0$, $Q \hookrightarrow \alpha^v x^2 + \alpha^{vq} y^2 + \alpha^{vq^2} z^2 + \alpha^{vq^3} t^2 = 0$, and $O \hookrightarrow xz - yt = 0$ which are hypersurfaces in $\mathrm{PG}(3, q^4)$ for some $u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. If $u = v$, then $|P \cap Q \cap O| \leq 2$.

Proof. Let $\Omega(L(\alpha^{l(q+1)})) \in P \cap Q \cap O$ for $l = 0, i, j$. Since $u = v$, $\Omega(L(\alpha^{2l(q+1)})) \in P$ for $l = 0, i, j$. This implies that $\{0, i, j, 2i, 2j\} \subseteq C_u$, which is impossible by Proposition 4.2.10. ∎

Theorem 4.2.17. Let $P \hookrightarrow \alpha^u x + \alpha^{uq} y + \alpha^{uq^2} z + \alpha^{uq^3} t = 0$, $Q \hookrightarrow \alpha^v x^2 + \alpha^{vq} y^2 + \alpha^{vq^2} z^2 + \alpha^{vq^3} t^2 = 0$, and $O \hookrightarrow xz - yt = 0$ be hypersurfaces in $\mathrm{PG}(3, q^4)$ for some $u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Then $|P \cap Q \cap O| \leq 4$.

Proof. Let $Q_c = Q \cap P$ and $O_c = O \cap P$, which are conics on P. If Q_c and O_c are two distinct conics, since five points determine a unique conic, then $|Q_c \cap O_c| \leq 4$, which implies $|Q \cap O \cap P| \leq 4$. The rest of the proof shows $Q_c \neq O_c$. Suppose, for the sake of contradiction, that $Q_c = O_c$. Note that since $u \neq \frac{(q^2+1)(q+1)}{2}$, by Proposition 4.2.15, $O_c = Q_c$ are non-singular conics. Let $P' = \Omega^{-1}(P)$, $Q' = \Omega^{-1}(Q)$, and $O' = \Omega^{-1}(O)$ be the set of points of P, Q, and O after transformation Ω^{-1}, respectively. We pick four points $L(\alpha^0)$, $L(\alpha^{i(q+1)})$, $L(\alpha^{j(q+1)})$, and $L(\alpha^{k(q+1)})$ in $P' \cap Q' \cap O'$. These four points are coplanar, no three collinear, so their span is a space of rank 3. Take $L(\alpha^{s(q+1)}) \in O' \setminus P'$, which together with any three of the previous points forms a basis. Let T be the linear transformation such that $T(L(\alpha^0)) = (1:0:0:0)$, $T(L(\alpha^{i(q+1)})) = (0:1:0:0)$, $T(L(\alpha^{j(q+1)})) = (0:0:1:0)$, and $T(L(\alpha^{s(q+1)})) = (0:0:0:1)$. Then the new equations of P', Q', and O' after transformation T are $P'' \hookrightarrow t = 0$, $Q'' \hookrightarrow a'_0 t^2 + a'_1 xt + a'_2 yt + a'_3 zt + a'xy + b'xz + c'yz = 0$, and $O'' \hookrightarrow 0t^2 + a_1 xt + a_2 yt + a_3 zt + axy + bxz + cyz = 0$, respectively. By intersecting the plane P'' with Q'' and O'', the equations of the resulting conics are $Q''_c \hookrightarrow a'xy + b'xz + c'yz = 0$, and $O''_c \hookrightarrow axy + bxz + cyz = 0$, respectively. Since O_c and Q_c are non-singular, they are irreducible, which implies that none of a, b, c, a', b', and c' can be zero. If $O''_c = Q''_c$, we must have $la = a'$, $lb = b'$ and $lc = c'$ for a non-zero $l \in \mathbb{F}_q$, then

$$Q'' - lO'' \hookrightarrow a'_0 t^2 + (-la_1 + a'_1)xt + (-la_2 + a'_2)yt + (-la_3 + a'_3)zt = \\ t\,(a'_0 t + (-la_1 + a'_1)x + (-la_2 + a'_2)y + (-la_3 + a'_3)z) = 0 \quad (4.2.21)$$

is the product of the equations of two planes in the pencil of Q'' and O''. This member of the pencil is reducible and hence singular. Since $Q'' - lO''$ is singular, the quadric $Q - lO$ is singular and Eq. (4.2.22) shows its associated matrix:

$$M = \begin{bmatrix} 2a & 0 & -l & 0 \\ 0 & 2a^q & 0 & l \\ -l & 0 & 2a^{q^2} & 0 \\ 0 & l & 0 & 2a^{q^3} \end{bmatrix}, \quad (4.2.22)$$

where $a = \alpha^v$. Since $Q - lO$ is singular, we have $\det(M) = 0$. However, we claim that no $l \in \mathbb{F}_q$ exists such that $\det(M) = 0$. For a contradiction, suppose there exists an l such that

$$\det(M) = l^4 + 4l^2(-a^{q^2+1} - a^{q^3+q}) + 16a^{q^3+q^2+q+1} = (4a^{q^3+q} - l^2)(4a^{q^2+1} - l^2) = 0 \quad (4.2.23)$$

This leads to four possible solutions for l:

$$2\alpha^{v\frac{q^2+1}{2}}, -2\alpha^{v\frac{q^2+1}{2}}, 2\alpha^{v\frac{q^3+q}{2}}, -2\alpha^{v\frac{q^3+q}{2}}. \tag{4.2.24}$$

First, suppose the solution is $\pm 2\alpha^{v\frac{q^2+1}{2}}$. Since $\pm 2, l \in \mathbb{F}_q$, then $\alpha^{v\frac{q^2+1}{2}} \in \mathbb{F}_q$, so we have $q^4-1 \mid v(q-1)\frac{q^2+1}{2}$, which leads to $v = 2g(q+1)$ for some $g \in \mathbb{Z}$. Since the only element in D which is a multiple of $q+1$ is $\frac{(q^2+1)(q+1)}{2}$, then $g = \frac{q^2+1}{4}$. However, since q is odd, q^4+1 is not divisible by 4, which leads to a contradiction. Now suppose the solution is $\pm 2\alpha^{v\frac{q^3+q}{2}}$. Then, we have $q^4-1 \mid vq(q-1)\frac{q^2+1}{2}$ which leads to $q+1 \mid \frac{vq}{2}$. Since q is odd and $\gcd(q, q+1) = 1$, we have $v = 2g(q+1)$ for some $g \in \mathbb{Z}$, which leads to the same contradiction as the first case. Therefore, $Q_c \neq O_c$. ∎

Lemma 4.2.18. Let l be an integer and α a primitive element in $\mathbb{F}_{q^4}$. Then $\alpha^{l(q+1)} = -\alpha^{l(q+1)}$ in $\mathrm{PG}(3,q)$.

Proof. Since $\alpha^{\frac{q^4-1}{2}} = -1$, then $-\alpha^{l(q+1)} = \alpha^{\frac{q^4-1}{2}+l(q+1)} = \alpha^{(q+1)(\frac{(q^2+1)(q-1)}{2}+l)}$. Since the exponents of elements of ovoid are modulo q^2+1 and $q-1$ is divisible by 2, then $\alpha^{(q+1)(\frac{(q^2+1)(q-1)}{2}+l)} = \alpha^{l(q+1)}$. ∎

Remark 4.2.19. Let $P \hookrightarrow \alpha^u x + \alpha^{uq} y + \alpha^{uq^2} z + \alpha^{uq^3} t = 0$, $H \hookrightarrow \alpha^v \sqrt{x} + \alpha^{vq}\sqrt{y} + \alpha^{vq^2}\sqrt{z} + \alpha^{vq^3}\sqrt{t} = 0$, and $O \hookrightarrow xz - yt = 0$ in $\mathrm{PG}(3,q^4)$ for some $u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \le i < \frac{q^2+1}{2}\}$. Let $p = \Omega(L(\alpha^{2i(q+1)}))$ such that $p \in O^{(e)} \cap P$ and $p \in O^{(e)} \cap H$ for some $0 \le i < \frac{q^2+1}{2}$. Consider the point $p' = \Omega(L(\alpha^{i(q+1)}))$. It is clear that $p' \in O \cap P'$ and $p' \in O \cap H'$ where $P' \hookrightarrow \alpha^u x^2 + \alpha^{uq} y^2 + \alpha^{uq^2} z^2 + \alpha^{uq^3} t^2 = 0$ and $H' \hookrightarrow \alpha^v x + \alpha^{vq} y + \alpha^{vq^2} z + \alpha^{vq^3} t = 0$. Therefore, we have $|O^{(e)} \cap P| \le |O \cap P'|$, and $|O^{(e)} \cap H| \le |O \cap H'|$. Thus by Theorem 4.2.17, $|P \cap H \cap O^{(e)}| \le 4$.

Theorem 4.2.20. Let $b = \alpha^u$, $c = \alpha^v$ for some $u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, and $Q \hookrightarrow cx^2 + c^q y^2 + c^{q^2} z^2 + c^{q^3} t^2 = 0$ which are hypersurfaces in $\mathrm{PG}(3,q^4)$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \le i < \frac{q^2+1}{2}\}$. If $b^2 c^{q^2} = b^{2q^2} c$, then $|O \cap P \cap Q| \le 3$, and $|O^{(e)} \cap P \cap Q| \le 2$.

Proof. First note that by raising both sides of the equality $b^2 c^{q^2} = b^{2q^2} c$ to the power q, we have $b^{2q} c^{q^3} = b^{2q^3} c^q$. We use several times in the proof that any powers of $b = \alpha^u$ are invertible. By using P and substituting $t = -b^{-q^3}(bx + b^q y + b^{q^2} z)$ in the equations of O and Q, we obtain the equations of the two conics in the plane P, O_c as described in Eq. (4.2.18), and Q_c:

$$\begin{aligned} Q_c \hookrightarrow \left(b^2 c^{q^3} + b^{2q^3} c\right) x^2 + \left(b^{2q} c^{q^3} + b^{2q^3} c^q\right) y^2 + \left(b^{2q^3} c^{q^2} + b^{2q^2} c^{q^3}\right) z^2 \\ + \left(2b^{q^2+q} c^{q^3}\right) yz + \left(2b^{q^2+1} c^{q^3}\right) xz + \left(2b^{q+1} c^{q^3}\right) xy = 0. \end{aligned} \tag{4.2.25}$$

Note that $O_c = O \cap P$, and $Q_c = Q \cap P$. Using O_c, we substitute $y^2 = \frac{-b^{q^2}yz - b^{q^3}xz - bxy}{b^q}$ in the equation of Q_c to obtain using $b^{2q}c^{q^3} = b^{2q^3}c^q$ an equation Γ:

$$\Gamma = \left(b^2c^{q^3} + b^{2q^3}c\right)x^2 + \left(2b^{2q}c^{q^3}\right)\left(\frac{-b^{q^2}yz - b^{q^3}xz - bxy}{b^q}\right) + \left(b^{2q^3}c^{q^2} + b^{2q^2}c^{q^3}\right)z^2 + \left(2b^{q^2+q}c^{q^3}\right)yz + \left(2b^{q^2+1}c^{q^3}\right)xz + \left(2b^{q+1}c^{q^3}\right)xy. \quad (4.2.26)$$

Note that points in $O \cap P \cap Q$ satisfy $\Gamma = 0$. To simplify things, apply $\beta^{q^4} = \beta$ for all $\beta \in \mathbb{F}_{q^4}$ to get $\left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3} = \left(b^{2q^3}c^{q^6} + b^{2q^6}c^{q^3}\right) = \left(b^{2q^3}c^{q^2} + b^{2q^2}c^{q^3}\right)$. After expanding Eq. (4.2.26) and using the fact that $\left(b^{2q^3}c^{q^2} + b^{2q^2}c^{q^3}\right) = \left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3}$ we have

$$\Gamma = \left(b^2c^{q^3} + b^{2q^3}c\right)x^2 + \left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3}z^2 + \left(2c^{q^3}\left(b^{q^2+1} - b^{q^3+q}\right)\right)xz. \quad (4.2.27)$$

Points in $O \cap P \cap Q$ are of the form $(\alpha^{i(q+1)} : \alpha^{iq(q+1)} : \alpha^{iq^2(q+1)} : \alpha^{iq^3(q+1)})$. We want to determine how many different such points exist. Since points in $O \cap P \cap Q$ satisfy $\Gamma = 0$.

$$\left(b^2c^{q^3} + b^{2q^3}c\right)\left(\alpha^{2i(q+1)}\right) + \left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3}\left(\alpha^{2iq^2(q+1)}\right) + \left(2c^{q^3}\left(b^{q^2+1} - b^{q^3+q}\right)\right)\alpha^{i(q+1)}\alpha^{iq^2(q+1)} = 0. \quad (4.2.28)$$

We divide the equation by $\alpha^{2i(q+1)}$, so

$$\left(b^2c^{q^3} + b^{2q^3}c\right) + \left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3}\left(\alpha^{2i(q^2-1)(q+1)}\right) + \left(2c^{q^3}\left(b^{q^2+1} - b^{q^3+q}\right)\right)\alpha^{i(q^2-1)(q+1)} = 0. \quad (4.2.29)$$

Thus $\alpha^{i(q^2-1)(q+1)}$ must satisfy:

$$\left(b^2c^{q^3} + b^{2q^3}c\right)^{q^3}X^2 + \left(2c^{q^3}\left(b^{q^2+1} - b^{q^3+q}\right)\right)X + \left(b^2c^{q^3} + b^{2q^3}c\right) = 0, \quad (4.2.30)$$

which is an equation of degree 2, and has at most two roots. We claim that each root $\bar{x}$ of Eq. (4.2.30) gives two possible solutions $i, i + \frac{q^2+1}{2} \in \mathbb{Z}_{q^2+1}$ of Eq. (4.2.29). To see this, suppose $\bar{x}$ is a solution of Eq. (4.2.30) such that there exists $i \neq j \in \mathbb{Z}_{q^2+1}$ where $\bar{x} = \alpha^{i(q^2-1)(q+1)} = \alpha^{j(q^2-1)(q+1)}$. So, $\alpha^{(i-j)(q^2-1)(q+1)} = 1$ which implies that $i - j = k(\frac{q^2+1}{2})$ for some integer k. Since $i, j \in \mathbb{Z}_{q^2+1}$, then $i - j = 0$ or $j = i + \frac{q^2+1}{2}$. Suppose Eq. (4.2.30) has two solutions $\bar{x}$ and $\bar{y}$ that corresponds to i, $i + \frac{q^2+1}{2}$, j, and $j + \frac{q^2+1}{2}$. Note that since $\frac{q^2+1}{2}$ is odd and exactly two of the four are even, then $|O^{(e)} \cap P \cap Q| \leq 2$. It is clear that $i = 0$

gives a solution of Eq. (4.2.30), since $(1:1:1:1)$ is on P, Q, and O. Thus, $\alpha^{l(q^2-1)(q+1)}$ for $l = 0, \frac{q^2+1}{2}, j, j+\frac{q^2+1}{2}$ are four possible solutions of Eq. (4.2.29). We claim that at most three of them can give solutions of Eq. (4.2.29). By contradiction, suppose Eq. (4.2.29) has four solutions. So, $\Omega(L(\alpha^{l(q+1)})) \in P$ for $l = 0, \frac{q^2+1}{2}, j, j+\frac{q^2+1}{2}$. Then, there exists a block B in 3-$(q^2+1, q+1, 1)$ design in Remark 4.1.2 such that $\left\{0, \frac{q^2+1}{2}, j, j+\frac{q^2+1}{2}\right\} \subseteq B$. By Proposition 4.2.7, $\left\{-j, -j+\frac{q^2+1}{2}\right\} \subseteq B$. Then $\left\{j, j+\frac{q^2+1}{2}, 2j, 2j+\frac{q^2+1}{2}, 0, \frac{q^2+1}{2}\right\} \subseteq B+j$, where $B+j$ is a translate of B. Since $\left\{0, \frac{q^2+1}{2}, j\right\} \subseteq B+j$, then by Proposition 4.2.7, $-j \in B+j$. Thus, $\{0, j, -j, 2j\} \subseteq B+j$, which is impossible by Proposition 4.2.8. Therefore, $|O \cap P \cap Q| \leq 3$. ∎

Theorem 4.2.21. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, and

$$\Psi \hookrightarrow \left(a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t}\right)\left(a\sqrt{x} - a^q\sqrt{y} + a^{q^2}\sqrt{z} - a^{q^3}\sqrt{t}\right) = 0,$$

in $\mathrm{PG}(3, q^4)$, where $a = \alpha^s$ and $b = \alpha^u$ for some $s, u \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \leq i < \frac{q^2+1}{2}\}$. If $a^2 b^{q^2} = a^{2q^2} b$, then $|O^{(e)} \cap P \cap \Psi| \leq 2$.

Proof. By substituting $t = -b^{-q^3}(bx + b^q y + b^{q^2} z)$ in the equation of Ψ, using $xz = yt$, and $a^2 b^{q^2} = a^{2q^2} b$, we have

$$\Gamma = \left(a^2 b^{q^3} + a^{2q^3} b\right) x + \left(a^{2q^2} b^{q^3} + a^{2q^3} b^{q^2}\right) z + 2b^{q^3}\left(a^{q^2+1} - a^{q^3+q}\right)\sqrt{xz} = 0. \tag{4.2.31}$$

Points in $O^{(e)} \cap P \cap \Psi$ are the form $(\alpha^{2i(q+1)} : \alpha^{2iq(q+1)} : \alpha^{2iq^2(q+1)} : \alpha^{2iq^3(q+1)})$ for $0 \leq i < \frac{q^2+1}{2}$. We want to determine how many different such points exist. Since $O^{(e)} \cap P \cap \Psi \hookrightarrow \Gamma = 0$, we have

$$\left(a^2 b^{q^3} + a^{2q^3} b\right)\alpha^{2i(q+1)} + \left(a^{2q^2} b^{q^3} + a^{2q^3} b^{q^2}\right)\alpha^{2iq^2(q+1)} + 2b^{q^3}\left(a^{q^2+1} - a^{q^3+q}\right)\alpha^{i(q^2+1)(q+1)} = 0. \tag{4.2.32}$$

We divide the equation by $\alpha^{2i(q+1)}$, so

$$\left(a^2 b^{q^3} + a^{2q^3} b\right) + \left(a^{2q^2} b^{q^3} + a^{2q^3} b^{q^2}\right)\alpha^{2i(q^2-1)(q+1)} + 2b^{q^3}\left(a^{q^2+1} - a^{q^3+q}\right)\alpha^{i(q^2-1)(q+1)} = 0. \tag{4.2.33}$$

Thus $\alpha^{i(q^2-1)(q+1)}$ must satisfy:

$$\left(a^{2q^2} b^{q^3} + a^{2q^3} b^{q^2}\right) X^2 + 2b^{q^3}\left(a^{q^2+1} - a^{q^3+q}\right) X + \left(a^2 b^{q^3} + a^{2q^3} b\right) = 0. \tag{4.2.34}$$

which is an equation of degree 2, and has at most two roots. We claim that each solution $\bar{x}$ of Eq. (4.2.34) determines a unique $i \in \mathbb{Z}_{\frac{q^2+1}{2}}$. To see this, suppose $\bar{x}$ is a solution of

Eq. (4.2.30) such that there exists $i \neq j \in \mathbb{Z}_{\frac{q^2+1}{2}}$ where $\bar{x} = \alpha^{i(q^2-1)(q+1)} = \alpha^{j(q^2-1)(q+1)}$. So, $\alpha^{(i-j)(q^2-1)(q+1)} = 1$ which implies that $i - j = k(\frac{q^2+1}{2})$ for some integer k. Since $i, j \in \mathbb{Z}_{\frac{q^2+1}{2}}$, then $i - j = 0$, which implies that $i = j$. Therefore, $|O^{(e)} \cap P \cap \Psi| \leq 2$. ∎

Remark 4.2.22. Let $b = \alpha^u$, $a = \alpha^s$ for some $u, s \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, and $H \hookrightarrow a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t} = 0$ in $\mathrm{PG}(3, q^4)$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \leq i < \frac{q^2+1}{2}\}$. If $a^2 b^{q^2} = a^{2q^2} b$, since $H \subseteq \Psi$, by Theorem 4.2.21, then $|O^{(e)} \cap P \cap H| \leq 2$.

Theorem 4.2.23. Let q be an odd prime power and α be a primitive element in $\mathbb{F}_{q^4}$. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow \alpha^u x + \alpha^{uq} y + \alpha^{uq^2} z + \alpha^{uq^3} t = 0$, $Q \hookrightarrow \alpha^v x^2 + \alpha^{vq} y^2 + \alpha^{vq^2} z^2 + \alpha^{vq^3} t^2 = 0$, and

$$\Psi \hookrightarrow \left(\alpha^s\sqrt{x} + \alpha^{sq}\sqrt{y} + \alpha^{sq^2}\sqrt{z} + \alpha^{sq^3}\sqrt{t}\right)\left(\alpha^s\sqrt{x} - a\alpha^{sq}\sqrt{y} + \alpha^{sq^2}\sqrt{z} - \alpha^{sq^3}\sqrt{t}\right) = 0,$$

in $\mathrm{PG}(3, q^4)$, where $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \leq i < \frac{q^2+1}{2}\}$. Then $|O^{(e)} \cap P \cap \Psi \cap Q| \leq 3$.

