Covering arrays from maximal sequences over finite fields

Georgios Tzanakis

Ph.D. Thesis

Covering arrays from maximal sequences over finite fields

Georgios Tzanakis

A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

School of Mathematics and Statistics
Ottawa-Carleton Institute for Mathematics and Statistics
Carleton University
Ottawa, Ontario

ii

Abstract

THE FOCUS OF THIS THESIS is the study and construction of covering arrays, relying on maximal period sequences and other tools from finite fields. A *covering array of strength t*, denoted $CA(N; t, k, v)$, is an $N \times k$ array with entries from an alphabet A of size v, with the property that in the $N \times t$ subarray defined by any t columns, each of the v^t vectors in A^t appears at least once as a row. Covering arrays generalize orthogonal arrays, which are classic combinatorial objects that have been studied extensively. Constructing covering arrays with a small row-to-column ratio is important in the design of statistical experiments, however it is also a challenging mathematical problem.

Linear feedback shift register (LFSR) sequences are sequences of elements from a finite field that satisfy a linear recurrence relation. It is well-known that these are periodic; LFSR sequences that attain the maximum possible period are *maximal (period) sequences*, often abbreviated to *m-sequences* in the literature. Arrays constructed from cyclic shifts of maximal sequences possess strong combinatorial properties and have been previously used to construct orthogonal and covering arrays [62], although only one of the known constructions is for covering arrays that are not orthogonal arrays [75]. In this thesis we present several new such constructions.

The cornerstone of our results is a study of the combinatorial properties of arrays constructed from maximal sequences, where we make fundamental connections with concepts from diverse areas of discrete mathematics, such as orthogonal arrays, error-correcting codes, divisibility of polynomials and structures of finite geometry.

One aspect of our work involves concatenating arrays corresponding to different maximal sequences and finding subarrays that are covering arrays. We express this as an optimization problem, to which we give an algorithmic solution based on backtracking, an underlying finite field theory and connections to other combinatorial objects. The results of our experiments include 37 new covering arrays of strength 4 and one of strength 5.

For integers $v \geq 2$, we introduce cyclic trace arrays modulo v, a variation of arrays from maximal sequences that we study using finite field characters - homomorphisms from the finite field to the unit circle of complex numbers. In particular, we use well-known bounds on character sums to derive conditions subject to which cyclic trace arrays modulo v are covering arrays, and we present new infinite families of covering arrays of strengths 3 and 4, as well as one of arbitrary strength which appears to be the second such family in the known literature [25]. We also express the number of times that different vectors appear in the rows of a cyclic trace array modulo v as the solution of a linear program.

To my parents, Maro and Nikos

Acknowledgments

First and foremost, I would like to thank Daniel Panario. Having him as my advisor was a privilege; the guidance, opportunities and friendship that he offered will always be deeply appreciated. I am also most grateful for having met and worked with Lucia Moura and Brett Stevens. I owe this piece of work and much more to the support, knowledge and enthusiasm of these three people.

I would like to extend my thanks to the members of my defence committee, Charlie Colbourn, Evangelos Kranakis, Mike Newman and David Thomson for their time, effort and insightful comments. Special thanks to Charlie Colbourn whose work on covering arrays has been essential to my research. I also wish to thank my undergraduate supervisor, Theodoulos Garefalakis, who introduced me to the area of finite fields and who was the one to encourage and help me to pursue my studies in Canada.

Completing my Ph.D. was a long process full of bright highs and dark lows; I would not have gotten through the latter without the endless love and support of my family. It is hard to express what they mean to me without making an understatement.

I was extremely fortunate to be surrounded by numerous wonderful friends throughout my studies. Ali Al-Bashabsheh has been a true and most invaluable friend. Lorena Ibacache was the closest thing that I had to family while being away from home. John Talboom and Ming-Ming Zhang where my companions along the way, from our first assignments to the celebration after my defence; I do not want to imagine how my long days and nights in Herzberg labs would be without them. Also essential to surviving my Ph.D. was having Ioannis Nomidis as my housemate and much needed Greek company, along with Aris Leivadeas and Manos Skevakis. Kate Trotter and Dragica Stanivuk have been my dearest friends since our university residence years and I cannot think of my time in Canada without thinking of them. Whether it was a lazy evening or a hike in the middle of the Canadian winter, hanging out with Chris Dionne, Aras Erzurumluoğlu, Nevena Francetić and Elizabeth Maltais was always a blast. I also greatly appreciate the friendship of Caio Fernandes, Camelia Karimianpour, José Matos, Patrick Niesink and Anna Rousso. Finally, I am thankful to Stelios Charitakis, the Gorgoraptis brothers, Isis Mouza and Christos Spatharakis, for being my beloved friends despite our distance.

Contents

Introduction

THIS THESIS IS CONCERNED WITH the study and construction of covering arrays, a combinatorial object that lies in the intersection of diverse fields such as discrete mathematics, statistics, computer science and software engineering, and is the topic of active research, ranging from purely theoretical mathematical studies to software development and industrial applications.

The origins of covering arrays are orthogonal arrays, which were first studied by Rao in the second half of the 1940s [76, 77, 78], and since then have became a classic mathematical object due to their natural definition and fundamental connections to other areas, such as finite fields, finite geometry and error-correcting codes. An *orthogonal array of strength t and index* λ, denoted $\mathrm{OA}_\lambda(t, k, v)$, is a $\lambda v^t \times k$ array with entries from an alphabet A of size v, with the property that in the $\lambda v^t \times t$ subarray defined by any t columns, each of the v^t vectors in A^t appears as a row precisely λ times. The requirement that every row appears λ times is very restrictive and, in the context of certain applications, also unnecessary; a covering array is the result of relaxing this part of the definition. More precisely, a *covering array of strength t*, denoted $\mathrm{CA}(N; t, k, v)$, is an $N \times k$ array with entries from an alphabet A of size v, with the property that in the $N \times t$ subarray defined by any t columns, each of the v^t vectors in A^t appears *at least* once as a row.

The primary application of covering arrays is the design of experiments. In areas such as software development and manufacturing, it is often infeasible to perform exhaustive system tests. However, empirical research shows that in many types of systems, errors are triggered only when a small number of factors interact [53]. In these cases, a practical alternative is *t-way interaction testing*, where the objective is to check every t-combination of factors. This approach can dramatically reduce the number of tests that need to be performed, while still being extremely effective in detecting errors [18, 53]. A $\mathrm{CA}(N; t, k, v)$ can be considered as a test suite for t-way interaction testing, where the rows provide a collection of N configurations for a system with k factors, represented by the columns, with each factor admitting v possible values. Performing experimental runs for all N configurations corresponding to the rows of the covering array, guarantees that every possible interaction of t factors is tested at least once.

In Figure 1.1 we give an example of 2-way interaction testing using a covering array. The software system in Figure 1.1a has 4 factors, namely a payment server, a web server, a browser, and a database. Each of them admits 3 possible values as shown in the table. Using a $\mathrm{CA}(10; 4, 3, 2)$ by representing each factor value with 0, 1 or 2, we obtain a collection of 10 tests corresponding to its rows, as shown in Figure 1.1b. Testing these 10 configurations guarantees that every interaction of two factors has been considered. The downside is that, if there exists

Payment Server	Web server	Browser	Database
Visa (0)	IIS (0)	Mozilla (0)	MySQL (0)
Master card (1)	Apache (1)	Chrome (1)	Oracle (1)
American express (2)	Sun (2)	Opera (2)	PostgreSQL (2)

(a) Factors of the system and their possible values

		Payment Server	Web server	Browser	Database
2 1 0 1	Test 1	American express	Apache	Mozilla	Oracle
1 0 2 2	Test 2	Master card	IIS	Opera	PostgreSQL
0 2 2 1	Test 3	Visa	Sun	Opera	Oracle
2 2 0 2	Test 4	American express	Sun	Mozilla	PostgreSQL
2 0 1 1 $\longrightarrow$	Test 5	American express	IIS	Chrome	Oracle
2 1 2 0	Test 6	American express	Apache	Opera	MySQL
1 2 1 0	Test 7	Master card	Sun	Chrome	MySQL
1 1 0 1	Test 8	Master card	Apache	Mozilla	Oracle
0 1 1 2	Test 9	Visa	Apache	Chrome	PostgreSQL
0 0 0 0	Test 10	Visa	IIS	Mozilla	MySQL

(b) Using a CA$(10; 2, 4, 3)$ to obtain the configurations for 2-way interaction testing of the system.

Figure 1.1. Testing of a software system using a covering array.

a combination of 3 or 4 factor values that causes the system to fail, then this type of testing is not guaranteed to reveal it; for this to be the case, up to $3^4 = 81$ configurations should be tested.

Although testing 81 configurations for the system in the previous example may be feasible, for systems with a large number of values per factor, exhaustive testing can be an enormous task. More precisely, a system with k factors each admitting v possible values requires v^k tests, so the number of tests required in exhaustive testing increases exponentially with respect to the number of factors. On the other hand, performing t-way interaction testing for the same system requires N tests, where N is the number of rows of a CA$(N; t, k, v)$, which can be significantly smaller than v^k. For example, for fixed t and v, it is proven that a CA$(N; t, k, v)$ with $N = O(\log(k))$ can be constructed in polynomial time using a greedy algorithm [11]. At the same time, empirical evidence has shown that t-way interaction testing, even for very small values of t, is sufficient for many types of systems in real life. Indeed, a review of fifteen years of medical device recall data by the US Food and Drug Administration (FDA), shows that t-way interaction testing with t equal to $2, 3$ or 4, could detect $97, 99$ and 100 percent of the defects, respectively [95]. For studies on the effectiveness of t-way interaction testing, we refer to [18, 53]. We also note that the National Institute of Standards and Technology (NIST) maintains an online database of covering arrays as part of its Automated Combinatorial Testing for Software (ACTS) program [67].

It is evident from our above discussion that constructing covering arrays with a small row-to-column ratio is an important problem. This leads to the definition of the *covering array number* $CAN(t, k, v)$, which is the smallest n such that a $CA(n; t, k, v)$ exists. For a $CA(N; t, k, v)$, comparing N to $CAN(t, k, v)$ provides a measure of how good the covering array is. A covering array that attains the minimum number of rows is *optimal*. A trivial lower bound for $CAN(t, k, v)$ is v^t, which is achieved by $OA_1(t, k, v)$. However, such orthogonal arrays are rare and, beyond that, few optimal families of covering arrays are known [13, 49, 52]. New constructions aim instead to improve upon the best currently known upper bounds for covering array numbers. The previously mentioned greedy algorithm implies a logarithmic upper bound on the covering array number with respect to the number of columns. Other upper bounds follow from numerous methods for obtaining covering arrays that exist in the literature. These include combinatorial and algebraic constructions, greedy and metaheuristic computer algorithms, and recursive methods for obtaining new covering arrays from existing ones. Colbourn actively maintains an online database of the best known upper bounds for $CAN(t, k, v)$, where $2 \leq t \leq 6$ and $2 \leq v \leq 25$ [29]. Other aspects of the research on covering arrays include existence results of probabilistic nature, and generalizations of covering arrays such as *mixed-level covering arrays*, whose columns contain entries from different alphabets. A very comprehensive survey on the subject is given by Colbourn [24]; for a more recent albeit more brief presentation, we refer to Kuliamin and Petukhov [54]. We also give a short overview of many important results in Chapter 2.

In this thesis we focus on the following two problems related to covering arrays:

1. find covering arrays of strength more than 3 that improve upon the currently best known upper bounds for covering array numbers, and

2. give a theoretical construction of covering arrays such that, for arbitrary t, k, v, a $CA(N; t, k, v)$ can be constructed for some N.

With regards to the first problem, we note that an increasing number of the best known upper bounds for covering array numbers for strengths 4 or higher are obtained recursively from other bounds [29], while the direct theoretical constructions in Colbourn's survey [24] are almost exclusively for strengths 2 and 3. Regarding the second problem, it appears that prior to this work and to the best of our knowledge, the construction by Colbourn [25] is the only direct (not algorithmic, recursive or probabilistic) answer. We address these two problems relying on powerful tools from the theory of finite fields.

A finite field - or Galois field, in honor of Évariste Galois - is an algebraic field with a finite number of elements. The theory of finite fields is a branch of algebra with a wide variety of applications in combinatorics, error-correcting codes, finite geometry, cryptography and other fields of mathematics. One area of finite fields that has gained a lot of interest in recent years is concerned with sequences of finite field elements that satisfy a linear recurrence relation. Although the study of such sequences can be traced back to the works of Lagrange in the 18th century, it came to fore again in the 1950s with the dawn of the digital age, when they were found to have applications of great importance in wireless communications. Due to their straightforward and widespread implementation in digital circuits using feedback shift

registers, they have come to be known as linear feedback shift register (LFSR) sequences. From both a mathematical and engineering standpoint, the works of Golomb [40, 42] played a crucial role in the revival of the topic during that time, and nowadays the algebraic properties of LFSR sequences have been studied extensively [40, 41]. For instance, it is well-known that they are periodic; LFSR sequences that attain the maximum possible period are *maximal (period) sequences* - often abbreviated to *m-sequences* in the literature.

Maximal sequences have been previously employed for the construction of orthogonal arrays. As we show in Chapter 3, some classic orthogonal array constructions can be translated into the language of maximal sequences. However, the first construction that relies primarily on using their properties appears to be a 1998 work by Munemasa [64], who constructs binary orthogonal arrays of strength 2 that are "close to" strength 3. This was followed by two generalizations about a decade later [31, 70], that provide binary and ternary covering arrays of strength 2 or 3. These results are based on the study of the divisibility properties of certain types of polynomials with coefficients from the finite fields with 2 or 3 elements. A different approach was adopted by Raaphorst et al. [75] (see also [74]) who exploited connections with combinatorial designs to construct a family of covering arrays of strength 3. This is the only construction, prior to our work, that is based on LFSR sequences and produces covering arrays which are not orthogonal arrays. Hence, despite the rich algebraic structure and many combinatorial properties of LFSR sequences, their use for the construction of covering arrays is a rather unknown territory. This thesis is a step towards this promising direction.

Our main contributions can be summarized in the following.

- We give a comprehensive study of the connections between maximal sequences and diverse concepts related to orthogonal arrays, error-correcting codes, divisibility of polynomials and structures from finite geometry. While these connections have been used or implied in previous research, we present them in a unified framework for the first time. This also allows us to describe the previous and new constructions of orthogonal and covering arrays from maximal sequences using the language of different areas of discrete mathematics, which we hope will facilitate further research on this topic.

- We develop a backtracking algorithm for the construction of covering arrays of arbitrary strength, that relies on an underlying finite field theory, properties of maximal sequences and connections to other combinatorial objects. Among our experimental results there are 37 new covering arrays of strength 4 and one of strength 5 that improve upon previously best known bounds listed in the online database by Colbourn [29]. This work appears in [93].

- Relying on properties of maximal sequences and an argument involving character sums, we give new infinite families of covering arrays of strengths 3 and 4, as well as an infinite family of covering arrays of arbitrary strength. This is one of the two known direct constructions of covering arrays of arbitrary strength along with a recent one due to Colbourn [25]. Furthermore, our constructions and that of Raaphorst et al. [75] are the only ones that rely on LFSR sequences and yield covering arrays that are not orthogonal arrays.

We conclude by outlining the structure of the thesis.

- Chapter 2 contains the necessary preliminaries to make our work self-contained. The first part is dedicated to several aspects of the theory and applications of finite fields, such as the existence and construction of finite fields, characters, maximal sequences, finite geometry, combinatorial designs, and coding theory. The second part gives the necessary background on orthogonal and covering arrays, as well as a presentation of the state of the current research on covering arrays.

- Chapter 3 serves both to provide tools necessary for the rest of the thesis, as well as to present in detail previously established constructions of orthogonal and covering arrays using maximal sequences. We start by proving fundamental connections between maximal sequences and concepts from other areas of discrete mathematics, and then we explore the previously established constructions in view of the above connections.

- Chapter 4 is concerned with the construction of covering arrays of any strength from maximal sequences, from the point of view of an optimization problem to which we give an algorithmic solution. The chapter starts with an in-depth look of the optimization problem we wish to solve, and continues with the development of the theory behind the algorithm, that requires several results from finite fields and the study of other combinatorial objects. Finally, we present our experimental results and discuss their importance.

- In Chapter 5 we introduce cyclic trace arrays modulo v, a new type of array based on maximal sequences, discrete logarithms and integer congruences that we study using characters - homomorphisms from the finite field to the unit circle of complex numbers. In particular, we use ideas from [25] to translate the problem of checking whether a cyclic trace array modulo v is a covering array into the problem of finding a lower bound to an expression that involves character sums. We then use properties of maximal sequences and well-known bounds of character sums to obtain conditions subject to which a cyclic trace array modulo v is a covering array. Based on that, we present new infinite families of covering arrays.

- Chapter 6 is preliminary work on some aspects of the arrays introduced in the previous chapter, using different techniques. More precisely, we count the number of different t-tuples that appear in the rows, and we express this count as the solution of a linear program. By providing computational lower bounds for this number, we hope to find cyclic trace arrays modulo v that are covering arrays which are not revealed by the conditions in Chapter 5. An extended abstract of this ongoing work has been submitted [69].

- Chapter 7 discusses potential future directions related to the thesis.

Preliminaries

IN THIS CHAPTER WE GIVE the minimum necessary background to make our thesis self-contained. This consists of well-known definitions and results from various topics related to finite fields as well as orthogonal and covering arrays. In Section 2.1 we present some fundamental theory of finite fields, and then we touch on characters, sequences, finite geometry and linear codes. In Section 2.2 we define orthogonal and covering arrays, and we give an overview of the research in this area, which includes a discussion about their applications and a presentation of some important results that have already been established.

2.1 Finite fields

2.1.1 Review of some basic finite field theory

In this section we give a number of fundamental definitions and facts about finite fields. Our presentation is brief as we only include things that we use in this thesis. For a complete and thorough introduction to finite fields, we refer the reader to [56]. We also assume some basic knowledge of ring and field theory.

Existence and uniqueness of finite fields

It follows from elementary algebra that if L is an extension field over a subfield K, then L can be seen as a vector space over K, under the usual field operations. For finite fields in particular, we have the following lemma.

> **Lemma 2.1 (A finite field is a vector space over any subfield).** *Let F be a finite field and K be a subfield containing q elements. Then F is a vector space over K, and $|F| = q^t$, where t is the dimension of F, viewed as a vector space over $\mathbb{F}_q$.*

Using Lemma 2.1, we can characterize the cardinality of finite fields.

> **Theorem 2.2 (Every finite field has cardinality a prime power [56, Theorem 2.2]).** *Let F be a finite field. Its prime subfield K has cardinality p, a prime number, which is also the characteristic of F. Then, $|F| = p^n$ where n is the dimension of F over K.*

The converse of Theorem 2.2 is also true.

> **Theorem 2.3 (Existence and uniqueness of finite fields [56, Theorem 2.5]).** *For every prime p and positive integer n, there exists a finite field with p^n elements. Furthermore, any finite field with p^n elements is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$.*

From Theorems 2.2 and 2.3 we conclude that every finite field has cardinality a prime power and, conversely, for every prime power q there exists a finite field with q elements. Furthermore, all finite fields with q elements are isomorphic since splitting fields of the same polynomial are isomorphic. Hence, we speak of *the* finite field with q elements, which we denote $\mathbb{F}_q$.

Properties and construction of finite fields

Having established the existence and uniqueness of finite fields, we list some of their basic properties and discuss their construction. We begin by a characterization of the subfields of a finite field.

> **Theorem 2.4 (Subfield criterion [56, Theorem 2.6]).** *Let p be a prime and n be a positive integer. Then, every subfield of $\mathbb{F}_{p^n}$ has order p^d, where d is a positive divisor of n. Conversely, if d is a positive divisor of n, then there is exactly one subfield of $\mathbb{F}_q$ with p^d elements.*

To every field element, we associate a unique polynomial as follows.

> **Definition 2.5 (Minimal polynomial of a finite field element).** Let K be a subfield of F, and $\alpha \in F$ be algebraic over K. Then, the uniquely determined monic irreducible polynomial $g \in K[x]$ generating the ideal $J = \{f \in K[x] \mid f(\alpha) = 0\}$ is the *minimal polynomial of α over K*. We denote this polynomial $m_{\alpha,K}$, however we simply write m_α when it is clear from the context what K is.

We use the following lemma regularly in the next chapters.

> **Lemma 2.6 ([56, Lemma 2.12]).** *Let t be a positive integer and $\alpha \in \mathbb{F}_{q^t}$. Then, for a polynomial $f \in \mathbb{F}_q[x]$, we have that α is a root of f if and only if f is divisible by m_α.*

For integers a, b with $a < b$, we denote $[a, b] = \{a, a+1, \ldots, b\}$. For a prime p, the field $\mathbb{F}_p$ is isomorphic to $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, so we identify $\mathbb{F}_p$ with the set $[0, p-1]$ along with the usual addition and multiplication modulo p. Next, we consider the representation of finite fields whose cardinality is a prime power.

> **Theorem 2.7 (Roots of irreducible polynomials over finite fields [56, Theorem 2.14]).** *If f is an irreducible polynomial in $\mathbb{F}_q[x]$ of degree t, then f has a root α in $\mathbb{F}_{q^t}$. Furthermore, all the roots of f are simple and are given by the t distinct elements $\alpha, \alpha^q, \ldots, \alpha^{q^t}$.*

Corollary 2.8 (Construction of finite fields [56, Corollary 2.15]). *Let $f \in \mathbb{F}_q[x]$ be irreducible with degree t. Then $\mathbb{F}_{q^t}$ is the splitting field of f over $\mathbb{F}_q$.*

We know (see for instance [56, Corollary 2.11]) that for every prime power q and positive integer t, there exists an irreducible polynomial $f \in \mathbb{F}_q[x]$ of degree t. It follows from Theorem 2.7 and Corollary 2.8 that for a root $\alpha \in \mathbb{F}_{q^t}$ of f, we have that $\mathbb{F}_{q^t} = \mathbb{F}_q(\alpha, \alpha^q, \ldots, \alpha^{q^t}) = \mathbb{F}_q(\alpha)$, therefore we can write

$$\mathbb{F}_{q^t} = \left\{ c_{t-1}\alpha^{t-1} + c_{t-2}\alpha^{t-2} + \cdots + c_1\alpha + c_0 \mid c_0, \ldots, c_{t-1} \in \mathbb{F}_q \right\}. \tag{2.1}$$

Definition 2.9 (Additive and multiplicative groups of a finite field). We refer to $(\mathbb{F}_q, +)$ as the *additive group of* $\mathbb{F}_q$, and $(\mathbb{F}_q^{\times}, \cdot)$ as the *multiplicative group of* $\mathbb{F}_q$, where $\mathbb{F}_q^{\times} = \mathbb{F}_q \setminus \{0\}$. We denote $(\mathbb{F}_q^{\times}, \cdot)$ simply as $\mathbb{F}_q^{\times}$.

Since $\mathbb{F}_q$ is a field, every nonzero element has a multiplicative inverse, hence $\mathbb{F}_q^{\times}$ consists of the $q - 1$ nonzero elements of $\mathbb{F}_q$. The following theorem gives an important property of $\mathbb{F}_q^{\times}$.

Theorem 2.10 (The multiplicative group of a finite field is cyclic [56, Theorem 2.8].). *For every prime power q, the multiplicative group $\mathbb{F}_q^{\times}$ of nonzero elements of $\mathbb{F}_q$ is cyclic.*

The next lemma gives a way to determine if an element belongs to a given finite field.

Lemma 2.11. *For a prime power q and a positive integer t, we have that $a \in \mathbb{F}_{q^t}$ if and only if $a^{q^t} = a$.*

Proof. The case $a = 0$ is trivial. If $a \neq 0$, then $a \in \mathbb{F}_{q^t}^{\times}$ and therefore the multiplicative order of a divides the group order $q^t - 1$, hence $a^{q^t - 1} = 1$; multiplying both sides by a gives $a^{q^t} = a$. Conversely, if a satisfies $a^{q^t} = a$, then it is a root of $x^{q^t} - x$ and as such it belongs to its splitting field; by Theorem 2.3, this is $\mathbb{F}_{q^t}$. $\square$

Generators of the multiplicative group of a finite field and their minimal polynomials are important in the area of finite fields and have been studied extensively in various contexts; see for example [63, Chapter 4] for an overview of related topics.

Definition 2.12 (Primitive elements and polynomials). For a prime power q, a generator of the cyclic group $\mathbb{F}_q^{\times}$ is a *primitive element of* $\mathbb{F}_q$. The minimal polynomial of a primitive element is a *primitive polynomial.*

Remark 2.13 (*Primitive polynomials are irreducible*). Any primitive polynomial is also irreducible. Indeed, for a root α of a primitive polynomial of degree t, we have that $\mathbb{F}_{q^t} = \mathbb{F}_q(\alpha)$, hence f has to be irreducible.

It follows from Definition 2.12 that for primitive $\alpha \in \mathbb{F}_q$, we have that

$$\mathbb{F}_q^{\times} = \left\{ \alpha^i \mid i \in [0, q - 2] \right\}.$$

Example 2.14 (Construction of the finite fields with 4 and 16 elements). For the polynomial $f(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$ we have that $f(0) = f(1) = 1$, so f does not have a root in $\mathbb{F}_2$ and therefore it is irreducible over $\mathbb{F}_2$, as a polynomial of degree 2 without roots. Let α be a root of f in $\mathbb{F}_4$. From the above, we have that the field with 4 elements satisfy

$$\mathbb{F}_4 = \mathbb{F}_2(\alpha) = \{c_0 + c_1\alpha \mid c_0, c_1 \in \mathbb{F}_2\} = \{0, 1, \alpha, \alpha + 1\}. \tag{2.2}$$

We note that since α is a root of $x^2 + x + 1$, we have that $\alpha^2 + \alpha + 1 = 0$, hence

$$\alpha^2 = -\alpha - 1 = \alpha + 1,$$

which we can use to write a product of elements from $\mathbb{F}_4$ in the form $c_0 + c_1\alpha$, $c_0, c_1 \in \mathbb{F}_2$. For example, the product of α and $\alpha + 1$ is given by

$$\alpha(\alpha + 1) = \alpha^2 + \alpha = (\alpha + 1) + \alpha = 2\alpha + 1 = 1.$$

Working this way, we create the multiplication table of $\mathbb{F}_4$, which we display along with the addition table below.

+	0	1	α	$\alpha + 1$
0	0	1	α	$\alpha + 1$
1	1	0	$\alpha + 1$	α
α	α	$\alpha + 1$	0	1
$\alpha + 1$	$\alpha + 1$	α	1	0

$\cdot$	0	1	α	$\alpha + 1$
0	0	0	0	0
1	0	1	α	$\alpha + 1$
α	0	α	$\alpha + 1$	1
$\alpha + 1$	0	$\alpha + 1$	1	α

We also note that, since $\alpha^0 = 1$ and $\alpha^2 = \alpha + 1$, we have that

$$\left\{\alpha^i \mid i \in [0, 2]\right\} = \{1, \alpha, \alpha + 1\} = \mathbb{F}_4^\times,$$

hence α is a primitive element of $\mathbb{F}_4$ and f is a primitive polynomial in $\mathbb{F}_2[x]$.

We now construct $\mathbb{F}_{16}$ as an extension of $\mathbb{F}_4$. Let β be a root of $g(x) = x^2 + x + \alpha \in \mathbb{F}_4[x]$. We calculate that $g(0) = g(1) = \alpha$, and $g(\alpha) = g(\alpha + 1) = \alpha + 1$, therefore no element of $\mathbb{F}_4$ is a root of g and hence g is irreducible over $\mathbb{F}_4$, as a polynomial of degree 2 without roots in $\mathbb{F}_4$.

Next, we show that β is a primitive element of $\mathbb{F}_{16}$. Since β is a root of g, we have that $\beta^2 + \beta + \alpha = 0$, which means that $\beta^2 = \beta + \alpha$. Then,

$$\beta^3 = \beta\beta^2 = \beta(\beta + \alpha) = \beta^2 + \alpha\beta = \beta(\alpha + 1) + \alpha = \alpha + (\alpha + 1)\beta.$$

Also,

$$\beta^5 = \beta^2\beta^3 = (\beta + \alpha)(\alpha + (\alpha + 1)\beta).$$

Expanding the last product and working out the powers of α and β as before, we find that $\beta^5 = \alpha$. Since $|\mathbb{F}_{16}^\times| = 15 = 3 \cdot 5$ and the multiplicative order of β is neither 3 or 5, then it must be 15. This means that β is a generator of $\mathbb{F}_{16}^\times$, that is, a primitive element of $\mathbb{F}_{16}$. We present the first 15 powers of β in Table 2.1; we observe that every element of $\mathbb{F}_{16}^\times$ appears in the table.

i	0	1	2	3	4
β^i	1	β	$\alpha + \beta$	$\alpha + (\alpha + 1)\beta$	$1 + \beta$
i	5	6	7	8	9
β^i	α	$\alpha\beta$	$\alpha + 1 + \alpha\beta$	$(\alpha + 1) + \beta$	$\alpha + \alpha\beta$
i	10	11	12	13	14
β^i	$\alpha + 1$	$(\alpha + 1)\beta$	$1 + (\alpha + 1)\beta$	$1 + \alpha\beta$	$(\alpha + 1) + (\alpha + 1)\beta$

Table 2.1. The first 15 powers of the primitive element $\beta \in \mathbb{F}_{16}$ described in Example 2.14. These are also precisely the nonzero elements of $\mathbb{F}_{16}$.

For a positive integer n, *Euler's function* $\phi(n)$ is the number of integers $k \in [1, n]$, with $\gcd(k, n) = 1$. The following lemma follows from well-known facts in group theory.

Lemma 2.15 (Number of primitive elements in $\mathbb{F}_q$). *Let q be a prime power, and $\alpha \in \mathbb{F}_q$ be primitive. There exist exactly $\phi(q - 1)$ primitive elements in $\mathbb{F}_q$, given by α^i, $i \in [0, q - 2]$ such that $\gcd(i, q - 1) = 1$.*

The trace function

An important function that we use extensively in this thesis, is defined as follows.

Definition 2.16 (The trace function over finite fields). Let q be a prime power, t be a positive integer, and $a \in \mathbb{F}_{q^t}$. The *trace of a over $\mathbb{F}_q$* is defined by

$$\mathrm{Tr}_{q^t/q}(a) = a + a^q + \cdots + a^{q^{t-1}}.$$

We have that $\mathrm{Tr}_{q^t/q}(a) \in \mathbb{F}_q$ for all $a \in \mathbb{F}_{q^t}$ (see [56, Section 2.3]). Furthermore, by Lemma 2.1 we have that $\mathbb{F}_{q^t}$ is a vector space over $\mathbb{F}_q$, and hence we can view the trace as a vector space mapping defined by

$$\mathrm{Tr}_{q^t/q} : \quad \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_q \qquad\qquad (2.3)$$
$$x \mapsto x + x^q + \cdots + x^{q^{t-1}}.$$

Theorem 2.17 (Properties of the trace function [56, Theorem 2.23]). *For a prime power q and positive integer t, the trace $\mathrm{Tr}_{q^t/q}$ satisfies the following properties:*

1. *$\mathrm{Tr}_{q^t/q}$ is a linear transformation from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$, where both $\mathbb{F}_{q^t}$ and $\mathbb{F}_q$ are viewed as vector spaces over $\mathbb{F}_q$;*

2. *$\mathrm{Tr}_{q^t/q}(a) = ta$, for all $a \in \mathbb{F}_q$;*

3. *$\mathrm{Tr}_{q^t/q}(a^q) = \mathrm{Tr}_{q^t/q}(a)$, for all $a \in \mathbb{F}_{q^t}$.*

Example 2.18. For α and β as in Example 2.14, we calculate $\mathrm{Tr}_{16/2}(\alpha\beta)$ and $\mathrm{Tr}_{16/4}(\alpha\beta)$. Using Table 2.1 we calculate

$$
\begin{aligned}
\mathrm{Tr}_{16/2}(\alpha\beta) &= \alpha\beta + (\alpha\beta)^2 + (\alpha\beta)^{2^2} + (\alpha\beta)^{2^3} \\
&= \beta^6 + \beta^{12} + \beta^{24} + \beta^{48} \\
&= \beta^6 + \beta^{12} + \beta^9 + \beta^3 \\
&= \alpha\beta + 1 + (\alpha + 1)\beta + \alpha + \alpha\beta + \alpha + (\alpha + 1)\beta \\
&= 1,
\end{aligned}
$$

and similarly we can calculate

$$
\mathrm{Tr}_{16/4}(\alpha\beta) = \alpha.
$$

As expected from Theorem 2.17, we observe in the above that $\mathrm{Tr}_{q^t/q}(a) \in \mathbb{F}_q$, for all $a \in \mathbb{F}_{q^t}$.

The fact that the trace defines a linear transformation over $\mathbb{F}_q$ implies the following proposition.

Proposition 2.19 ([41, Corollary 5.1]). *Let q be a prime power, and t be a positive integer. Then, the mapping defined in Equation (2.3) is a $(q-1)$-to-1 mapping. Furthermore, for every $c \in \mathbb{F}_q$ and $\beta \in \mathbb{F}_{q^t}$, the equation $\mathrm{Tr}_{q^t/q}(\beta x) = c$ has exactly q^{t-1} solutions $x \in \mathbb{F}_{q^t}$.*

2.1.2 Characters

Characters are an important class of group homomorphisms. For groups related to finite fields, they are powerful tools which have been studied extensively and used in many applications [63, Chapter 6].

Characters of arbitrary groups

Definition 2.20 (Group character and related notions). A *character* of a finite Abelian group G is a homomorphism from G into the multiplicative group $\mathbb{C}^*$ of complex roots of unity. The set of all characters of G is denoted $\widehat{G}$. The *trivial character* χ_0 is defined by $\chi_0(g) = 1_G$, for all $g \in G$; all other characters are referred to as *non-trivial*. For each character χ there is a conjugate character $\overline{\chi}$ defined by $\overline{\chi}(g) = \overline{\chi(g)}$ for all $g \in G$.

Let G be a finite Abelian group, and $\chi_1, \ldots, \chi_n \in \widehat{G}$. The *product of $\chi_1, \ldots, \chi_n$* is the character defined by

$$
(\chi_1 \cdots \chi_n)(g) = \chi_1(g) \cdots \chi_n(g),
$$

and $\widehat{G}$ is a group under this multiplication. If $\chi_1, \ldots, \chi_n$ are the same character χ, then we write $\chi_1 \cdots \chi_n = \chi^n$. When G is cyclic, we can describe the characters of $\widehat{G}$ as follows.

Proposition 2.21 (Characters of a finite cyclic group). *Let G be a finite cyclic group with a generator g. We consider the mapping on G defined by*

$$\chi(g^k) = e^{\frac{2\pi i k}{|G|}}, \quad k \in \mathbb{Z}, \tag{2.4}$$

so that, for an integer j, we have

$$\chi^j(g^k) = e^{\frac{2\pi i j k}{|G|}}, \quad k \in \mathbb{Z}. \tag{2.5}$$

Then, $\widehat{G}$ is a cyclic group of order $|G|$, and

$$\widehat{G} = \left\{ \chi^j \mid j \in [0, |G| - 1] \right\}.$$

Proof. For a fixed $j \in [0, |G| - 1]$, the mapping in Equation (2.5) is a character of G. Conversely, for any character $\psi \in \widehat{G}$ and any $g \in G$, $\psi(g)$ is a $|G|$-th root of unity and thus $\psi(g) = e^{2\pi i j/|G|}$, for some $j \in [0, |G| - 1]$. Since ψ is multiplicative and g generates G, it follows that $\psi = \chi^j$, hence χ generates the cyclic group $\widehat{G}$. ∎

The following theorem is a classic result regarding character sums.

Theorem 2.22 (Orthogonality relations for characters [56, Section 5]). *Let ψ be a character of a group G. Then*

$$\sum_{g \in G} \psi(g) = \begin{cases} |G| & \text{if } \psi \text{ is trivial;} \\ 0 & \text{otherwise.} \end{cases}$$

Furthermore, if $g \in G$ and $\widehat{G}$ is the group of all characters of G, we have

$$\sum_{\psi \in \widehat{G}} \psi(g) = \begin{cases} |G| & \text{if } g = 1_G; \\ 0 & \text{otherwise.} \end{cases}$$

Characters of a finite field

There are two kinds of characters associated to a finite field, corresponding to its additive and multiplicative groups; in this thesis we use exclusively characters of the latter kind.

Definition 2.23 (Multiplicative character of a finite field). For a prime power q, a character of the multiplicative group $\mathbb{F}_q^\times$ is a *multiplicative character of $\mathbb{F}_q$*. A multiplicative character χ of $\mathbb{F}_q$ is extended to a function on $\mathbb{F}_q$ by setting $\chi(0) = 0$. The multiplicative character χ_0 that maps every nonzero element to 1 is the *trivial multiplicative character of $\mathbb{F}_q$*.

As per Theorem 2.10, the multiplicative group of a finite field is cyclic. Therefore, by Proposition 2.21, we have the following characterization of multiplicative finite field characters.

Corollary 2.24 (Characterization of multiplicative characters of a finite field). *Let q be a prime power, and α be a primitive element of $\mathbb{F}_q$. We consider the mapping*

$$\chi(\alpha^k) = e^{\frac{2\pi i k}{q-1}}, \quad k \in \mathbb{Z}, \tag{2.6}$$

so that, for an integer j, we have

$$\chi^j(\alpha^k) = e^{\frac{2\pi i j k}{q-1}}, \quad k \in \mathbb{Z}. \tag{2.7}$$

Then, the group $\widehat{\mathbb{F}_q^\times}$ of multiplicative characters of $\mathbb{F}_q$ is a cyclic group of order $q - 1$, and

$$\widehat{\mathbb{F}_q^\times} = \left\{ \chi^j \mid j \in [0, q-2] \right\}.$$

We now look at products of multiplicative characters.

Lemma 2.25. *Let v be an integer with $v \geq 2$ and $j_0, j_1, \ldots, j_{n-1} \in [1, v-1]$. Then the mapping $X : (\mathbb{F}_q^\times)^n \to \mathbb{C}^*$ defined by*

$$X(x_1, \ldots, x_n) = \prod_{i=0}^{n-1} \chi^{j_i}(x_i)$$

is a nontrivial character of the group $(\mathbb{F}_q^\times)^n$, and

$$\sum_{x_0, \ldots, x_{n-1} \in \mathbb{F}_q^\times} \prod_{i=0}^{n-1} \chi^{j_i}(x_i) = 0. \tag{2.8}$$

Proof. We have that X is a homomorphism whose order is $\mathrm{lcm}(\mathrm{ord}(\chi^{j_0}), \ldots, \mathrm{ord}(\chi^{j_{n-1}}))$, which is greater than 1 since the orders of χ^{j_i}, $i \in [0, n-1]$ are all greater than 1. Thus X is a non-trivial character, and Equation (2.8) follows from Theorem 2.22. $\blacksquare$

Finally, we introduce Jacobi sums and a related important result.

Definition 2.26 (Jacobi sum). For $\chi_1, \ldots, \chi_n$ multiplicative characters on $\mathbb{F}_q$, the *Jacobi sum* $J(\chi_1, \ldots, \chi_n)$ over $\mathbb{F}_q$ is defined by

$$\mathcal{J}(\chi_1, \ldots, \chi_n) = \sum_{\substack{s_1, \ldots, s_n \in \mathbb{F}_q \\ s_1 + \cdots + s_n = 1}} \chi_1(s_1) \ldots \chi_n(s_n).$$

Theorem 2.27 (Absolute value of Jacobi sum [63, Theorem 6.1.38]). *Let $\chi_1, \ldots, \chi_n$ be characters of $\mathbb{F}_q^\times$ such that $\chi_1, \ldots, \chi_n$, and $\prod_{i=1}^{n} \chi_i$ are all nontrivial. Then,*

$$|\mathcal{J}(\chi_1, \ldots, \chi_n)| = q^{\frac{n-1}{2}}.$$

2.1.3 Sequences over finite fields

In this section we give the background required in this thesis about sequences over finite fields. For a comprehensive presentation we refer the reader to [56, Chapter 5], as well as [41] for a textbook on the subject.

LFSR sequences and their minimal polynomials

Definition 2.28 ((Ultimately) periodic sequence). Let $(s_i)_{i \geq 0}$ be a sequence of elements from a finite set. If there exist integers r, u such that $r > 0, u \geq 0$ and $s_{i+r} = s_i$, for all $i \geq u$, then the sequence is *ultimately periodic*, with *period* r. The smallest r with that property is the *least period* of the sequence. If $u = 0$, the sequence is just called *periodic*.

Definition 2.29 (Linear feedback shift register (LFSR) sequence). Let t be a positive integer and let $I = (c_0, c_1, \ldots, c_{t-1})$ be a fixed t-tuple of elements in $\mathbb{F}_q$. A sequence $\mathbf{s} = (s_0, s_1, \ldots)$ of elements in $\mathbb{F}_q$ satisfying the homogeneous linear recurrence relation

$$s_{j+t} = \sum_{i=0}^{t-1} c_i s_{j+i}, \quad j = 0, 1, \ldots$$

is a *linear feedback shift register (LFSR) sequence over* $\mathbb{F}_q$. The t-tuple I is the *initial state vector* of $\mathbf{s}$, the integer t is its *order*, and the polynomial

$$f(x) = x^t - c_{t-1} x^{t-1} - \cdots - c_1 x - c_0 \in \mathbb{F}_q[x]$$

is a *characteristic polynomial* of $\mathbf{s}$. We say that $\mathbf{s}$ *is generated by* f *with initial state* I. If $\mathbf{s}$ is generated by f with some initial state, then we simply say that f *generates* $\mathbf{s}$.

In the following, we denote by $\overline{(s_0, \ldots, s_{r-1})}$ the infinite periodic sequence with period r, whose first r elements are $s_0, \ldots, s_{r-1}$, that is, the sequence $(s_0, \ldots, s_{r-1}, s_0, \ldots, s_{r-1}, \ldots)$.

Example 2.30. The linear recurrence relation in $\mathbb{F}_2$ given by

$$s_{i+3} = s_{i+2} + s_{i+1} + s_i, \quad i = 0, 1, \ldots \tag{2.9}$$

generates the following sequences.

- The zero sequence $\overline{(0)} = (0, 0, \ldots)$, with initial state $(0, 0, 0)$;

- the constant sequence $\overline{(1)} = (1, 1, \ldots)$, with initial state $(1, 1, 1)$;

- the sequence $\overline{(0, 0, 1, 1)}$, with initial state $(0, 0, 1)$, and

- the sequence $\overline{(1, 0)}$, with initial state $(1, 0, 1)$.

All other initial states generate one of the sequences above, possibly after a shift. For example, the initial state $(1, 1, 0)$ yields the sequence $\overline{(1, 1, 0, 0)}$, which is equal to the

sequence constructed by $\overline{(0,0,1,1)}$ with the first two elements removed. We conclude that the polynomial $x^3 - x^2 - x - 1 = x^3 + x^2 + x + 1 \in \mathbb{F}_2[x]$ generates the sequences $\overline{(0)}$, $\overline{(1)}$, $\overline{(1,1,0,0)}$, $\overline{(0,0,1,1)}$, and $\overline{(1,0)}$ among others, so it is a characteristic polynomial for all of them. On the other hand, we observe that the sequence $\overline{(1,0)}$ is also generated by $x^2 + 1$ with initial state $(1,0)$, therefore both $x^3 + x^2 + x + 1$ and $x^2 + 1$ are characteristic polynomials of the sequence $\overline{(1,0)}$ over $\mathbb{F}_2$.

It follows from Example 2.30 that a characteristic polynomial of an LFSR sequence is not unique. However, for any LFSR sequence, a unique polynomial associated to it does exist; this is described in the following result, along with one of its most important properties.

Theorem 2.31 ([41, Theorem 4.5 and Lemma 4.2]). *Let* **s** *be an LFSR sequence over* $\mathbb{F}_q$, *and* $f \in \mathbb{F}_q[x]$ *be a characteristic polynomial of* **s** *that has the lowest degree. Then, the following statements hold:*

1. *The polynomial* f *is unique. In other words, if* $g \in \mathbb{F}_q[x]$ *is a monic polynomial of the lowest degree that generates* **s**, *then we have that* $g = f$.

2. *A polynomial* $h \in \mathbb{F}_q[x]$ *generates* **s** *if and only if it is divisible by* f.

Definition 2.32 (Minimal polynomial of an LFSR sequence). Let **s** be an LFSR sequence over $\mathbb{F}_q$. The (unique) monic characteristic polynomial of **s** that has the lowest degree is the *minimal polynomial of* **s**.