Proof. Let $a = \alpha^s$, $b = \alpha^u$, and $c = \alpha^v$. We can assume, without loss of generality that $|O^{(e)} \cap P \cap \Psi| > 2$, thus by Theorem 4.2.21, $a^2 b^{q^2} \neq a^{2q^2} b$, otherwise we would be done.

Suppose $p = (x : y : z : t) \in O^{(e)} \cap \Psi$. We have

$$\begin{aligned}\left(a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t}\right)\left(a\sqrt{x} - a^q\sqrt{y} + a^{q^2}\sqrt{z} - a^{q^3}\sqrt{t}\right) &= 0,\\ a^2x + a^{2q^2}z - a^{2q}y - a^{2q^3}t &= 2a^{q^3+q}\sqrt{yt} - 2a^{q^2+1}\sqrt{xz},\\ \left(a^2x + a^{2q^2}z - a^{2q}y - a^{2q^3}t\right)^2 &= \left(2a^{q^3+q}\sqrt{yt} - 2a^{q^2+1}\sqrt{xz}\right)^2,\end{aligned} \tag{4.2.35}$$

$$\begin{aligned}&a^4x^2 + a^{4q}y^2 + a^{4q^2}z^2 + a^{4q^3}t^2\\ &\quad - 2a^2a^{2q}xy + 2a^2a^{2q^2}xz - 2a^2a^{2q^3}xt - 2a^{2q}a^{2q^2}yz + 2a^{2q}a^{2q^3}yt - 2a^{2q^2}a^{2q^3}zt =\\ &\qquad 4a^2a^{2q^2}xz + 4a^{2q}a^{2q^3}yt - 8aa^qa^{q^2}a^{q^3}\sqrt{xyzt}.\end{aligned} \tag{4.2.36}$$

Since $xz = yt$, then $p \in \Phi$, where

$$\begin{aligned}\Phi \hookrightarrow\ &a^4x^2 + a^{4q}y^2 + a^{4q^2}z^2 + a^{4q^3}t^2\\ &- 2a^2a^{2q}xy - 2a^2a^{2q^2}xz - 2a^2a^{2q^3}xt - 2a^{2q}a^{2q^2}yz - 2a^{2q}a^{2q^3}yt - 2a^{2q^2}a^{2q^3}zt\\ &+ 8aa^qa^{q^2}a^{q^3}xz = 0.\end{aligned} \tag{4.2.37}$$

This shows that $O^{(e)} \cap P \cap Q \cap \Psi \subseteq O^{(e)} \cap P \cap Q \cap \Phi$. Next, we will show that $|P \cap O^{(e)} \cap \Phi \cap Q| \leq 3$, which implies $|P \cap O^{(e)} \cap \Psi \cap Q| \leq 3$. Assume that the intersection of P, Q, Φ, and $O^{(e)}$

has at least four points. Using the equation of P, we substitute $t = -b^{-q^3}(bx + b^q y + b^{q^2} z)$ in the equation of O, Q, and Φ, and obtain the equation of three conics in the plane P, namely O_c, Q_c as described in Eq. (4.2.18) and Eq. (4.2.25), and Φ_c:

$$\begin{aligned}\Phi_c \hookrightarrow &\left(a^2b^{q^3} + a^{2q^3}b\right)^2 x^2 + \left(a^{2q}b^{q^3} + a^{2q^3}b^q\right)^2 y^2 + \left(a^{2q^2}b^{q^3} + a^{2q^3}b^{q^2}\right)^2 z^2 \\ &+ \left(2\left(a^{2q}b^{q^2} + a^{2q^2}b^q\right)a^{2q^3}b^{q^3} - 2a^{2q^2+2q}b^{2q^3} + 2a^{4q^3}b^{q^2+q}\right) yz \\ &+ \left(2\left(a^2b^{q^2} + a^{2q^2}b\right)a^{2q^3}b^{q^3} + 2\left(4a^{q^3+q^2+q+1} - a^{2q^2+2}\right)b^{2q^3} + 2a^{4q^3}b^{q^2+1}\right) xz \\ &+ \left(2\left(a^2b^q + a^{2q}b\right)a^{2q^3}b^{q^3} - 2a^{2q+2}b^{2q^3} + 2a^{4q^3}b^{q+1}\right) xy = 0. \quad (4.2.38)\end{aligned}$$

Since we assume there are four points in $O^{(e)} \cap Q \cap \Phi \cap P$, then by Proposition 2.3.16, Φ_c should be in the pencil of O_c and Q_c. Consider the 3×6 matrix M' where each row corresponds to the coefficients of x^2, y^2, z^2, yz, xz, xy for O_c, Q_c, and Φ_c, respectively:

$$M' = \begin{bmatrix} 0 & b^q & 0 & b^{q^2} & b^{q^3} & b \\ (b^2c^{q^3} + b^{2q^3}c) & (b^{2q}c^{q^3} + b^{2q^3}c^q) & (b^{2q^2}c^{q^3} + b^{2q^3}c^{q^2}) & (2b^{q^2+q}c^{q^3}) & (2b^{q^2+1}c^{q^3}) & (2b^{q+1}c^{q^3}) \\ (a^2b^{q^3} + a^{2q^3}b)^2 & (a^{2q}b^{q^3} + a^{2q^3}b^q)^2 & (a^{2q^2}b^{q^3} + a^{2q^3}b^{q^2})^2 & A & B & C \end{bmatrix}, \quad (4.2.39)$$

where A, B, and C are the coefficient of yz, xz, and xy in Φ_c, respectively:

$$A = \left(2\left(a^{2q}b^{q^2} + a^{2q^2}b^q\right)a^{2q^3}b^{q^3} - 2a^{2q^2+2q}b^{2q^3} + 2a^{4q^3}b^{q^2+q}\right), \quad (4.2.40)$$

$$B = \left(2\left(a^2b^{q^2} + a^{2q^2}b\right)a^{2q^3}b^{q^3} + 2\left(4a^{q^3+q^2+q+1} - a^{2q^2+2}\right)b^{2q^3} + 2a^{4q^3}b^{q^2+1}\right), \quad (4.2.41)$$

$$C = \left(2\left(a^2b^q + a^{2q}b\right)a^{2q^3}b^{q^3} - 2a^{2q+2}b^{2q^3} + 2a^{4q^3}b^{q+1}\right). \quad (4.2.42)$$

We consider the last three columns of the above matrix and call it M. We calculate $\det(M)$ and show that $\det(M) \neq 0$.

$$\det(M) = 2bb^{q+1}c^{q^3}\begin{vmatrix} b^{q^2-1} & b^{q^3-1} & 1 \\ b^{q^2-1} & b^{q^2-q} & 1 \\ A & B & C \end{vmatrix} = 2bb^{q+1}c^{q^3}\begin{vmatrix} b^{q^2-1} & b^{q^3-1} & 1 \\ 0 & b^{q^2-q} - b^{q^3-1} & 0 \\ A & B & C \end{vmatrix}. \quad (4.2.43)$$

Note that $b^{q^2-q} - b^{q^3-1}$ cannot be equal to zero: if $b^{q^2-q} = b^{q^3-1}$, then $b^{(q-1)(q^2+1)} = 1$ and we have $q^4 - 1 \mid u(q^2+1)(q-1)$ which leads to $q+1 \mid u$. Hence $u = k(q+1)$, for some integer k. Since $u \in D$, then the only element in D which is multiple of $q+1$ is $\frac{(q^2+1)(q+1)}{2}$. Hence, $u = \frac{(q^2+1)(q+1)}{2}$ which contradicts the choice of u in the assumption. So, we have

$$\det(M) = 2bb^{q+1}c^{q^3}\left(b^{q^2-q} - b^{q^3-1}\right)\begin{vmatrix} b^{q^2-1} & 0 & 1 \\ 0 & 1 & 0 \\ A & 0 & C \end{vmatrix} = -2bc^{q^3}\left(b^{q^3+q} - b^{q^2+1}\right)\begin{vmatrix} b^{q^2-1} & 1 \\ A & C \end{vmatrix}. \tag{4.2.44}$$

Since b, c are powers of α, and $-b^{q+1}\left(b^{q^2-q} - b^{q^3-1}\right) = \left(b^{q^3+q} - b^{q^2+1}\right) \neq 0$, then $\det(M) \neq 0$ if and only if $b\left(b^{q^2-1}C - A\right) \neq 0$. For the final step, we calculate $b\left(b^{q^2-1}C - A\right)$:

$$\begin{aligned} b\left(b^{q^2-1}C - A\right) &= 2(a^{2q^3}b^{q^3}b^q a^2 b^{q^2} + a^{2q}a^{2q^3}bb^{q^3}b^{q^2} - a^{2q}b^{2q^3}a^2b^{q^2} + a^{4q^3}b^{q^2}b^q b \\ &\quad - a^{2q}a^{2q^3}bb^{q^3}b^{q^2} - a^{2q^3}b^{q^3}b^q a^{2q^2}b + a^{2q}b^{2q^3}a^{2q^2}b - a^{4q^3}b^{q^2}b^q b), \quad (4.2.45) \\ &= 2\left(a^{2q^3}b^{q^3}b^q\left(a^2b^{q^2} - a^{2q^2}b\right) - a^{2q}b^{2q^3}\left(a^2b^{q^2} - a^{2q^2}b\right)\right), \quad (4.2.46) \\ &= -2b^{q^3}\left(a^2b^{q^2} - a^{2q^2}b\right)\left(a^{2q}b^{q^3} - a^{2q^3}b^q\right), \quad (4.2.47) \\ &= -2b^{q^3}\left(a^2b^{q^2} - a^{2q^2}b\right)^{q+1}. \quad (4.2.48) \end{aligned}$$

Note that in Eq. (4.2.47), we have used the fact that $a^{2q}b^{q^3} - a^{2q^3}b^q = \left(a^2b^{q^2} - a^{2q^2}b\right)^q$. Hence,

$$\det(M) = 4b^{q^3}c^{q^3}\left(b^{q^3+q} - b^{q^2+1}\right)\left(a^2b^{q^2} - a^{2q^2}b\right)^{q+1}. \tag{4.2.49}$$

By Theorem 4.2.21, and using that $|O^{(e)} \cap P \cap \Psi| > 2$, we know $\left(a^2b^{q^2} - a^{2q^2}b\right) \neq 0$, and since $4b^{q^3}c^{q^3} \neq 0$, we have $\det(M) \neq 0$. Therefore, the rank of M and M' is equal to 3. This implies Φ_c is not in the pencil of O_c and Q_c, and we reach the desired contradiction. ∎

Corollary 4.2.24. Let $O \hookrightarrow xz - yt = 0$, $P \hookrightarrow \alpha^u x + \alpha^{uq}y + \alpha^{uq^2}z + \alpha^{uq^3}t = 0$, $Q \hookrightarrow \alpha^v x^2 + \alpha^{vq}y^2 + \alpha^{vq^2}z^2 + \alpha^{vq^3}t^2 = 0$, and $H \hookrightarrow \alpha^s\sqrt{x} + \alpha^{sq}\sqrt{y} + \alpha^{sq^2}\sqrt{z} + \alpha^{sq^3}\sqrt{t} = 0$ in $\mathrm{PG}(3, q^4)$, where $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $O^{(e)} = \{\Omega(L(\alpha^{2i(q+1)})) \in O : 0 \leq i < \frac{q^2+1}{2}\}$. Then $|O^{(e)} \cap P \cap H \cap Q| \leq 3$.

Proof. Since $H \subseteq \Psi$, then the result is immediate by Theorem 4.2.23. ∎

As a direct consequence of Corollary 4.2.24, we have the following central result of this chapter.

Theorem 4.2.25. Let q be an odd prime power. Let $M_1 = (\mathcal{M}^{(e)}, \{C \cap \mathcal{M}^{(e)} : C \in \mathcal{C}\})$, $M_2 = (\mathcal{M}^{(e)}, \{(C \cap \mathcal{M}^{(e)})/2 : C \in \mathcal{C}\})$, and $M_{1/2} = (\mathcal{M}^{(e)}, \{2C \cap \mathcal{M}^{(e)} : C \in \mathcal{C}\})$ be three truncated Möbius planes in Construction 4.2.11. Then, $M_{1/2}$, M_1, and M_2 give a set of 3 anti-cocircular truncated Möbius planes.

Proof. Let $B_{1/2}$, B_1, and B_2 be circles of $M_{1/2}$, M_1, and M_2, respectively. Let $I = B_{1/2} \cap B_1 \cap B_2$. We must prove $|I| \leq 3$. Let $d \in I$ and $I_0 = \{i - d \ : \ i \in I\}$; note that $0 \in I_0$. Assume without loss of generality that $|I_0| > 1$. By Remark 4.2.5, for $i \in B_l$, $l = 1/2, 1, 2$, there exists $x \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$ such that $li \in C_x$ and $i \in C_{x,l}$. Therefore, there exists $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$ such that $I_0 \subseteq C_{s,1/2} \cap C_{u,1} \cap C_{v,2}$. Let $I_L = \{\Omega(L(\alpha^{i(q+1)})) : i \in I_0\}$. By Proposition 4.2.13, $I_L \subseteq O^{(e)} \cap H \cap P \cap Q$, where $H \hookrightarrow a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t} = 0$, $P \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, $Q \hookrightarrow cx^2 + c^q y^2 + c^{q^2} z^2 + c^{q^3} t^2 = 0$, and $a = \alpha^s$, $b = \alpha^u$, and $c = \alpha^v$. Corollary 4.2.24 implies $|I_L| \leq 3$, therefore $|I| = |B_{1/2} \cap B_1 \cap B_2| \leq 3$. ∎

Table 4.3 provides circles of $M_{1/2}$, M_1, and M_2 containing zero, for $q = 5$. By Theorem 4.2.25, the common intersection of any choice of three circles, one from each, has size at most three.

Lemma 4.2.26. Let $P_a \hookrightarrow ax + a^q y + a^{q^2} z + a^{q^3} t = 0$, $Q_b \hookrightarrow bx^2 + b^q y^2 + b^{q^2} z^2 + b^{q^3} t^2 = 0$, $R_c \hookrightarrow cx^4 + c^q y^4 + c^{q^2} z^4 + c^{q^3} t^4 = 0$. Let

$$\Psi_a \hookrightarrow \left(a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t}\right)\left(a\sqrt{x} - a^q\sqrt{y} + a^{q^2}\sqrt{z} - a^{q^3}\sqrt{t}\right) = 0,$$

$P_b \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, and $Q_c \hookrightarrow cx^2 + c^q y^2 + c^{q^2} z^2 + c^{q^3} t^2 = 0$, where $a = \alpha^s$, $b = \alpha^u$, and $c = \alpha^v$ for some $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $p' = \Omega(L(\alpha^{(l+p_l\frac{q^2+1}{2})(q+1)}))\}$, where $p_l \in \{0, 1\}$, and $p = \Omega(L(\alpha^{2l(q+1)}))$. Then the following hold:

1. if $p' \in P_a$, then $p \in \Psi_a$;
2. if $p' \in Q_b$, then $p \in P_b$;
3. if $p' \in R_c$, then $p \in Q_c$.

Proof.

We first prove Item 1. Note that for any $0 \leq l < \frac{q^2+1}{2}$, we have $\Omega(L(\alpha^{(l+\frac{q^2+1}{2})(q+1)})) = (\alpha^{l(q+1)} : -\alpha^{lq(q+1)} : \alpha^{lq^2(q+1)} : -\alpha^{lq^3(q+1)})$. So, $p' \in P_a$ implies $a\alpha^{l(q+1)} + a^q\alpha^{lq(q+1)} + a^{q^2}\alpha^{lq^2(q+1)} + a^{q^3}\alpha^{lq^3(q+1)} = 0$ if $p_l = 0$, or $a\alpha^{l(q+1)} - a^q\alpha^{lq(q+1)} + a^{q^2}\alpha^{lq^2(q+1)} - a^{q^3}\alpha^{lq^3(q+1)} = 0$ if $p_l = 1$. In either case, $p \in \Psi_a$. Now, we prove Item 2 and Item 3. From $p' \in Q_b$ and $p' \in R_c$, we have $b\alpha^{2l(q+1)} + b^q\alpha^{2lq(q+1)} + b^{q^2}\alpha^{2lq^2(q+1)} + b^{q^3}\alpha^{2lq^3(q+1)} = 0$ and $c\alpha^{4l(q+1)} + c^q\alpha^{4lq(q+1)} + c^{q^2}\alpha^{4lq^2(q+1)} + c^{q^3}\alpha^{4lq^3(q+1)} = 0$ which leads to $p \in P_b$ and $p \in Q_c$, respectively. ∎

Theorem 4.2.27. Let q be an odd prime power and α be a primitive element in $\mathbb{F}_{q^4}$. Let $O \hookrightarrow xz - yt = 0$, Let $P_a \hookrightarrow ax + a^q y + a^{q^2} z + a^{q^3} t = 0$, $Q_b \hookrightarrow bx^2 + b^q y^2 + b^{q^2} z^2 + b^{q^3} t^2 = 0$, $R_c \hookrightarrow cx^4 + c^q y^4 + c^{q^2} z^4 + c^{q^3} t^4 = 0$ in $\mathrm{PG}(3, q^4)$, where $a = \alpha^s$, $b = \alpha^u$, and $c = \alpha^v$ for some $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$. Let $\vec{p} = (p_0, p_1, \ldots, p_i, \ldots, p_{\frac{q^2-1}{2}}) \in \{0, 1\}^{\frac{q^2+1}{2}}$, and $O^{(\vec{p})} = \{\Omega(L(\alpha^{(i+p_i\frac{q^2+1}{2})(q+1)})) \in O : 0 \leq i < \frac{q^2+1}{2}\}$. Then, $|O^{(\vec{p})} \cap P_a \cap Q_b \cap R_c| \leq 3$.

Proof. By contradiction, assume $|O^{(\vec{p})} \cap P_a \cap Q_b \cap R_c| \geq 4$. Then, there exists

$$F = \left\{ \Omega(L(\alpha^{(l+p_l \frac{q^2+1}{2})(q+1)})) : l \in \{0, i, j, k\} \right\} \subseteq O^{(\vec{p})} \cap P_a \cap Q_b \cap R_c,$$

such that $l = 0, i, j, k \pmod{\frac{q^2+1}{2}}$ are distinct. Then,

$$F^{(2)} = \left\{ \Omega(L(\alpha^{2l(q+1)})) : l \in \{0, i, j, k\} \right\}$$

has four distinct points. Then, by Lemma 4.2.26, $F^{(2)} \subseteq O^{(e)} \cap P_b \cap Q_c \cap \Psi_a$, where

$$\Psi_a \hookrightarrow \left(a\sqrt{x} + a^q\sqrt{y} + a^{q^2}\sqrt{z} + a^{q^3}\sqrt{t} \right) \left(a\sqrt{x} - a^q\sqrt{y} + a^{q^2}\sqrt{z} - a^{q^3}\sqrt{t} \right) = 0,$$

$P_b \hookrightarrow bx + b^q y + b^{q^2} z + b^{q^3} t = 0$, and $Q_c \hookrightarrow cx^2 + c^q y^2 + c^{q^2} z^2 + c^{q^3} t^2 = 0$. By Theorem 4.2.23, $|O^{(e)} \cap P_b \cap Q_c \cap \Psi_a| \leq 3$, which is a contradiction with $|F^{(2)}| = 4$. ∎

Remark 4.2.28. Let f be the natural bijection between $\{0,1\}^{\frac{q^2+1}{2}}$ and the set $S = \{B \subseteq \mathbb{Z}_{q^2+1} : |B| = \frac{q^2+1}{2}$ and for all $0 \leq i < \frac{q^2+1}{2}$, either $i \in B$ or $i + \frac{q^2+1}{2} \in B\}$; more specifically, let $f(\vec{p}) = \{i + p_i(\frac{q^2+1}{2}) : 0 \leq i < \frac{q^2+1}{2}\}$. The set S is closed under cyclic shifts, that is, if $B \in S$ then $B + l \in S$, since the fact that any $i, j \in B$ has $i - j \neq \frac{q^2+1}{2}$ implies the same fact for $B + l$. Therefore, if $B = f(\vec{p})$, then there exist a $\vec{p'}$ such that $B + l = f(\vec{p'})$.

Notation 4.2.29. Let $\vec{p} = (p_0, p_1, \ldots, p_{\frac{q^2-1}{2}}) \in \{0,1\}^{\frac{q^2+1}{2}}$. We denote the $4 \times \frac{q^2+1}{2}$ sub-matrix of $G_{q^2+1}^{l(q+1)}$ with column indices $\{i + p_i(\frac{q^2+1}{2}) : 0 \leq i < \frac{q^2+1}{2}\}$ by $\left[G_{q^2+1}^{l(q+1)}\right]_{\vec{p}}$.