Example 2.33. As stated in Example 2.30, both $x^2 + 1$ and $x^3 + x^2 + x + 1$ are characteristic polynomials of $\overline{(1,0)}$. Since x and $x + 1$ do not generate $\overline{(1,0)}$, then $x^2 + 1$ is the characteristic polynomial of $\overline{(1,0)}$ that has the lowest degree, i.e. it is the minimal polynomial of $\overline{(1,0)}$. Furthermore, we have that $x^3 + x^2 + x + 1 = (x^2 + 1)(x + 1)$, which agrees with the second statement of Theorem 2.31.

Theorem 2.34 (Period of an LFSR sequence [41, Theorem 4.8], [56, Theorems 8.7, 8.29]). *Let* **s** *be an LFSR sequence over* $\mathbb{F}_q$ *of order* t, *and minimal polynomial* f. *Then, we have the following results regarding the periodicity of* **s**:

1. **s** *is ultimately periodic with least period* $r \leq q^t - 1$;

2. **s** *is periodic if and only if* $f(0) \neq 0$;

3. *if* f *is irreducible, then* **s** *is periodic and* $r | q^t - 1$;

4. **s** *is periodic with* $r = q^t - 1$ *if and only if* f *is primitive.*

Example 2.35 (Periods of LFSR sequences). We examine the periodicity of some LFSR sequences and compare with Theorem 2.34.

1. The polynomial $f(x) = x^3 + x^2 + x \in \mathbb{F}_2[x]$ has a zero root and is the minimal polynomial of the sequence $(0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, 1, \dots)$, which is ultimately periodic, but not periodic. On the other hand, the polynomial $x^2 + 1 \in \mathbb{F}_2$ does not have a zero root and generates $\overline{(1, 0)}$ which is periodic.

2. The converse of the third statement of Theorem 2.34 is not true. For example the sequence $\overline{(1, 0)}$ over $\mathbb{F}_3$ is generated by $x^2 + 1 \in \mathbb{F}_3[x]$. This is also its minimal polynomial, since none of $x, x + 1, x + 2$ generate $\overline{(1, 0)}$. Now $x^2 + 1 = (x + 1)(x + 2)$, so that minimal polynomial is reducible, while the period of $\overline{(1, 0)}$ is 2, which divides $3^2 - 1$.

3. The polynomial $g(x) = x^2 + 1 \in \mathbb{F}_3[x]$ is irreducible but not primitive; it generates the sequence $\overline{(1, 0)}$, whose period 2 divides $3^2 - 1$. On the other hand, the polynomial $h(x) = x^2 + x + 2 \in \mathbb{F}_3[x]$ is primitive and, with initial state $(1, 0)$, it generates the sequence $\overline{(1, 0, 1, 2, 2, 0, 2, 1)}$, which has period exactly $3^2 - 1$.

Maximal period sequences

We now turn our focus on a type of sequence fundamental to our work.

Definition 2.36 (Maximal period sequence). An LFSR sequence over $\mathbb{F}_q$ whose minimal polynomial is primitive is a *maximal (period) sequence*. A maximal sequence is often referred to as an *m-sequence* in the literature.

It follows from the last statement of Theorem 2.34 that a maximal period sequence over $\mathbb{F}_q$ of order t is periodic with period $q^t - 1$ which, as the name suggests, is the maximum that the period of an LFSR sequence of order t can attain. An example of a maximal sequence of order 2 over $\mathbb{F}_3$ is given in part 3 of Example 2.35. We present another example of a maximal sequence that we also use later in the thesis.

Example 2.37 (A maximal sequence over $\mathbb{F}_4$). We recall that in Example 2.14 the finite field $\mathbb{F}_4$ is constructed using a root α of $x^2 + x + 1 \in \mathbb{F}_2[x]$, as shown in Equation (2.2). Then, the polynomial $g(x) = x^2 + x + \alpha$ is shown to be primitive and, as such, it is the minimal polynomial of a maximal sequence $\mathbf{s} = (s_i)_{i \geq 0}$, that has period $4^2 - 1$, and is generated by the linear recursion

$$s_{i+2} = -s_{i+1} - \alpha s_i = s_{i+1} + \alpha s_i, \quad i \geq 0.$$

With initial state $(1, 0)$, this yields the maximal sequence over $\mathbb{F}_4$ of period $4^2 - 1$ given by

$$\overline{(1, 0, \alpha, \alpha, 1, \alpha, 0, \alpha + 1, \alpha + 1, \alpha, \alpha + 1, 0, 1, 1, \alpha + 1)}.$$

The following theorem provides a very useful way of representing maximal sequences.

Theorem 2.38 ([41, Corollary 4.6],[56, Theorem 8.24]). *An LFSR sequence* $\mathbf{s} = (s_i)_{i \geq 0}$ *over* $\mathbb{F}_q$ *is a maximal sequence with period* $q^t - 1$ *if and only if the elements of* $\mathbf{s}$ *can be represented by*

$$s_i = \mathrm{Tr}_{q^t/q}(\theta \alpha^i), \quad i \geq 0, \tag{2.10}$$

where $\alpha, \theta \in \mathbb{F}_{q^t}$, *with* α *being primitive and* θ *nonzero. For each maximal sequence* $\mathbf{s}$, *the* θ *in Equation (2.10) is unique, and* α *is a root of the minimal polynomial of* $\mathbf{s}$ *in* $\mathbb{F}_q[x]$.

Definition 2.39 (The trace representation of a maximal sequence). For a maximal sequence $\mathbf{s} = (s_i)_{i \geq 0}$ of order t over $\mathbb{F}_q$, the representation of $\mathbf{s}$ given by Equation (2.10) is the *trace representation of* $\mathbf{s}$.

The trace representation also applies to LFSR sequences that are not maximal, however we do not discuss this since we only use maximal sequences in this thesis. For an in-depth presentation of the trace representation in general, we refer the reader to [41, Section 6.2].

Example 2.40 (The trace representation of a maximal sequence over $\mathbb{F}_3$). The recursion corresponding to the primitive polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$ is

$$s_{i+2} = 2s_{i+1} + s_i, \quad i \geq 0.$$

With initial state $(0, 1)$, this yields the maximal sequence

$$\mathbf{s} = (s_i)_{i \geq 0} = \overline{(0, 1, 2, 2, 0, 2, 1, 1)}.$$

Let α be a root of $x^2 + x + 2$, so that $\alpha^2 = 2\alpha + 1$. Denoting $\mathrm{Tr}_{3^2/3} = \mathrm{Tr}$, we compute

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^3 = \alpha + \alpha\alpha^2 = \alpha + \alpha(2\alpha + 1) = 2\alpha + 2\alpha^2 = 2\alpha + 2(2\alpha + 1) = 6\alpha + 2 = 2.$$

Similarly, we have that

$$\mathrm{Tr}(\alpha^2) = 0, \mathrm{Tr}(\alpha^3) = 2, \mathrm{Tr}(\alpha^4) = 1, \mathrm{Tr}(\alpha^5) = 1, \mathrm{Tr}(\alpha^6) = 0, \mathrm{Tr}(\alpha^7) = 1,$$

and also $\mathrm{Tr}(\alpha^0) = \mathrm{Tr}(1) = 2$. By Lemma 2.11, we have that $\alpha^9 = \alpha$ and hence $\mathrm{Tr}(a^{i+9}) = \mathrm{Tr}(\alpha^i)$, for all $i \geq 0$. Therefore, the sequence over $\mathbb{F}_3$ given by $(\mathrm{Tr}(\alpha^i))_{i \geq 0}$ is periodic with period 9, and it is equal to $\overline{(2, 2, 0, 2, 1, 1, 0, 1)}$. We observe that this is a cyclic shift of $\mathbf{s}$ with $s_i = \mathrm{Tr}(\alpha^{i+6})$, $i \geq 0$. Thus, setting $\theta = \alpha^6$, we have that

$$\mathrm{Tr}(\theta \alpha^i) = \mathrm{Tr}(\alpha^6 \alpha^i) = \mathrm{Tr}(\alpha^{i+6}) = s_i,$$

which gives the trace representation for $\mathbf{s}$.

In the following example we give the trace representation of the maximal sequence over $\mathbb{F}_4$ discussed in Example 2.37. This is obtained by working similarly to Example 2.40; we omit

the details and we just state the result for future reference.

Example 2.41 (The trace representation of a maximal sequence over $\mathbb{F}_4$). We assume the notation of Example 2.37 and the results established thereof. Setting $\theta = \beta^{13} = 1 + \alpha\beta$, we have that the maximal sequence $\mathbf{s} = (s_i)$, $i \geq 0$ over $\mathbb{F}_4$ defined by

$$\mathbf{s} = \overline{(1, 0, \alpha, \alpha, 1, \alpha, 0, \alpha + 1, \alpha + 1, \alpha, \alpha + 1, 0, 1, 1, \alpha + 1)},$$

has trace representation given by $s_i = \mathrm{Tr}_{4^2/4}(\theta\alpha^i)$, $i \geq 0$.

Maximal sequences have a rich algebraic structure and a variety of statistical properties that make them ideal for use in applications such as radar, sonar, and wireless communications [39, 41]; and cryptography [61, Chapter 6]. One of their most fundamental properties is the following.

Proposition 2.42 (Balance property of maximal sequences [41, Property 5.3]). *Let* $\mathbf{s} = (s_i)_{i \geq 0}$ *be a maximal sequence over* $\mathbb{F}_q$ *of order* t *and, for every* $a \in \mathbb{F}_q$, *let*

$$N_{\mathbf{s}}(a) = \left| \{ i | i \in [0, q^t - 1], s_i = a \} \right|.$$

Then, we have that

$$N_{\mathbf{s}}(a) = \begin{cases} q^{t-1}, & \text{if } a \neq 0; \\ q^{t-1} - 1, & \text{otherwise}. \end{cases}$$

The balanced distribution of the elements of a maximal sequence goes beyond Proposition 2.42; for example, the following well-known generalization shows a similar property for pairs of elements. We denote

$$[t]_q = \frac{q^t - 1}{q - 1},$$

a notation that we use extensively from now on.

Proposition 2.43 (Two-tuple balance property of maximal sequences [41, Corollary 4.6]). *Let* $\mathbf{s} = (s_i)_{i \geq 0}$ *be a maximal sequence over* $\mathbb{F}_q$ *of order* t. *Then, for any integer* τ *and pair* (a, b) *of elements* $a, b \in \mathbb{F}_q$, *we denote*

$$N_{\mathbf{s},\tau}(a, b) = \left| \{ i \mid i \in [0, q^t - 1], (s_i, s_{i+\tau}) = (a, b) \} \right|$$

Then, we have that

$$N_{\mathbf{s},\tau}(a, b) = \begin{cases} q^{t-2} & \text{if } \tau \not\equiv 0 \;(\text{mod } [t]_q) \text{ and } (a, b) \neq (0, 0); \\ q^{t-2} - 1 & \text{if } \tau \not\equiv 0 \;(\text{mod } [t]_q) \text{ and } (a, b) = (0, 0); \\ q^{t-1} & \text{if } \tau \equiv 0 \;(\text{mod } [t]_q) \text{ and } b = ca \text{ for some } c \in \mathbb{F}_q^{\times}; \\ 0 & \text{otherwise.} \end{cases}$$

It follows from Proposition 2.43 that elements in a maximal sequence whose indexes are multiples of $[t]_q$ are constant multiples of each other. This property is described in more detail in Proposition 2.45. First, we need a lemma.

Lemma 2.44 (Characterization of constant multiples in $\mathbb{F}_{q^t}$). *Let q be a prime power, t be a positive integer, and α be a primitive element of $\mathbb{F}_{q^t}$. Then, $\alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q$, and for any $i, j \in [0, q^t - 2]$, we have that $\alpha^j = c\alpha^i$ for some $c \in \mathbb{F}_q^{\times}$ if and only if $j \equiv i \pmod{[t]_q}$.*

Proof. First, we show that $\alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q$. Indeed, we have that

$$\mathrm{ord}(\alpha^{[t]_q}) = \frac{\mathrm{ord}(\alpha)}{\gcd\left(\mathrm{ord}(\alpha), [t]_q\right)} = \frac{q^t - 1}{\gcd\left(q^t - 1, \frac{q^t-1}{q-1}\right)} = \frac{q^t - 1}{\frac{q^t-1}{q-1}} = q - 1, \tag{2.11}$$

which proves our claim; it follows that $c \in \mathbb{F}_q^{\times}$ if and only if $c = \alpha^{l[t]_q}$ for some integer l.

If $j \equiv i \pmod{[t]_q}$, then $j = i + l[t]_q$ for some l, thus $\alpha^j = \alpha^i \alpha^{l[t]_q} = c\alpha^i$, for $c = \alpha^{l[t]_q} \in \mathbb{F}_q^{\times}$. Conversely, we suppose that $\alpha^j = c\alpha^i$, for some $c \in \mathbb{F}_q^{\times}$. Since $\alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q^{\times}$, $c = (\alpha^{[t]_q})^l = \alpha^{l[t]_q}$, for some l. Therefore, $\alpha^j = c\alpha^i = \alpha^{l[t]_q}\alpha^i = \alpha^{i+l[t]_q}$, which implies that $\alpha^{i-j+l[t]_q} = 1$. Since α is a primitive element of $\mathbb{F}_{q^t}^{\times}$, its order is $q^t - 1$, so the last equation implies that $q^t - 1$ divides $i - j + l[t]_q$. Furthermore, since $[t]_q$ divides $q^t - 1$, we also have that $[t]_q$ divides $i - j + l[t]_q$, and therefore $i \equiv j \pmod{[t]_q}$. $\square$

Proposition 2.45 (Projective property of maximal sequences [41, Section 5.3.2]). *Let $\mathbf{s} = (s_i)_{i\geq 0}$ be a maximal sequence of order t over $\mathbb{F}_q$, and let $\alpha \in \mathbb{F}_{q^t}$ be a root of its minimal polynomial. Denoting $w = [t]_q$ and*

$$P_i = (s_{o+iw}, s_{1+iw}, \ldots, s_{w-1+iw}), \quad i \in [0, q - 2],$$

we have that $P_i = \alpha^{iw} P_0$, for all $i \in [0, q - 2]$.

In other words, Proposition 2.45 states that if we arrange the sequence in a $(q-1) \times w$ array, and denoting $c_i = \alpha^{wi}$ so that $\mathbb{F}_q^{\times} = \{c_i \mid i \in [0, q-2]\}$, we have that

$$
\begin{bmatrix}
s_0 & s_1 & \cdots & s_{w-1} \\
s_w & s_{w+1} & \cdots & s_{2w-1} \\
s_{2w} & s_{2w+1} & \cdots & s_{3w-1} \\
\vdots & \vdots & \ddots & \vdots \\
s_{(q-2)w} & s_{(q-2)w+1} & \cdots & s_{(q-2)w-1}
\end{bmatrix}
=
\begin{bmatrix}
s_0 & s_1 & \cdots & s_{w-1} \\
\alpha^w s_0 & \alpha^w s_1 & \cdots & \alpha^w s_{w-1} \\
\alpha^{2w} s_0 & \alpha^{2w} s_1 & \cdots & \alpha^{2w} s_{w-1} \\
\vdots & \vdots & \ddots & \vdots \\
\alpha^{(q-2)w} s_0 & \alpha^{(q-2)w} s_1 & \cdots & \alpha^{(q-2)w} s_{w-1}
\end{bmatrix}
$$

$$
=
\begin{bmatrix}
P_0 \\
\alpha^w P_0 \\
\alpha^{2w} P_0 \\
\vdots \\
\alpha^{w(q-2)} P_0
\end{bmatrix}
=
\begin{bmatrix}
P_0 \\
c_1 P_0 \\
c_2 P_0 \\
\vdots \\
c_{q-2} P_0
\end{bmatrix}.
$$

Example 2.46. We assume the notation used in Propositions 2.42, 2.43 and 2.45, and consider the sequence

$$\mathbf{s} = (s_i)_{i \geq 0} = \overline{(0, 1, 2, 2, 0, 2, 1, 1)}$$

which is the maximal sequence discussed in Example 2.40. We observe that $N_{\mathbf{s}}(1) = N_{\mathbf{s}}(2) = 3^{2-1}$, and $N_{\mathbf{s}}(0) = 3^{2-1} - 1$, as per Proposition 2.42. To demonstrate Proposition 2.43, we construct the table below.

i	0	1	2	3	4	5	6	7
s_i	0	1	2	2	0	2	1	1
s_{i+1}	1	2	2	0	2	1	1	0
s_{i+4}	0	2	1	1	0	1	2	2.

Using the first two rows of the table to count the pairs of the form (s_i, s_{i+1}), we see that $N_{\mathbf{s},1}(a, b) = 3^{2-2} = 1$ for all nonzero (a, b), and $N_{\mathbf{s},1}(0, 0) = 3^{2-2} - 1 = 0$, as expected from Proposition 2.43 with $\tau = 1$, which is not divisible by $[2]_3 = 4$. On the other hand, using the first and third rows of the table we count that $N_{\mathbf{s},4}(1, 2) = 3 = 3^{2-1}$ and $N_{\mathbf{s},4}(0, 2) = 0$, as expected from Proposition 2.43 with $\tau = 4$, which is divisible by $[2]_3 = 4$. Finally, we arrange $\mathbf{s}$ in a $(q - 1) \times [t]_q = 2 \times 4$ array below.

$$\begin{bmatrix} 0 & 1 & 2 & 2 \\ 0 & 2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \end{bmatrix} = \begin{bmatrix} P_0 \\ P_1 \end{bmatrix}.$$

This shows that $P_0 = (0, 1, 2, 2)$, and $P_1 = (0, 2, 1, 1) = 2P_0$. We note that a root α of the minimal polynomial $x^2 + x + 2 \in \mathbb{F}_3[x]$ satisfies $\alpha^{[2]_3} = \alpha^4 = 2$, hence $P_1 = \alpha^{[2]_3} P_0$, as per Proposition 2.45.

Example 2.47. We assume the notation used in Propositions 2.42, 2.43 and 2.45, and define the sequence

$$\mathbf{s} = \overline{(1, 0, \alpha, \alpha, 1, \alpha, 0, \alpha + 1, \alpha + 1, \alpha, \alpha + 1, 0, 1, 1, \alpha + 1)}$$

which is the maximal sequence discussed in Example 2.41. We observe that $N_{\mathbf{s}}(1) = N_{\mathbf{s}}(\alpha) = N_{\mathbf{s}}(\alpha + 1) = 4 = 4^{2-1}$, and $N_{\mathbf{s}}(0) = 3 = 4^{2-1} - 1$, as per Proposition 2.42. To demonstrate Proposition 2.43, we construct the table below.

i	0	1	2	3	4	5	6	7
s_i	1	0	α	α	1	α	0	
s_{i+1}	0	α	α	1	α	0	$\alpha + 1$	$\alpha + 1$
s_{i+10}	$\alpha + 1$	0	1	1	$\alpha + 1$	1	0	α
i	8	9	10	11	12	13	14	
s_i	$\alpha + 1$	α	$\alpha + 1$	0	1	1	$\alpha + 1$	
s_{i+1}	α	$\alpha + 1$	0	1	1	$\alpha + 1$	1	
s_{i+10}	α	1	α	0	$\alpha + 1$	$\alpha + 1$	α	

Using the first two rows of the table to count the pairs of the form (s_i, s_{i+1}), we see that $N_{\mathbf{s},1}(a, b) = 4^{2-2} = 1$ for all nonzero (a, b), and $N_{\mathbf{s},1}(0, 0) = 4^{2-2} - 1 = 0$; this is as expected from Proposition 2.43 with $\tau = 1$, which is not divisible by $[2]_4 = 5$. On the other hand, from the first and third rows of the table we count that $N_{\mathbf{s},10}(1, \alpha + 1) = 4 = 4^{2-1}$ and $N_{\mathbf{s},4}(1, \alpha) = 0$, as expected from Proposition 2.43 with $\tau = 10$, which is divisible by $[2]_4 = 5$. Now, we see in Table 2.1 that $\beta^{[2]_4} = \beta^5 = \alpha$ and $\beta^{[2]_4} = \beta^{10} = \alpha + 1$. We arrange $\mathbf{s}$ in a $(q-1) \times [t]_q = 3 \times 5$ array below.

$$\begin{bmatrix} s_0 & s_1 & s_2 & s_3 & s_4 \\ s_5 & s_6 & s_7 & s_8 & s_9 \\ s_{10} & s_{11} & s_{12} & s_{13} & s_{14} \end{bmatrix} = \left[\begin{array}{c|c|c|c|c} 1 & 0 & \alpha & \alpha & 1 \\ \alpha & 0 & \alpha+1 & \alpha+1 & \alpha \\ \alpha+1 & 0 & 1 & 1 & \alpha+1 \end{array}\right] = \begin{bmatrix} P_0 \\ P_1 \\ P_2 \end{bmatrix}.$$

Indeed, $P_1 = \alpha P_0 = \beta^{[4]_2} P_0$ and $P_2 = (\alpha + 1)P_0 = \beta^{2[2]_2} P_0$, as per Proposition 2.45.

2.1.4 Finite geometry and combinatorial designs

We continue with some aspects of finite geometry that we need in the next chapters.

Definition 2.48 (Finite projective space). An *incidence structure* or *finite geometry* is a pair of finite sets of *points* and *lines*, along with a reflexive and symmetric relation on the set of points, called an *incidence relation*. A *finite projective space* P is a finite incidence structure that satisfies all of the following statements.

1. Any two distinct points of P belong to exactly one line.

2. Let A, B, C, D be four distinct points of which no three are collinear. 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 2.49 (The $(t-1)$-dimensional projective space $PG(t-1, q)$). Let t be a positive integer, q be a prime power, and V be a vector space of dimension t over $\mathbb{F}_q$. The finite geometry $PG(t-1, q)$ that has as its points and lines the 1-dimensional and 2-dimensional vector subspaces of V, respectively, is *the $(t-1)$-dimensional projective space over $\mathbb{F}_q$*.

For $v \in V \setminus \{0\}$, let

$$[v] = \{cv \mid c \in \mathbb{F}_q^{\times}\}, \tag{2.12}$$

where cv is the scalar multiplication of v by c. We use the symbols $[v]$ to represent the points of $PG(t-1, q)$ and we write $PG(t-1, q) = \{[v] \mid v \in V \setminus \{0\}\}$. For any $u \in [v]$, u is a *representative vector for the point* $[v]$. For a subspace S of V with dimension $k+1$, the set of points

$\{[v] \mid v \in S \setminus \{0\}\}$ is a *k-flat* of $PG(t-1,q)$. A k-flat with $k = 0, 1, 2, t-2$ is a *point, line, plane, hyperplane* of $PG(t-1,q)$, respectively. The flats have properties which give a fundamental connection between finite projective spaces and the designs in the next definition.