Construction 4.2.30. Let $\vec{p} = (p_0, p_1, \ldots, p_{\frac{q^2-1}{2}}) \in \{0,1\}^{\frac{q^2+1}{2}}$ and $(\mathcal{M}, \mathcal{C})$ be the Möbius plane given in Remark 4.1.2. We construct three truncated Möbius planes $M_1^{(\vec{p})}$, $M_2^{(\vec{p})}$, and $M_4^{(\vec{p})}$, with the same point set $\mathcal{M}^{(\vec{p})} = \left\{ i + p_i(\frac{q^2+1}{2}) : 0 \leq i < \frac{q^2+1}{2} \right\}$, where each corresponds to $\left[G_{q^2+1}^{q+1}\right]_{\vec{p}}$, $\left[G_{q^2+1}^{2(q+1)}\right]_{\vec{p}}$, and $\left[G_{q^2+1}^{4(q+1)}\right]_{\vec{p}}$, respectively. More specifically,

1. $M_1^{\vec{p}} = (\mathcal{M}^{\vec{p}}, \{C \cap \mathcal{M}^{\vec{p}} : C \in \mathcal{C}\})$.
2. $M_2^{\vec{p}} = (\mathcal{M}^{\vec{p}}, \{\{j \in \mathcal{M}^{\vec{p}} : 2j \in C\} : C \in \mathcal{C}\})$.
3. $M_4^{\vec{p}} = (\mathcal{M}^{\vec{p}}, \{\{j \in \mathcal{M}^{\vec{p}} : 4j \in C\} : C \in \mathcal{C}\})$.

By Remark 4.1.2, $G_{q^2+1}^{q+1}$ is in correspondence with $(\mathcal{M}, \mathcal{C})$. Since each $\left[G_{q^2+1}^{q+1}\right]_{\vec{p}}$, $\left[G_{q^2+1}^{2(q+1)}\right]_{\vec{p}}$, and $\left[G_{q^2+1}^{4(q+1)}\right]_{\vec{p}}$ with columns labeled with $i + p_i(\frac{q^2+1}{2})$ is a subarray of $G_{q^2+1}^{q+1}$, having half of its columns, $M_1^{(\vec{p})}$, $M_2^{(\vec{p})}$, $M_4^{(\vec{p})}$ are each a truncated Möbius plane.

Theorem 4.2.31. $M_1^{(\vec{p})}$, $M_2^{(\vec{p})}$, and $M_4^{(\vec{p})}$ in Construction 4.2.30 give a set of 3 anti-cocircular truncated Möbius planes.

Proof.

Let B_1, B_2, and B_4 be circles of $M_1^{\vec{p}}$, $M_2^{\vec{p}}$, and $M_4^{\vec{p}}$, respectively. Let $I = B_1 \cap B_2 \cap B_4$. We must prove $|I| \leq 3$. Let $d \in I$ and $I_0 = \{i - d : i \in I\}$; note that $0 \in I_0$. Assume without loss of generality that $|I_0| > 1$. By Remark 4.2.5, for $i \in B_l$, $l = 1, 2, 4$, there exists $x \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$ such that $li \in C_x$. Hence, there exist C_s, C_u, and C_v, for $s, u, v \in D \setminus \{\frac{(q^2+1)(q+1)}{2}\}$ such that $i \in C_s$, $2i \in C_u$, and $4i \in C_v$ for any $i \in I_0$. Let $I_L = \{\Omega(L(\alpha^{i(q+1)})) : i \in I_0\}$. From Remark 4.2.28, we note that after the shift by d, we have changed $\vec{p}$ to $\vec{p'}$. Thus, by Proposition 4.2.13, $I_L \subseteq O^{(\vec{p'})} \cap P_a \cap Q_b \cap R_c$, where $P_a \hookrightarrow ax + a^q y + a^{q^2} z + a^{q^3} t = 0$, $Q_b \hookrightarrow bx^2 + b^q y^2 + b^{q^2} z^2 + b^{q^3} t^2 = 0$, $R_c \hookrightarrow cx^4 + c^q y^4 + c^{q^2} z^4 + c^{q^3} t^4 = 0$, ($a = \alpha^s$, $b = \alpha^u$, $c = \alpha^v$). Theorem 4.2.27 implies $|I_L| \leq 3$, therefore $|I| = |B_1 \cap B_2 \cap B_4| \leq 3$. ∎

In Table 4.4 and Table 4.5, we display the circles of $M_1^{(\vec{p})}$, $M_2^{(\vec{p})}$, and $M_4^{(\vec{p})}$ containing zero, for $q = 5$ with $\vec{p} = (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$ and $\vec{p} = (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$, respectively. By Theorem 4.2.31, the common intersection of any choice of three circles, one from each, has size at most three.

4.3 Construction of strength-4 covering arrays

In this section, we prove the existence of a CA$(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ in Theorem 4.3.1, which can be considered as an extension of Theorem 3.2.2 to higher dimension.

Theorem 4.3.1. Let q be an odd prime power. Let $\vec{p} = (p_0, p_1, \ldots, p_{\frac{q^2-1}{2}}) \in \{0, 1\}^{\frac{q^2+1}{2}}$. Let α be a primitive element in $\mathbb{F}_{q^4}$ and let $A_1 = A\left(\left[G_{q^2+1}^{q+1}\right]_{\vec{p}}\right)$, $A_2 = A\left(\left[G_{q^2+1}^{2(q+1)}\right]_{\vec{p}}\right)$, and $A_4 = A\left(\left[G_{q^2+1}^{4(q+1)}\right]_{\vec{p}}\right)$ be arrays obtained from α in Construction 3.1.1. The vertical concatenation of A_1, A_2, and A_4 with two copies of the all-zero rows removed is a CA$(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$.

Proof. Let M be the vertical concatenation of A_1, A_2, and A_4. Consider any four distinct columns i, j, k, l of M. Note that i, j, k, l are elements of truncated Möbius planes $M_1^{\vec{p}}$, $M_2^{\vec{p}}$, and $M_4^{\vec{p}}$, corresponding to A_1, A_2, and A_4, respectively. By Theorem 4.2.31, there exists no circles containing i, j, k, l in at least one of these three Möbius planes, say $M_x^{\vec{p}}$ for $x \in \{1, 2, 4\}$. By Remark 4.1.2, every non-zero row of the corresponding $q^4 \times 4$ sub-matrix of A_x indexed by column indices i, j, k, l has at most three zeros. By Theorem 3.1.5, all distinct 4-tuples corresponding to column indices i, j, k, l are covered in A_x and therefore in M. ∎

In Table 4.6, we display the size N_s of the CA$(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ obtained by Theorem 4.3.1 and the size N_c of the best-known covering arrays with $k = \frac{q^2+1}{2}$ obtained from [15], for any odd prime power $q \leq 25$. The column indicated by "Method" shows the method by which

Table 4.4: List of elements of the set D constructed in Construction 4.2.1, $\mathcal{M}^{\vec{p}}$ and circles of $(\mathcal{M}, \mathcal{C})$, $M_1^{\vec{p}}$, $M_2^{\vec{p}}$, and $M_4^{\vec{p}}$, containing zero, for $q = 5$, and $\vec{p} = (0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1)$.

$D = \{1, 5, 8, 11, 13, 25, 39, 40, 44, 55, 56, 62, 64, 65, 78, 87, 91, 106, 111, 117, 119, 123, 124, 125, 127, 136, 143, 146, 147, 152, 154\}$

$\mathcal{M}^{\vec{p}} = \{0, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25\}$

$x \in D \setminus \{78\}$	C_x	$C_x \cap \mathcal{M}^{\vec{p}}$	$\{j \in \mathcal{M}^{\vec{p}} : 2j \in C_x\}$	$\{j \in \mathcal{M}^{\vec{p}} : 4j \in C\}$
1	$\{0, 2, 4, 9, 15, 21\}$	$\{0, 15, 21\}$	$\{0, 14, 15\}$	$\{0, 14, 20\}$
5	$\{0, 1, 10, 19, 20, 23\}$	$\{0, 19, 20, 23\}$	$\{0, 18, 23\}$	$\{0, 18, 22\}$
8	$\{0, 6, 8, 9, 23, 24\}$	$\{0, 23, 24\}$	$\{0, 16, 17, 25\}$	$\{0, 15, 19, 21\}$
11	$\{0, 9, 18, 19, 22, 25\}$	$\{0, 18, 19, 22, 25\}$	$\{0, 22, 24\}$	$\{0, 24, 25\}$
13	$\{0, 2, 7, 13, 19, 24\}$	$\{0, 19, 24\}$	$\{0, 14, 25\}$	$\{0, 19, 20\}$
25	$\{0, 5, 11, 17, 22, 24\}$	$\{0, 17, 22, 24\}$	$\{0, 24, 25\}$	$\{0, 19, 25\}$
39	$\{0, 8, 12, 13, 14, 18\}$	$\{0, 14, 18\}$	$\{0, 17, 19, 20, 22\}$	$\{0, 15, 16, 23, 24\}$
40	$\{0, 4, 11, 14, 16, 19\}$	$\{0, 14, 16, 19\}$	$\{0, 15, 20, 21\}$	$\{0, 14, 17, 23\}$
44	$\{0, 2, 3, 17, 18, 20\}$	$\{0, 17, 18, 20\}$	$\{0, 14, 22, 23\}$	$\{0, 18, 20, 24\}$
55	$\{0, 6, 12, 17, 19, 21\}$	$\{0, 17, 19, 21\}$	$\{0, 16, 19\}$	$\{0, 16, 21\}$
56	$\{0, 1, 15, 16, 18, 24\}$	$\{0, 15, 16, 18, 24\}$	$\{0, 21, 22, 25\}$	$\{0, 17, 19, 24\}$
62	$\{0, 14, 15, 17, 23, 25\}$	$\{0, 14, 15, 17, 23, 25\}$	$\{0, 20\}$	$\{0, 23\}$
64	$\{0, 7, 10, 12, 15, 22\}$	$\{0, 15, 22\}$	$\{0, 18, 19, 24\}$	$\{0, 16, 22, 25\}$
65	$\{0, 9, 10, 13, 16, 17\}$	$\{0, 16, 17\}$	$\{0, 18, 21\}$	$\{0, 17, 22\}$
87	$\{0, 4, 5, 6, 10, 18\}$	$\{0, 18\}$	$\{0, 15, 16, 18, 22\}$	$\{0, 14, 21, 22, 24\}$
91	$\{0, 6, 11, 13, 15, 20\}$	$\{0, 15, 20\}$	$\{0, 16, 23\}$	$\{0, 18, 21\}$
106	$\{0, 3, 5, 8, 15, 19\}$	$\{0, 15, 19\}$	$\{0, 17\}$	$\{0, 15\}$
111	$\{0, 1, 2, 6, 14, 22\}$	$\{0, 14, 22\}$	$\{0, 14, 16, 20, 24\}$	$\{0, 20, 21, 23, 25\}$
117	$\{0, 1, 5, 13, 21, 25\}$	$\{0, 21, 25\}$	$\{0\}$	$\{0\}$
119	$\{0, 1, 4, 7, 8, 17\}$	$\{0, 17\}$	$\{0, 15, 17\}$	$\{0, 14, 15\}$
123	$\{0, 4, 12, 20, 24, 25\}$	$\{0, 20, 24, 25\}$	$\{0, 15, 19, 23, 25\}$	$\{0, 14, 16, 18, 19\}$
124	$\{0, 2, 5, 12, 16, 23\}$	$\{0, 16, 23\}$	$\{0, 14, 19, 21\}$	$\{0, 16, 17, 20\}$
125	$\{0, 3, 6, 7, 16, 25\}$	$\{0, 16, 25\}$	$\{0, 16, 21\}$	$\{0, 17, 21\}$
127	$\{0, 5, 7, 9, 14, 20\}$	$\{0, 14, 20\}$	$\{0, 20, 23\}$	$\{0, 18, 23\}$
136	$\{0, 3, 10, 14, 21, 24\}$	$\{0, 14, 21, 24\}$	$\{0, 18, 20, 25\}$	$\{0, 19, 22, 23\}$
143	$\{0, 3, 4, 13, 22, 23\}$	$\{0, 22, 23\}$	$\{0, 15, 24\}$	$\{0, 14, 25\}$
146	$\{0, 1, 3, 9, 11, 12\}$	$\{0\}$	$\{0, 19\}$	$\{0, 16\}$
147	$\{0, 8, 16, 20, 21, 22\}$	$\{0, 16, 20, 21, 22\}$	$\{0, 17, 21, 23, 24\}$	$\{0, 15, 17, 18, 25\}$
152	$\{0, 2, 8, 10, 11, 25\}$	$\{0, 25\}$	$\{0, 14, 17, 18\}$	$\{0, 15, 20, 22\}$
154	$\{0, 7, 11, 18, 21, 23\}$	$\{0, 18, 21, 23\}$	$\{0, 22\}$	$\{0, 24\}$

each of the best-known arrays was obtained. The reference for each method is mentioned. The column indicated by "$N_s - N_c$" shows the difference between the size of the array obtained by Theorem 4.3.1 and the size of the best-known covering array in [15]. We can see that for $q \geq 11$, we have an improvement of 21% to 25% in the size of covering arrays obtained in Theorem 4.3.1.

Corollary 4.3.2. For an odd prime power q, a CPHF$(3; \frac{q^2+1}{2}, q, 4)$ exists where each row is a CPHF$(1; \frac{q^2+1}{2}, q, 3)$.

Table 4.5: List of elements of the set D constructed in Construction 4.2.1, $\mathcal{M}^{\vec{p}}$ and circles of $(\mathcal{M}, \mathcal{C})$, $M_1^{\vec{p}}$, $M_2^{\vec{p}}$, and $M_4^{\vec{p}}$, containing zero, for $q = 5$, and $\vec{p} = (0, 1, 1, 1, 0, 0, 1, 1, 1, 1, 1, 1, 0)$.

$D = \{1, 5, 8, 11, 13, 25, 39, 40, 44, 55, 56, 62, 64, 65, 78, 87, 91, 106, 111, 117, 119, 123, 124, 125, 127, 136, 143, 146, 147, 152, 154\}$

$\mathcal{M}^{\vec{p}} = \{0, 4, 5, 12, 14, 15, 16, 19, 20, 21, 22, 23, 24\}$

$x \in D \setminus \{78\}$	C_x	$C_x \cap \mathcal{M}^{\vec{p}}$	$\{j \in \mathcal{M}^{\vec{p}} : 2j \in C_x\}$	$\{j \in \mathcal{M}^{\vec{p}} : 4j \in C\}$
1	$\{0, 2, 4, 9, 15, 21\}$	$\{0, 4, 15, 21\}$	$\{0, 14, 15\}$	$\{0, 14, 20\}$
5	$\{0, 1, 10, 19, 20, 23\}$	$\{0, 19, 20, 23\}$	$\{0, 5, 23\}$	$\{0, 5, 22\}$
8	$\{0, 6, 8, 9, 23, 24\}$	$\{0, 23, 24\}$	$\{0, 4, 12, 16\}$	$\{0, 15, 19, 21\}$
11	$\{0, 9, 18, 19, 22, 25\}$	$\{0, 19, 22\}$	$\{0, 22, 24\}$	$\{0, 12, 24\}$
13	$\{0, 2, 7, 13, 19, 24\}$	$\{0, 19, 24\}$	$\{0, 12, 14\}$	$\{0, 19, 20\}$
25	$\{0, 5, 11, 17, 22, 24\}$	$\{0, 5, 22, 24\}$	$\{0, 12, 24\}$	$\{0, 12, 19\}$
39	$\{0, 8, 12, 13, 14, 18\}$	$\{0, 12, 14\}$	$\{0, 4, 19, 20, 22\}$	$\{0, 15, 16, 23, 24\}$
40	$\{0, 4, 11, 14, 16, 19\}$	$\{0, 4, 14, 16, 19\}$	$\{0, 15, 20, 21\}$	$\{0, 4, 14, 23\}$
44	$\{0, 2, 3, 17, 18, 20\}$	$\{0, 20\}$	$\{0, 14, 22, 23\}$	$\{0, 5, 20, 24\}$
55	$\{0, 6, 12, 17, 19, 21\}$	$\{0, 12, 19, 21\}$	$\{0, 16, 19\}$	$\{0, 16, 21\}$
56	$\{0, 1, 15, 16, 18, 24\}$	$\{0, 15, 16, 24\}$	$\{0, 12, 21, 22\}$	$\{0, 4, 19, 24\}$
62	$\{0, 14, 15, 17, 23, 25\}$	$\{0, 14, 15, 23\}$	$\{0, 20\}$	$\{0, 23\}$
64	$\{0, 7, 10, 12, 15, 22\}$	$\{0, 12, 15, 22\}$	$\{0, 5, 19, 24\}$	$\{0, 12, 16, 22\}$
65	$\{0, 9, 10, 13, 16, 17\}$	$\{0, 16\}$	$\{0, 5, 21\}$	$\{0, 4, 22\}$
87	$\{0, 4, 5, 6, 10, 18\}$	$\{0, 4, 5\}$	$\{0, 5, 15, 16, 22\}$	$\{0, 14, 21, 22, 24\}$
91	$\{0, 6, 11, 13, 15, 20\}$	$\{0, 15, 20\}$	$\{0, 16, 23\}$	$\{0, 5, 21\}$
106	$\{0, 3, 5, 8, 15, 19\}$	$\{0, 5, 15, 19\}$	$\{0, 4\}$	$\{0, 15\}$
111	$\{0, 1, 2, 6, 14, 22\}$	$\{0, 14, 22\}$	$\{0, 14, 16, 20, 24\}$	$\{0, 12, 20, 21, 23\}$
117	$\{0, 1, 5, 13, 21, 25\}$	$\{0, 5, 21\}$	$\{0\}$	$\{0\}$
119	$\{0, 1, 4, 7, 8, 17\}$	$\{0, 4\}$	$\{0, 4, 15\}$	$\{0, 14, 15\}$
123	$\{0, 4, 12, 20, 24, 25\}$	$\{0, 4, 12, 20, 24\}$	$\{0, 12, 15, 19, 23\}$	$\{0, 5, 14, 16, 19\}$
124	$\{0, 2, 5, 12, 16, 23\}$	$\{0, 5, 12, 16, 23\}$	$\{0, 14, 19, 21\}$	$\{0, 4, 16, 20\}$
125	$\{0, 3, 6, 7, 16, 25\}$	$\{0, 16\}$	$\{0, 16, 21\}$	$\{0, 4, 21\}$
127	$\{0, 5, 7, 9, 14, 20\}$	$\{0, 5, 14, 20\}$	$\{0, 20, 23\}$	$\{0, 5, 23\}$
136	$\{0, 3, 10, 14, 21, 24\}$	$\{0, 14, 21, 24\}$	$\{0, 5, 12, 20\}$	$\{0, 19, 22, 23\}$
143	$\{0, 3, 4, 13, 22, 23\}$	$\{0, 4, 22, 23\}$	$\{0, 15, 24\}$	$\{0, 12, 14\}$
146	$\{0, 1, 3, 9, 11, 12\}$	$\{0, 12\}$	$\{0, 19\}$	$\{0, 16\}$
147	$\{0, 8, 16, 20, 21, 22\}$	$\{0, 16, 20, 21, 22\}$	$\{0, 4, 21, 23, 24\}$	$\{0, 4, 5, 12, 15\}$
152	$\{0, 2, 8, 10, 11, 25\}$	$\{0\}$	$\{0, 4, 5, 14\}$	$\{0, 15, 20, 22\}$
154	$\{0, 7, 11, 18, 21, 23\}$	$\{0, 21, 23\}$	$\{0, 22\}$	$\{0, 24\}$

Proof. The proof is immediate by Theorem 4.3.1. ∎

The generator matrices $G^{q+1}_{\frac{q^2+1}{2}}$, $G^{2(q+1)}_{\frac{q^2+1}{2}}$, and $G^{4(q+1)}_{\frac{q^2+1}{2}}$ with respect to the primitive polynomial $f(x) = x^4 + 5x^2 + 4x + 3$ over $\mathbb{F}_7$ is given in Fig. 4.3. Each of $G^{q+1}_{\frac{q^2+1}{2}}$, $G^{2(q+1)}_{\frac{q^2+1}{2}}$, and $G^{4(q+1)}_{\frac{q^2+1}{2}}$ corresponds to a row of a CPHF$(3; 25, 7, 4)$, and each column vector of these arrays, correspond to an entry in the corresponding column of the CPHF$(3; 25, 7, 4)$.