> **Definition 2.50 (Balanced incomplete block design (BIBD)).** For integers v, s with $2 < s < v$, a (v, s, λ)-*BIBD (balanced incomplete block design)* is a pair $(V, \mathcal{B})$ where V is a set with $|V| = v$ and $\mathcal{B}$ is a multiset consisting of s-sets of V, such that for every 2-set $T \subset V$, there are exactly λ sets $B \in \mathcal{B}$ such that $T \subset B$. The sets V and $\mathcal{B}$ are the *points* and *blocks* of the BIBD, whereas λ is its *index*.

For positive integers a, b and prime power q, the number

$$\begin{bmatrix} a \\ b \end{bmatrix}_q = \begin{cases} \frac{(q^a-1)(q^{a-1}-1)\cdots(q^{a-b+1})}{(q^b-1)(q^{b-1}-1)\cdots(q-1)}, & \text{if} \quad a \geq b; \\ 0 & \text{otherwise.} \end{cases}$$

is a *Gaussian binomial coefficient*. We note that this is the number of subspaces of dimension b in a vector space of dimension a over $\mathbb{F}_q$.

> **Proposition 2.51 (Flats as blocks of a BIBD [27, Proposition 2.35]).** *Let d be a positive integer and q be a prime power. For $k \in [0, d-2]$, the points of $PG(d-1,q)$ with the k-flats as blocks form a (v, s, λ)-BIBD with parameters*
>
> $$v = [d+1]_q, \ s = [k+1]_q, \ \lambda = \begin{bmatrix} d \\ i \end{bmatrix}_q.$$

Then next lemma gives a translation of the notion of linear independence in a finite vector space over $\mathbb{F}_q$ into the language of flats in the corresponding projective space.

> **Lemma 2.52.** *Let V be a t-dimensional vector space over $\mathbb{F}_q$ and $v_0, \ldots, v_{n-1} \in V$, where $v \leq t$. Then, $v_0, \ldots, v_{n-1}$ are linearly independent if and only if there is no $(n-2)$-flat in $PG(t-1,q)$ that contains $[v_0], \ldots, [v_{n-1}]$.*

Proof. From the definition of flats, $[v_0], \ldots, [v_{n-1}]$ belong in the same $(n-2)$-flat if and only if $v-0, \ldots, v_{n-1}$ belong in the same $(n-1)$-dimensional subspace of V, which is true if and only if they are linearly dependent. ∎

In this thesis we use exclusively $\mathbb{F}_{q^t}$ as our t-dimensional vector space V when constructing $PG(t-1,q)$. To demonstrate this construction, we need the next lemma.

> **Proposition 2.53 (Construction of $PG(t-1,q)$ using $\mathbb{F}_{q^t}$).** *Let q be a prime power, t be a positive integer, and α be a primitive element of $\mathbb{F}_{q^t}$. Then, the set*
>
> $$\{[\alpha^i] \mid i \in [0, [t]_q - 1]\}$$
>
> *contains exactly all the $[t]_q$ points of $PG(t-1,q)$.*

Proof. First, there are $q^t - 1$ nonzero vectors in $\mathbb{F}_{q^t}$, considered as a vector space, and each has $q - 1$ nonzero scalar multiples. Therefore, there are precisely $(q^t - 1)/(q - 1) = [t]_q$ distinct 1-dimensional vector subspaces of $\mathbb{F}_{q^t}$, which means that $PG(t - 1, q)$ has exactly $[t]_q$ points. It suffices to show that the elements $[\alpha^i]$, $i \in [0, [t]_q - 1]$ are distinct. We assume by means of contradiction that this is not the case, so that there exist $i, j \in [0, [t]_q - 1]$, $i \neq j$, such that $[\alpha^i] = [\alpha^j]$. By Equation (2.12), this means that $\alpha^j = c\alpha^i$ for some $c \in \mathbb{F}_q^\times$ which, by Lemma 2.44 is equivalent to $j \equiv i \pmod{[t]_q}$. Hence, we have that $[t]_q \mid j - i$, which implies that $[t]_q \leq j - i$ or $j - i = 0$; this contradicts the definition of i and j. ∎

Example 2.54 (The projective space $PG(2, 3)$).

Let α be a root of the primitive polynomial $x^3 + 2x + 1$ over $\mathbb{F}_3$, so that α is a primitive element in $\mathbb{F}_{3^3}$. From Proposition 2.53 there are exactly $[3]_3 = (3^3 - 1)/(3 - 1) = 13$ points in $PG(2, 3)$, given by $[\alpha^i]$, $i \in [0, 12]$. In the following table, we list these powers of α in the form $c_2\alpha^2 + c_1\alpha + c_0$, as per Equation (2.1), as well as the coordinate vector (c_2, c_1, c_0) to emphasize how we view $\mathbb{F}_{3^3}$ as a 3-dimensional vector space over $\mathbb{F}_q$.

i	0	1	2	3	4	5	6
α^i	1	α	α^2	$\alpha + 2$	$\alpha^2 + 2\alpha$	$2\alpha^2 + \alpha + 2$	$\alpha^2 + \alpha + 1$
Coord.	$(0, 0, 1)$	$(0, 1, 0)$	$(1, 0, 0)$	$(0, 1, 2)$	$(1, 2, 0)$	$(2, 1, 2)$	$(1, 1, 1)$
i	7	8	9	10	11	12	
α^i	$\alpha^2 + 2\alpha + 2$	$2\alpha^2 + 2$	$\alpha + 1$	$\alpha^2 + \alpha$	$\alpha^2 + \alpha + 2$	$\alpha^2 + 2$	
Coord.	$(1, 2, 2)$	$(2, 0, 2)$	$(0, 1, 1)$	$(1, 1, 0)$	$(1, 1, 2)$	$(1, 0, 2)$	

Using the table, in Figure 2.1 we provide a visual representation of the points and lines of $PG(2, 3)$ that also demonstrates the incidence relations between the points. For example, the 1-dimensional subspace of $\mathbb{F}_3^3$ spanned by $(0, 0, 1)$ corresponds to the point labeled c in the figure. Similarly, the points labeled b to m, correspond to the remaining 1-dimensional subspaces of $\mathbb{F}_3^3$, as shown on the left of the figure. Next, we consider the 2-dimensional subspace of $\mathbb{F}_3^3$, given by

$$S = \{(x, 0, y) \mid x, y \in \mathbb{F}_3\}.$$

This corresponds to the line (1-flat) of $PG(2, 3)$ whose points correspond to the 1-dimensional subspaces contained in S. There are four such subspaces, and they are spanned by the vectors $(0, 0, 1), (1, 0, 0), (1, 0, 2)$ and $(2, 0, 2)$, respectively. These are representative vectors for the points labeled a, b, c and k, respectively, which are indeed shown to be collinear in the diagram.

Example 2.55.

The points a, b and e in Figure 2.1 are collinear, which means that they belong in the same $(3 - 2)$-flat. The vectors $(1, 0, 2), (2, 0, 2)$ and $(1, 1, 1)$, which are respective representative vectors for these points, are indeed linearly independent as per Lemma 2.52.
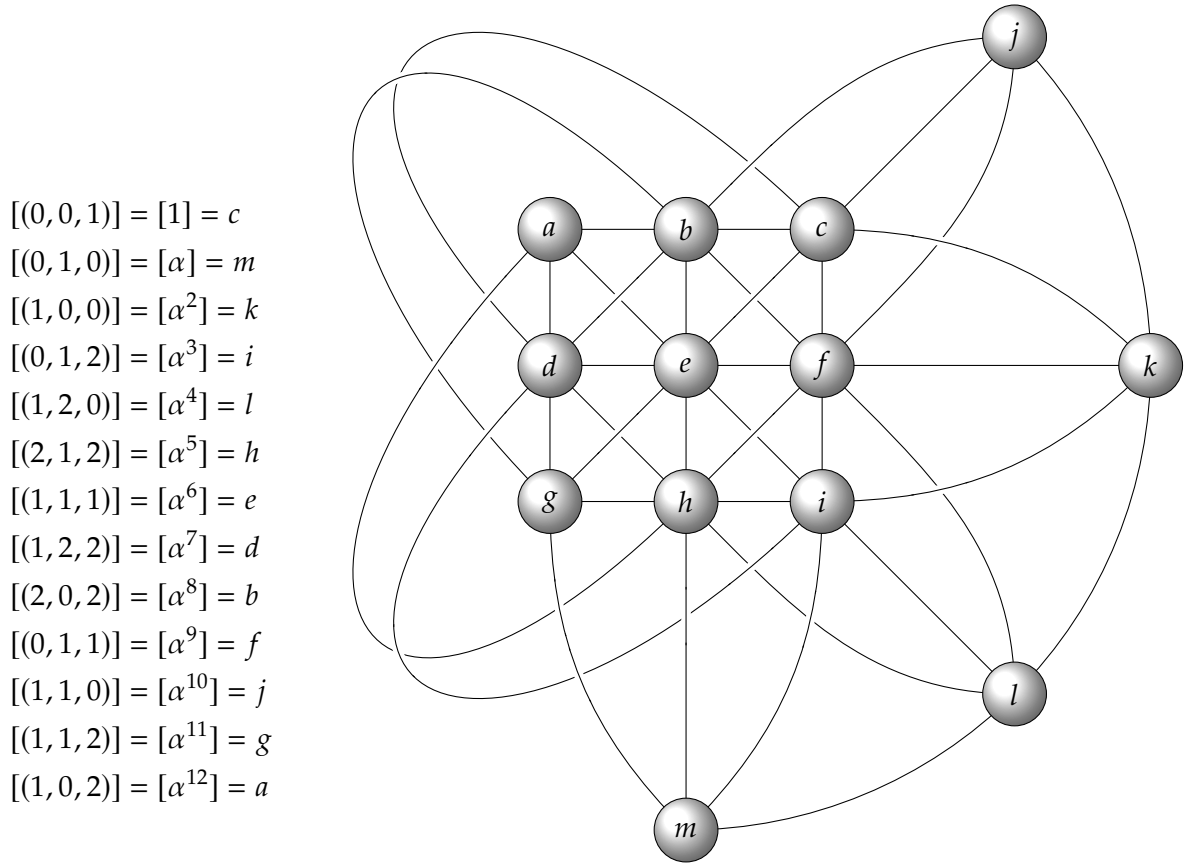
$$[(0,0,1)] = [1] = c$$
$$[(0,1,0)] = [\alpha] = m$$
$$[(1,0,0)] = [\alpha^2] = k$$
$$[(0,1,2)] = [\alpha^3] = i$$
$$[(1,2,0)] = [\alpha^4] = l$$
$$[(2,1,2)] = [\alpha^5] = h$$
$$[(1,1,1)] = [\alpha^6] = e$$
$$[(1,2,2)] = [\alpha^7] = d$$
$$[(2,0,2)] = [\alpha^8] = b$$
$$[(0,1,1)] = [\alpha^9] = f$$
$$[(1,1,0)] = [\alpha^{10}] = j$$
$$[(1,1,2)] = [\alpha^{11}] = g$$
$$[(1,0,2)] = [\alpha^{12}] = a$$

Figure 2.1. A visual representation of the points and lines of $PG(2,3)$, constructed using either $\mathbb{F}_3^3$ or $\mathbb{F}_{3^3}$ as discussed in Example 2.54.

We close this section with a definition of a structure that is useful in the next chapter.

Definition 2.56 (Arcs, tracks and caps). Let S be a set of k points in $PG(t-1,q)$.

- S is a *k-arc* if there is no $(t-2)$-flat (hyperplane) in $PG(t-1,q)$ that contains t points from S.

- S is a *k-track* if it is not a k-arc and there is no $(t-3)$-flat in $PG(t-1,q)$ that contains $t-1$ points from S.

- S is a *k-cap* if no 3 points in S are collinear.

Remark 2.57 (*Arcs, tracks, caps and linear independence*). Let $S = \{[v_0], \dots, [v_{k-1}]\}$ be a set of points from $PG(t-1, q)$. The following are a straightforward implication of Lemma 2.52 and Definition 2.56.

- S is a k-arc if and only if every t vectors among $v_0, \dots, v_{k-1}$ are linearly independent over $\mathbb{F}_q$.

- S is a k-track if and only if every $t-1$ vectors among $v_0, \dots, v_{k-1}$ are linearly independent over $\mathbb{F}_q$ but there are some t vectors that are linearly dependent.

- S is a k-cap if and only if every 3 vectors among $v_0, \dots, v_{k-1}$ are linearly independent over $\mathbb{F}_q$.

2.1.5 Linear codes

In this section we give some background on linear codes that is essential for our thesis.

Definition 2.58 (Hamming distance and Hamming weight). Let $\mathbf{x} = (x_0, \dots, x_{n-1})$, $\mathbf{y} = (y_0, \dots, y_{n-1}) \in \mathbb{F}_q^n$. The *Hamming distance between* $\mathbf{x}$ *and* $\mathbf{y}$ is the cardinality of the set $\{i \mid x_i \neq y_i\}$. The *(Hamming) weight* of $\mathbf{x}$, denoted by $w(\mathbf{x})$, is the number of its nonzero coordinates.

Definition 2.59 (Linear codes over a finite field and related notions). Let q be a prime power. A *q-ary linear code C* of *length n*, *dimension k*, and *minimum distance d*, referred to as an $[n, k, d]_q$ code, is a subspace of $\mathbb{F}_q^n$ with dimension k, such that the minimum Hamming distance between distinct elements is d. The elements of C are referred to as the *words* or *codewords* of C. A $k \times n$ matrix whose rows are a basis for C is a *generating matrix* for C. The *dual code* of C, denoted $C^\perp$, is the orthogonal complement of C in $\mathbb{F}_q^n$, i.e. it is the code of length n and dimension $n - k$ given by

$$C^\perp = \left\{ x \in \mathbb{F}_q^n \mid x \cdot y = 0 \text{ for all } y \in C \right\}.$$

A $(n - k) \times n$ matrix that is a generator matrix for $C^\perp$ is a *parity check matrix* for C.

From the definition of the Hamming distance and weight it follows that for $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$, we have $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. An immediate consequence is the following lemma.

Lemma 2.60. *The minimum distance d of a q-ary linear code satisfies*

$$d = \min \left\{ w(\mathbf{x}) \mid x \in C, x \neq 0 \right\}.$$

An implication of Lemma 2.60 is the following classic result, that shows a connection between the minimum distance of a linear code with the linear independence of the columns of a parity check matrix.

> **Proposition 2.61 (Minimum weight and linear independence).** *The minimum distance d of a linear code C over $\mathbb{F}_q$ with parity check matrix H satisfies*
>
> $$d = \min \left\{ s \mid \text{there exist } s \text{ columns of } H \text{ that are linearly dependent} \right\}.$$

Proof. Let n be the length of C and denote the column vectors of H by $H_0, \ldots, H_{n-1}$. From Lemma 2.60, it suffices to show that, for every positive integer s, there exists a nonzero word $x \in C$ of weight at most s if and only if there exist s columns of H that are linearly dependent.

Assume that $x = (x_0, \ldots, x_{n-1}) \in C$ has weight at most s, so that there exists an s-set $I \subseteq [0, n-1]$ such that $x_i = 0$ if $i \notin I$. Every row s of H is a codeword of $C^{\perp}$, thus it satisfies $r \cdot \mathbf{x} = 0$. Since this is true for every row, the column vectors $H_0, \ldots, H_{n-1}$ of H satisfy $\sum_{i=0}^{n-1} x_i C_i = 0$, which implies that $\sum_{i \in I} x_i C_i = 0$; this means that the columns $H_i, i \in I$ are linearly dependent.

Conversely, assume there are s linearly dependent columns in A, say $H_{i_0}, \ldots, H_{i_{s-1}}$, for some $\{i_0, \ldots, i_{s-1}\} \subseteq [0, n-1]$. Then, $\sum_{j=0}^{s-1} x_{i_j} H_{i_j} = 0$ for some $x_{i_j} \in \mathbb{F}_q$, not all zero. Hence, the vector $(x_0, \ldots, x_{n-1})$ so that $x_i = 0$ if $i \notin \{i_0, \ldots, i_{s-1}\}$, is in C and has weight at most s. $\quad\blacksquare$

2.2 Orthogonal and covering arrays

2.2.1 Introduction

We begin with some necessary notions.

> **Definition 2.62 (Covered vectors).** Let V be a finite set, t, n be positive integers, S be a set of t vectors from V^n, and let A_S be a $n \times t$ array whose columns are the vectors in S. We have the following definitions for S.
>
> - If every t-tuple in V^t appears *at least* λ times as a row of A_S, then S is λ-*covered*.
>
> - If every t-tuple in V^t appears *exactly* λ times as a row of A_S, then S is *uniformly* λ-*covered*.
>
> - If S is 1-covered, we simply refer to it as *covered*.
>
> - If S is uniformly 1-covered, we simply refer to it as *uniformly covered*.
>
> The vectors $v_1, \ldots, v_s$ are (uniformly) λ-covered, if the set $\{v_1, \ldots, v_s\}$ is (uniformly) λ-covered.

In his 1943 Master's thesis, Rao introduced hypercubes of strength d. In a series of subsequent papers [76, 77, 78], he extended these to a wider class of combinatorial objects, which became known as orthogonal arrays. These are closely connected with other combinatorial objects, such as mutually orthogonal latin squares, transversal designs, projective geometries, and linear codes; we refer to [27] for more on the subject and to [46] for a textbook treatment.

Definition 2.63 (Orthogonal array). Let A be an $N \times k$ array with entries from an alphabet of cardinality v, $t \leq k$ be a positive integer such that $v^t | N$, and $\lambda = N/v^t$. If every t-set of column vectors of A is uniformly λ-covered, then A is an *orthogonal array of strength t and index* λ, denoted $OA_\lambda(t, k, v)$. When $\lambda = 1$ the orthogonal array has *index unity*, and we simply write $OA(t, k, v)$.

Definition 2.64 (Linear orthogonal array). Let q be a prime power. An $OA_\lambda(t, k, q)$ with elements from the finite field $\mathbb{F}_q$ is *linear* if its row vectors are distinct and form a subspace of $\mathbb{F}_q^k$.

Example 2.65. An example of an $OA_3(2, 11, 2)$ is given in Figure 2.2. By definition, every two columns of such an array are uniformly 3-covered. As an example, we verify this with the two highlighted columns in the same figure: since every pair from $\{0, 1\}^2$ appears exactly 3 times as a row of the subarray corresponding to these columns, then they are uniformly 3-covered. The same is true for any other pair of columns, which means that this is an orthogonal array of strength $t = 2$ and index $\lambda = 3$.

Since their introduction, orthogonal arrays have been studied extensively in the context of different mathematical areas, and have been used in a variety of applications, notably the design of statistical experiments. In particular, the rows of an $OA(t, k, v)$ provide a collection of configurations for a system of k factors represented by the columns, where each factor admits v possible values. Performing experimental runs for all v^t configurations corresponding to the rows, guarantees that every combination of t factors and their values is tested exactly once. However, most applications require that each such combination is tested *at least* once instead. Moreover, there exist many combinations of parameters t, k, v for which an $OA(t, k, v)$ does not exist. This motivates the generalization of orthogonal arrays to covering arrays, for which the requirement that every t-tuple appears the same number of times is relaxed.

Definition 2.66 (Covering array). Let A be an $N \times k$ array with entries from an alphabet of cardinality v, λ and t be positive integers such that $t \leq k$ and $\lambda v^t \leq N$. If every t-set of column vectors of A is λ-covered, then A is a *covering array of strength t and index* λ, denoted $CA_\lambda(N; , t, k, v)$. When $\lambda = 1$, we simply write $CA(N; t, k, v)$.

Example 2.67. An example of a $CA(13; 3, 10, 2)$ is given in Figure 2.3. By definition, every two columns of such an array are covered. We verify this with the two highlighted columns in the same figure. Since every pair from $\{0, 1, 2\}^2$ appears at least once as a row of the subarray corresponding to these columns, then these are covered; however they are not uniformly covered, since the pair (0,0) appears twice. The same type of coverage is true for any other pair of columns, which means that this is a covering array of strength $t = 2$.

$$
\begin{array}{ccccccccccc}
1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
$$

$$OA_3(2, 11, 2)$$

(0,0) appears 3 times   (0,1) appears 3 times   (1,0) appears 3 times   (1,1) appears 3 times

Figure 2.2. Above, an example of an $OA_3(2, 11, 2)$; below, checking that the highlighted columns are uniformly 3-covered, as per the definition of an orthogonal array.