Table 4.6: Covering arrays of strength 4 obtained by Theorem 4.3.1 compared with the previously best-known CAs of strength 4 in [15] for odd prime power $q \leq 25$. Improvements in size are shown in bold.

q	$k=\frac{q^2+1}{2}$	CAs from Theorem 4.3.1	The previously best-known CAs [15]			
		$N_s = 3q^4-2$	N_c	Method	$N_s - N_c$	$(N_s-N_c)/N_c$
3	5	241	81	Derived from strength 5	160	1.975
5	13	1873	1225	2-Restricted SCPHF RE (CL) [18]	648	0.528
7	25	7201	6853	3-Restricted SCPHF RE (CL) [18]	348	0.050
9	41	19681	19593	2-Restricted SCPHF RE (CL) [18]	88	0.004
11	61	**43921**	55891	3,3-Restricted SCPHF RE (CL) [18]	−11970	−0.214
13	85	**85681**	109837	3,3-Restricted SCPHF RE (CL) [18]	−24156	−0.219
17	145	**250561**	329137	3-Restricted SCPHF RE (CL) [18]	−78576	−0.238
19	181	**390961**	520543	2,2-Restricted SCPHF RE (CL) [18]	−129582	−0.248
23	265	**839521**	1119361	CPHF IPO 4 (WCS) [66]	−279840	−0.249
25	313	**1171873**	1562497	CPHF IPO 4 (WCS) [66]	−390606	−0.249

Figure 4.3: The generator matrices $G^{q+1}_{\frac{q^2+1}{2}}$, $G^{2(q+1)}_{\frac{q^2+1}{2}}$, and $G^{4(q+1)}_{\frac{q^2+1}{2}}$ with respect to the primitive polynomial $f(x) = x^4 + 5x^2 + 4x + 3$ over $\mathbb{F}_7$.

$$G^{q+1}_{\frac{q^2+1}{2}} = \begin{bmatrix} 0&5&1&4&2&1&0&5&0&6&0&1&6&1&6&6&0&4&6&3&1&0&6&2&3 \\ 0&5&6&6&4&5&1&6&2&0&6&1&4&0&5&3&5&5&5&5&1&6&0&6&3 \\ 0&1&1&1&5&5&3&1&0&1&3&6&3&1&2&0&5&0&4&6&5&2&3&3&0 \\ 1&4&6&5&0&2&0&3&1&2&5&4&4&0&1&2&3&2&4&5&1&0&6&5&1 \end{bmatrix}$$

$$G^{2(q+1)}_{\frac{q^2+1}{2}} = \begin{bmatrix} 0&1&2&0&0&0&6&6&0&6&1&6&3&3&1&1&1&4&1&2&5&3&5&4&6 \\ 0&6&4&1&2&6&4&5&5&5&1&0&3&6&6&6&0&3&5&6&0&6&5&3&3 \\ 0&1&5&3&0&3&3&2&5&4&5&3&0&5&5&2&0&2&0&4&1&3&3&0&6 \\ 1&6&0&0&1&5&4&1&3&4&1&6&1&2&2&6&4&1&1&5&4&4&6&4&4 \end{bmatrix}$$

$$G^{4(q+1)}_{\frac{q^2+1}{2}} = \begin{bmatrix} 0&2&0&6&0&1&3&1&1&1&5&5&6&3&0&0&4&4&4&2&3&5&6&2&5 \\ 0&4&2&4&5&1&3&6&0&5&0&5&3&4&3&4&1&1&0&4&4&2&4&4&2 \\ 0&5&0&3&5&5&0&5&0&0&1&3&6&3&2&2&6&5&2&1&6&6&5&2&0 \\ 1&0&1&4&3&1&1&2&4&1&4&6&4&4&0&1&3&5&4&6&4&3&1&5&5 \end{bmatrix}$$

4.4 A recursive construction of strength-4 covering arrays using all points of the ovoid

In this section, we construct a strength-4 covering array using a recursive method. The main ingredients are the $\mathrm{CA}(q^4; 3, q^2+1, q)$ in Corollary 4.1.3 and the $\mathrm{CA}(3q^4-1; 4, \frac{q^2+1}{2}, 1)$ in Theorem 4.3.1 for an odd prime power q.

Theorem 4.4.1. Let q be an odd prime power. Suppose there exists a $\mathrm{CA}(N; 3, \frac{q^2+1}{2}, q)$. Then a $\mathrm{CA}(3q^4 + N(q-2); 4, q^2+1, q)$ exists.

Proof. Let $A(G^{q+1}_{q^2+1})$ be the $\mathrm{CA}_q(q^4; 3, q^2+1, q)$ in Corollary 4.1.3, and $A(G^{2(q+1)}_{\frac{q^2+1}{2}})$ and $A(G^{4(q+1)}_{\frac{q^2+1}{2}})$ be two $\mathrm{CA}_q(q^4; 3, \frac{q^2+1}{2}, q)$, which are sub-arrays of $A(G^{q+1}_{q^2+1})$. Note that $\left[A(G^{2(q+1)}_{q^2+1})\right.$

$= \left[A(G^{2(q+1)}_{\frac{q^2+1}{2}})|A(G^{2(q+1)}_{\frac{q^2+1}{2}})\right]$ and $\left[A(G^{4(q+1)}_{q^2+1})\right] = \left[A(G^{4(q+1)}_{\frac{q^2+1}{2}})|A(G^{4(q+1)}_{\frac{q^2+1}{2}})\right]$. Let R be a CA$(N; 3, \frac{q^2+1}{2}, q)$. Let X be the $3q^4 + N(q-2) \times (q^2+1)$ array described via its subarrays in Table 4.7, displayed using $q+1$ row blocks labeled from 0 to q. We show X is a CA$(3q^4 + N(q-2); 4, q^2+1, q)$.

$$X = \begin{array}{|c|c|}\hline A(G^{q+1}_{q^2+1}) & \\ \hline A(G^{2(q+1)}_{\frac{q^2+1}{2}}) & A(G^{2(q+1)}_{\frac{q^2+1}{2}}) \\ \hline A(G^{4(q+1)}_{\frac{q^2+1}{2}}) & A(G^{4(q+1)}_{\frac{q^2+1}{2}}) + e^0 \\ \hline R & R + e^1 \\ \hline R & R + e^2 \\ \hline \vdots & \vdots \\ \hline R & R + e^{q-2} \\ \hline \end{array}$$

Table 4.7: A CA$(3q^4 + N(q-2); 4, q^2+1, q)$ constructed in Theorem 4.4.1.

Every column c of X can be represented as (x_c, p_c) where $c = x_c + p_c(\frac{q^2+1}{2})$ and $0 \leq x_c < \frac{q^2+1}{2}$, $p_c \in \{0, 1\}$. Let $\{c_1, c_2, c_3, c_4\}$ be a set of four distinct column indices of X represented in this way by $\{(i, p_{c_1}), (j, p_{c_2}), (k, p_{c_3}), (l, p_{c_4})\}$, respectively. We analyze the three possible cases based on the multiset $\{i, j, k, l\}$, which by constructions have elements of multiplicity at most 2, since $p_{c_i} \in \{0, 1\}$; these cases are listed next:

1. i, j, k, l all distinct,
2. $l = i$; i, j, k distinct,
3. $i = k, j = l$, $0 \leq i < j < \frac{q^2+1}{2}$.

Case 1: In this case, we show that the coverage of c_1, c_2, c_3, c_4 is guaranteed by the first three row blocks of X. Since i, j, k, l are all distinct, there exists a $\vec{p} \in \{0, 1\}^{\frac{q^2+1}{2}}$ such that $p_i = p_{c_1}$, $p_j = p_{c_2}$, $p_k = p_{c_3}$, and $p_l = p_{c_4}$. By Theorem 4.3.1, the 4×4 sub-matrix corresponding to these column indices has rank equal to 4 in at least one of $\left[G^{q+1}_{q^2+1}\right]_{\vec{p}}$, $\left[G^{2(q+1)}_{q^2+1}\right]_{\vec{p}}$, and $\left[G^{4(q+1)}_{q^2+1}\right]_{\vec{p}}$. This means that the set of columns $S = \{i, j, k, l\}$ is covered is in at least one of $A\left(\left[G^{q+1}_{q^2+1}\right]_{\vec{p}}\right)$, $A\left(\left[G^{2(q+1)}_{q^2+1}\right]_{\vec{p}}\right)$, and $A\left(\left[G^{4(q+1)}_{q^2+1}\right]_{\vec{p}}\right)$. If S is covered in one of the first two arrays, then so is $\{c_1, c_2, c_3, c_4\}$ in X. In the case S is only covered in $A\left(\left[G^{4(q+1)}_{q^2+1}\right]_{\vec{p}}\right)$, we need to verify $\{c_1, c_2, c_3, c_4\}$ is covered in the third row block of X where for column x with $p_x = 1$, the elements have the element $e^0 = 1$ added to every element of this column. Indeed, since the set of covered tuples in the submatrix of $\left[A(G^{4(q+1)}_{\frac{q^2+1}{2}})|A(G^{4(q+1)}_{\frac{q^2+1}{2}})\right]$ indexed

by $\{c_1, c_2, c_3, c_4\}$ is $\mathbb{F}_q^4$, then the tuples in the sub-matrix of $\left[A(G^{4(q+1)}_{\frac{q^2+1}{2}})|A(G^{4(q+1)}_{\frac{q^2+1}{2}}) + e^0\right]$ is

$$\mathbb{F}_q^4 + (p_i, p_j, p_k, p_l) = \{(a, b, c, d) + (p_i, p_j, p_k, p_l) : (a, b, c, d) \in \mathbb{F}_q^4\} = \mathbb{F}_q^4,$$

which means $\{c_1, c_2, c_3, c_4\}$ is covered in X. Therefore, one of the first three row blocks of X guarantees coverage of all distinct four-tuples for c_1, c_2, c_3, c_4 in X.

Case 2: Let $\mathbb{F}_q = \{x_1, x_2, \ldots, x_q\}$ where $x_1 = 0$, $x_r = e^{r-2}$ for $2 \leq r \leq q$. The set $S_r = \{(a, b + p_{c_2}x_r, c + p_{c_3}x_r, a + x_r) : a, b, c \in \mathbb{F}_q, p_{c_2}, p_{c_3} \in \{0, 1\}\}$ is the set of four-tuples covered in row blocks $1 \leq r \leq q$ in columns c_i, c_j, c_k, c_l. First note that $|S_r| = q^3$, for all $1 \leq r \leq q$. We will show $S_r \cap S_{r'} = \emptyset$, whenever $r \neq r'$. Let $1 \leq r, r^{'} \leq q$ and $(a, b, c, d) \in S_r \cap S_{r'}$. Then $(a, b, c, a + x_r) = (a, b, c, a + x_{r'})$ which implies $r = r'$. Hence, $S_r \cap S_{r'} = \emptyset$, whenever $r \neq r'$. Let $S = \bigcup_{1 \leq r \leq q} S_r$. Then $|S| = q^4$, which implies $S = \mathbb{F}_q^4$. Thus, all distinct four-tuples are covered for c_1, c_2, c_3, c_4 in X.

Case 3: We claim that the 4×4 sub-matrix of $G^{q+1}_{q^2+1}$ in the row block zero and corresponding to column indices $i, j, i + \frac{q^2+1}{2}, j + \frac{q^2+1}{2}$ has rank equal to 4. Indeed, Lemma 4.2.9 shows that no blocks contain $i, j, i + \frac{q^2+1}{2}, j + \frac{q^2+1}{2}$ in the Möbius plane from Remark 4.1.2. Therefore, the corresponding points in the ovoid are not co-planar, and the rank of the 4×4 sub-matrix is four. Thus, all distinct four-tuples are covered in the row block zero. ∎

Remark 4.4.2. The first three row blocks of the array X in Theorem 4.4.1 give the coverage for all column indices i, j, k, l except when exactly three of them are distinct. This shows that the array obtained by the first three row blocks is a strength-3 covering array and "almost" a strength-4 covering array.

Remark 4.4.3. There exists a $\text{CA}(2q^3 - q; 3, \frac{q^2+1}{2}, q)$ for any prime power q. This has the best-known size for $\frac{q^2+1}{2}$ in [15]. This covering array can be obtained by using the first $\frac{q^2+1}{2}$ columns of the $\text{CA}(2q^3 - q; 3, q^2 - q + 3, q)$ from Theorem 3.3.8.

Corollary 4.4.4. For an odd prime power q, there exists a $\text{CA}(3q^4 + (q-2)(2q^3 - q); 4, q^2 + 1, q)$.

Proof. The result is obtained by using the $\text{CA}(2q^3 - q; 3, \frac{q^2+1}{2}, q)$ from Remark 4.4.3 in Theorem 4.4.1. ∎

In Table 4.8, we compare the size N_s of the strength-4 covering array obtained in Corollary 4.4.4, namely $N_s = 3q^4 + (2q^3 - q)(q - 2)$, with N_c, the size of the best-known strength-4 covering array with $k = q^2 + 1$ columns, and q symbols found in [15] as shown in Corollary 4.4.4. For odd prime powers $q \geq 11$, Corollary 4.4.4 improves bounds.

Table 4.8: Covering arrays of strength 4 obtained by Corollary 4.4.4 compared with the previously best-known CAs of strength 4 in [15] for odd prime power $q \leq 25$. Improvements in rows are shown in bold.

q	$k = q^2 + 1$	Obtained by Corollary 4.4.4	The previously best-known CAs [15]			
		$N_s = 3q^4 + (2q^3 - q)(q - 2)$	N_c	Method	$N_s - N_c$	$(N_s - N_c)/N_c$
3	10	294	159	CPHF 3-stage (TJ-IM) [32]	135	0.849
5	26	2610	1865	Restricted CPHF Sim Annealing (TJ-IM) [15]	745	0.399
7	50	10598	9247	3-Restricted SCPHF RE (CL) [18]	1351	0.146
9	62	29826	26241	CPHF IPO 4 (WCS) [66]	3585	0.136
11	122	**67782**	70521	3,3-Restricted SCPHF RE (CL) [18]	−2739	−0.038
13	170	**133874**	138385	3,3-Restricted SCPHF RE (CL) [18]	−4511	−0.032
17	290	**397698**	412369	3,2-Restricted SCPHF RE (CL) [18]	−14671	−0.035
19	362	**623846**	644347	3,2-Restricted SCPHF RE (CL) [18]	−20501	−0.031
23	530	**1350054**	1398101	2,2-Restricted SCPHF RE (CL) [18]	−48047	−0.034
25	626	**1890050**	1951825	2,2-Restricted SCPHF RE (CL) [18]	−61775	−0.031

Chapter 5

New families of strength-3 covering arrays using linear feedback shift register sequences

The results presented in this chapter have been published in [55].

The strength-3 covering array $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ in Theorem 3.2.2 has a strong property: it is constructed by the vertical concatenation of two $\mathrm{OA}_q(q^3;2,q^2+q+1,q)$, which correspond to the generator matrices $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ in Construction 3.1.1. This property makes the $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ suitable for use in a recursive construction to obtain larger strength-3 covering arrays, which is the objective of this chapter.

Roux [53] pioneered a type of recursive construction for covering arrays of strength 3, which is generalized for strength t [36, 37], especially for $t=3$ [10, 11, 20] and $t=4$ [20, 29, 30, 36]. In this chapter, we use Roux-type constructions for covering arrays of strength $t=3$ and present a new generalization of Roux-type construction in Theorem 5.2.6. Roux-type constructions require several combinatorial designs as ingredients. We present the ingredients for our constructions next. Let q be a prime power. We employ $\mathrm{OA}_{q^{m-2}}(q^m;2,\frac{q^m-1}{q-1},q)$ Section 3.1, $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ Theorem 3.2.2, $\mathrm{OA}(q^t;t,q+1,q)$ Theorem 5.1.1, $\mathrm{CA}(2q^2-q;2,q^2+q+1,q)$ [19], $\mathrm{CA}(2q^3-1;3,q^2,q)$ [48], $\mathrm{CA}(2q^3-q;3,q^2,q)$ for even prime powers [17], and $\mathrm{CA}(2q^3-q;3,q^2-q+1,q)$, and as well as difference covering arrays $\mathrm{DCA}(q;2,q,q)$ and $\mathrm{DCA}(2q-1;2,q^2,q)$, defined in Section 5.1.3 as the main ingredients of our general theorem.

As seen in Theorem 3.2.2, the $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ has a significant property: for q prime power, $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ is constructed by the vertical concatenation of two $\mathrm{OA}_q(q^3;2,q^2+q+1,q)$. This fact is a key property exploited in our constructions. Another vital property exploited in our constructions is the existence of a special connection between the ingredients which produces redundant rows that can be removed. Using these two properties allows us to obtain new families of covering arrays of strength 3. We employ x copies of $\mathrm{CA}(2q^3-1;3,q^2+q+1,q)$ where $x\in\{2,q,q+1,q^2,q^2-q+1\}$ that we call x-plication and obtain $\mathrm{CA}(4q^3-5q^2+2q;3,2(q^2+q+1),q)$, $\mathrm{CA}(5q^3-6q^2+2q;3,q(q^2+q+1),q)$,

$\mathrm{CA}(8q^3-10q^2+4q-1;3,q^2(q^2+q+1),q)$, $\mathrm{CA}(8q^3-10q^2+3q;3,(q^2-q+1)(q^2+q+1),q)$, for every prime power q, $\mathrm{CA}(8q^3-10q^2+3q;3,q^2(q^2+q+1),q)$ for every even prime power q, and $\mathrm{CA}(6q^3-\frac{13}{2}q^2+\frac{5}{2}q-1;3,(q+1)(q^2+q+1),q)$ for every odd prime power q. These covering arrays improve several upper bounds on best covering array numbers of strength 3 found in [15].

The structure of this chapter is as follows. In Section 5.1, we give the necessary background and auxiliary arrays that will be used in our new construction in Section 5.2. In Section 5.2, we give a general construction (Theorem 5.2.6) and use it to construct new families of covering arrays of strength 3. In Section 5.3, we show improvements in the best-known upper bounds obtained with our constructions.

5.1 Necessary background on auxiliary arrays

5.1.1 Bush's construction and related results

In [8], Bush studied the construction of orthogonal arrays of index unity. Two main results of Bush are given in Theorem 5.1.1 and Theorem 5.1.3.

Theorem 5.1.1 (Bush's construction, [31])**.** If q is a prime power and $q \geq t-1 \geq 0$, then an $\mathrm{OA}(q^t;t,q+1,q)$ exists.

The proof of Theorem 5.1.1 gives a construction of an $\mathrm{OA}(q^t;t,q+1,q)$ as follows; let $\mathbb{F}_q=\{a_1,a_2,\ldots,a_q\}$ and $f_i(x)=c_{t-1}^i x^{t-1}+c_{t-2}^i x^{t-2}+\cdots+c_1^i x+c_0^i$ over $\mathbb{F}_q$, $i=1,\ldots,q^t$, be distinct polynomials of degree at most $t-1$ over $\mathbb{F}_q$. Build array $A=(A_{i,j})$ where $A_{i,j}=f_i(a_j)$ and $A_{i,q+1}=c_{t-1}^i$, $1\leq j\leq q$. This construction is displayed in Fig. 5.1. Bush's construction of an $\mathrm{OA}(q^t;t,q+1,q)$ for $q=2$, $t=3$ and $q=3$, $t=2$ are displayed in Fig. 5.2. The orthogonal array in Corollary 5.1.2 can be built by removing column $q+1$ of Bush's construction, which provides an $\mathrm{OA}(q^t;t,q,q)$ with q distinct constant rows corresponding to polynomials $f_i(x)=c_0^i$, for each $c_0^i\in\mathbb{F}_q$.

Corollary 5.1.2. If q is a prime power and $q\geq t-1\geq 0$, then an $\mathrm{OA}(q^t;t,q,q)$ exists, containing q distinct constant rows.

An extra column can be added when q is a power of two and $t=3$: $A_{i,q+2}=c_1^i$, $1\leq i\leq q^3$.

Theorem 5.1.3 ([31])**.** If $q=2^m$, $m\geq 1$, then there exist an $\mathrm{OA}(q^3;3,q+2,q)$.

Definition 5.1.4. A *covering ordered design* denoted by $\mathrm{COD}(N;t,k,v)$ is an $N\times k$ array over an alphabet of v symbols with the property that every $N\times t$ sub-array contains each non-constant t-tuple on the v symbols at least once.

Proposition 5.1.5. Let q be a prime power. Then a $\mathrm{COD}(q^t-q;t,q,q)$ exists.

Proof. Consider the $\mathrm{OA}(q^t;t,q,q)$ in Corollary 5.1.2. Remove the identical rows $[c_0^i,\ldots,c_0^i]$ corresponding to the polynomials $f_i(x)=c_0^i$ for every $c_0^i\in\mathbb{F}_q$. ∎

Figure 5.1: Bush's construction of an $\mathrm{OA}(q^t; t, q+1, q)$ for prime power q.

$f_1(a_1)$	$f_1(a_2)$	$f_1(a_3)$	$\ldots$	$f_1(a_j)$	$\ldots$	$f_1(a_q)$	c^1_{t-1}
$f_2(a_1)$	$f_2(a_2)$	$f_2(a_3)$	$\ldots$	$f_2(a_j)$	$\ldots$	$f_2(a_q)$	c^2_{t-1}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$	$\vdots$
$f_i(a_1)$	$f_i(a_2)$	$f_i(a_3)$	$\ldots$	$f_i(a_j)$	$\ldots$	$f_i(a_q)$	c^i_{t-1}
$\vdots$	$\vdots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$	$\vdots$	$\ldots$
$f_{q^t}(a_1)$	$f_{q^t}(a_2)$	$f_{q^t}(a_3)$	$\ldots$	$f_{q^t}(a_j)$	$\ldots$	$f_{q^t}(a_q)$	$c^{q^t}_{t-1}$

Figure 5.2: Bush's construction of an $\mathrm{OA}(8; 3, 3, 2)$ (left) and an $\mathrm{OA}(9; 2, 4, 3)$ (right). The column labeled by C displays the coefficient of x^{t-1} in f.

f	$f(0)$	$f(1)$	C
0	0	0	0
1	1	1	0
x	0	1	0
$x+1$	1	0	0
x^2	0	1	1
x^2+1	1	0	1
x^2+x	0	0	1
x^2+x+1	1	1	1

f	$f(0)$	$f(1)$	$f(2)$	C
0	0	0	0	0
1	1	1	1	0
2	2	2	2	0
x	0	1	2	1
$x+1$	1	2	0	1
$x+2$	2	0	1	1
$2x$	0	2	1	2
$2x+1$	1	0	2	2
$2x+2$	2	1	0	2

Figure 5.3: $\mathrm{COD}(6; 2, 3, 3)$.

0	1	2
1	2	0
2	0	1
0	2	1
1	0	2
2	1	0

Fig. 5.3 shows a $\mathrm{COD}(6; 2, 3, 3)$ obtained by removing the first three rows and the rightmost column of the $\mathrm{OA}(9; 2, 4, 3)$ presented in Fig. 5.2.

5.1.2 Product of arrays of strength two and partitioned covering arrays

Let $S = (s_{v,w})$ be an $M \times k$ array and let $T = (t_{v',w'})$ be an $N \times l$ array, then the product of S and T, denoted by $S \bigotimes T = (x_{i,jk+z})$ is an $(M+N) \times kl$ array with:

$$x_{i,jk+z} = \begin{cases} s_{i,z} & 0 \le i \le M-1, 0 \le j \le l-1, 0 \le z \le k-1, \\ t_{i-M,j} & M \le i \le M+N-1, 0 \le j \le l-1, 0 \le z \le k-1. \end{cases}$$

Let A be an $m \times n$ array and $1 \leq i \leq n$. The matrix kA^i denotes an $m \times k$ array where the columns are equal and identical to the column i of A. Using this notation, we can write

$$S \bigotimes T = \begin{array}{|c|c|c|c|} \hline S & S & \dots & S \\ \hline kT^1 & kT^2 & \dots & kT^l \\ \hline \end{array}.$$

Lemma 5.1.6 ([19])**.** Let S be a CA$(N; 2, k, s)$ and let T be a CA$(M; 2, l, s)$. Then $S \bigotimes T$ is a CA$(N + M; 2, kl, s)$.

Definition 5.1.7. A *partitioned covering array* denoted by PCA$(N; 2, (k_1, k_2), v)$ is a covering array of strength 2 which admits the structure below:

$$\begin{array}{|c|c|} \hline A_1 & A_2 \\ \hline P & X \\ \hline \end{array},$$

where A_1 is an $(N - v) \times k_1$ array, A_2 is an $(N - v) \times k_2$ array, P is a $v \times k_1$ array of constant rows $[a, \dots, a]$ for each $a \in [1, v]$, and X is a $v \times k_2$ array. An SCA$(N; 2, (k_1, k_2), v)$ is a PCA$(N; 2, (k_1, k_2), v)$ with the additional property that all elements of X are equal.

Theorem 5.1.8 ([19])**.** If a PCA$(N; 2, (k_1, k_2), v)$ and an SCA$(M; 2, (l_1, l_2), v)$ both exist, then a PCA$(N + M - v; 2, (k_1 l_1, k_1 l_2 + k_2 l_1), v)$ exists.

Suppose the PCA$(N; 2, (k_1, k_2), v)$ has ingredients A_1, A_2, D, X, and the SCA$(M; 2, (l_1, l_2), v)$ has ingredients B_1, B_2, D, and O; where D is an array of v distinct rows each with identical symbols, and O is an array with zero elements with appropriate dimension. The proof of Theorem 5.1.8 gives a PCA$(N + M - v; 2, (k_1 l_1, k_1 l_2 + k_2 l_1), v)$ constructed as follows where $l_1 X$ denotes l_1 copies of X side by side:

$$\begin{array}{|c|c|c|} \hline A_1 \bigotimes B_1 & A_2 \bigotimes B_1 & A_1 \bigotimes B_2 \\ \hline D & l_1 X & O \\ \hline \end{array}.$$

Corollary 5.1.9. Let q be a prime power. Then there exists CA$(2q^2 - q; 2, q^2 + 2q, q)$.

Proof. For q prime power, let B be the OA$(q^2; 2, q + 1, q)$ constructed in Theorem 5.1.1. Then B is a SCA$(q^2; 2, (q, 1), q)$, as it can be partitioned as

$$B = \begin{array}{|c|c|} \hline F & C \\ \hline P & O \\ \hline \end{array},$$

where the second row block corresponds to the polynomials of degree 0, and the first row block corresponds to the polynomials of degree 1, with subarrays F and C being, respectively, the $COD(q^2 - q; 2, q, q)$ in Proposition 5.1.5 and the corresponding $(q^2 - q) \times 1$ array which is the last column of B without entries equal to zero. Then, using B as both ingredients in Theorem 5.1.8, a PCA$(2q^2 - q; 2, (q^2, 2q), q)$ exists which is a CA$(2q^2 - q; 2, q^2 + 2q, q)$. The structure of the constructed array is displayed in Fig. 5.4 where O is a $q \times q$ array with zero entries and D is a $q \times q^2$ array where each row is $[a, \dots, a]$ for each $a \in \mathbb{F}_q$. ∎

Figure 5.4: Construction of a $\mathrm{CA}(2q^2-q;2,q^2+2q,q)$ for prime power q.

$F \bigotimes F$	$C \bigotimes F$	$F \bigotimes C$
D	O	O

Fig. 5.5 shows a $\mathrm{PCA}(9;2,(3,1),3)$, which is obtained by relocating the first the three rows of $\mathrm{OA}(9;2,4,3)$ in Fig. 5.2 to the last three rows. Since the last three entries of the rightmost column are identical to zero, it is an $\mathrm{SCA}(9;2,(3,1),3)$. In Fig. 5.5, the arrays F, C, P, and O introduced in the proof of Corollary 5.1.9 are shown. Fig. 5.6 presents the $\mathrm{CA}(15;2,15,3)$ obtained in Corollary 5.1.9.

Figure 5.5: $\mathrm{PCA}(9;2,(3,1),3)$.

$$\begin{array}{|c|c|}\hline F & C \\ \hline P & O \\ \hline \end{array} = \left[\begin{array}{ccc|c} 0&1&2&1\\ 1&2&0&1\\ 2&0&1&1\\ 0&2&1&2\\ 1&0&2&2\\ 2&1&0&2 \\ \hline 0&0&0&0\\ 1&1&1&0\\ 2&2&2&0 \end{array}\right]$$

Figure 5.6: $\mathrm{CA}(15;2,15,3)$ obtained in Corollary 5.1.9 for $q=3$.

$$\begin{array}{|c|c|c|}\hline F \bigotimes F & C \bigotimes F & F \bigotimes C \\ \hline D & O & O \\ \hline \end{array} = \left[\begin{array}{ccc|ccc|ccc||ccc||ccc} 0&1&2&0&1&2&0&1&2&1&1&1&0&1&2\\ 1&2&0&1&2&0&1&2&0&1&1&1&1&2&0\\ 2&0&1&2&0&1&2&0&1&1&1&1&2&0&1\\ 0&2&1&0&2&1&0&2&1&2&2&2&0&2&1\\ 1&0&2&1&0&2&1&0&2&2&2&2&1&0&2\\ 2&1&0&2&1&0&2&1&0&2&2&2&2&1&0 \\ \hline 0&0&0&1&1&1&2&2&2&0&1&2&1&1&1\\ 1&1&1&2&2&2&0&0&0&1&2&0&1&1&1\\ 2&2&2&0&0&0&1&1&1&2&0&1&1&1&1\\ 0&0&0&2&2&2&1&1&1&0&2&1&2&2&2\\ 1&1&1&0&0&0&2&2&2&1&0&2&2&2&2\\ 2&2&2&1&1&1&0&0&0&2&1&0&2&2&2 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ 1&1&1&1&1&1&1&1&1&0&0&0&0&0&0\\ 2&2&2&2&2&2&2&2&2&0&0&0&0&0&0 \end{array}\right]$$

5.1.3 Difference covering arrays

Difference covering arrays have a fundamental role in this chapter. Our purpose is to construct difference covering arrays with entries from a finite field $\mathbb{F}_q$.

Definition 5.1.10. A difference covering array $D = (d_{ij})$ over a finite group G of order v, with $\bigodot$ as its binary operation, denoted by $\mathrm{DCA}(N; G, t, k, v)$, is an $N \times k$ array with entries from G having the property that for any t distinct columns $j_1, j_2, ..., j_t$, the set $\{((d_{(i,j_1)} \bigodot d^{-1}_{(i,j_2)}), (d_{(i,j_1)} \bigodot d^{-1}_{(i,j_3)}), \ldots, (d_{(i,j_1)} \bigodot d^{-1}_{(i,j_t)})) : 1 \leq i \leq N\}$ contains every non-zero $(t-1)$-tuple over G at least once. Here, N is the *size* and t is the *strength* of the difference covering array.

In this section, a difference covering array of strength 2 is introduced and studied. Unless otherwise specified, a difference covering array will always mean a DCA of strength 2 throughout this chapter. When $G = \mathbb{F}_q$ for a prime power q (additive group of $\mathbb{F}_q$), we omit it from the notation and write $\mathrm{DCA}(N; t, k, v)$. We denote by $\mathrm{DCAN}(t, k, v)$ the minimum N for which a $\mathrm{DCA}(N; t, k, v)$ exists. It seems difficult to find difference covering arrays of general strength t. The existence of $\mathrm{DCA}(q+1; G, 2, 4, q)$ where G is a group of order q and $q \equiv 2 \pmod 4$ is proven in [68]. It is well-known that the multiplication table for the finite field $\mathbb{F}_q$ is a $\mathrm{DCA}(q; 2, q, q)$ [20], which has an important role in our new families of covering arrays of strength 3 in Section 5.2. Using $\mathrm{DCA}(q; 2, q, q)$, we show that for a prime power q and $n \geq 1$ a $\mathrm{DCA}(nq - (n-1); 2, q^n, q)$ exists.

Theorem 5.1.11 ([20])**.** The multiplication table for the finite field $\mathbb{F}_q$ is a $\mathrm{DCA}(q; 2, q, q)$.

The $\mathrm{DCA}(q; 2, q, q)$ is given in Fig. 5.7, where e is the primitive element of $\mathbb{F}_q$.

Figure 5.7: Construction of a $\mathrm{DCA}(q; 2, q, q)$ for a prime power q. Here e is a primitive element of $\mathbb{F}_q$.

$$\begin{bmatrix}
0 & 0 & 0 & \ldots & 0 & 0 \\
0 & 1 & e & \ldots & e^{q-3} & e^{q-2} \\
0 & e & e^2 & \ldots & e^{q-2} & 1 \\
0 & e^2 & e^3 & \ldots & 1 & e \\
\vdots & \vdots & \vdots & \ldots & \vdots & \vdots \\
0 & e^{q-3} & e^{q-2} & \ldots & e^{q-5} & e^{q-4} \\
0 & e^{q-2} & 1 & \ldots & e^{q-4} & e^{q-3}
\end{bmatrix}$$

We can use the product of two arrays to construct new difference covering arrays which is presented in the next theorem.

Before presenting the theorems, we define the notion of "column block" and "row block" which facilitates our notations in the proofs. Let X be an array arbitrarily divided into a number of array blocks $A_{i,j}$, $0 \leq i \leq r-1$ and $0 \leq j \leq c-1$, where all $A_{i,j}$ with same column index j has an equal number of columns, and all $A_{i,j}$ with same row index i has an equal number of rows, as given below:

$$X = \begin{array}{|c|c|c|c|} \hline A_{0,0} & A_{0,1} & \cdots & A_{0,c-1} \\ \hline A_{1,0} & A_{1,1} & \cdots & A_{1,c-1} \\ \hline \vdots & \vdots & \cdots & \vdots \\ \hline A_{r-1,0} & A_{r-1,1} & \cdots & A_{r-1,c-1} \\ \hline \end{array}.$$

We use *column block* $c^\star$ to refer to all $A_{i,c^\star}$, $0 \leq i \leq r-1$ in order, and *row block* $r^\star$ to refer to all $A_{r^\star,j}$, $0 \leq j \leq c-1$ in order.

Theorem 5.1.12. If A is a DCA$(N_1; 2, k_1, v)$ and B is a DCA$(N_2; 2, k_2, v)$, then $A \bigotimes B$ is a DCA$(N_1 + N_2; 2, k_1 k_2, v)$.

Proof. Let i and j be two column indices of $A \bigotimes B$. If i and j are in the same column block, then by considering the first row block of $A \bigotimes B$, i and j are two distinct column indices of A. Since A is a difference covering array, then for this choice of column indices, we have all possible differences. If i and j are in different column blocks, then by considering the second row block of $A \bigotimes B$, i and j are two distinct column indices of B. Since B is a difference covering array, then for this choice of column indices, we have all possible differences. Therefore $A \bigotimes B$ is a difference covering array. ∎

Theorem 5.1.13. For any prime power q, and $n \geq 1$, there exist a DCA$(n(q-1)+1; 2, q^n, q)$.

Proof. Let D be the DCA$(q; 2, q, q)$ given in Theorem 5.1.11. Iterating Theorem 5.1.12, using n copies of D in a product $((((D \bigotimes D) \bigotimes D) \cdots \bigotimes D) \bigotimes D)$ yields a DCA$(nq; 2, q^n, q)$. Since the constructed array has n rows consisting of only zeroes, $n-1$ such rows can be removed to obtain a DCA$(n(q-1)+1; 2, q^n, q)$. ∎

By Theorem 5.1.13, there exist a DCA$(2q-1; 2, q+1, q)$. The next theorem establishes an improvement on the size by $\frac{q-1}{2} - 1$ rows when q is an odd prime power.

Theorem 5.1.14. For an odd prime power q, there exist a DCA$(q + \frac{q-1}{2}; 2, q+1, q)$.

Proof. Let D be the DCA$(q; 2, q, q)$ in Theorem 5.1.11 with given construction in Fig. 5.7 where e is a primitive element of $\mathbb{F}_q$ and $D^\star$ be the array obtained by removing the first row and column of D. Let D_1 be the array consist of the first $\frac{q-1}{2}$ rows of $D^\star$, and D_2 be the array consist of the last $\frac{q-1}{2}$ rows of $D^\star$. Let O be a $\frac{q-1}{2} \times 1$ array with zero entries. Let $X_1 = [e^1, e^2, \ldots, e^{(q-1)/2}]^T$ be a $\frac{q-1}{2} \times 1$ array. Let G^q be the array constructed from D_1, D_2, O, X_1, and X_2 with a zero row as the last row as given below:

$$G^q = \begin{array}{|c|c|c|} \hline D_1 & X_1 & O \\ \hline D_1 & O & X_1 \\ \hline D_2 & O & O \\ \hline 0 \ldots 0 & 0 & 0 \\ \hline \end{array}.$$

An example for G^5 is given in Fig. 5.8.

Let i and j be two column indices of G^q. If i and j are in the first two column blocks, then differences are covered, since the sub-matrix obtained by deleting the first row block and the last column block is equivalent to D. A similar argument holds if i and j are contained in the union of the first and the third column blocks, as deleting the second column block and the second row block gives a matrix equivalent to D. If i and j are in the two last column blocks, the differences are covered using the first, second and fourth row blocks, since $\mathbb{F}_q = \{0, e^i, -e^i \ : \ i = 0, \ldots, (q-1)/2 - 1\}$. Indeed, this comes from the fact that $-1 = e^{(q-1)/2}$ which implies $-e^i = e^{(q-1)/2+i}$ for an odd prime power q. Therefore, for any odd prime power q, a DCA$(q + \frac{q-1}{2}; 2, q+1, q)$ exists. ∎

Figure 5.8: G^5 is a DCA$(7; 2, 6, 5)$ constructed by Theorem 5.1.14. Here e is a primitive element of $\mathbb{F}_5$.

$$G^5 = \left[\begin{array}{cccccc} 1 & e^1 & e^2 & e^3 & e^1 & 0 \\ e^1 & e^2 & e^3 & 1 & e^2 & 0 \\ \hline 1 & e^1 & e^2 & e^3 & 0 & e^1 \\ e^1 & e^2 & e^3 & 1 & 0 & e^2 \\ \hline e^2 & e^3 & 1 & e^1 & 0 & 0 \\ e^3 & 1 & e^1 & e^2 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right] \qquad G^5 = \left[\begin{array}{cccccc} 1 & 2 & 4 & 3 & 2 & 0 \\ 2 & 4 & 3 & 1 & 3 & 0 \\ \hline 1 & 2 & 4 & 3 & 0 & 2 \\ 2 & 4 & 3 & 1 & 0 & 3 \\ \hline 4 & 1 & 3 & 2 & 0 & 0 \\ 3 & 1 & 2 & 4 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

$$e^1 = -e^3$$
$$e^2 = -e^4$$

Using $e = 2$ in $\mathbb{F}_5 \cong \mathbb{Z}_5$
$$2 = -3$$
$$1 = -4$$

We define *added arrays* which will be used widely in Section 5.2, as well as in Proposition 5.1.16.

Definition 5.1.15. Let $A = (a_{ij})$ where $1 \leq i \leq m$ and $1 \leq j \leq n$ be an array with entries from $\mathbb{F}_q$ and let $x \in \mathbb{F}_q$. The matrix $B = (b_{ij})$ where $b_{ij} = a_{ij} + x$ is an *added array* with respect to A and denoted by $B = A + x$.

We can construct a covering array of strength 2 by using difference covering arrays.

Proposition 5.1.16. Let D be the DCA$(N; 2, k, q)$ where q is a prime power, then the vertical concatenation of $D+x_t$ for each distinct $x_t \in \mathbb{F}_q$, where $1 \leq t \leq q$ is a CA$(qN; 2, k, q)$.

Proof. Let A be an array constructed by vertical concatenation of $D+x_t$ for each $1 \leq t \leq q$. Let $\{i, j\}$ be a pair of arbitrary column indices of A. Let S_{i,j,x_t} be the set of all tuples that are rows of the sub-array of $D + x_t$ indexed by columns $\{i, j\}$; and let $S_{i,j} = S_{i,j,x_1} \cup S_{i,j,x_2} \cup \cdots \cup S_{i,j,x_q}$. Since $S_{i,j,x_t} \cap S_{i,j,x_{t'}} = \emptyset$ for $t \neq t'$, and $|S_{i,j,x_t}| = q$, then $|S_{i,j}| = q^2$, and A is CA$(qN; 2, k, q)$. ∎

5.2 New families of covering arrays of strength 3

The following theorems are Roux-type constructions for covering arrays of strength 3. In [20, 57], a theorem from Roux's Ph.D. dissertation [53] is given.

Theorem 5.2.1 (Roux, [53]). $\mathrm{CAN}(3, 2k, 2) \leq \mathrm{CAN}(3, k, 2) + \mathrm{CAN}(2, k, 2)$.

A generalization of Roux's theorem for any alphabet v is given in the next theorem.

Theorem 5.2.2 (Chateauneuf-Kreher doubling, [10]). For $v \geq 2$, $\mathrm{CAN}(3, 2k, v) \leq \mathrm{CAN}(3, k, v) + (v-1)\,\mathrm{CAN}(2, k, v)$.

The next theorem considers l-plication instead of duplication. This theorem uses a difference covering array.

Theorem 5.2.3 (Cohen-Colbourn-Ling, [11]). $\mathrm{CAN}(3, lk, v) \leq \mathrm{CAN}(3, k, v) + \mathrm{CAN}(3, l, v) + \mathrm{CAN}(2, l, v) \times \mathrm{DCAN}(2, k, v)$.

The next theorem is a different generalization of Roux's construction for strength 3, and q a prime power.

Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker, [20]). For any prime power $q \geq 3$, $\mathrm{CAN}(3, qk, q) \leq \mathrm{CAN}(3, k, q) + (q-1)\,\mathrm{CAN}(2, k, q) + q^3 - q^2$.

This section presents a different generalization of Roux-type constructions, which we call "the general theorem". For a prime power q, we use a $\mathrm{CPHF}(n; k, q, 3)$ such that each row is a $\mathrm{CPHF}(1; k, q, 2)$. The covering array of strength 2 constructed by each $\mathrm{CPHF}(1; k, q, 2)$ plays two roles simultaneously: it is an ingredient of the covering array of strength 3 and is a covering array of strength 2. Theorem 5.2.6 takes advantage of this property to reduce the size of CAs obtained in Roux-type constructions. First, we present Lemma 5.2.5 which will be used in Theorem 5.2.6. The proof of Lemma 5.2.5 is trivial and it is not given here.