Similarly to orthogonal arrays, the rows of a $CA(N; t, k, v)$ provide a collection of N configurations for a system with k factors, represented by the columns, where each factor admits v possible values. Performing experimental runs for all N configurations corresponding to the rows of the covering array guarantees that every possible interaction of t factors is tested at least once. This is known as *t-way interaction testing*. An example of 2-way interaction testing is given in Figure 1.1; see also the related discussion in Chapter 1. For studies on the effectiveness of t-way interaction testing, we refer the reader to [18, 53].
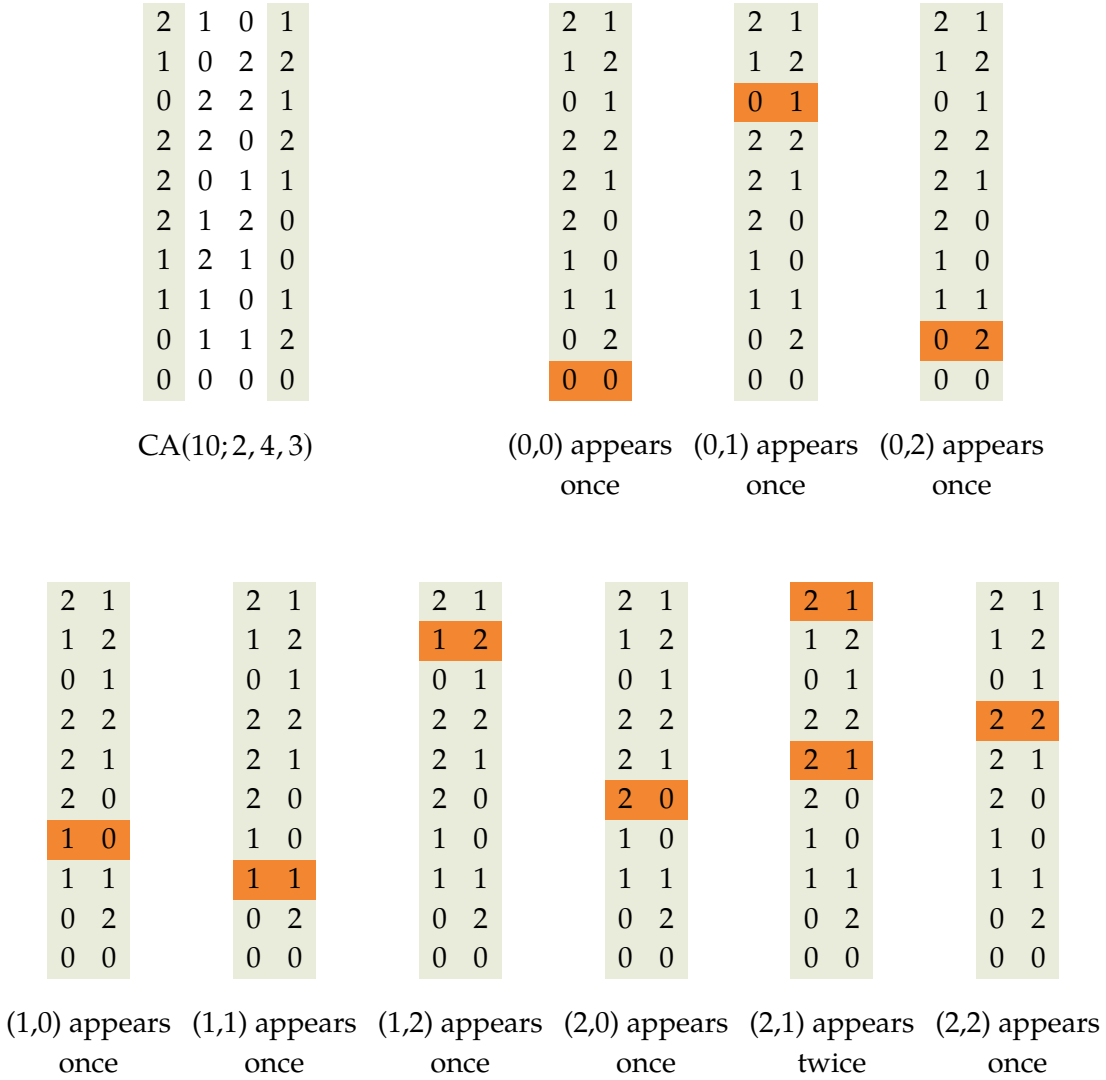
Figure 2.3. An example of a CA$(10; 2, 4, 3)$ and a demonstration that the highlighted columns are covered, but not uniformly covered.

2.2.2 Current state of research on covering arrays

In order to discuss the research on covering arrays, we first need to explain one fundamental underlying problem. First, we note that for any integers t, k, and v, a CA(N, t, k, v) can be constructed for large enough N. Indeed, we consider the following naive construction: for each one of the $\binom{k}{t}$ t-sets of columns, and for each one of the v^t t-tuples in $[0, v-1]^t$, we create a row whose elements in the position of these t columns are the elements of the t-tuple, with the rest of the elements having any value. This yields a CA$(v^t \binom{k}{t}; t, k, v)$.

Having established the existence of a CA(N, t, k, v) for some N which is a function of t, k and v, a natural question to ask is how small this N can be. This is a question integral to the

research on covering arrays, also because of the implications in testing applications, where a smaller number of rows means a smaller number of tests, and thus a reduction on the time and cost that is needed for a system to be tested. This leads to the following definition.

> **Definition 2.68 (Covering array number).** Let t, k and v be positive integers. The *covering array number for t, k, and v*, denoted CAN(t, k, v), is the smallest integer N for which a CA$(N; t, k, v)$ exists. A covering array CA$(N; t, k, v)$ with $N = $ CAN(t, k, v) is *optimal*.

There is active research on covering arrays, where the focus is to improve upon previously known bounds for covering array numbers, either by providing constructions of covering arrays, or by establishing theoretical bounds, including asymptotic results. In the following, we present an overview of some of the most important results from this research, that we categorize as follows:

- Bounds and asymptotics

- Algebraic constructions

- Recursive constructions

- Algorithmic constructions

Part of our presentation is based on [24], a somewhat dated but very thorough survey on the subject. We note that the vast majority of the research on covering arrays that are not orthogonal arrays, focuses on CA(N, t, k, v) rather than CA$_\lambda(N; t, k, v)$ with $\lambda > 1$.

Bounds and asymptotics

We start with some trivial bounds. First, we have that

$$v^t \leq \text{CAN}(t, k, v) \leq \binom{k}{t} v^t,$$

where the lower bound comes from the covering array definition, and the upper bound comes from our discussion in the beginning of the section.

A rather straightforward recursive bound can be obtained as follows. We choose any column c of a CA$(N; t, k, v)$ and any element x, and we create an array by removing that column and keeping only those rows whose element at the position of column c is x. Then, this array is a CA$(N'; t-1, k-1, v)$, where N' is the number of occurrences of x in column c, which implies that

$$\text{CAN}(t-1, k-1, v) \leq \frac{1}{v}\text{CAN}(t, k, v).$$

Apart from the above, there exist more sophisticated bounds of an asymptotic nature. For $t = 2$ and $v > 2$ Gargano et al. [33] show that

$$N = \frac{v}{2}\log(k)(1 + o(1)).$$

Furthermore, the following classic result is obtained using a method by Stein [87], Lovász [58] and Johnson [48]; see [84, Theorem 1] for a proof.

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

Improvements of this bound have been obtained using various techniques. For example, Godbole et al. [38] give an improved bound by employing the Stein-Chen method on random $N \times k$ arrays with elements from an alphabet of size v, to obtain a Poisson approximation for the number of uncovered t-sets of columns. For the binary case, an implication from the study of certain probability spaces [4, 65, 66] implies that

$$\mathrm{CAN}(t, k, 2) \leq 2^t t^{O(\log(t))} \log(k).$$

A more recent improvement due to Francetić and Stevens is based on the Lovász local lemma (see [2]) – also known as entropy compression. Apart from a tighter bound, the authors give bounds in closed form for strengths 2 and 3. A series of improvements on these bounds are given by Sarkar and Colbourn in [84], where an overview of the recent advances on this topic is also presented.

Other results come from work on t-qualitatively independent partitions of sets, which are equivalent to a covering array of strength t [24]. In [34] Gargano et al. determine the asymptotics of the largest size of a family of 2-independent k-partitions of an n-set, which at the time was a longstanding problem in combinatorics posed in its generality by Rényi in 1971 [79]. In the context of covering arrays, their result implies that the ratio of $CAN(2, k, v)$ to $\log(k)$ is asymptotic to $v/2$.

For strengths higher than 2, it follows from [71, 72] that the largest k for which a $CA(N; t, k, v)$ exists satisfies

$$\frac{et}{v} e^{\frac{N}{tv^t}} \leq k \leq \frac{K_{v,n}}{\sqrt{N}} 4^{\frac{N}{v^{t-1}}},$$

where $K_{v,n}$ is a constant depending only upon v and N.

Orthogonal arrays

Since an $\mathrm{OA}_\lambda(t, k, v)$ is also a $\mathrm{CA}_\lambda(\lambda v^t; t, k, v)$, orthogonal arrays are also relevant here. However, the research on orthogonal arrays is too big a subject to be in the scope of this section, so we limit our presentation to some important constructions that use finite fields. For a thorough presentation on the subject, we refer the reader to [27, Chapter III], as well as [46] for a textbook treatment.

We recall that we denote $[n]_q = (q^n - 1)/(q - 1)$. An early construction is for linear $\mathrm{OA}_{q^{n-2}}(2, [n]_q, q)$ for all $n \geq 2$, where q is a prime power. These arrays, at the time named hypercubes of strength 2, are due to Rao [77] and they are optimal in the sense that, for all prime powers q and $n \geq 2$, there do not exist $\mathrm{OA}_{q^{n-2}}(2, k, q)$ with $k > [n]_q$ [46, Corollary 3.21]. Different equivalent constructions can be found in the literature, with a notable one being very similar to the construction of Hamming codes. In fact, when constructed this way, the

rows of such orthogonal arrays are precisely the codewords of the dual of a Hamming code. Because of this, sometimes these arrays are referred to as *Rao-Hamming* orthogonal arrays. In Section 3.2.1 we present a construction of Rao-Hamming orthogonal arrays using sequences over finite fields, which is fundamental to the results of this thesis.

For a prime power $q > t$, Bush [13] constructs linear orthogonal arrays $OA(t, k, q)$ for all $k \leq q + 1$. Such arrays are optimal, in the sense that they have the minimum possible number of rows. In this construction, columns are indexed by the elements of $\mathbb{F}_q$ and rows are indexed by the polynomials in $\mathbb{F}_q$ of degree at most $t - 1$; then, each entry of the array is the evaluation of the corresponding column polynomial at the corresponding row element. The rows of such a linear orthogonal array are precisely the words of an extended Reed-Solomon code, although these codes were introduced several years after Bush's construction; see [46, Section 5.5].

For an *odd* prime power q and integer $n \geq 2$, Addelman and Kempthorne [1] give a construction of $OA_{2q^{n-2}}(2, 2[n]_q, q)$. This is similar to Bush's construction, with certain functions being used instead of polynomials; however, the resulting arrays are not linear.

Algebraic constructions

Rényi [79] determines covering array numbers for optimal binary covering arrays of strength 2 with an even number of rows. Kleitman and Spencer [52] and Katona [49] independently generalized this to any number of rows. In particular they show that, for any N, an optimal $CA(N; 2, k, 2)$ has $\binom{N-1}{\lceil N/2 \rceil}$ columns. The construction is given by forming an array whose columns consist of all distinct binary N-tuples of weight $\lceil N/2 \rceil$ that have zero in the first position.

Chateauneuf et al. [15] construct covering arrays of strength 3 whose entries are the result of a finite group acting on the symbols, as follows. Let M be an $n \times k$ array with entries M_{ij} from an alphabet Ω of size $v > 2$, and G be a subgroup of $Sym(\Omega)$, the symmetric group of permutations on the symbols in Ω. For $g \in G$, let M^g be the $n \times k$ array whose (i, j)-th element is M_{ij}^g, the image of M_{ij} under g. Finally, let M^G be the $(n|G| + v) \times k$ array that is the vertical concatenation of M^g, $g \in G$ and the constant row vectors $(x, ..., x) \in \Omega^k$, for all $x \in \Omega$. The array M is the *starter array* with respect to G. The authors show that it is possible to choose a group G and a starter array M so that M^G is a covering array of strength 3. Using further refinements, they construct $CA(N; 3, 2v, v)$ for all $v > 2$ and prime powers $q \geq v - 1$.

Meagher and Stevens [60] use a similar method to create covering arrays of strength 2. For a subgroup G of $Sym(\mathbb{Z}_v)$, $k \geq 2$ and $a \in (\mathbb{Z}_v \cup \infty)^k$, they consider a circulant $k \times k$ matrix M whose rows are precisely the cyclic shifts of a. Then, a is a *starter vector* with respect to G if M has the property that, for any $k \times 2$ subarray, there exists as a row a representative of every orbit of the action of G on $(\mathbb{Z}_v \cup \infty)^2$, where ∞ is fixed by the action. The authors show that if a starter vector exists in $\mathbb{Z}_v^k$ with respect to $G = \langle (1, 2, \ldots, v-1) \rangle$, then the vertical concatenation of M^g, $g \in G$ is a $CA(k(v-1) + 1; 2, k, v)$. They provide starter vectors for various values of v and k using computer search. This work has been generalized by Lobb et al. [57] who use arbitrary groups up to certain size instead of $\mathbb{Z}_v$, as well as multiple fixed symbols (infinities).

A different effective technique that combines algebraic elements and computations is due

to Sherwood et al. who introduce a type of array in a compacted form using permutation vectors, and connect the covering array definition with the existence of (covering) perfect hash families.

Recursive constructions

A covering array can be obtained by combining one or more existing covering arrays, using recursive constructions. The following product of strength 2 covering arrays is a construction of this nature. Given $A = \mathrm{CA}(N; 2, k, v)$ and $B = \mathrm{CA}(M; 2, l, v)$, a $\mathrm{CA}(N + M; 2, kl, v)$ can be constructed by appending k copies of B to l copies of A. More precisely, denoting $A = (A_{ij})$ and $B = (B_{ij})$, this is the $(N + M) \times kl$ array $C = (C_{ij})$ given by

$$C_{i,(f-1)k+g} = A_{i,g}, \text{ for } i \in [1, N], f \in [1, l], g \in [1, k]$$

and

$$C_{N+i,(f-1)k+g} = B_{i,f}, \text{ for } i \in [1, M], f \in [1, l], g \in [1, k].$$

This method is also the essence behind results on related combinatorial objects, such as qualitatively independent systems [16, 71] and transversal covers [90]; see also [24, Section 4.1] for extensions and further discussion on this recursive construction.

An important category of recursive constructions are the *Roux-type constructions*. In his PhD thesis, Roux [81] shows that for integers N, M, k, arranging four covering arrays as in the following diagram, where the array at the bottom right is the bit complement of the array on the bottom left, is a $\mathrm{CA}(N + M; 3, 2k, 2)$.

$\mathrm{CA}(N; 3, k, 2)$	$\mathrm{CA}(N; 3, k, 2)$
$\mathrm{CA}(M; 2, k, 2)$	$\overline{\mathrm{CA}(M; 2, k, 2)}$

This implies the following bound for covering array numbers.

$$\mathrm{CAN}(3, 2k, 2) \leq \mathrm{CAN}(3, k, 2) + \mathrm{CAN}(2, k, 2).$$

A generalization of this recursive construction that is not restricted to the binary alphabet is given by Chateauneuf and Kreher [14]. Let π be a cyclic permutation of v symbols. Then, the following arrangement of covering arrays yields a $\mathrm{CA}(N + (v - 1)M; 3, 2k, v)$.

$\mathrm{CA}(N; 3, k, v)$	$\mathrm{CA}(N; 3, k, v)$
$\mathrm{CA}(M; 2, k, v)$	$\pi\,(\mathrm{CA}(M; 2, k, v))$
$\mathrm{CA}(M; 2, k, v)$	$\pi^2\,(\mathrm{CA}(M; 2, k, v))$
$\vdots$	$\vdots$
$\mathrm{CA}(M; 2, k, v)$	$\pi^{v-1}\,(\mathrm{CA}(M; 2, k, v))$

This implies the following bound for covering array numbers.

$$\mathrm{CAN}(3, 2k, v) \leq \mathrm{CAN}(3, k, v) + (v - 1)\mathrm{CAN}(2, k, v).$$

A number of generalizations exist for strengths greater than 3 [8, 44, 45, 59] as well as a generalization due to Cohen et al. [21] that permits multiplying the number of columns by any $l \geq 2$.

In [28] Colbourn et al. give two recursive methods that they call *fusion* and *factor increase*. The first is a generalization of a result from [26] and is a method to obtain a $CA(N-2;t,k,v-1)$ from a $CA(N;t,k,v)$. The procedure is as follows. First we note that permuting the symbols in a column of a covering array does not affect the covering array property. We assume without loss of generality that the alphabet is $[0, v-1]$. For every column a suitable permutation of the symbols is applied so that a row consisting entirely of the symbol $v-1$ is created; this row is then dropped. Then, another row $r = (r_0, \ldots, r_{k-1})$ is chosen at random and subsequently for every column c_i, $i \in [1, k-1]$, every instance of $v-1$ is replaced by r_i if $r_i \neq v-1$ and 0 otherwise. In the array resulting from the above, all the t-tuples that did not involve $v-1$ that were covered in row r, are covered in other rows. Hence, removing row r yields a $CA(N-2,t,k,v-1)$. This implies the following inequality of covering array numbers.

$$CAN(t,k,v-1) \leq CAN(t,k,v) - 2. \tag{2.13}$$

We use the above inequality in Chapter 4 to improve upon previously best known bounds for covering array numbers.

For the factor increase construction, we start with two covering arrays $CA(N;t,k,v)$ and $CA(M;t-2,k-1,v)$, with columns $A_1, \ldots, A_k$ and $B_1, \ldots, B_{k-1}$, respectively. We assume without loss of generality that the alphabet is $[0, v-1]$. For $x \in [0, v-1]$, we denote C_x to be the column vector with M coordinates all equal to x. Then, the vertical concatenation of the $N \times (k+1)$ arrays $[A_1|A_2|\ldots|A_{k-1}|A_k|A_k]$ and $[B_1|B_2|\ldots|B_{k-1}|C_x|C_y]$, for all pairs $(x, y) \in [0, v-1]^2$, $x \neq y$, is a $CA(N + v(v-1)M; t, k, v)$. This implies the following inequality of covering array numbers.

$$CAN(t, k+1, v) \leq CAN(t, k, v) + v(v-1)CAN(t-2, k-1, v).$$

Other combinatorial structures can also be used to obtain covering arrays recursively. Cohen et al. [21] construct strength-3 covering arrays using ordered designs along with a covering array of strength 2; a refinement of this construction [24, Section 4.3] gives $CA(N; 3, q+1, q+1)$ where q is any prime power and $N = q^3 - q + \binom{q+1}{2}CAN(3, q+1, 2) - q^2 + 1$. See also [24, Sections 4.4 and 4.5] for a number of recursive constructions that rely on generalized Hadamard matrices and perfect hash families.

Algorithmic constructions

There exists a large number of greedy algorithms for computer generation of covering arrays. As a detailed overview is beyond our scope, we only enumerate here some of the most well-known results. For a survey we refer to [24]; see also [11] for a thorough analysis on some of these algorithms. Greedy algorithms include AETG [17], TCG [92], DDA [12], IPO [55], and BBA [80]. Notably in [11], generalizing results from [12], Bryce and Colbourn give an algorithm which, for fixed t and v, constructs a $CA(N; t, k, v)$ with $N = O(\log(k))$ in polynomial time.

While the existence of covering arrays that satisfy this upper bound have been previously established [24], this is the first deterministic polynomial-time algorithm that provides such a construction. Furthermore, there has been work with metaheuristic algorithms that use techniques such as tabu search [68], and simulated annealing [19, 20, 21, 22, 23, 35, 86, 89].

Combinatorial arrays from maximal sequences over finite fields

IN THIS CHAPTER WE STUDY connections between maximal sequences and concepts from other areas of discrete mathematics, and we present previously established constructions of orthogonal and covering arrays using maximal sequences in view of these connections.

We first present two classic theorems that give the essence of the main results in this chapter. The first theorem is stated explicitly by Bose [10], although its first half is due to Kempthorne [50]. It is also the special case of a generalization for the non-linear case due to Delsarte [30]; an in-depth presentation of Delsarte's result can be found in [46, Section 4.4].

> **Theorem 3.1 (Linear codes and linear orthogonal arrays are equivalent objects [46, Theorem 4.6]).** *Let q be a prime power, and C be a linear code of length k and dimension n, whose dual code has minimum distance $d^\perp$. Then, the $q^n \times k$ array whose rows are the codewords of C, is a linear $\mathrm{OA}_{q^{n-d^\perp+1}}(d^\perp - 1, k, q)$. Conversely, the q^n rows of a linear $\mathrm{OA}_{q^{n-t}}(t, k, q)$ are the codewords of a q-ary linear code with length k and dimension n, whose dual code has minimum distance $d^\perp \geq t + 1$. If the orthogonal array has strength t but not $t + 1$, then $d^\perp$ is precisely $t + 1$.*

The second theorem gives a necessary and sufficient condition for an array to be a linear orthogonal array, that is related to the linear independence of its columns.

> **Theorem 3.2 (Linear orthogonal arrays and linear independence [46, Theorem 3.29]).** *Let A be a $q^n \times k$ array whose rows form a q-ary linear code of length k and dimension n. Then, A is a linear $\mathrm{OA}_{q^{n-t}}(t, k, q)$ if and only if every t-set of its column vectors is linearly independent over $\mathbb{F}_q$.*

The structure of the rest of the chapter is as follows. In Section 3.1 we give a method for constructing arrays from maximal sequences, with the property that their rows are the words of a linear code. We study these arrays and present results closely related to Theorems 3.1 and 3.2 applied to these arrays, that also demonstrate how certain properties of maximal sequences can be translated into the language of orthogonal arrays, linear codes, divisibility of polynomials, and finite geometry. In Section 3.2 we show how arrays from maximal sequences can be used to construct several previously known families of orthogonal arrays. In Section 3.3 we present a method due to Raaphorst et al. [75] that uses arrays from maximal sequences as building blocks to construct larger covering arrays of strength 3.

The main contribution of this chapter is a framework that allows us to express previous results in a consistent manner and emphasize the ties between maximal sequences and other areas of discrete mathematics. Although these ties have been previously explored or implied, we offer a detailed overview of all the different points of view that, to the best of our knowledge, has not been given before as explicitly.

3.1 Cyclic trace arrays and their properties

We begin with the definition of a type of array that plays a fundamental role for the results in this thesis.

Definition 3.3 (Cyclic trace array of a primitive element). Let t, k be positive integers, α be a primitive element of $\mathbb{F}_{q^t}$ and $C = \{c_0, \ldots, c_{k-1}\}$ be an ordered subset of $[0, q^t - 2]$. Then, the *cyclic trace array corresponding to α and C*, denoted $\mathcal{A}_{q^t/q}(\alpha, C)$, is the $(q^t - 1) \times k$ array with elements

$$\mathcal{A}_{q^t/q}(\alpha, C)_{ij} = \mathrm{Tr}_{q^t/q}(\alpha^{i+c_j}), \quad (i, j) \in [0, q^t - 2] \times [0, k - 1].$$

We denote by $\mathcal{A}_{0, q^t/q}(\alpha, C)$ the $q^t \times k$ array obtained by appending a row of zeros to $\mathcal{A}_{q^t/q}(\alpha, C)$, i.e.

$$\mathcal{A}_{0, q^t/q}(\alpha, C)_{ij} = \begin{cases} \mathcal{A}_{q^t/q}(\alpha, C)_{ij} = \mathrm{Tr}_{q^t/q}(\alpha^{i+c_j}), & \text{if } i \in [0, q^t - 2], j \in [0, k - 1]; \\ 0, & \text{if } i = q^t - 1, j \in [0, k - 1]. \end{cases}$$

When it is clear from the context that the fields are $\mathbb{F}_{q^t}$ and $\mathbb{F}_q$, we simply write $\mathcal{A}$ instead of $\mathcal{A}_{q^t/q}$. Furthermore, we simply write $\mathcal{A}(\alpha)$ to denote $\mathcal{A}(\alpha, [0, [t]_q - 1])$, $\mathcal{A}_0(\alpha)$ to denote $\mathcal{A}_0(\alpha, [0, [t]_q - 1])$, and we refer to $\mathcal{A}_0(\alpha)$ as the *principal cyclic trace array of α*.

We use a dedicated name and notation for $\mathcal{A}_0(\alpha) = \mathcal{A}_0(\alpha, [0, [t]_q - 1])$ for reasons that we discuss at the end of this section. Furthermore, there is a close connection between cyclic trace arrays and maximal sequences which we give in Remark 3.6. First, we need to introduce some notation related to sequences.

Definition 3.4 (Sequence associated with finite field elements). Let q be a prime power and t be a positive integer. For $\alpha \in \mathbb{F}_{q^t}$, the *(LFSR) sequence over $\mathbb{F}_q$ associated to α* is

$$\mathrm{Seq}_{q^t/q}(\alpha) = \left(\mathrm{Seq}_{q^t/q}(\alpha)_i\right)_{i \geq 0} = \left(\mathrm{Tr}_{q^t/q}(\alpha^i)\right)_{i \geq 0}.$$

When it is clear that the underlying field is $\mathbb{F}_q$, we simply write $\mathrm{Seq}(\alpha)$ instead of $\mathrm{Seq}_{q^t/q}(\alpha)$.

We note that, by Theorem 2.38, if α is primitive, then $\mathrm{Seq}_{q^t/q}(\alpha)$ is a maximal sequence with period $q^t - 1$.

Definition 3.5 (Left shift operator). For a sequence $\mathbf{s} = (s_i)_{i \geq 0}$ we define the *left shift operator on* $\mathbf{s}$, denoted L, by

$$L^j(\mathbf{s}) = (s_{i+j})_{i \geq 0}, \quad j \in \mathbb{Z}.$$

We say that $L^j(\mathbf{s})$ is the *left cyclic shift of* $\mathbf{s}$ *by* j and we simply write $L(\mathbf{s})$ to denote $L^1(\mathbf{s})$. Furthermore, for a positive integer n, we denote

$$L_n^j(\mathbf{s}) = (s_{i+j})_{i=0}^{n-1}, \quad j \in \mathbb{Z}.$$

Remark 3.6. The next statements are straightforward implications of Definitions 3.3, 3.4 and 3.5.

1. The columns of $\mathcal{A}(\alpha, C)$ are the left cyclic shifts of $\mathrm{Seq}_{q^t/q}(\alpha)$ by the elements in C, that is,

$$\mathcal{A}(\alpha, C) = \left[L_{q^t-1}^{c_0}\left(\mathrm{Seq}_{q^t/q}(\alpha)\right) \mid L_{q^t-1}^{c_1}\left(\mathrm{Seq}_{q^t/q}(\alpha)\right) \mid \cdots \mid L_{q^t-1}^{c_{k-1}}\left(\mathrm{Seq}_{q^t/q}(\alpha)\right) \right].$$

2. If $C = \{c_0, \ldots, c_{k-1}\}$, then for $(i, j) \in [0, q^t - 2] \times [0, k - 1]$, the (i, j)-th element of $\mathcal{A}_{q^t/q}(\alpha, C)$ is

$$\mathcal{A}_{q^t/q}(\alpha, C)_{i,j} = \mathrm{Seq}_{q^t/q}(\alpha)_{i+c_j}.$$

3. The rows of $\mathcal{A}(\alpha)$ are the vectors $L_{[t]_q}^i(\mathrm{Seq}_{q^t/q}(\alpha))$, $i \in [0, q^t - 2]$.

4. For $C \subseteq C'$, we have that $\mathcal{A}_0(\alpha, C)$ is a subarray of $\mathcal{A}_0(\alpha, C')$.

Example 3.7. For a root α of the primitive polynomial $x^3 + 2x + 1$ over $\mathbb{F}_3$, we compute

$$\mathrm{Seq}_{q^t/q}(\alpha) = 00101211201110020212210222.$$

For $C = \{6, 8, 12\}$, the arrays $\mathcal{A}(\alpha, [0, q^t - 2])$, $\mathcal{A}_0(\alpha)$, $\mathcal{A}(\alpha, C)$ and $\mathcal{A}_0(\alpha, C)$, are shown in Table 3.1.

The rows of a cyclic trace array form the words of a linear code. To prove this we need the next lemma.

Lemma 3.8. *Let t be a positive integer and $\beta \in \mathbb{F}_{q^t}$. Then, we have that $\mathrm{Tr}_{q^t/q}(\beta x) = 0$ for all $x \in \mathbb{F}_{q^t}$, if and only if $\beta = 0$.*

Proof. From Theorem 2.17, the trace is a linear transformation from $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$ and, if $\beta \neq 0$, the mapping $x \mapsto \beta x$ permutes the elements of $\mathbb{F}_{q^t}$. Therefore, $\mathrm{Tr}_{q^t/q}(\beta x)$ maps $\mathbb{F}_{q^t}$ onto $\mathbb{F}_q$ as well, hence it is not true that $\mathrm{Tr}_{q^t/q}(\beta x) = 0$ for all $x \in \mathbb{F}_{q^t}$. The other direction is clear. ∎

Theorem 3.9 (The rows of $\mathcal{A}_0(\alpha, C)$ as a q-ary linear code). *Let t be a positive integer, α be a primitive element of $\mathbb{F}_{q^t}$, and C be a nonempty subset of $[0, q^t - 2]$, with $|C| = k$. Then, the set of rows of $\mathcal{A}_0(\alpha, C)$ is a linear code of length k and dimension $d = \dim(\mathrm{span}\{\alpha^i \mid i \in C\})$.*

$$\mathcal{A}(\alpha, [0, q^t - 2]) =$$

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

$$\mathcal{A}_0(\alpha) = \begin{array}{ccccccccccccc}
0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 \\
1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 \\
1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 \\
2 & 1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 \\
1 & 1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 \\
1 & 2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 \\
2 & 0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 \\
0 & 1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 \\
1 & 1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 \\
1 & 1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 \\
1 & 0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 \\
0 & 0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 \\
0 & 2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 \\
2 & 0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 \\
0 & 2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 \\
2 & 1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 \\
1 & 2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 \\
2 & 2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 \\
2 & 1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 \\
1 & 0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 \\
0 & 2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 \\
2 & 2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 \\
2 & 2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 \\
2 & 0 & 0 & 1 & 0 & 1 & 2 & 1 & 1 & 2 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{array}$$

$$\mathcal{A}(\alpha, C) = \begin{array}{ccc}
1 & 2 & 1 \\
1 & 0 & 0 \\
2 & 1 & 0 \\
0 & 1 & 2 \\
1 & 1 & 0 \\
1 & 0 & 2 \\
1 & 0 & 1 \\
0 & 2 & 2 \\
0 & 0 & 2 \\
2 & 2 & 1 \\
0 & 1 & 0 \\
2 & 2 & 2 \\
1 & 2 & 2 \\
2 & 1 & 2 \\
2 & 0 & 0 \\
1 & 2 & 0 \\
0 & 2 & 1 \\
2 & 2 & 0 \\
2 & 0 & 1 \\
2 & 0 & 2 \\
0 & 1 & 1 \\
0 & 0 & 1 \\
1 & 1 & 2 \\
0 & 2 & 0 \\
1 & 1 & 1 \\
2 & 1 & 1
\end{array}
\qquad
\mathcal{A}_0(\alpha, C) = \begin{array}{ccc}
1 & 2 & 1 \\
1 & 0 & 0 \\
2 & 1 & 0 \\
0 & 1 & 2 \\
1 & 1 & 0 \\
1 & 0 & 2 \\
1 & 0 & 1 \\
0 & 2 & 2 \\
0 & 0 & 2 \\
2 & 2 & 1 \\
0 & 1 & 0 \\
2 & 2 & 2 \\
1 & 2 & 2 \\
2 & 1 & 2 \\
2 & 0 & 0 \\
1 & 2 & 0 \\
0 & 2 & 1 \\
2 & 2 & 0 \\
2 & 0 & 1 \\
2 & 0 & 2 \\
0 & 1 & 1 \\
0 & 0 & 1 \\
1 & 1 & 2 \\
0 & 2 & 0 \\
1 & 1 & 1 \\
2 & 1 & 1 \\
0 & 0 & 0
\end{array}$$

Table 3.1. The arrays $\mathcal{A}(\alpha, [0, q^t - 2])$, $\mathcal{A}_0(\alpha)$, $\mathcal{A}(\alpha, C)$, $\mathcal{A}_0(\alpha, C)$, with α and $C = [6, 8, 12]$, as described in Example 3.7. The highlighted columns of $\mathcal{A}(\alpha)$ are those with indexes in C.

Proof. Let $C = \{c_0, \ldots, c_{k-1}\}$. The set of rows of $\mathcal{A}_0(\alpha, C)$ is given by

$$\mathcal{R} = \left\{ \left(\text{Tr}(\alpha^i \alpha^{c_0}), \ldots, \text{Tr}(\alpha^i \alpha^{c_{k-1}}) \right) \mid i \in [0, q^t - 2] \right\} \cup \{(0, \ldots, 0)\}$$
$$= \left\{ (\text{Tr}(x\alpha^{c_0}), \ldots, \text{Tr}(x\alpha^{c_{k-1}}) \mid x \in \mathbb{F}_{q^t} \right\}.$$

Let $r_1, r_2 \in \mathcal{R}$ and $c \in \mathbb{F}_q$. Then there exist $x, y \in \mathbb{F}_{q^t}$ such that

$$r_1 = (\text{Tr}(x\alpha^{c_0}), \ldots, \text{Tr}(x\alpha^{c_{k-1}}))$$
$$r_2 = \left(\text{Tr}(y\alpha^{c_0}), \ldots, \text{Tr}(y\alpha^{c_{k-1}}) \right)$$

and hence

$$r_1 + cr_2 = (\text{Tr}(x\alpha^{c_0}), \ldots, \text{Tr}(x\alpha^{c_{k-1}})) + c \left(\text{Tr}(y\alpha^{c_0}), \ldots, \text{Tr}(y\alpha^{c_{k-1}}) \right)$$
$$= \left(\text{Tr}(x\alpha^{c_0}) + c\text{Tr}(y\alpha^{c_0}), \ldots, \text{Tr}(x\alpha^{c_{k-1}}) + c\text{Tr}(y\alpha^{c_{k-1}}) \right).$$

By Statement 1 of Theorem 2.17, the trace is linear, so the latter is equal to

$$\left(\text{Tr}((x + cy)\alpha^{c_0}), \ldots, \text{Tr}((x + cy)\alpha^{c_{k-1}}) \right),$$

which is an element of $\mathcal{R}$. We conclude that $\mathcal{R}$ is a subspace of $\mathbb{F}_q^k$, that is, linear code of length k.

Now, we observe that the dimension of $\mathcal{R}$ is the dimension of the row space of $\mathcal{A}_0(\alpha, C)$, which is also the dimension of its column space. Hence, to complete the proof it suffices to show that the dimension of the column space is equal to $\dim(\text{span}\{\alpha^c \mid c \in C\})$. To do that, we show that for every $I \subseteq [0, k-1]$, the column vectors of $\mathcal{A}_0(\alpha, C)$ indexed by $c_i, i \in I$, are linearly dependent if and only if the elements $\alpha^{c_i}, i \in I$, are linearly dependent. We denote the i-th column vector of $\mathcal{A}_0(\alpha, C)$ by C_i, and consider nonempty $I \subseteq [0, k-1]$ and elements $y_i \in \mathbb{F}_q, i \in I$ that are not all zero. Then, we have that $\sum_{i \in I} y_i C_i = 0$ if and only if every row of the array consisting of the columns $C_i, i \in I$, satisfies the same linear dependence relation, that is, $\sum_{i \in I} y_i \text{Tr}(x\alpha^{c_i}) = 0$, for all $x \in \mathbb{F}_{q^t}$. From the linearity of the trace, as per Theorem 2.17, the latter is equivalent to $\text{Tr}(x \sum_{i \in I} y_i \alpha^{c_i}) = 0$, for all $x \in \mathbb{F}_{q^t}$. Furthermore, by Lemma 3.8, this is equivalent to $\sum_{i \in I} y_i \alpha^{c_i} = 0$. We conclude that $\sum_{i \in I} y_i C_i = 0$ if and only if $\sum_{i \in I} y_i \alpha^{c_i} = 0$. From our earlier discussion, this completes the proof. $\qquad\blacksquare$

It follows from Theorems 3.1 and 3.9 that a cyclic trace array $\mathcal{A}_0(\alpha, C)$ is a $q^t \times |C|$ orthogonal array, whose strength depends on the minimum distance of the dual code of the linear code whose codewords are the rows of the orthogonal array. By Theorem 3.2, its strength is also the largest number t such that every t of its column vectors are linearly independent over $\mathbb{F}_q$. Therefore, to specify the strength it is useful to characterize the subsets of column vectors of cyclic trace arrays that are linearly independent. This is done in the next proposition, which is a generalization of a result due to Raaphorst et al. [75, Theorem 2]. We have added Statements 1, 4 and 5, as well as the index q^{t-s} in Statement 3, which is missing from [75, Theorem 2].

Proposition 3.10. *Let t, s be positive integers with $s \leq t$, α be a primitive element of $\mathbb{F}_{q^t}$ with minimal polynomial m_α, and $I = \{i_0, \ldots, i_{s-1}\}$ be a nonempty subset of $[0, q^t - 2]$. Then, the following statements are equivalent:*

1. *The $q^t \times s$ array $\mathcal{A}_0(\alpha, I)$ is an $OA_{q^{t-s}}(t, s, q)$.*

2. *The set $\{\alpha^{i_j} \mid j \in [0, s-1]\}$ is linearly independent over $\mathbb{F}_q$.*

3. *The set $\{L_{q^t-1}^{i_j}(\mathrm{Seq}_{q^t/q}(\alpha)) \mid j \in [0, s-1]\}$ is linearly independent over $\mathbb{F}_q$.*

4. *For every $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$ not all zero, $m_\alpha(x)$ does not divide $\sum_{j=0}^{s-1} d_j x^{i_j}$.*

5. *There is no $(s-2)$-flat of $PG(t-1, q)$ that contains the points $[\alpha^{i_0}], \ldots, [\alpha^{i_{s-1}}]$.*

For the special case when $s = t$, the following is also equivalent to the statements above.

6. *There is no zero row in $\mathcal{A}(\alpha, C)$.*

Proof. "$2 \Rightarrow 1$". We denote $\mathrm{Tr} = \mathrm{Tr}_{q^t/q}$. We assume that Statement 2 holds and we need to show that, for every $(b_0, \ldots, b_{s-1}) \in \mathbb{F}_q^s$, there exist exactly q^{t-s} rows of $\mathcal{A}_0(\alpha, I)$ equal to $(b_0, \ldots, b_{s-1})$, i.e. there exist exactly q^{t-s} elements $i \in [0, q^t - 1]$ such that

$$(\mathcal{A}_0(\alpha, I)_{i,0}, \ldots, \mathcal{A}_0(\alpha, I)_{i,s-1}) = (b_0, \ldots, b_{s-1}). \tag{3.1}$$

From Definition 3.3, for all $(i, j) \in [0, q^t - 1] \times [0, s - 1]$ we have that

$$\mathcal{A}_0(\alpha)_{i,j} = \begin{cases} \mathrm{Tr}(\alpha^i \alpha^{i_j}), & \text{if } i \in [0, q^t - 2], j \in [0, s-1]; \\ 0 = \mathrm{Tr}(0 \cdot \alpha^{i_j}), & \text{if } i = q^t - 1, j \in [0, s-1]. \end{cases}$$

Furthermore, since α is a primitive element of $\mathbb{F}_{q^t}$, we have that

$$\mathbb{F}_{q^t} = \left\{ \alpha^i \mid i \in [0, q^t - 2] \right\} \cup \{0\} .$$

Therefore, we equivalently need to show that, for every $(b_0, \ldots, b_{s-1}) \in \mathbb{F}_q^s$, there exist exactly q^{t-s} elements $x \in \mathbb{F}_{q^t}$ such that

$$\left(\mathrm{Tr}(x\alpha^{i_0}), \ldots, \mathrm{Tr}(x\alpha^{i_{s-1}}) \right) = (b_0, \ldots, b_{s-1}). \tag{3.2}$$

We consider the mapping

$$\varphi : \mathbb{F}_{q^t} \longrightarrow \mathbb{F}_q^s$$
$$x \mapsto \left(\mathrm{Tr}(x\alpha^{i_0}), \ldots, \mathrm{Tr}(x\alpha^{i_{s-1}}) \right). \tag{3.3}$$

From the linearity of the trace over $\mathbb{F}_q$, it follows that φ is a linear transformation between vector spaces over $\mathbb{F}_q$. We show that φ is surjective; assume by means of contradiction that

this is not the case. Then $\text{Im}(\varphi)$ is a proper subspace of $\mathbb{F}_q^s$ and therefore $\text{Im}(\varphi)^\perp \neq \{\mathbf{0}\}$. Let $\mathbf{d} = (d_0, \ldots, d_{s-1}) \in \text{Im}(\varphi)^\perp \setminus \{\mathbf{0}\}$, so we have that

$$0 = \mathbf{d} \cdot \varphi(x) = \sum_{k=0}^{s-1} d_k \text{Tr}(x\alpha^{i_k}) = \text{Tr}\left(x \sum_{k=0}^{s-1} i_k \alpha^{i_k}\right), \quad \text{for all } x \in \mathbb{F}_{q^t}. \tag{3.4}$$

Equation (3.4) along with Lemma 3.8 implies that $\sum_{i=0}^{s-1} d_i \alpha^{s_i} = 0$. Since $\mathbf{d} \neq \mathbf{0}$, this contradicts the assumption that $\alpha^{i_0}, \ldots, \alpha^{i_{s-1}}$ are linearly independent, and completes the proof that φ is surjective. It follows that the rank of φ is s and, hence, for all $(b_0, \ldots, b_{s-1}) \in \mathbb{F}_q^s$, there exist exactly q^{t-s} elements $x \in \mathbb{F}_q$ such that $\varphi(x) = (b_0, \ldots, b_{s-1})$ or, equivalently, such that Equation (3.2) holds, as we needed to prove.

"1 $\Rightarrow$ 2" We assume that *Statement* 1 holds, that is, the columns of $\mathcal{A}_0(\alpha, I)$ are uniformly q^{t-s}-covered. From the previous part of the proof, this implies that φ is surjective, hence we have $\text{Im}(\varphi) = \mathbb{F}_q^s$ and, therefore, $\text{Im}(\varphi)^\perp = \{\mathbf{0}\}$. Now, we assume by means of contradiction that $\{\alpha^{i_j} \mid j \in [0, s-1]\}$ is linearly dependent over $\mathbb{F}_q$. Then, there exist $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$ not all zero, such that $\sum_{j=0}^{s-1} d_j \alpha^{i_j} = 0$, which implies that $\sum_{j=0}^{s-1} d_j \alpha^{i_j} x = 0$ for all $x \in \mathbb{F}_{q^t}$. From the linearity of the trace over $\mathbb{F}_q$ we have that, for all $x \in \mathbb{F}_{q^t}$,

$$0 = \text{Tr}(0) = \text{Tr}\left(\sum_{j=0}^{s-1} d_j \alpha^{i_j} x\right) = \sum_{j=0}^{s-1} d_j \text{Tr}\left(x\alpha^{i_j}\right)$$
$$= (d_0, \ldots, d_{s-1}) \cdot (\text{Tr}(x\alpha^{i_0}), \ldots, \text{Tr}(x\alpha^{i_{s-1}}))$$
$$= (d_0, \ldots, d_{s-1}) \cdot \varphi(x).$$

The above means that $(d_0, \ldots, d_{s-1}) \in \text{Im}(\varphi)^\perp = \{\mathbf{0}\}$, which contradicts the assumption that $d_0, \ldots, d_{s-1}$ are not all zero.

"2 $\Leftrightarrow$ 3" We prove the contrapositive of this equivalence. We assume that the set in Statement 2 is linearly dependent, i.e. there exist $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$ not all zero, such that $\sum_{j=0}^{s-1} d_j \alpha^{i_j} = 0$. By Lemma 3.8, this is equivalent to $\text{Tr}(x \sum_{j=0}^{s-1} d_j \alpha^{i_j}) = 0$, for all $x \in \mathbb{F}_{q^t}$. Since α is a primitive element, the latter holds if and only if $\text{Tr}(\alpha^i \sum_{j=0}^{s-1} d_j \alpha^{i_j}) = 0$, for all $i \in [0, q^t - 2]$. From the linearity of the trace, as per Theorem 2.17, this is equivalent to

$$\sum_{j=0}^{s-1} d_j \text{Tr}(\alpha^{i_j+i}) = 0, \text{ for all } i \in [0, q^t - 2]. \tag{3.5}$$

However, by Definition 3.5 we have that

$$\left(\text{Tr}(\alpha^{i_j+i})\right)_{i=0}^{q^t-2} = L_{q^t-1}^{i_j}\left(\left(\text{Tr}(\alpha^i)\right)_{i\geq 0}\right) = L_{q^t-1}^{i_j}\left(\text{Seq}_{q^t/q}(\alpha)\right),$$

hence Equation (3.5) is equivalent to

$$\sum_{j=0}^{s-1} d_j L_{q^t-1}^{i_j}\left(\text{Seq}_{q^t/q}(\alpha)\right) = 0,$$

i.e. the set in Statement 3 is linearly dependent.

"2 ⟺ 4" We show the contrapositive of this equivalence. We have that $\{\alpha^{ij} \mid j \in [0, s-1]\}$ is linearly dependent over $\mathbb{F}_q$ if and only if there exist $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$, not all zero, satisfying $\sum_{j=0}^{s-1} d_j \alpha^{ij} = 0$. From Lemma 2.6 the latter holds if and only if there exists a nonzero polynomial $f(x) = \sum_{j=0}^{s-1} d_j x^{ij} \in \mathbb{F}_q[x]$ such that $m_\alpha(x) | f(x)$, where m_α is the minimal polynomial of α.

"2 ⟺ 5" We recall that in view of Proposition 2.53, $\{[\alpha^i] \mid i \in [0, q^t - 2]\}$ is the set of points of $PG(t-1, q)$. Then, the proof for this part is a direct consequence of Lemma 2.52 and Remark 2.57.