Lemma 5.2.5. Let $t \geq 1$ and let $T = \mathbb{F}_q^t$ be the set of t-tuples over $\mathbb{F}_q$. Let $a = (a_1, a_2, \ldots, a_t) \in \mathbb{F}_q^t$. Then $T + a = \{x + a : x \in T\} = T$.

Theorem 5.2.6 (The general theorem). Let q be a prime power. Suppose the following ingredients exist:

1. a $\mathrm{CPHF}(n; k, q, 3)$ such that each of its rows is a $\mathrm{CPHF}(1; k, q, 2)$ (Each row generates a covering array of strength 2.);
2. a $\mathrm{CA}(N_1; 2, k, q)$;
3. a $\mathrm{DCA}(m; 2, x, q)$;
4. a $\mathrm{CA}(N_2; 3, x, q)$.

Let $p = max\{m - n, 0\}$. Then, there exists a $\mathrm{CA}(nq^3 + pN_1 + N_2; 3, xk, q)$.

Proof. Let A be such a CPHF$(n;k,q,3)$ and let $A_1, A_2, \ldots, A_n$ be the covering arrays of strength 2 produced by each row of A. Let P be a CA$(N_1;2,k,q)$, let $D = (d_{ij})$ be a DCA$(m;2,x,q)$ where $1 \leq i \leq m$ and $1 \leq j \leq x$, and let C be a CA$(N_2;3,x,q)$. Consider the case $m \geq n$. We describe the construction of the CA$(nq^3+(m-n)N_1+N_2;3,xk,q)$ next. Index the columns of X from 0 to $xk-1$ and organize them in x consecutive column blocks where each block has k columns. Index the rows of X from 0 to $nq^3+(m-n)N_1+N_2-1$ and organize them in $m+1$ row blocks with q^3 consecutive rows for each of the first n row blocks, N_1 rows for each of the next $m-n$ row blocks, and N_2 rows for the last row block. For row block $1 \leq r \leq n$ and column block c use added array $A_r + d_{rc}$, for row block $n+1 \leq r \leq m$ and column block c use added array $P + d_{rc}$, and for row block $m+1$ and column block c use kC^c which is an $N_2 \times k$ array with column indexed by c of C repeated k times. We claim X is a CA$(nq^3+(m-n)N_1+N_2;3,xk,q)$. Fig. 5.9 shows the construction of X.

Figure 5.9: A CA$(nq^3+(m-n)(N_1)+N_2;3,xk,q)$, constructed in Theorem 5.2.6.

$$X = \begin{array}{|c|c|c|c|}
\hline
A_1 + d_{11} & A_1 + d_{12} & \ldots & A_1 + d_{1x} \\
\hline
A_2 + d_{21} & A_2 + d_{22} & \ldots & A_2 + d_{2x} \\
\hline
\vdots & \vdots & \ldots & \vdots \\
\hline
A_n + d_{n1} & A_n + d_{n2} & \ldots & A_n + d_{nx} \\
\hline
P + d_{(n+1)1} & P + d_{(n+1)2} & \ldots & P + d_{(n+1)x} \\
\hline
P + d_{(n+2)1} & P + d_{(n+2)2} & \ldots & P + d_{(n+2)x} \\
\hline
\vdots & \vdots & \ldots & \vdots \\
\hline
P + d_{m1} & P + d_{m2} & \ldots & P + d_{mx} \\
\hline
kC^1 & kC^2 & \ldots & kC^x \\
\hline
\end{array}$$

Let $T = \{u, v, w\}$ be a set of three distinct column indices of X in column block l, l', l'', respectively; that is $u = lk + i$, $v = l'k + i'$, $w = l''k + i''$ for $0 \leq i, i', i'' < k$.

Case 1: $(i \neq i' \neq i'' \neq i)$

Since A is a CPHF of strength 3, there exist an r, $1 \leq r \leq n$ such that the set of column indices $\{i, i', i''\}$ of A_r cover every tuple in $\mathbb{F}_q^3$ (i.e contains every tuple of $\mathbb{F}_q^3$ as those columns). Therefore, the set of columns $\{u, v, w\}$ of X cover every tuple in $\mathbb{F}_q^3 + (d_{rl}, d_{rl'}, d_{rl''})$ which by Lemma 5.2.5 is equal to $\mathbb{F}_q^3$.

Case 2: $(i = i'' \neq i')$

For each column l and column l'' of $D = \text{DCA}(m;2,x,q)$, there are at least q rows $\{r_1, r_2, \ldots, r_q\}$ such that $\{d_{r_t l} - d_{r_t l''} \mid 1 \leq t \leq q\}$ contains all possible differences of any two elements of $\mathbb{F}_q$.

Let j be the column block containing columns i and i'. In each block $A_r + d_{rj}$, $1 \leq r \leq n$ and in each block $P + d_{rj}$, $n+1 \leq r \leq m$, the pair of columns indexed by $\{i, i'\}$ covers $\mathbb{F}_q^2 = \{(a,b) : a, b \in \mathbb{F}_q\}$. Therefore, for columns $\{u, v, w\}$, row blocks $\{r_1, r_2, \ldots, r_q\}$ of matrix X jointly cover $S = S_{r_1} \cup S_{r_2} \cup \cdots \cup S_{r_q}$, where $S_{r_t} = \{(a, b, a) + (d_{r_t l}, d_{r_t l'}, d_{r_t l''}) : a, b \in \mathbb{F}_q\}$. For any $1 \leq t, t' \leq q$, $t \neq t'$, we have $d_{r_t l''} - d_{r_t l} \neq d_{r_{t'} l''} - d_{r_{t'} l}$, which implies $S_{r_t} \cap S_{r_{t'}} = \emptyset$.

Since $|S_{r_t}| = q^2$, we have $|S| = q^3$. Hence, $S = \mathbb{F}_q^3$ and columns $\{u, v, w\}$ of X cover every tuple in $\mathbb{F}_q^3$.

Case 3: $(i = i^{'} = i^{''})$ This implies $l \neq l^{'} \neq l^{''} \neq l$.

Consider the last row block; these columns u, v, w are, respectively, columns $(l+1)$, $(l^{'}+1)$, and $(l^{''}+1)$ of C which is a covering array of strength 3 and so, the set of columns $\{u, v, w\}$ of X cover every tuple in $\mathbb{F}_q^3$. Thus, X is a CA$(nq^3 + (m-n)N_1 + N_2; 3, xk, q)$. It is easy to see that if $m < n$, then row blocks $n+1, \ldots, m$ are empty and we have a CA$(nq^3+N_2; 3, xk, q)$. ∎

In the following theorems, we apply Theorem 5.2.6 when $x = 2$, $x = q$, $x = q+1$, $x = q^2$, and $x = q^2 - q + 1$, and further optimize the construction by removing redundant rows. They all use x copies of the CA$(2q^3-1; 3, q^2+q+1, q)$ by Raaphorst et al. [48] given in Theorem 3.2.2. The redundant rows can be identified by identical rows in the CA$(mq; 2, x, q)$ obtained by the DCA$(m; 2, x, q)$, and the CA$(N_2; 3, x, q)$ in Theorem 5.2.6. We remove these redundant rows from the last row block of array X constructed in the proof of Theorem 5.2.6. This gives various new covering arrays, yielding new best-known upper bounds for the covering array number for the given parameters, which we discuss in Section 5.3.

Theorem 5.2.7 (2-plication)**.** For prime power $q \geq 2$, there exists CA$(4q^3-5q^2+2q; 3, 2(q^2+q+1), q)$.

Proof. Apply Theorem 5.2.6 with $x = 2$ for the following ingredients. Let Z be the CPHF$(2; q^2+q+1, 3, q)$ in Theorem 3.2.4 where each row corresponds to columns of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ constructed by a primitive polynomial f over $\mathbb{F}_q$ and its reciprocal. Let $A = A(G^1_{q^2+q+1})$ and $A_r = A(G^{-1}_{q^2+q+1})$ be vertically concatenated to form a CA$(2q^3; 3, q^2+q+1, 3)$ (Theorem 3.2.2). By Proposition 3.1.4, A and A_r are orthogonal arrays of strength 2. Let P be the CA$(2q^2-q; 2, q^2+q+1, q)$ in Corollary 5.1.9. Pick any two columns of the difference covering array D in Theorem 5.1.11 to form a DCA$(q; 2, 2, q)$. The difference covering array D is given in Fig. 5.7 where e is a primitive element of $\mathbb{F}_q$. We can use any of the two constructions shown in Fig. 5.10; for M_2, $s \neq t$, where $0 \leq s, t \leq q-2$.

Figure 5.10: CA$(2q^3 + (q-2)(2q^2-q); 3, 2(q^2+q+1), q)$ for a prime power q. Here e is a primitive element of $\mathbb{F}_q$.

$M_1 =$

A	A
A_r	$A_r + e^s$
P	$P + e^{s+1}$
P	$P + e^{s+2}$
$\vdots$	$\vdots$
P	$P + e^{s+q-2}$

$M_2 =$

A	A
$A_r + e^t$	$A_r + e^s$
$P + e^{t+1}$	$P + e^{s+1}$
$P + e^{t+2}$	$P + e^{s+2}$
$\vdots$	$\vdots$
$P + e^{t+q-2}$	$P + e^{s+q-2}$

By Theorem 5.2.6, M_1 and M_2 are covering arrays of strength 3, with $2(q^2+q+1)$ columns and q symbols. We note that since $x = 2$, we use an empty array for the array C in Theorem 5.2.6. ∎

Figure 5.11: Structure of duplication for $q = 2$ and the corresponding array. Here $f = x^3+x+1$ is the primitive polynomial, and $C_0^7(S(f,(0,0,1))$ and $C_0^7(S(f_r,(1,1,1))$ are shown in bold.

$$\begin{array}{|c|c|}\hline A & A \\ \hline A_r & A_r+1 \\ \hline\end{array} = \left[\begin{array}{ccccccc|ccccccc} 0&0&0&0&0&0&0&0&0&0&0&0&0&0\\ \mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{1}&0&0&1&0&1&1&1\\ 0&1&0&1&1&1&0&0&1&0&1&1&1&0\\ 1&0&1&1&1&0&0&1&0&1&1&1&0&0\\ 0&1&1&1&0&0&1&0&1&1&1&0&0&1\\ 1&1&1&0&0&1&0&1&1&1&0&0&1&0\\ 1&1&0&0&1&0&1&1&1&0&0&1&0&1\\ 1&0&0&1&0&1&1&1&0&0&1&0&1&1\\ \hline 0&0&0&0&0&0&0&1&1&1&1&1&1&1\\ \mathbf{1}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{0}&0&0&0&1&0&1&1\\ 1&1&0&1&0&0&1&0&0&1&0&1&1&0\\ 1&0&1&0&0&1&1&0&1&0&1&1&0&0\\ 0&1&0&0&1&1&1&1&0&1&1&0&0&0\\ 1&0&0&1&1&1&0&0&1&1&0&0&0&1\\ 0&0&1&1&1&0&1&1&1&0&0&0&1&0\\ 0&1&1&1&0&1&0&1&0&0&0&1&0&1 \end{array}\right]$$

An example for $q = 2$ is given in Fig. 5.11.

Theorem 5.2.8 (q-plication)**.** For prime power $q \geq 3$, there exists $\mathrm{CA}(5q^3-6q^2+2q; 3, q(q^2+q+1), q)$.

Proof. Apply Theorem 5.2.6 with $x = q$ for the following ingredients. Let Z be a $\mathrm{CPHF}(2; q^2+q+1, 3, q)$ in Theorem 3.2.4 where each row corresponds to columns of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$. Let A and A_r be the $\mathrm{CA}(q^3; 2, q^2+q+1, q)$ constructed by $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$, respectively. Recall that vertically concatenating A and A_r yields a $\mathrm{CA}(2q^3; 3, q^2+q+1, q)$ (Theorem 3.2.2). Let P be the $\mathrm{CA}(2q^2-q; 2, q^2+q+1, q)$ in Corollary 5.1.9. Let D be the difference covering array $\mathrm{DCA}(q; 2, q, q)$ in Theorem 5.1.11, given in Fig. 5.7, where e is a primitive element of $\mathbb{F}_q$. Let B be the $\mathrm{OA}(q^3; 3, q, q)$ constructed in Corollary 5.1.2. By Theorem 5.2.6, we obtain the $\mathrm{CA}(2q^3+(q-2)(2q^2-q)+q^3; 3, q(q^2+q+1), q)$, $k = q^2+q+1$, given as array M in Fig. 5.12.

We claim that we can remove q^2 rows from M to obtain a CA with the same parameters but with $2q^3+(q-2)(2q^2-q)+q^3-q^2$ rows.

Let $i_1, i_2, \ldots, i_q$ be distinct columns congruent modulo q^2+q+1 where $0 \leq i_j \leq q^2+q$ for $1 \leq j \leq q$. Table 5.1 displays the rows in the sub-array indexed by the chosen columns that appear in each of the first q row blocks of M, for every $c \in \mathbb{F}_q$.

Consider the q^2 rows of matrix B corresponding to the polynomials of degree at most 1, $c+c_1x$, $0 \leq c_1, c \leq e^{q-2}$; Table 5.2 displays the q rows corresponding to a fixed $0 \leq c \leq e^{q-2}$.

Figure 5.12: The CA$(2q^3+(q-2)(2q^2-q)+q^3; 3, q(q^2+q+1), q)$ constructed in Theorem 5.2.8.

$$M = \begin{array}{|c|c|c|c|}\hline A & A & \dots & A \\ \hline A_r & A_r+1 & \dots & A_r+e^{q-2} \\ \hline P & P+e & \dots & P+1 \\ \hline P & P+e^2 & \dots & P+e \\ \hline \vdots & \vdots & \dots & \vdots \\ \hline P & P+e^{q-2} & \dots & P+e^{q-3} \\ \hline kB^1 & kB^2 & \dots & kB^q \\ \hline \end{array}$$

Table 5.1: For each $c \in \mathbb{F}_q$, rows corresponding to $i_1, i_2, \dots, i_q$.

Row blocks	i_1	i_2	$\dots$	i_q
1	c	c	$\dots$	c
2	c	$c+1$	$\dots$	$c+e^{q-2}$
$\vdots$				
t	c	$c+e^t$	$\dots$	$c+e^{t+q-2}$
$\vdots$				
q	c	$c+e^{q-2}$	$\dots$	$c+e^{q-3}$

Thus, in columns $i_1, i_2, \dots, i_q$, the rows of M in the last row block (shown in Table 5.2) cover the same 3-tuples as the rows of M in the first q row blocks shown in Table 5.1. Therefore we can remove q^2 rows of B corresponding to polynomials $c+c_1x$, $0 \le c_1, c \le e^{q-2}$ from B in the last row block of M and obtain a CA$(2q^3+(q-2)(2q^2-q)+q^3-q^2; 3, q(q^2+q+1), q)$. ∎

Remark 5.2.9. Applying Theorem 5.2.2 and Theorem 5.2.4 with CA$(2q^3-1; 3, q^2+q+1, 3)$ (Theorem 3.2.2) and CA$(2q^2-q; 2, q^2+q+1, q)$ (Corollary 5.1.9) as the ingredients gives CAN$(3, 2(q^2+q+1), q) \le 4q^3-3q^2+q-1$ and CAN$(3, q(q^2+q+1), q) \le 5q^3-4q^2+q-1$, respectively. Using Theorem 5.2.7 and Theorem 5.2.8, we obtain CAN$(3, 2(q^2+q+1), q) \le 4q^3-5q^2+2q$ and CAN$(3, q(q^2+q+1), q) \le 5q^3-6q^2+2q$, respectively, which give an improvement of $2q^2-q-1$ in these upper bounds.

Theorem 5.2.10 ($(q+1)$-plication)**.** For odd prime power $q \ge 3$, there exists a CA$(6q^3 - \frac{13}{2}q^2 + \frac{5}{2}q - 1; 3, (q+1)(q^2+q+1), q)$.

Proof. Apply Theorem 5.2.6 with $x = q+1$ for the following ingredients. Let Z be the CPHF$(2; q^2+q+1, 3, q)$ in Theorem 3.2.4 where each row corresponds to columns of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$. Let A and A_r be the CA$(q^3; 2, q^2+q+1, q)$ constructed by $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$, respectively. Recall that vertically concatenating A and A_r yields a CA$(2q^3; 3, q^2+q+1, q)$ (Theorem 3.2.2). Let P be the CA$(2q^2-q; 2, q^2+q+1, q)$ in Corollary 5.1.9. Let D be the difference covering array DCA$(q+\frac{q-1}{2}; 2, q+1, q)$ in Theorem 5.1.14 and B be the

Table 5.2: For each $c \in \mathbb{F}_q$, we display q rows of B corresponding to polynomials $c + c_1 x$, $0 \leq c_1 \leq e^{q-2}$.

Polynomials	0	1	...	e^{q-2}
$c + 0x$	c	c	...	c
$c + e^0 x$	c	$c+1$	...	$c + e^{q-2}$
$\vdots$				
$c + e^t x$	c	$c + e^t$	...	$c + e^{t+q-2}$
$\vdots$				
$c + e^{q-2} x$	c	$c + e^{q-2}$	...	$c + e^{q-3}$

$\mathrm{OA}(q^3; 3, q+1, q)$ in Theorem 5.1.1. By Theorem 5.2.6, and removing one repeated zero row, we obtain a $\mathrm{CA}(2q^3 + (q + \frac{q-1}{2} - 2)(2q^2 - q) + q^3 - 1; 3, (q+1)(q^2+q+1), q)$. ∎

Theorem 5.2.11 (q^2-plication)**.** For prime power $q \geq 2$, there exists a $\mathrm{CA}(8q^3 - 10q^2 + 4q - 1; 3, q^2(q^2+q+1), q)$.

Proof. Apply Theorem 5.2.6 with $x = q^2$ for the following ingredients. Let Z be the $\mathrm{CPHF}(2; q^2+q+1, 3, q)$ in Theorem 3.2.4 where each row corresponds to columns of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$. Let A and A_r be the $\mathrm{CA}(q^3; 2, q^2+q+1, q)$ constructed by $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ respectively. Recall that vertically concatenating A and A_r yields a $\mathrm{CA}(2q^3; 3, q^2+q+1, q)$ (Theorem 3.2.2). Let P be the $\mathrm{CA}(2q^2 - q; 2, q^2+q+1, q)$ in Corollary 5.1.9. Let D be the difference covering array $\mathrm{DCA}(q; 2, q, q)$ in Theorem 5.1.11, where e is a primitive element of $\mathbb{F}_q$. In the proof of Theorem 5.1.13 a $\mathrm{DCA}(2q-1; 2, q^2, q)$ is constructed by taking $D \bigotimes D$, where D is given in Fig. 5.7, with one redundant zero row removed. By removing columns with zero as the first entry of columns of $G^1_{q^2+q+1}$, and corresponding columns from $G^{-1}_{q^2+q+1}$, we obtain the generators G_1 and G_2, respectively. They have precisely q^2 columns since the number of columns that start with zero entry is exactly $q+1$. We multiply each column of G_1 by the multiplicative inverse of the first entry so that the first entry becomes 1. This operation on columns has no effect on the rank of sub-matrices. Then, we change the order of columns to derive the generator matrix G_1' given in Table 5.3. Changing the order of columns determines a permutation of columns. By using the same permutation, we change the order of columns of G_2 to obtain a new generator matrix G_2'. Let C be the $\mathrm{CA}(2q^3 - 1; 3, q^2, q)$ constructed by vertical concatenation of linear combination of rows of G_1' and G_2'. Using ingredients above, by Theorem 5.2.6, we have a covering array M of strength 3 with $q^2(q^2+q+1)$ columns and $2q^3 + (2q-3)(2q^2-q) + 2q^3 - 1$ rows. We claim that we can remove $2q^2 - q$ rows of M to construct a CA with $2q^3 + (2q-3)(2q^2-q) + 2q^3 - 2q^2 + q - 1 = 8q^3 - 10q^2 + 4q - 1$ rows. Let r_1, r_2, and r_3 denote the first, the second and the third rows of G_1'. Let $i_1, i_2, \ldots, i_{q^2}$ be distinct columns congruent modulo q^2+q+1 and $0 \leq i_j \leq q^2+q$ for $1 \leq j \leq q^2$. Table 5.4 displays the rows in the sub-array indexed by the chosen columns that appear in each of the first $2q-1$ row blocks of M, for every $c \in \mathbb{F}_q$. The first row of Table 5.5 shows q rows of C produced by $cr_1 + 0r_2 + 0r_3$, where $c \in \mathbb{F}_q$ which are the same

as the entries of the first row block of Table 5.4. The second row of Table 5.5 shows $q(q-1)$ rows of C produced by $cr_1 + d_2r_2 + 0r_3$, where $c, d_2 \in \mathbb{F}_q$ and $d_2 \neq 0$ which are the same as the entries of the row block r where $2 \leq r \leq q$ of Table 5.4. The third row of Table 5.5 shows $q(q-1)$ rows of C produced by $cr_1 + 0r_2 + d_3r_3$, where $c, d_3 \in \mathbb{F}_q$ and $d_3 \neq 0$ which are the same as the entries of the row blocks r where $q+1 \leq r \leq 2q-1$ of the Table 5.4. Therefore, we can remove $q + q(q-1) + q(q-1) = 2q^2 - q$ rows of C used in the last row block of M and we obtain a $\mathrm{CA}(8q^3 - 10q^2 + 4q - 1; 3, q^2(q^2+q+1), q)$. ∎

Table 5.3: The modified generator matrix for q^2-plication.