"1 ⟹ 6" We assume that $s = t$ and Statement 1 holds. Then, the rows of the $q^t \times t$ array $\mathcal{A}_0(\alpha, C)$ are precisely all the vectors of $\mathbb{F}_q^t$, without repetitions. Since $\mathcal{A}_0(\alpha, C)$ is constructed by adding a row of zeros to $\mathcal{A}(\alpha, C)$, Statement 1 implies that the rows of $\mathcal{A}(\alpha, C)$ are precisely all the nonzero vectors of $\mathbb{F}_q^t$, hence Statement 6 holds.

"6 ⟹ 1" We assume that Statement 6 holds. Then, there exists no $i \in [0, q^t - 2]$ such that

$$\left(\mathrm{Tr}(\alpha^i \alpha^{i_0}), \ldots \mathrm{Tr}(\alpha^i \alpha^{i_{t-1}}) \right) = (0, \ldots, 0).$$

Since α is primitive, equivalently, there is no $x \in \mathbb{F}_{q^t}^\times$ such that

$$\left(\mathrm{Tr}(x \alpha^{i_0}), \ldots \mathrm{Tr}(x \alpha^{i_{t-1}}) \right) = (0, \ldots, 0).$$

We consider again the mapping

$$\begin{aligned} \varphi: \quad \mathbb{F}_{q^t} &\longrightarrow \mathbb{F}_q^t \\ x &\mapsto \left(\mathrm{Tr}(x \alpha^{i_0}), \ldots, \mathrm{Tr}(x \alpha^{i_{t-1}}) \right). \end{aligned}$$

From the above, there is no $x \in \mathbb{F}_q^\times$ such that $\varphi(x) = \mathbf{0} \in \mathbb{F}_q^t$, hence $\ker(\varphi) = \{0\}$, which implies that φ is injective, and hence also surjective. As we have argued in the proof for $2 \Rightarrow 1$, the surjectivity of φ implies that Statement 1 holds. ∎

Example 3.11. Let α be a root of the primitive polynomial $x^3 + 2x + 1 \in \mathbb{F}_3[x]$, so that α is a primitive element in $\mathbb{F}_{3^3}$, and let $C = \{6, 8, 12\}$. Considering Example 2.54, we have that the set $\{\alpha^c \mid c \in C\} = \{\alpha^6, \alpha^8, \alpha^{12}\}$ is linearly independent, therefore Statement 2 holds for this case. We also observe that $\mathcal{A}_0(\alpha, C) = \mathcal{A}_0(\alpha, \{6, 8, 12\})$ which we show in Table 3.1 is an OA$(3, 3, 3)$, as per Statement 1. Furthermore, the set $\{L_{3^3-1}^c \mathrm{Seq}_{q^t/q}(\alpha)) \mid c \in C\}$ is the set of columns of $\mathcal{A}(\alpha, C)$ that is also shown in Table 3.1, and is also linearly independent, so Statement 3 holds. Finally, the points α^c, $c \in C = \{6, 8, 12\}$ are the points a, b and e in Figure 2.1, which are not contained in the same 1-flat (line), as per Statement 5.

In Theorem 3.13 that follows, we give several necessary and sufficient conditions for a cyclic trace array to be a linear orthogonal array of a given strength. The proof relies on Proposition 3.10 and the theorem is an extension of Theorem 3.2 applied to cyclic trace arrays. First, we need to introduce the following notion.

Definition 3.12 ((k,s)-set). Let k,s be positive integers such that $s \le k$, and S be a set of k elements from a vector space over a field F. If every subset of S of size s is linearly independent, then S is a (k,s)-*set over* F, or simply a (k,s)-set when it is clear from the context that the underlying field is F.

Theorem 3.13. *Let t,s be positive integers, α be a primitive element of $\mathbb{F}_{q^t}$ with minimal polynomial m_α, and C be a nonempty subset of $[0, q^t - 2]$. Then, the following statements are equivalent.*

1. *The $q^t \times |C|$ array $\mathcal{A}_0(\alpha, C)$ is a linear $\mathrm{OA}_{q^{t-s}}(s, |C|, q)$.*

2. *The set $\{\alpha^c \mid c \in C\}$ is a $(|C|, s)$-set over $\mathbb{F}_q$.*

3. *The set $\{L^c_{q^t-1}(\mathrm{Seq}_{q^t/q}(\alpha)) \mid c \in C\}$ is a $(|C|, s)$-set over $\mathbb{F}_q$.*

4. *For every $c_0, \ldots, c_{s-1} \in C$ and $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$ not all zero, $m_\alpha(x)$ does not divide $\sum_{j=0}^{s-1} d_j x^{c_j}$.*

5. *For every s points in $\{[\alpha^c] \mid c \in C\}$, there is no $(s-2)$-flat in $PG(t-1, q)$ that contains them.*

Proof. In the following, we index the columns of $\mathcal{A}_0(\alpha, C)$ by the elements of C and the columns of $\mathcal{A}_0(\alpha)$ by $[0, t-1]$.

"1 $\Leftrightarrow$ 2" We have that $\mathcal{A}_0(\alpha, C)$ is a linear $\mathrm{OA}_{q^{t-s}}(s, k, q)$ if and only if any s-set of its columns is uniformly q^{s-2}-covered. In other words, if and only if for any $I \subseteq C$ with $|I| = s$, the $q^t \times s$ array $\mathcal{A}_0(\alpha, I)$ is an $\mathrm{OA}_{q^{t-s}}(s, s, q)$. We conclude that $\mathcal{A}_0(\alpha, C)$ is an $\mathrm{OA}_{q^{t-s}}(s, |C|, q)$ if and only if for every $I \subseteq C$ with $|I| = t$ we have that $\{\alpha^i \mid i \in I\}$ is linearly independent. However, the second statement is the definition of $\{\alpha^c \mid c \in C\}$ being a $(|C|, s)$-set, hence we have proven the equivalence of the first two statements.

"1 $\Leftrightarrow$ 4" We show the contrapositive of this equivalence. From the equivalence of the first two statements, we have that Statement 1 does not hold if and only if there exists a subset $\{c_0, \ldots, c_{s-1}\} \subseteq C$ so that $\{\alpha^{c_j} \mid j \in [0, s-1]\}$ is linearly dependent. From Statements 2 and 4 of Proposition 3.10, this is true if and only if there also exist $d_0, \ldots, d_{s-1} \in \mathbb{F}_q$ not all zero such that $m_\alpha(x)$ divides $\sum_{j=0}^{s-1} d_j x^{c_j}$, which is the negation of Statement 4.

Finally, the equivalence of Statement 2 with Statements 3, 4 and 5 is a straightforward implication of the equivalence of the statements with the same numbers in Proposition 3.10.

$\blacksquare$

Remark 3.14. For a primitive element $\alpha \in \mathbb{F}_{q^t}$ and integers i, j, Lemma 2.44 states that α^i and α^j are constant multiples of each other if and only if $i \equiv j \pmod{[t]_q}$. In other words, for every $j \in [0, q^t - 2]$ there exists some $i \in [0, [t]_q - 1]$ such that α^i and α^j are linearly dependent. It follows from Statement 2 of Proposition 3.10 and Theorem 3.13 that, for any C that is a subset of $[0, q^t - 2]$, there exists some C' that is a subset of $[0, [t]_q - 1]$ such that $\mathcal{A}_0(\alpha, C)$ and $\mathcal{A}_0(\alpha, C')$ have the same number of column subsets with the orthogonal array property. Therefore, for the construction of an orthogonal array of the form $\mathcal{A}_0(\alpha, C)$, without loss of generality the

set C can be considered to be a subset of $[0, [t]_q - 1]$. This also justifies the definition of the principal cyclic trace array in Definition 3.3.

3.2 Orthogonal arrays from cyclic trace arrays

In this section we present two classic orthogonal array constructions, as well as several more recent orthogonal and covering array constructions. All these results are adapted in the context of the previous section; in particular, the orthogonal and covering arrays are defined using the notation of Definition 3.3, and the results are justified using Theorem 3.13. We note that every proof that we present is one of several equivalent proofs that result by focusing on different statements of the theorem.

3.2.1 Two classic orthogonal array constructions

In the next corollary we show that a principal cyclic trace array is equivalent to the Rao-Hamming construction that we discuss in Section 2.2.2. Rao was the first to study these arrays [76, 77, 78] whose rows are exactly the words of the dual of q-ary Hamming codes [46], thus the references in the name. An in-depth discussion of this result that includes its history and several different constructions is given in [46, Section 3.4].

> **Corollary 3.15 (The Rao-Hamming construction using maximal sequences).** *Let t be a positive integer and α be a primitive element of $\mathbb{F}_{q^t}$. Then $\mathcal{A}_0(\alpha)$ is an $\mathrm{OA}_{q^{t-2}}(2, [t]_q, q)$. Furthermore, there is no $C \subset [0, q^t - 2]$ with $|C| > [t]_q$ such that $\mathcal{A}_0(\alpha, C)$ is a linear orthogonal array of strength 2.*

Proof. By Proposition 2.53, the points $[\alpha^i]$, $i \in [0, [t]_q - 1]$ are exactly all the points in $PG(t-1, q)$, which means that every two of them are distinct. In other words, any two points do not belong in the same 0-flat. Then, by Statements 1 and 5 of Theorem 3.13, we have that $\mathcal{A}_0(\alpha, [0, [t]_q - 1]) = \mathcal{A}_0(\alpha)$ is an $\mathrm{OA}_{q^{t-2}}(2, [t]_q, q)$.

Now, we assume by means of contradiction that there exists $C \subset [0, q^t - 2]$ such that $|C| > [t]_q$ and $\mathcal{A}_0(\alpha, C)$ is a linear orthogonal array of strength 2. Then, the points $[\alpha^c]$, $c \in C$ are all distinct elements of $PG(t - 1, q)$ which contradicts the fact that $PG(t - 1, q)$ contains exactly $[t]_q$ elements. ∎

The Rao-Hamming construction using maximal sequences is the cornerstone of many previously established results. In [31, 64, 70] the authors consider subarrays of Rao-Hamming orthogonal arrays, generated by maximal sequences whose minimal polynomials generated certain conditions, and push the strength to 3 (or "nearly" 3 in the case of [64], as we discuss later). In [74] (see also [75]) Raaphorst et al. explore in more depth the properties of Rao-Hamming arrays using maximal sequences and use them as building blocks to construct covering arrays of strength 3. We discuss these results in detail in the subsequent sections.

Next, we show a construction for orthogonal arrays of strength 3. To formulate this construction in terms of cyclic trace arrays, we rely on a theorem due to Ebert [32].

Theorem 3.16 (Partition of finite projective spaces into caps [32, Theorem 3]). *Let q be a prime power, t be a positive integer divisible by 4, and α be a primitive element of $\mathbb{F}_{q^t}$. We define*

$$\Omega_i = \left\{ \alpha^{i+j[t/2]_q} \mid j \in [0, q^{t/2}] \right\}, \quad i \in [0, [t/2]_q - 1].$$

Then, for every $i \in [0, [t/2]_q - 1]$ we have that the set Ω_i is a $(q^{t/2} + 1)$-cap and the points in $PG(t-1, q)$ are partitioned by

$$PG(t-1, q) = \bigsqcup_{i=0}^{[t/2]_q - 1} \Omega_i.$$

Corollary 3.17 (Orthogonal arrays of strength 3 from maximal sequences). *Let q be a prime power, t be a positive integer divisible by 4, and α be a primitive element of $\mathbb{F}_{q^t}$. For*

$$C = \left\{ j[t/2]_q \mid j \in [0, q^{t/2}] \right\},$$

we have that $\mathcal{A}_0(\alpha, C)$ is an $OA_{q^{t-3}}(3, q^{t/2} + 1, q)$.

Proof. We observe that $\{\alpha^c \mid c \in C\} = \Omega_0$, where Ω_0 is defined in Theorem 3.13. By the same theorem, we have that Ω_0 is a $(q^{[t/2]_q+1})$-cap, which means that no 3 points in Ω_0 are collinear. In other words, there is no 1-flat in $PG(t-1, q)$ that contains any 3 points from Ω_0, so the proof is complete by Statements 1 and 5 of Theorem 3.13. ∎

The special case of Corollary 3.17 for $t = 4$ is of particular interest. A k-cap in $PG(3, q)$ is an *ovoid*. Early on, Bose [9] showed that the maximum size of an ovoid is $q^2 + 1$ when q is odd, and soon after Qvist [73] showed that the same is true for even q. It follows that the $OA_q(3, q^2 + 1, q)$ obtained in Corollary 3.17 for $t = 4$ has the maximum number of columns among linear orthogonal arrays. We refer to [46, Section 5.9] for further discussion about this orthogonal array, and to [47, Section 4] and [27, Section VII.2.11] for details about the problem of finding maximum k-caps in $PG(d, q)$.

3.2.2 Orthogonal arrays from polynomials with few nonzero terms

In this section we present three constructions of orthogonal arrays that are of the form $\mathcal{A}_0(\alpha, [0, 2t])$, where α is a primitive element of $\mathbb{F}_{q^t}$ with a minimal polynomial that satisfies certain divisibility properties.

Divisibility of trinomials by trinomials and orthogonal arrays of strength close to 3 in $\mathbb{F}_2$

A *trinomial* is a polynomial with exactly three nonzero coefficients, i.e. a polynomial of the form $ax^t + bx^l + cx^k$, where a, b, c are nonzero. The next theorem due to Munemasa [64], characterizes all the polynomials of degree up to $2t$ over $\mathbb{F}_2$ that are divisible by trinomials of degree t that satisfy certain conditions.

> **Theorem 3.18 ([64, Corollary 3.3]).** *Let $f(x) = x^t + x^l + 1$ be a primitive trinomial over $\mathbb{F}_2$ with $t \geq 4$. If $g(x)$ is a trinomial of degree at most $2t$ divisible by $f(x)$, then $g(x) = f(x)^2$ or $g(x) = x^{t-\deg(g)}f(x)$.*

Using this theorem, Munemasa constructs orthogonal arrays of strength 2 that are close to being strength 3, in the sense that most but not all triples of columns have the orthogonal array property. To formalize this notion and give Munemasa's result, we need the following definition.

> **Definition 3.19.** Let A be a $n \times k$ array with elements A_{ij} from a set V with $|V| = v$. For an ordered set $J = \{j_0, \ldots, j_{s-1}\} \subseteq [0, k-1]$ and s-tuple $\mathbf{b} = (b_0, \ldots, b_{s-1}) \in V^s$, we define
> $$\lambda_{\mathbf{b}}^J(A) = \left|\left\{ i \mid (A_{ij_0}, \ldots, A_{ij_{s-1}}) = (b_0, \ldots, b_{s-1}), \ i \in [0, n-1] \right\}\right|.$$

> **Theorem 3.20 ([64, Main Theorem]).** *Let t be a positive integer, α be a primitive element of $\mathbb{F}_{2^t}$ with minimal polynomial $m_\alpha(x) = x^t + x^l + 1$, and define*
> $$U = \{(i, i+l, i+t) \mid i \in [0, t]\} \cup \{(0, 2l, 2t)\}.$$
> *Then, for any $J = \{j_0, j_1, j_2\} \subseteq [0, 2t]$ and $(b_0, b_1, b_2) \in \mathbb{F}_2^3$, we have that*
> $$\lambda_b^J(\mathcal{A}_0(\alpha, [0, 2t])) = \begin{cases} 2^{t-3} & \text{if } J \notin U; \\ 2^{t-2} & \text{if } J \in U \text{ and } b_1 + b_2 + b_3 = 0; \\ 0 & \text{if } J \in U \text{ and } b_1 + b_2 + b_3 \neq 0. \end{cases}$$

Proof. In this proof we denote $\mathrm{Tr} = \mathrm{Tr}_{2^3/2}$. First we consider the case when $t \geq 4$. If $J \notin U$, then by Theorem 3.18, the polynomial $g(x) = x^{j_0} + x^{j_1} + x^{j_2}$ is not divisible by $m_\alpha(x)$. By Statements 3 and 4 of Proposition 3.10 this means that the column vectors of $\mathcal{A}_0(\alpha)$ with indexes in J are uniformly 2^{t-3}-covered, so in particular $\mathbf{b} = (b_0, b_1, b_2)$ appears at those columns in exactly q^{t-3} rows; in other words, $\lambda_{\mathbf{b}}^J(\mathcal{A}_0(\alpha, [0, 2t])) = 2^{t-3}$.

If $J \in U$, then $m_\alpha(x)$ divides $x^{j_0} + x^{j_1} + x^{j_2}$ which, by Lemma 2.6, means that $\alpha^{j_0} + \alpha^{j_1} + \alpha^{j_2} = 0$, or
$$\alpha^{j_2} = \alpha^{j_0} + \alpha^{j_1}. \tag{3.6}$$

We note that since $j_0, j_1 < [t]_q$, the elements $\alpha^{j_0}, \alpha^{j_1}$ are linearly independent over $\mathbb{F}_2$, hence, by Proposition 3.10 the columns of $\mathcal{A}_0(\alpha, [0, 2t])$ are uniformly 2^{t-2}-covered. From the definition of the entries of $\mathcal{A}_0(\alpha, [0, 2t])$ this means that for every triple $(b_0, b_1, b_2) \in \mathbb{F}_2^3$, there exist exactly 2^{t-2} elements $x \in \mathbb{F}_2^3$ such that
$$(\mathrm{Tr}(\alpha^{j_0}x), \mathrm{Tr}(\alpha^{j_1}x)) = (b_0, b_1).$$

By Equation (3.6), we have that
$$\mathrm{Tr}(\alpha^{j_2}x) = \mathrm{Tr}(\alpha^{j_0}x + \alpha^{j_1}x) = \mathrm{Tr}(\alpha^{j_0}x) + \mathrm{Tr}(\alpha^{j_1}x) = b_0 + b_1.$$

We conclude that

$$(\text{Tr}(\alpha^{j_0}x), \text{Tr}(\alpha^{j_1}x), \text{Tr}(\alpha^{j_2}x)) = (b_0, b_1, b_2)$$

if and only if $b_2 = \text{Tr}(\alpha^{j_2}x)$, and the proof follows. ▢

Divisibility of trinomials by pentanomials and orthogonal arrays of strength 3 in $\mathbb{F}_2$

A *pentanomial* is a polynomial with exactly five nonzero coefficients. Dewar et al. [31] extend the idea of Munemasa to pentanomials over $\mathbb{F}_2$, by describing the polynomials $g(x)$ of degree up to $2t$ that are divisible by pentanomials $f(x) = x^t + x^l + x^k + x^j + 1$ with $\gcd(t, l, k, j) = 1$. The following theorem is a special case of [31, Theorem 1.2], where $f(x)$ is primitive and $g(x)$ is a trinomial.

> **Theorem 3.21 (A special case of [31, Theorem 1.2]).** *Let $f(x) = x^t + x^l + x^k + x^j + 1 \in \mathbb{F}_2[x]$ be primitive with $\gcd(t, l, k, j) = 1$. Then, $f(x)$ divides a trinomial $g(x)$ of degree up to $2t$ if and only if $g(x) = f(x)h(x)$ with $f(x)$ and $h(x)$ as shown in the table below.*
>
> | $f(x)$ | $h(x)$ |
> |---|---|
> | $x^5 + x^4 + x^3 + x^2 + 1$ | $x^3 + x^2 + 1$ |
> | $x^5 + x^3 + x^2 + x + 1$ | $x^3 + x + 1$ |
> | $x^5 + x^3 + x^2 + x + 1$ | $x^4 + x + 1$ |
> | $x^5 + x^4 + x^3 + x + 1$ | $x^2 + x + 1$ |
> | $x^6 + x^4 + x^3 + x + 1$ | $x^2 + x + 1$ |
> | $x^7 + x^4 + x^3 + x^2 + 1$ | $x^3 + x^2 + 1$ |

> **Corollary 3.22.** *Let α be a primitive element of $\mathbb{F}_{2^t}$ with minimal polynomial $m_\alpha(x) = x^t + x^l + x^k + x^j + 1$, such that $t > l, k, j$ and $\gcd(t, l, k, j) = 1$. If $m_\alpha(x)$ is not one of the polynomials $f(x)$ listed in Theorem 3.21, then $\mathcal{A}_0(\alpha, [0, 2t])$ is an $\text{OA}_{2^{t-3}}(3, 2t + 1, 2)$.*

Proof. First, we observe that $\mathcal{A}_0(\alpha, [0, 2t])$ is an orthogonal array of strength 2, as a subarray of $\mathcal{A}_0(\alpha)$ which has strength 2 by Corollary 3.15. By Statements 1 and 4 of Theorem 3.13, we have that for every $c_0, c_1 \in [0, 2t]$, and $d_0, d_1 \in \mathbb{F}_2$ not all zero, $m_\alpha(x)$ does not divide $d_0 x^{c_0} + d_1 x^{c_1}$. Furthermore, since $m_\alpha(x)$ is not one of the polynomials listed in the table, it does not divide any trinomials of degree up to $2t$, i.e. for any $c_0, c_1, c_2 \in [0, 2t]$, we have that $m_\alpha(x)$ does not divide $x^{c_0} + x^{c_1} + x^{c_2}$.

From the above, we conclude that for every $c_0, c_1, c_2 \in [0, 2t]$ and $d_0, d_1, d_2 \in \mathbb{F}_2$ not all zero, we have that $m_\alpha(x)$ does not divide $d_0 x^{c_0} + d_1 x^{c_1} + d_2 x^{c_2}$ and hence, by Statements 1 and 4 of Proposition 3.10, we have that $\mathcal{A}_0(\alpha, [0, 2t])$ is an $\text{OA}_{2^{t-3}}(3, 2t + 1, 2)$. ▢

Divisibility of trinomials by trinomials and orthogonal arrays of strength 3 in $\mathbb{F}_3$

Another extension of Munemasa's work is given by Panario et al. [70], where they study the divisibility of trinomials over $\mathbb{F}_3$ and completely describe the trinomials that divide other

trinomials of up to three times their degree, as follows.