1	1	...	1	1	1	...	1	...	1	1	...	1
0	e^0	...	e^{q-2}	0	e^0	...	e^{q-2}	...	0	e^0	...	e^{q-2}
0	0	...	0	e^0	e^0	...	e^0	...	e^{q-2}	e^{q-2}	...	e^{q-2}

Table 5.4: Rows of M corresponding to the first $2q-1$ row blocks and column indices $i_1, i_2, \ldots, i_{q^2}$.

Row blocks	i_1	i_2	...	i_q	i_{q+1}	...	i_{2q}	...	i_{q^2-q}	...	i_{q^2}
1	c	c	...	c	c	...	c	...	c	...	c
2	c	$c+1$	...	$c+e^{q-2}$	c	...	$c+e^{q-2}$	...	c	...	$c+e^{q-2}$
⋮			...			...		...		...	
t	c	$c+e^t$	...	$c+e^{t+q-2}$	c	...	$c+e^{t+q-2}$	...	c	...	$c+e^{t+q-2}$
⋮			...			...		...		...	
q	c	$c+e^{q-2}$	...	$c+e^{q-3}$	c	...	$c+e^{q-3}$	...	c	...	$c+e^{q-3}$
$q+1$	c	c	...	c	$c+1$	...	$c+1$	...	$c+e^{q-2}$	...	$c+e^{q-2}$
$q+2$	c	c	...	c	$c+e$	...	$c+e$	...	c	...	c
⋮			...			...		...		...	
s	c	c	...	c	$c+e^s$	...	$c+e^s$	...	$c+e^{s+q-2}$	...	$c+e^{s+q-2}$
⋮			...			...		...		...	
$2q-1$	c	c	...	c	$c+e^{q-2}$	...	$c+e^{q-2}$	...	$c+e^{q-3}$	...	$c+e^{q-3}$

Table 5.5: $2q^2 - q$ rows of C identical to rows of M.

i_1	i_2	...	i_q	i_{q+1}	...	i_{2q}	...	i_{q^2-q}	...	i_{q^2}
c	c	...	c	c	...	c	...	c	...	c
c	$c+d_2(1)$	...	$c+d_2(e^{q-2})$	c	...	$c+d_2(e^{q-2})$	...	c	...	$c+d_2(e^{q-2})$
c	c	...	c	$c+d_3(1)$	...	$c+d_3(1)$	...	$c+d_3(e^{q-2})$	...	$c+d_3(e^{q-2})$

By Proposition 3.3.3 and Proposition 3.3.4, for even prime powers q and for $q = 3$, there exists generator G_2' such that the first entry of columns is not zero. Thus, for even prime

power q, we can reduce the number of rows of the CA constructed in Theorem 5.2.11 as follows.

Corollary 5.2.12. If q is an even prime power or $q = 3$, then there exists CA$(8q^3 - 10q^2 + 3q; 3, q^2(q^2 + q + 1), q)$.

Proof. We choose G_1 and G_2 in Proposition 3.3.3 for even prime power and Proposition 3.3.4 for $q = 3$ and use them in Theorem 5.2.11 in the last row block. We do not change the other ingredients of Theorem 5.2.11. Since G_1 and G_2 have two identical rows of 1s, the corresponding covering array of strength 3 has $2q^3 - q$ rows and q^2 columns. Using this CA$(2q^3-q; 3, q^2, q)$ as an ingredient for the last row block of Theorem 5.2.11 yields a CA$(8q^3-10q^2 + 3q; 3, q^2(q^2 + q + 1), q)$. ∎

Theorem 5.2.13 ($(q^2 - q + 1)$-plication)**.** For prime power $q \geq 2$, there exists a CA$(8q^3 - 10q^2 + 3q; 3, (q^2 - q + 1)(q^2 + q + 1), q)$.

Proof. We modify the CA$(8q^3 - 10q^2 + 4q - 1; 3, q^2(q^2 + q + 1), q)$ in Theorem 5.2.11. We change the last row block and the DCA which were used in Theorem 5.2.11. Let $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ be two generator matrices constructed in Lemma 3.1.2. Since the first row of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ start with $(1, 0, 0)$, they have exactly two zeros in the same position. We remove from $G^1_{q^2+q+1}$ the $q + 1$ columns with the first entry equal to zero and corresponding columns from $G^{-1}_{q^2+q+1}$ to obtain G_1 and G_2, respectively. We reorder columns of G_1 and G_2 to deduce G_1' and G_2' as we did in Theorem 5.2.11. Since the first row of $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ has exactly two zeros in the same position, we have exactly $q - 1$ columns of G_2' with a zero in the first entry. We remove from G_2' the $q - 1$ columns with the first entry equal to zero and corresponding columns from G_1' to construct G_2'' and G_1''. We remove the corresponding columns of DCA$(2q-1; 2, q^2, q)$ from Theorem 5.2.11 to obtain the DCA$(2q-1; 2, q^2-q+1, q)$. The CA$(2q^3 - q; 3, q^2 - q + 1, q)$ is the vertical concatenation of a linear combination of rows of G_1'' and G_2'' after removing q redundant rows. We replace the DCA$(2q - 1; 2, q^2, q)$ by DCA$(2q - 1; 2, q^2 - q + 1, q)$ and CA$(2q^3 - 1; 3, q^2, q)$ by CA$(2q^3 - q; 3, q^2 - q + 1, q)$ in Theorem 5.2.11 and we keep other ingredients without change. With this modification, we removed $q - 1$ rows from CA$(8q^3 - 10q^2 + 4q - 1; 3, q^2(q^2 + q + 1), q)$, therefore, we have CA$(8q^3 - 10q^2 + 3q; 3, (q^2 - q + 1)(q^2 + q + 1), q)$. ∎

Fig. 5.13 presents $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ for the degree-3 primitive polynomial $f(x) = x^3 + x^2 + 2x + 1$ over $\mathbb{F}_3$, and the modified generator matrices G_1' and G_2' used in Theorem 5.2.11 and Theorem 5.2.13. Fig. 5.14 shows a CA$(137; 3, 117, 3)$ constructed in Theorem 5.2.11 for $q = 3$, before removing redundant rows. The ingredients in Fig. 5.14 are explained next. Arrays A and A_r are the CA$(27; 2, 13, 3)$ constructed by $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$, respectively in Fig. 5.13. Array P is the CA$(15; 2, 13, 3)$ in Corollary 5.1.9 for $q = 3$, and C is the CA$(53; 3, 9, 3)$ constructed by vertical concatenation of linear combinations of rows of G_1' and G_2' in Fig. 5.13.

Figure 5.13: Generator matrices $G^1_{q^2+q+1}$ and $G^{-1}_{q^2+q+1}$ and modified generator matrices G'_1 and G'_2 in Theorem 5.2.11 and Theorem 5.2.13, when $f(x) = x^3 + x^2 + 2x + 1$ over $\mathbb{F}_3$.

$G^1_{q^2+q+1} =$

1	2	3	4	5	6	7	8	9	10	11	12	13
1	0	0	2	1	1	1	2	1	0	2	0	2
0	1	0	1	1	0	0	2	1	1	1	2	1
0	0	1	2	2	2	1	2	0	1	0	1	1

$G^{-1}_{q^2+q+1} =$

1	0	0	2	2	0	2	0	1	2	1	1	1
0	1	0	2	1	2	2	2	1	0	0	2	2
0	0	1	1	0	1	0	2	1	2	2	2	1

$G'_1 =$

1	9	11	7	8	4	6	5	13
1	1	1	1	1	1	1	1	1
0	1	2	0	1	2	0	1	2
0	0	0	1	1	1	2	2	2

$G'_2 =$

1	1	1	1	0	1	0	1	1
0	1	0	1	2	1	2	2	2
0	1	2	0	2	2	1	0	1

Figure 5.14: CA$(137; 3, 117, 3)$ constructed in Theorem 5.2.11 for $q = 3$, before removing redundant rows.

A	A	A	A	A	A	A	A	A
A_r	$A_r + 1$	$A_r + 2$	A_r	$A_r + 1$	$A_r + 2$	A_r	$A_r + 1$	$A_r + 2$
P	$P + 2$	$P + 1$	P	$P + 2$	$P + 1$	P	$P + 2$	$P + 1$
P	P	P	$P + 1$	$P + 1$	$P + 1$	$P + 2$	$P + 2$	$P + 2$
P	P	P	$P + 2$	$P + 2$	$P + 2$	$P + 1$	$P + 1$	$P + 1$
kC^1	kC^2	kC^3	kC^4	kC^5	kC^6	kC^7	kC^8	kC^9

5.3 Improvements on the best-known upper bounds

Tables of the best-known upper bounds on the covering arrays number CAN(t, k, v), for $2 \leq t \leq 6$, $1 \leq k \leq 10000$ and $2 \leq v \leq 25$, are maintained by Colbourn [15]. In this section, we show improvements on some of these upper bounds on CAN for strength 3 obtained by Theorem 5.2.7, Theorem 5.2.8, Theorem 5.2.11, Theorem 5.2.13 and Corollary Corollary 5.2.12, which are given in Table 5.6. In this table, for each prime power $2 \leq q \leq 25$, and the number of columns given in the column labeled "Columns", we provide the best previous upper bound on the number of rows (column labeled "Previous rows"), the new number of rows given by new constructions (column labeled "New rows"), and the difference between the new and the previous number of rows (column labeled "Difference"). We also specify the method for which the previous number of rows was obtained in the column labeled "Previous method", according to the information obtained in [15]; when the array is readily available in a reference, then we cite it, otherwise, the citation is [15]. The method used to obtain "New rows" is one of the theorems or corollaries in this chapter which is specified in column "New Method". Improved upper bounds for the number of rows are indicated in bold, while results with no improvements are displayed to show how far the bounds obtained by our constructions are from existing best records.

Whenever the previous bound in [15] is given by Theorem 5.2.2 or Theorem 5.2.4 for $v = q$ and $k = q^2 + q + 1$, we obtain an improvement of $2q^2 - q - 1$ rows with Theorem 5.2.7 and Theorem 5.2.8, respectively (see Table 5.6).

Let us first consider the impact of 2-plication (Theorem 5.2.7) in Table 5.6. For $q = 2$, Sloane [57] gives a CA$(16; 3, 16, 2)$ using a 16×16 Hadamard matrix, and we obtained a covering array with the same parameters given in Fig. 5.11. For $q = 3, 4, 5, 7$, we have improvements

over the CAN upper bounds previously obtained by various computer searches. When $q = 8, 11$, the method of cyclotomy [14] still holds the CAN record. For $q = 9, 13, 16, 17, 19, 23, 25$, our improvement is explained by saving $2q^2-q-1$ rows over the Chateauneuf-Kreher doubling construction (Theorem 5.2.2).

For q-plication (Theorem 5.2.8) in Table 5.6, we have improvements for all upper bounds for $q \geq 3$. For $q = 3$ and 39 columns, we have a new record with respect to the doubling of an array with 20 columns that gives CA$(89; 3, 40, 3)$. For $q = 4$, our new record replaces a computational search for CPHF. All other prime powers up to 25 give an improvement on the CAN upper bound explained by saving $2q^2 - q - 1$ rows over Theorem 5.2.4 by Colbourn, Martirosyan, Trung, and Walker [20].

For $(q + 1)$-plication (Theorem 5.2.10), no upper bounds were improved (Table 5.7).

For $(q^2 - q + 1)$-plication (Theorem 5.2.13) and q^2-plication (Theorem 5.2.11) comparisons in Table 5.6, best upper bounds are only available for $q \leq 9$ [15]. These theorems improve the upper bounds for $q = 4, 5, 7, 8$, using both methods over restricted CPHF, except in the case of $(q^2 - q + 1)$-plication for $q = 8$ where the new upper bound ties with the current bound. No improvements were found for $q = 2, 3, 9$.

In conclusion, the constructions in this chapter improved 29 out of the 47 upper bounds in the covering array tables [15] that they could be compared with. Even when our constructions do not improve the CAN upper bound, there are some clear advantages in using them. In these cases, the number of rows is not much bigger than the one obtained by other constructions, but all constructions (except Corollary 5.2.12) can be done directly using primitive elements in the finite field. In particular, various computational searches can be substituted by our direct constructions with a relatively small increase in the number of rows.

Table 5.6: Improvements on the size of CA of strength 3 are shown in bold.

q	Columns	Previous method	Previous rows	New rows	New method	Difference
2	14	Sloane [57]	16	16	Theorem 5.2.7 (2-plication)	0
	21	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	19	30	Theorem 5.2.13 ((q^2-q+1)-plication)	11
	28	simulated annealing (TJ-RT) [63]	23	30	Corollary 5.2.12 (q^2-plication)	7
3	26	Simulated annealing [15]	72	**69**	Theorem 5.2.7 (2-plication)	−3
	39	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	89	**87**	Theorem 5.2.8 (q-plication)	−2
	91	two-stage SA (TJ-AG-I) [60]	125	135	Theorem 5.2.13 ((q^2-q+1)-plication)	10
	117	two-stage SA (TJ-AG-I) [60]	129	135	Corollary 5.2.12 (q^2-plication)	6
4	42	CPHF 3-stage [32]	191	**184**	Theorem 5.2.7 (2-plication)	−7
	84	CPHF 3-stage (IM-TJ-AJ-AG) [32]	253	**232**	Theorem 5.2.8 (q-plication)	−21
	273	CPHF 3-stage (IM-TJ-AJ-AG) [32]	370	**364**	Theorem 5.2.13 ((q^2-q+1)-plication)	−6
	336	CPHF 3-stage (IM-TJ-AJ-AG) [32]	395	**364**	Corollary 5.2.12 (q^2-plication)	−31
5	62	Torres Jimenez [15]	404	**385**	Theorem 5.2.7 (2-plication)	−19
	155	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	529	**485**	Theorem 5.2.8 (q-plication)	−44
	651	Restricted CPHF Ext 7(3,7) WCS [66]	785	**765**	Theorem 5.2.13 ((q^2-q+1)-plication)	−20
	775	Restricted CPHF Ext 7(2,7) WCS [66]	805	**769**	Theorem 5.2.11 (q^2-plication)	−36
7	114	Cyclotomy (Torres-Jimenez) [15]	1183	**1141**	Theorem 5.2.7 (2-plication)	−42
	399	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	1525	**1435**	Theorem 5.2.8 (q-plication)	−90
	2451	Restricted CPHF Ext 7(2,6) WCS [15]	2281	**2275**	Theorem 5.2.13 ((q^2-q+1)-plication)	−6
	2793	Restricted CPHF Ext 7(1,7) WCS [15]	2317	**2281**	Theorem 5.2.11 (q^2-plication)	−36
8	146	Cyclotomy [14]	1552	1744	Theorem 5.2.7 (2-plication)	192
	584	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	2311	**2192**	Theorem 5.2.8 (q-plication)	−119
	4161	Restricted CPHF Ext 7(1,7) WCS [15]	3480	3480	Theorem 5.2.13 ((q^2-q+1)-plication)	0
	4672	Restricted CPHF Ext 7(1,3) WCS [15]	3508	**3480**	Corollary 5.2.12 (q^2-plication)	−28
9	182	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	2681	**2529**	Theorem 5.2.7 (2-plication)	−152
	819	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	3329	**3177**	Theorem 5.2.8 (q-plication)	−152
	6643	Restricted CPHF Ext 7(1,6) WCS [15]	4985	5049	Theorem 5.2.13 ((q^2-q+1)-plication)	64
	7371	Restricted CPHF Ext 7(0,7) WCS [15]	5049	5057	Theorem 5.2.11 (q^2-plication)	8
11	266	Cyclotomy [14]	4378	4741	Theorem 5.2.7 (2-plication)	363
	1463	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	6181	**5951**	Theorem 5.2.8 (q-plication)	−230
13	366	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	8293	**7969**	Theorem 5.2.7 (2-plication)	−324
	2379	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	10321	**9997**	Theorem 5.2.8 (q-plication)	−324
16	546	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	15631	**15136**	Theorem 5.2.7 (2-plication)	−495
	4368	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	19471	**18976**	Theorem 5.2.8 (q-plication)	−495
17	614	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	18801	**18241**	Theorem 5.2.7 (2-plication)	−560
	5219	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	23425	**22865**	Theorem 5.2.8 (q-plication)	−560
19	762	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	26371	**25669**	Theorem 5.2.7 (2-plication)	−702
	7239	Theorem 5.2.4 (Colbourn-Martirosyan-Trung-Walker) [20]	32869	**32167**	Theorem 5.2.8 (q-plication)	−702
23	1106	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	47103	**46069**	Theorem 5.2.7 (2-plication)	−1034
25	1302	Theorem 5.2.2 (Chateauneuf-Kreher doubling) [10]	60649	**59425**	Theorem 5.2.7 (2-plication)	−1224

Table 5.7: No improvement found on the size of CA of strength 3 by Theorem 5.2.10 ($(q+1)$-plication).

q	Columns	Previous method	Previous rows	New rows	Difference
3	52	simulated annealing (AG-TJ-H) [15]	102	110	7
5	186	Restricted CPHF Sim Annealing (TJ-IM) [15]	573	599	26
7	456	Restricted CPHF Ext 5(1,2) WCS [15]	1663	1756	93
9	910	Restricted CPHF Ext 5(0,5) WCS [15]	3609	3869	260
11	1596	Restricted CPHF Ext 5(0,5) WCS [15]	6611	7226	615
13	2562	Restricted CPHF Ext 5(0,5) WCS [15]	10933	12115	1182
17	5526	Restricted CPHF Ext 5(0,5) WCS [15]	24497	27641	3144
19	7620	Cohen-Colbourn-Ling [15]	37494	38854	1360

Chapter 6

Conclusion

6.1 Major contributions

Our contributions lie in two main directions: proving the existence of 3 anti-cocircular truncated Möbius planes and related constructions of strength-4 covering arrays (Chapter 4); and exploiting the structure of the CA$(2q^3-1; 3, q^2+q+1, q)$ from Theorem 3.2.2 to optimize the size of the strength-3 covering arrays in recursive constructions that use it as an ingredient (Chapter 5).

In Chapter 4, we proved the existence of three truncated Möbius planes for any odd prime power q, where for any choice of blocks from each plane, the intersection size is at most three. This result is a generalization of the existence of orthogoval planes studied in [2, 6, 17, 25, 28, 34, 45, 48, 65], and played a key role to build a CA$(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ in Theorem 4.3.1. The CA$(2q^3 - 1; 3, q^2 + q + 1, q)$ constructed by Raaphorst et al. [48], which is obtained from orthogoval projective planes, improved the size of the best-known arrays by almost 33% and are still the best-known covering arrays in [15] for their number of columns. Similarly, for odd prime power $q \geq 11$, we obtain an improvement by almost 25 percent in Theorem 4.3.1 on the size of the previously best-known strength-4 covering arrays with the same parameters.

We used the CA$(3q^4 - 2; 4, \frac{q^2+1}{2}, q)$ in a recursive construction as the main ingredient to double the number of columns and less than double the number of rows, constructing a CA$(3q^4+(q-2)(3q^3-q), 4, q^2+1, q)$ for an odd prime power q (Corollary 4.4.4). For $q \geq 11$, these covering arrays slightly improve the known bounds, but more importantly they are easy to construct using finite fields and have a lot of structure.

In Chapter 5, we have introduced a new constructive approach for covering arrays of strength 3 (Theorem 5.2.6), and employed the vital fact that for q prime power, a CA$(2q^3 - 1; 3, q^2 + q + 1, q)$ is constructed by the vertical concatenation of two OA$_q(q^3; 2, q^2 + q + 1, q)$, and corresponds to a CPHF$(2; q^2 + q + 1, q, 3)$ (Theorem 3.2.2 and Theorem 3.2.4) or to a pair of orthogoval Desarguesian projective (affine) planes. We employ x copies of CA$(2q^3 - 1; 3, q^2 + q + 1, q)$ where $x \in \{2, q, q + 1, q^2, q^2 - q + 1\}$ that we call x-plication and obtain CA$(4q^3 - 5q^2 + 2q; 3, 2(q^2 + q + 1), q)$, CA$(5q^3 - 6q^2 + 2q; 3, q(q^2 + q + 1), q)$, CA$(8q^3 -$

$10q^2+4q-1; 3, q^2(q^2+q+1), q)$, CA$(8q^3-10q^2+3q; 3, (q^2-q+1)(q^2+q+1), q)$, for every prime power q, CA$(8q^3-10q^2+3q; 3, q^2(q^2+q+1), q)$ for every even prime power q, and CA$(6q^3-\frac{13}{2}q^2+\frac{5}{2}q-1; 3, (q+1)(q^2+q+1), q)$ for every odd prime power q. These covering arrays improve several upper bounds on best covering array numbers of strength 3 found in [15].

6.2 Future directions

In the following, we list several future directions for this research, some of which are already under investigation.

A set of s mutually orthogoval projective (affine) planes and m anti-cocircular (truncated) Möbius planes show that constructive methods using structures from geometry can make a significant improvement in the size of covering arrays. These two constructions for $t = 3, 4$ strongly suggest continuing this approach for strength-5 covering arrays. There are two examples that are obtained by vertical concatenation of two strength-4 covering arrays, which suggests this structure; the first is a CA$(485; 5, 11, 3)$ [64], the second one is a CA$(6249; 5, 11, 5)$, which we found using experiments. These examples suggest the construction of strength-5 covering arrays by the vertical concatenation of four strength-4 covering arrays for any prime power q. Understanding the geometry in these two examples and finding such a construction is among our plans for future work.

An ultimate problem concerning the connection with strength-t covering arrays is the existence of proper geometric objects analogous to ovoids in PG$(3, q)$. We can define a set of points in PG$(m-1, q)$ such that no $m-1$ points in that set are contained in a subspace of dimension $m-2$. Determining upper bounds on the size of such sets and studying their structure can lead to the discovery of new geometric objects, analogous to orthogoval planes and anti-cocircular Möbius planes in higher dimensions, which may be used to construct covering arrays of higher strength.

New families of strength-3 covering arrays were constructed in Chapter 5 by horizontal concatenation of x copies of CA$(2q^3-1; 3, q^2+q+1, 3)$ where $x \in \{2, q, q^2, q^2-q+1\}$ for a prime power q. The next step is to leverage our geometric construction from Chapter 4 with recursive methods using more than two copies of CA$(3q^4-2; 4, \frac{q^2+1}{2}, q)$. Investigating the possibility of effective approaches to construct strength-4 covering arrays using recursive methods is a natural problem to explore next.

The first clue leading us to construct the CA$(3q^4-2; 4, \frac{q^2+1}{2}, q)$ in Theorem 4.3.1 for an odd prime power q was the existence of the CA$(511; 4, 17, 4)$ obtained by Tzanakis et al. [64] where $q = 4$. Using experimental approaches, we obtained a CA$(262141; 4, 257, 16)$ by the vertical concatenation of four strength-3 covering arrays employing all 16^2+1 points of the ovoid; more specifically, we used $G^{q+1}_{q^2+1}$, $G^{3(q+1)}_{q^2+1}$, $G^{5(q+1)}_{q^2+1}$, and $G^{7(q+1)}_{q^2+1}$, for $q = 16$. This observation strengthens the idea of finding a general construction of anti-cocircular Möbius planes for even prime powers.

Improving the size of any of the ingredients of Theorem 5.2.6 in Chapter 5 could yield new bounds. For instance, we have used DCA$(q+\frac{q-1}{2}; 2, q+1, q)$ (Theorem 5.1.14) in

Theorem 5.2.10 to present a new family of covering arrays. An improvement on the size of $\mathrm{DCA}(q+\frac{q-1}{2}; 2, q+1, q)$ could improve these upper bounds, strengthening Theorem 5.2.10. In general, improving the size of the best-known difference covering arrays has a fundamental role in improving the size of covering arrays using Theorem 5.2.6. Therefore, developing methods to construct difference covering arrays, especially with q symbols where q is a prime power can be the next step to improve applications of Theorem 5.2.6.

An extension of the method we have used in Theorem 5.2.6 for the case of strength 4 is possible by employing a $\mathrm{CPHF}(n; k, q, 4)$ where each row is a $\mathrm{CPHF}(1; k, q, 3)$, combined with Roux-type constructions for $t = 4$ [20, 29, 30, 36]. Three anti-cocircular truncated Möbius planes (Theorem 4.3.1) gives a $\mathrm{CPHF}(3; \frac{q^2+1}{2}, q, 4)$ where each row is a $\mathrm{CPHF}(1; \frac{q^2+1}{2}, q, 3)$. This structure is suitable for recursive constructions, as shown in Theorem 4.4.1. This motivates us trying to generalize Theorem 5.2.6 for $t = 4$ in order to obtain new families of strength-4 covering arrays.

Bibliography

[1] Yossi Azar, Rajeev Motwani, and Joseph Naor. "Approximating probability distributions using small sample spaces". *Combinatorica* 18.2 (1998), 151–171 (cit. on p. 9).

[2] R. D. Baker, J. M. N. Brown, G. L. Ebert, and J. C. Fisher. "Projective bundles". In: vol. 1. 3. 1994, 329–336 (cit. on pp. 5, 26, 39, 76).

[3] Simeon Ball. *Finite geometry and combinatorial applications*. Vol. 82. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 2015, xii+285. ISBN: 978-1-107-51843-8; 978-1-107-10799-1 (cit. on pp. 11, 13).

[4] Adriano Barlotti. "Un'estensione del teorema di Segre-Kustaanheimo". *Boll. Un. Mat. Ital. (3)* 10 (1955), 498–506 (cit. on p. 16).

[5] R. C. Bose. "Mathematical theory of the symmetrical factorial design". *Sankhyā* 8 (1947), 107–166. ISSN: 0036-4452 (cit. on p. 16).

[6] R. H. Bruck. "Circle geometry in higher dimensions. II". *Geometriae Dedicata* 2 (1973), 133–188 (cit. on pp. 5, 26, 29, 76).

[7] Renée C. Bryce and Charles J. Colbourn. "The density algorithm for pairwise interaction testing". *Software Testing, Verification and Reliability* 17.3 (2007), 159–182 (cit. on p. 9).

[8] K. A. Bush. "Orthogonal arrays of index unity". *Ann. Math. Statistics* 23 (1952), 426–434. ISSN: 0003-4851 (cit. on p. 58).

[9] Rey Casse. *Projective geometry: an introduction*. Oxford University Press, Oxford, 2006, xii+198. ISBN: 978-0-19-929886-0; 0-19-929886-6 (cit. on p. 17).

[10] M. Chateauneuf and D. L. Kreher. "On the state of strength-three covering arrays". *J. Combin. Des.* 10.4 (2002), 217–238. ISSN: 1063-8539,1520-6610 (cit. on pp. 57, 65, 75).

[11] Myra B. Cohen, Charles J. Colbourn, and Alan C. H. Ling. "Constructing strength three covering arrays with augmented annealing". *Discrete Math.* 308.13 (2008), 2709–2722. ISSN: 0012-365X,1872-681X (cit. on pp. 57, 65).

[12] Charles J. Colbourn. "Combinatorial aspects of covering arrays". *Matematiche (Catania)* 59.1-2 (2004), 125–172. ISSN: 0373-3505,2037-5298 (cit. on pp. 8–10).

[13] Charles J. Colbourn. "Covering Arrays". In: *Handbook of combinatorial designs*. Ed. by Charles J. Colbourn and Jeffrey H. Dinitz. Second. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. Chap. VI.10, 361–365. ISBN: 978-1-58488-506-1; 1-58488-506-8 (cit. on p. 9).

[14] Charles J. Colbourn. "Covering arrays from cyclotomy". *Des. Codes Cryptogr.* 55.2-3 (2010), 201–219. ISSN: 0925-1022,1573-7586 (cit. on pp. 74, 75).

[15] Charles J. Colbourn. *Covering Array Table*. `https://github.com/ugroempi/CAs/blob/main/ColbournTables.md`. [Online; accessed August-2025] (cit. on pp. 4, 9, 50, 51, 53, 55, 56, 58, 73–77).

[16] Charles J. Colbourn and Jeffrey H. Dinitz, eds. *Handbook of combinatorial designs*. Second. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007, xxii+984. ISBN: 978-1-58488-506-1; 1-58488-506-8.

[17] Charles J. Colbourn, Colin Ingalls, Jonathan Jedwab, Mark Saaltink, Ken W. Smith, and Brett Stevens. "Sets of mutually orthogoval projective and affine planes". *Comb. Theory* 4.1 (2024), Paper No. 8, 21. ISSN: 2766-1334 (cit. on pp. 5, 26–29, 57, 76).

[18] Charles J. Colbourn and Erin Lanus. "Subspace restrictions and affine composition for covering perfect hash families". *Art Discrete Appl. Math.* 1.2 (2018), Paper No. 2.03, 19. ISSN: 2590-9770 (cit. on pp. 25, 53, 56).

[19] Charles J. Colbourn, Sosina S. Martirosyan, Gary L. Mullen, Dennis Shasha, George B. Sherwood, and Joseph L. Yucas. "Products of mixed covering arrays of strength two". *J. Combin. Des.* 14.2 (2006), 124–138. ISSN: 1063-8539,1520-6610 (cit. on pp. 57, 60).

[20] Charles J. Colbourn, Sosina S. Martirosyan, Tran Van Trung, and Robert A. Walker II. "Roux-type constructions for covering arrays of strengths three and four". *Des. Codes Cryptogr.* 41.1 (2006), 33–57. ISSN: 0925-1022,1573-7586 (cit. on pp. 57, 62, 65, 74, 75, 78).

[21] Gary L. Ebert. "Partitioning projective geometries into caps". *Canad. J. Math.* 37.6 (1985), 1163–1175. ISSN: 0008-414X,1496-4279 (cit. on p. 30).

[22] John B. Fraleigh. *A first course in abstract algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1967, xvi+447 (cit. on p. 11).

[23] Nevena Francetić and Brett Stevens. "Asymptotic Size of Covering Arrays: An Application of Entropy Compression". *Journal of Combinatorial Designs* 25.6 (2017), 243–257 (cit. on p. 9).

[24] Luisa Gargano, János Körner, and Ugo Vaccaro. "Sperner capacities". *Graphs and combinatorics* 9.1 (1993), 31–46 (cit. on p. 9).

[25] David G. Glynn. "Finite Projective Planes and Related Combinatorial Systems". PhD thesis. University of Adelaide, 1978 (cit. on pp. 5, 26, 29, 76).

[26] Anant P. Godbole, Daphne E. Skipper, and Rachel A. Sunley. "t-covering arrays: upper bounds and Poisson approximations". *Combinatorics, Probability and Computing* 5.2 (1996), 105–117 (cit. on p. 9).

[27] Solomon W. Golomb and Guang Gong. *Signal Design for Good Correlation: For Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005 (cit. on pp. 14, 15).

[28] Marshall Hall Jr. "Cyclic projective planes". *Duke Math. J.* 14 (1947), 1079–1090. ISSN: 0012-7094,1547-7398 (cit. on pp. 5, 26, 29, 76).

[29] Alan Hartman. "Software and hardware testing using combinatorial covering suites". In: *Graph theory, combinatorics and algorithms*. Springer, New York, 2005, 237–266. ISBN: 978-0387-24347-4; 0-387-24347-X (cit. on pp. 57, 78).

[30] Alan Hartman and Leonid Raskin. "Problems and algorithms for covering arrays". *Discrete Math.* 284.1-3 (2004), 149–156. ISSN: 0012-365X,1872-681X (cit. on pp. 57, 78).

[31] A. S. Hedayat, N. J. A. Sloane, and John Stufken. *Orthogonal arrays*. Springer Series in Statistics. Springer-Verlag, New York, 1999, xxiv+416. ISBN: 0-387-98766-5 (cit. on p. 58).

[32] Idelfonso Izquierdo-Marquez, Jose Torres-Jimenez, Brenda Acevedo-Juárez, and Himer Avila-George. "A greedy-metaheuristic 3-stage approach to construct covering arrays". *Inform. Sci.* 460/461 (2018), 172–189. ISSN: 0020-0255,1872-6291 (cit. on pp. 56, 75).

[33] Dieter Jungnickel, Alexander Pott, and Ken W. Smith. "Difference sets". In: *Handbook of combinatorial designs*. Ed. by Charles J. Colbourn and Jeffrey H. Dinitz. Second. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. Chap. VI.18, 419–435. ISBN: 978-1-58488-506-1; 1-58488-506-8 (cit. on p. 31).

[34] Dieter Jungnickel and Klaus Vedder. "On the geometry of planar difference sets". *European J. Combin.* 5.2 (1984), 143–148. ISSN: 0195-6698,1095-9971 (cit. on pp. 5, 26, 29, 76).

[35] Rudolf Lidl and Harald Niederreiter. *Introduction to finite fields and their applications*. first. Cambridge University Press, Cambridge, 1994, xii+416. ISBN: 0-521-46094-8 (cit. on p. 11).

[36] Sosina Martirosyan and Tran Van Trung. "On t-covering arrays". *Des. Codes Cryptogr.* 32.1-3 (2004), 323–339. ISSN: 0925-1022,1573-7586 (cit. on pp. 57, 78).

[37] Sosina S. Martirosyan and Charles J. Colbourn. "Recursive constructions of covering arrays". *Bayreuth. Math. Schr.* 74 (2005), 266–275. ISSN: 0172-1062 (cit. on p. 57).

[38] Lucia Moura, Gary L. Mullen, and Daniel Panario. "Finite field constructions of combinatorial arrays". *Des. Codes Cryptogr.* 78.1 (2016), 197–219. ISSN: 0925-1022,1573-7586 (cit. on p. 22).

[39] Akihiro Munemasa. "Orthogonal arrays, primitive trinomials, and shift-register sequences". *Finite Fields Appl.* 4.3 (1998), 252–260. ISSN: 1071-5797,1090-2465 (cit. on pp. 3, 20).

[40] Joseph Naor and Moni Naor. "Small-bias probability spaces: Efficient constructions and applications". In: *Proceedings of the twenty-second annual ACM symposium on Theory of computing*. 1990, 213–223 (cit. on p. 9).

[41] Moni Naor, Leonard J Schulman, and Aravind Srinivasan. "Splitters and near-optimal derandomization". In: *Proceedings of IEEE 36th Annual Foundations of Computer Science*. IEEE. 1995, 182–191 (cit. on p. 9).

[42] W. Keith Nicholson. *Introduction to abstract algebra*. Third. Wiley-Interscience [John Wiley & Sons], Hoboken, NJ, 2007, xxii+511. ISBN: 978-0-471-69492-2; 0-471-69492-4 (cit. on pp. 11, 12).

[43] Changhai Nie and Hareton Leung. "A survey of combinatorial testing". *ACM Comput. Surv.* 43.2 (Feb. 2011). ISSN: 0360-0300 (cit. on pp. 8, 10).

[44] Christine M. O'Keefe. "Ovoids in PG$(3, q)$: a survey". In: vol. 151. 1-3. Graph theory and combinatorics (Manila, 1991). 1996, 175–188 (cit. on p. 17).

[45] Daniel Panario, Mark Saaltink, Brett Stevens, and Daniel Wevrick. "An extension of a construction of covering arrays". *J. Combin. Des.* 28.11 (2020), 842–861. ISSN: 1063-8539,1520-6610 (cit. on pp. 5, 20, 21, 26, 76).

[46] Gianfranco Panella. "Caratterizzazione delle quadriche di uno spazio (tridimensionale) lineare sopra un corpo finito". *Boll. Un. Mat. Ital. (3)* 10 (1955), 507–513 (cit. on p. 16).

[47] B. Qvist. "Some remarks concerning curves of the second degree in a finite plane". *Ann. Acad. Sci. Fennicae Ser. A. I. Math.-Phys.* 1952.134 (1952), 27. ISSN: 0365-2300 (cit. on p. 16).

[48] Sebastian Raaphorst, Lucia Moura, and Brett Stevens. "A construction for strength-3 covering arrays from linear feedback shift register sequences". *Des. Codes Cryptogr.* 73.3 (2014), 949–968. ISSN: 0925-1022,1573-7586 (cit. on pp. 4, 5, 15, 20, 22, 24–26, 28, 29, 57, 67, 76).

[49] C. Radhakrishna Rao. "Hypercubes of strength 'd' leading to confounded designs in factorial experiments". *Bull. Calcutta Math. Soc.* 38 (1946), 67–78. ISSN: 0008-0659 (cit. on p. 20).

[50] C. Radhakrishna Rao. "Factorial experiments derivable from combinatorial arrangements of arrays". *Suppl. J. Roy. Statist. Soc.* 9 (1947), 128–139. ISSN: 1466-6162,2517-617X (cit. on p. 20).

[51] C. Radhakrishna Rao. "On a class of arrangements". *Proc. Edinburgh Math. Soc. (2)* 8 (1949), 119–125. ISSN: 0013-0915,1464-3839 (cit. on p. 20).

[52] M. S. Raunak, D. R. Kuhn, R. N. Kacker, and Jeff Y. Lei. "Combinatorial Testing for Building Reliable Systems". *IEEE Reliability Magazine* 1.1 (2024), 15–19 (cit. on pp. 9, 10).

[53] G. Roux. "k-Propriétés dans les tableaux de n colonnes: cas particulier de la k-surjectivité et de la k-permutivité". PhD thesis. Université de Paris, 1987 (cit. on pp. 57, 65).

[54] Esther Seiden. "A theorem in finite projective geometry and an application to statistics". *Proc. Amer. Math. Soc.* 1 (1950), 282–286. ISSN: 0002-9939,1088-6826 (cit. on p. 16).

[55] Kianoosh Shokri and Lucia Moura. "New Families of Strength-3 Covering Arrays Using Linear Feedback Shift Register Sequences". *J. Combin. Des.* 33.4 (2025), 156–171. ISSN: 1063-8539,1520-6610 (cit. on pp. 7, 57).

[56] Kianoosh Shokri, Lucia Moura, and Brett Stevens. *Existence of 3 anti-cocircular truncated Möbius planes and constructions of strength-4 covering arrays*. 2025. arXiv: 2510.13122 [math.CO] (cit. on pp. 6, 29).

[57] N. J. A. Sloane. "Covering arrays and intersecting codes". *J. Combin. Des.* 1.1 (1993), 51–63. ISSN: 1063-8539,1520-6610 (cit. on pp. 65, 73, 75).

[58] Brett Stevens, Lucia Moura, and Eric Mendelsohn. "Lower bounds for transversal covers". *Des. Codes Cryptogr.* 15.3 (1998), 279–299. ISSN: 0925-1022,1573-7586 (cit. on p. 9).

[59] Leo Storme. "Finite Geometry". In: *Handbook of combinatorial designs*. Ed. by Charles J. Colbourn and Jeffrey H. Dinitz. Second. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2007. Chap. VII.2, 702–729. ISBN: 978-1-58488-506-1; 1-58488-506-8 (cit. on p. 16).

[60] Jose Torres-Jimenez, Himer Avila-George, and Idelfonso Izquierdo-Marquez. "A two-stage algorithm for combinatorial testing". *Optim. Lett.* 11.3 (2017), 457–469. ISSN: 1862-4472,1862-4480 (cit. on p. 75).

[61] Jose Torres-Jimenez and Idelfonso Izquierdo-Marquez. "Covering arrays of strength three from extended permutation vectors". *Des. Codes Cryptogr.* 86.11 (2018), 2629–2643. ISSN: 0925-1022,1573-7586 (cit. on pp. 27, 29).

[62] Jose Torres-Jimenez, Idelfonso Izquierdo-Marquez, and Himer Avila-George. "Methods to Construct Uniform Covering Arrays". *IEEE Access* 7 (2019), 42774–42797 (cit. on pp. 8, 9).

[63] Jose Torres-Jimenez and Eduardo Rodriguez-Tello. "New bounds for binary covering arrays using simulated annealing". *Inform. Sci.* 185.1 (2012), 137–152. ISSN: 0020-0255 (cit. on p. 75).

[64] Georgios Tzanakis, Lucia Moura, Daniel Panario, and Brett Stevens. "Constructing new covering arrays from LFSR sequences over finite fields". *Discrete Math.* 339.3 (2016), 1158–1171. ISSN: 0012-365X,1872-681X (cit. on pp. 28, 29, 77).

[65] Oswald Veblen and John Wesley Young. *Projective geometry. Vol. 1*. Blaisdell Publishing Co. [Ginn and Co.], New York-Toronto-London, 1938, x+345 (cit. on pp. 5, 26, 29, 76).

[66] Michael Wagner, Charles J. Colbourn, and Dimitris E. Simos. "In-parameter-order strategies for covering perfect hash families". *Appl. Math. Comput.* 421 (2022), Paper No. 126952, 21. ISSN: 0096-3003,1873-5649 (cit. on pp. 53, 56, 75).

[67] Richard M. Wilson and Qing Xiang. "Cyclotomy, Half Ovoids and Two-weight Codes". Unpublished manuscript, 1997 (cit. on p. 29).

[68] Jianxing Yin. "Constructions of difference covering arrays". *J. Combin. Theory Ser. A* 104.2 (2003), 327–339. ISSN: 0097-3165,1096-0899 (cit. on p. 62).