Theorem 3.23 ([70, Theorem 8]). *Let $f(x) = x^t + bx^k + a \in \mathbb{F}_3[x]$ with $t > k$, $a, b \neq 0$, and $g(x)$ be a monic trinomial of degree up to $3t$ divisible by $f(x)$. Then $g(x) = f(x)^3$, or $f(x), g(x)$ are among the polynomials listed below, or the reciprocals of the polynomials listed below, i.e. $x^n f(1/x)$ and $x^n g(1/x)$.*

$f(x)$	$g(x)$	$f(x)$	$g(x)$
$x^t + bx^{t/2} - 1$	$x^{3t} - bx^{t/2} - 1$	$x^t - x^{t/3} + a$	$x^{8t/3} + x^{2t/3} + 1$
$x^t + bx^{t/2} + 1$	$x^{5t/2} + x^{t/2}b$	$x^t + x^{t/3} + a$	$x^{7t/3} + ax^{2t/3} + a$
$x^t + bx^{t/2} - 1$	$x^{5t/2} - bx^t b$	$x^t - x^{t/3} + a$	$x^{7t/3} - ax^{4t/3} + a$
$x^t + bx^{t/2} - 1$	$x^{5t/2} - x^{3t/2} - b$	$x^t - x^{t/3} + a$	$x^{7t/3} + x^{5t/3} - a$
$x^t + bx^{t/2} + 1$	$x^{5t/2} + bx^{4t/2}b$	$x^t + x^{t/3} + a$	$x^{2t} + ax^{5t/3} + 1$
$x^t + bx^{t/2} + 1$	$x^2 t + x^t 1$	$x^t - x^{t/3} + a$	$x^{5t/3} + ax^{4t/3} + a$
$x^t + bx^{t/2} - 1$	$x^{3t/2} + x^t b$	$x^t + bx^{t/4} - 1$	$x^{11t/4} + bx^{6t/4} - b$
$x^t + bx^{t/2} - 1$	$x^{3t/2} - bx^t - b$	$x^t + bx^{t/4} + 1$	$x^{10t/4} + bx^{9t/4} + 1$
$x^t - x^{t/3} + a$	$x^{3t} - x^{t/3} - a$		

The following corollary is not stated explicitly in [70] although the application of Theorem 3.23 for the construction of orthogonal arrays is discussed. The proof is along the same lines with that of Corollary 3.22.

Corollary 3.24. *Let α be a primitive element of $\mathbb{F}_{3^t}$ with minimal polynomial $m_\alpha(x) = x^t + bx^k + a \in \mathbb{F}_3[x]$, where $t > k$ and $a, b \neq 0$. If $m_\alpha(x)$ is not among the polynomials $f(x)$ listed in Theorem 3.23 or their reciprocals, then $\mathcal{A}(\alpha, [0, 3t - 1])$ is an $OA_{3^{t-3}}(3, 3t, 3)$.*

The proof of Theorem 3.23 requires examining a rather large number of cases for trinomial forms, and it is stated in [70] that the method becomes increasingly complicated to apply to larger finite fields. The same method has been applied recently to study the binary tetranomials divisible by pentanomials with consecutive inner coefficients [51]. However, it is suggested in [70] that the next important step in this area of research would be to find a different method of studying the divisibility of polynomials of a certain weight that applies to arbitrary fields, rather than extending the method in [70] to other specific finite fields and polynomial weights.

3.2.3 Orthogonal arrays from AMDS codes

It follows from Theorem 3.1 that linear codes and orthogonal arrays are equivalent objects. In this section we focus on a certain type of linear code and study the corresponding orthogonal arrays. These orthogonal arrays are also relevant to Chapter 5, where we use them to construct an infinite family of covering arrays.

We begin with two auxiliary results related to linear codes. The first is a connection between the minimum distance of a linear code and the sets of Definition 3.12.

Proposition 3.25. *A linear code C of length n and dimension k has minimum distance d if and only if the columns of its parity check matrix form an $(n, d-1)$-set of vectors in $\mathbb{F}_q^{n-k}$ that is not a (n, d)-set.*

Proof. Let H be a parity check matrix of C. The columns of H are a $(n, d-1)$-set that is not a (n, d)-set if and only if every $d-1$ columns are linearly independent, but some d columns are not. This is equivalent to the following equation:

$$d = \min\{x \mid \text{there exist } x \text{ linearly dependent columns in } H\},$$

which is equivalent to d being the minimum distance, by Proposition 2.61. □

The second auxiliary result gives an explicit method of using the parity check matrix of a linear code with minimum distance d to construct a cyclic trace array that is an orthogonal array of strength $d-1$.

Theorem 3.26 (Orthogonal arrays from maximal sequences and linear codes). *Let C be a linear code with parameters $[n, k, d]_q$ and parity check matrix $H = (H_{ij})$, $i \in [0, n-k-1]$, $j \in [0, n-1]$, and let α be a primitive element of $\mathbb{F}_{q^{n-k}}$. We define*

$$C = \left\{ \log_\alpha \left(\sum_{i=0}^{k-1} H_{ij} \alpha^i \right) \mid j \in [0, n-1] \right\}.$$

Then $\mathcal{A}_0(\alpha, C)$ is an $\mathrm{OA}_{q^{n-k-d+1}}(d-1, n, q)$ that is not an $\mathrm{OA}_{q^{n-k-d}}(d, n, q)$.

Proof. Denoting the j-th column of H by H_j, we have by Proposition 3.25 that the set

$$S' = \{H_j \mid j \in [0, n-1]\}$$

is an $(n, d-1)$-set that is not an (n, d)-set over $\mathbb{F}_q$. Consider the vector space isomorphism φ, defined by

$$\varphi: \ \mathbb{F}_q^{n-k} \to \mathbb{F}_{q^{n-k}}$$
$$(x_0, \ldots, x_{n-k-1}) \mapsto \sum_{i=0}^{n-k-1} x_i \alpha^i.$$

Then, we have that

$$S = \{\varphi(H_j) \mid j \in [0, n-1]\} = \varphi(S').$$

This implies that S is an $(n, d-1)$-set that is not an (n, d)-set, since this is true for S' and φ respects linear independence, as a vector space isomorphism. The proof is complete by Statements 1 and 3 of Theorem 3.13. □

The following is a classic bound for linear codes.

Lemma 3.27 (Singleton bound [85]). *For a q-ary linear $[n, k, d]$-code we have that*

$$n - k - d + 1 \geq 0.$$

Linear codes with parameters that achieve or are close to equality in Lemma 3.27 are of special interest.

> **Definition 3.28 (Singleton defect and related codes).** The *Singleton defect* of a linear $[n, k, d]$-code is the number
> $$s(C) = n - k + 1 - d.$$
>
> If $s(C) = 0$, then C is *maximum distance separable (MDS)*. If $s(C) = 1$, then C is *almost maximum distance separable (AMDS)*. If both C and $C^\perp$ are AMDS, then C is *near maximum distance separable (NMDS)*.

From Definition 3.28 we have that a code is AMDS if it has parameters $[n, n-d, d]_q$ for some n, d. Then, by Proposition 3.25, the columns $H_0, \ldots, H_{n-1}$ of a parity check matrix form an $(n, d-1)$-set that is not an (n, d)-set, which by Remark 2.57 is equivalent to $\{[H_i] \mid i \in [0, n-1]\}$ being an n-track in $PG(d - 1, q)$. We conclude that the following are equivalent objects:

- An n-track in $PG(d - 1, q)$.

- An AMDS code with parameters $[n, n - d, d]_q$.

- An $OA_q(d - 1, n, q)$.

Let $M(r, q)$ be the maximum number n such that a maximum n-track exists in $PG(r, q)$. Some exact values of $M(r, q)$ for general prime power q are shown in Table 3.2a. In particular, we have that $M(2, q) = q^2 + q + 1$ and that $M(3, q) = q^2 + 1$ for $q > 2$, which means that the orthogonal arrays in Corollaries 3.15 and 3.17 have the maximum number of columns that can be obtained from our type of construction. However, finding exact values for $M(r, q)$ for $r \geq 4$ is a difficult problem [47]. In Table 3.2b we show the known values and bounds for small values of r and q. For other bounds on $M(r, q)$ that rely on bounds on the size of other objects in finite geometry, we refer the reader to the survey by Hirschfeld and Storme [47].

Other than that, we have an infinite class of AMDS codes from elliptic curves. We recall that an NMDS code is an AMDS code whose dual is also AMDS. The original rather challenging proof of the next theorem appears in [91]; see [37] for a more accessible proof.

> **Theorem 3.29 ([37, Theorem 1.1]).** *Let q be a prime power and suppose that there exists an elliptic curve with n rational points over $\mathbb{F}_q$. Then, for every $k \in [2, n - 1]$, there exists an $[n, k, d]_q$ NMDS code.*

It is known, see for example [91, Theorem 2.3.17] that if $q = p^r$ then there exists and elliptic curve with N_q rational points over $\mathbb{F}_q$, where

$$N_q = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } p | 2\sqrt{q} \text{ and } r \geq 3, r \text{ odd;} \\ q + \lfloor 2\sqrt{q} \rfloor + 1, & \text{otherwise.} \end{cases} \tag{3.7}$$

Hence, from Theorem 3.29 there exists an AMDS (that is moreover NMDS) code with parameters $[N_q, N_q - r, r]_q$ which, from the previously mentioned equivalence of AMDS codes and orthogonal arrays, yields the following result.

d	q	$M(d,q)$
2	any	$q^2 + q + 1$
3	$q > 2$	$q^2 + 1$
$2q - 2$	$q > 3$	$2q + 1$
$2q - 1$	$q > 3$	$2q + 2$
$\geq 2q$	any	0

(a) Known exact values of $M(d,q)$ [47, Table 8.1].

q $\backslash$ N	2	3	4	5	7	8	9	11
2	7	13	21	31	57	73	91	133
3	8	10	17	26	50	65	82	122
4		11	11	$12-20$	$16-30$	$14-36$	$16-43$	$22-57$
5		12	12	$12-14$	$15-31$	$15-37$	$17-44$	$23-58$
6			9	$10-15$	$13-28$	$14-34$	$17-39$	$18-49$
7			10	$11-16$	$13-20$	$14-35$	$18-40$	$18-50$
8				11	$13-21$	$14-23$	$19-36$	$19-50$
9				12	$13-22$	$14-24$	$20-26$	$20-51$
10					$14-23$	$14-25$	$16-27$	$18-44$
11					$15-24$	$15-26$	$16-28$	$18-32$
12					15	$15-27$	$16-29$	$18-33$
13					16	$16-28$	$17-30$	$18-34$

(b) Known values of $M(d,q)$ for small d and q [47, Table 8.4].

Table 3.2. Values of $M(d,q)$.

> **Corollary 3.30.** *Let q be a prime power and α be a primitive element of $\mathbb{F}_{q^t}$. Then there exists $C \subset [0, [t]_q - 1]$ with $|C| = N_q$, such that $\mathcal{A}_0(\alpha, C)$ is an $OA_q(t - 1, N_q, q)$.*

3.2.4 Orthogonal arrays from arcs

Every result that we have presented so far follows from Theorem 3.13 for some $s < t$. In this section we briefly discuss the case $s = t$. From the equivalence of Statements 1 and 2 of Theorem 3.13 for $s = t$ and the definition of an arc, we have the following.

Corollary 3.31 (Orthogonal arrays from arcs). *Let α be a primitive element of $\mathbb{F}_{q^t}$ and C be a nonempty subset of $[0, q^t - 2]$. Then, the following statements are equivalent:*

- *The $q^t \times |C|$ array $\mathcal{A}_0(\alpha, C)$ is a linear $\mathrm{OA}(t, |C|, q)$.*

- *The set $\{[\alpha^c] \mid c \in C\}$ is a $|C|$-arc in $PG(t - 1, q)$.*

Therefore, to obtain an orthogonal array with the maximum number of columns, we equivalently need to obtain a k-arc in $PG(t - 1, q)$ where k is the maximum possible.

Let $m(d, q)$ be the maximum k for which a k-arc exists in $PG(d, q)$. Determining $m(d, q)$ for various values of d, q is a well-researched problem of finite geometry. However, the currently known values of $m(d, q)$ correspond to orthogonal arrays with a very small number of columns compared to the number of rows. In fact, a well-known conjecture [47] is that

$$m(d, q) = \begin{cases} d + 2 & \text{if } d \geq q - 1; \\ q + 2 & \text{if } q \text{ is even and } d \in [2, q - 2]; \\ q + 1 & \text{otherwise.} \end{cases}$$

We refer to Sections 2 and 3 of [47] for a survey on the currently known constructions and sizes of arcs, all of which support the above conjecture. A discussion of the problem in the context of orthogonal arrays and linear codes can be found in Section 5.6 of [46].

3.3 Covering arrays from cyclic trace arrays

Other than our work in the next chapters, there is only one previous construction of covering arrays that are not orthogonal arrays which uses maximal sequences. In [75] (see also [74]) Raaphorst et al. study the combinatorial properties of arrays of the form $\mathcal{A}_0(\alpha)$ where α is a primitive element of $\mathbb{F}_{q^t}$. Moreover, for the case when $t = 3$, they exploit these properties to provide a method to construct covering arrays of strength 3. One of their most powerful results is a connection between the positions of the zero entries in the array and the blocks of a BIBD.

Theorem 3.32 (A BIBD from $\mathcal{A}(\alpha)$ [75, Theorem 3]). *For a primitive element $\alpha \in \mathbb{F}_{q^t}$, each row of $\mathcal{A}_0(\alpha)$ has exactly $z = [t - 1]_q$ zeros, and the set*

$$\mathcal{B} = \big\{\{a_0, \dots, a_{z-1}\} \mid \mathcal{A}(\alpha)_{i, a_0} = \dots = \mathcal{A}(\alpha)_{i, a_{z-1}} = 0 \text{ for some } i \in [0, k - 1]\big\}$$

is the set of blocks of a $([t]_q, [t - 1]_q, [t - 2]_q)$-BIBD.

The positions of the zero entries are also connected to another combinatorial object, as given in the next proposition. For positive integers n, k and a set $S \subseteq \mathbb{Z}_n$, the set $\{k + s \mod n \mid s \in S\}$ is a *translate* of S. A (v, k, λ)-*difference set* is a k-subset H of an Abelian group G (written additively) of order v such that for every $i \in G \setminus \{0\}$, we can write $i = w - v$ for λ distinct choices of $w, v \in H$.

Proposition 3.33 ([75]). *Let q be a prime power, t be an integer with $t \geq 2$ and α be a primitive element of $\mathbb{F}_{q^t}$. We define*

$$H_i = \left\{ j \mid j \in [0, [t]_q - 1] \text{ such that } \mathcal{A}(\alpha)_{i,j} = 0 \right\}, \quad i \in [0, q^t - 1].$$

Then, for every $i \in [0, q^t - 1]$, we have that H_i is a $([t]_q, [t-1]_q, [t-2]_q)$-difference set. Furthermore, these are all the translates of H_0 as a subset of $\mathbb{Z}_{[t]_q}$.

For the case $t = 3$, the sets H_i of Proposition 3.33 are $(q^2 + q + 1, q + 1, 1)$-difference sets. Raaphorst et al. use properties of this type of a difference set in order to show that if a triple of columns with indexes $a, b, c \subset [0, q^2 + q]$ are not covered in $\mathcal{A}_0(\alpha)$, then the columns of $\mathcal{A}_0(\alpha^{-1})$ with indexes a, b, c are covered. This leads to the following result.

Theorem 3.34 ([75, Theorem 6]). *Let q be a prime power and α be a primitive element of $\mathbb{F}_{q^3}$. Then, the vertical concatenation of $\mathcal{A}(\alpha)$ with $\mathcal{A}(\alpha^{-1})$, as well as a row of zeros, is a $\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$.*

Focusing on the fact that $\mathcal{A}(\alpha^{-1})$ consists of the columns of $\mathcal{A}(\alpha)$ in reverse order, the authors of [75] considered a generalization where $\mathcal{A}(\alpha)$, with α is a primitive element of $\mathbb{F}_{q^t}$, $t \geq 4$, is vertically concatenated with copies of $\mathcal{A}(\alpha)$ with the columns permuted in various ways. More precisely, search algorithms were ran to find a permutation group of smallest order $s(t, q)$, such that vertically concatenating the $s(t, q)$ permuted copies of $\mathcal{A}(\alpha)$ and adding a zero row yields a $\mathrm{CA}(s(t, q)(q^t - 1) + 1; t, [t]_q, q)$. Since $s(2, q) = 1$ from Corollary 3.15, and $s(3, q) = 2$ from Corollary 3.17 the hope was that s would be a function depending only on t and not q, however the experiments seemed to indicate otherwise. Moreover, in all cases that were examined for $t \geq 4$, due to the large size of $s(t, q)$, the resultant arrays did not improve the known best upper bounds for covering array numbers. We refer to [74, Section 4.4] for details on the experiments.

New covering arrays from maximal sequences and backtracking

IN SECTION 3.3 WE DISCUSSED a covering array construction due to Raaphorst et al. [75] where, for a primitive element $\alpha \in \mathbb{F}_{q^3}$, the arrays $\mathcal{A}(\alpha), \mathcal{A}(\alpha^{-1})$ and a row of zeros are vertically concatenated to produce a covering array of strength 3. At the end of Chapter 2, we also discussed how the authors attempted to generalize this construction by considering a primitive element $\alpha \in \mathbb{F}_{q^t}$, $t \geq 4$, and the vertical concatenation of $\mathcal{A}(\alpha)$ with copies of itself with the columns permuted in various ways. In this chapter, we consider a generalization where, instead of vertically concatenating copies of a cyclic trace array with the columns permuted, we use cyclic trace arrays corresponding to different primitive elements. Then, we search for subarrays of that vertical concatenation with the covering array property.

The structure of this chapter is as follows. In Section 4.1 we give some preliminary definitions and we express our objectives as solving two optimization problems that we state therein. Section 4.2 is dedicated to the first problem, which is concerned with finding covering arrays among subarrays of the vertical concatenation of cyclic trace arrays. We give an algorithmic solution to this problem based on backtracking with several optimizations. Section 4.3 is dedicated to the second problem which is about finding the optimum way of choosing the cyclic trace arrays to concatenate in the first problem. We also give an algorithmic solution that uses finite field theory. In Section 4.4 we discuss our computer implementation of the algorithms of the previous sections and our experimental results, that include the improvement of 38 previously best known covering array numbers.

The results of this chapter appear in [93].

4.1 Problem statement

We begin by generalizing the concept of a cyclic trace array.

Definition 4.1. Let t, k be positive integers, $P = \{\alpha_0, \ldots, \alpha_{l-1}\}$ be a set of primitive elements of $\mathbb{F}_{q^t}$, and $C = \{c_0, \ldots, c_{k-1}\}$ be a nonempty subset of $[0, q^t - 2]$. We define the following arrays.

- $\mathcal{A}_{q^t/q}(P, C)$ is the $l(q^t - 1) \times k$ array that is the vertical concatenation of $\mathcal{A}_{q^t/q}(\alpha_i, C)$, $i \in [0, l-1]$.

- $\mathcal{A}_{q^t/q,\mathbf{0}}(P, C)$ is the $\left(l(q^t - 1) + 1\right) \times k$ array that we obtain by appending a row of

zeros to $\mathcal{A}_{q^t/q}(P, C)$.

- We simply write $\mathcal{A}_{q^t/q}(P)$ to denote $\mathcal{A}_{q^t/q}(P, [0, [t]_q - 1])$ and $\mathcal{A}_{q^t/q,\mathbf{0}}(P)$ to denote $\mathcal{A}_{q^t/q,\mathbf{0}}(P, [0, [t]_q - 1])$.

When it is clear from the context that the fields are $\mathbb{F}_{q^t}$ and $\mathbb{F}_q$, we simply write $\mathcal{A}$ instead of $\mathcal{A}_{q^t/q}$ in the above definitions.

Definition 4.1 generalizes Definition 3.3 in the sense that, for a singleton $P = \{\alpha\}$, the arrays $\mathcal{A}(P, C)$ (resp. $\mathcal{A}_{\mathbf{0}}(P, C)$) and $\mathcal{A}(\alpha, C)$ (resp. $\mathcal{A}_{\mathbf{0}}(\alpha, C)$) are identical.

Remark 4.2. Let $(i, j) \in [0, l(q^t - 1) - 1] \times [0, k - 1]$. Then, there exists $m \in [0, l - 1]$ such that $m(q^t - 1) \leq i < (m + 1)(q^t - 1)$, and it follows from Definitions 3.3 and 4.1 and the fact that $\alpha_m^{q^m - 1} = 1$, that the (i, j)-th element of $\mathcal{A}(P, C)$ is given by $\mathcal{A}(P, C)_{ij} = \mathcal{A}(\alpha_m, C)_{ij} = \mathrm{Tr}_{q^t/q}(\alpha_m^{i + c_j})$.

Example 4.3. For a root α of the primitive polynomial $x^3 + 2x + 1$ over $\mathbb{F}_3$, we compute

$$\mathrm{Seq}_{q^t/q}(\alpha) = 00101211201110020212210222.$$

We have already presented $\mathcal{A}_{\mathbf{0}}(\alpha)$ in Table 3.1. Now, we observe that α^5 is also a primitive element of $\mathbb{F}_{3^3}$, since the order of $\mathbb{F}_{3^3}^\times$ is $3^3 - 1 = 26$ and $\gcd(5, 26) = 1$. We have

$$\mathrm{Seq}_{q^t/q}(\alpha^5) = 02122210022020121112011010,$$

and $\mathcal{A}_{\mathbf{0}}(\{\alpha, \alpha^5\})$ is as shown in Table 4.1.

The orthogonal and covering arrays described in Sections 3.2 and 3.3 can all be expressed in terms of the cyclic trace arrays in Definition 4.1, as shown in Table 4.2. In this chapter we extend this table by finding sets P and C such that $\mathcal{A}_{\mathbf{0}}(P, C)$ is a $\mathrm{CA}(|P|(q^t - 1) + 1; t, |C|, q)$. Searching for such sets is naturally related to the following two problems.

Problem 1. *Let q be a prime power, $t \geq 2$, $l \geq 1$ and $\alpha_0, \ldots, \alpha_{l-1}$ be primitive elements of $\mathbb{F}_{q^t}$. Find $C \subseteq [0, [t]_q - 1]$ of maximum size with the property that, for every $I \subseteq C$ with $|I| = t$, there exists $i \in [0, l - 1]$ such that $\mathcal{A}_{\mathbf{0}}(\alpha_i, I)$ is an $\mathrm{OA}(t, t, q)$.*

Remark 4.4. For a solution C of Problem 1, $\mathcal{A}_{\mathbf{0}}(\{\alpha_0, \ldots, \alpha_{l-1}\}, C)$ is a $\mathrm{CA}(l(q^t - 1) + 1; t, |C|, q)$.

Problem 2. *Let q be a prime power, $t \geq 2$ and $l \geq 1$. Find an l-set of primitive elements $P = \{\alpha_0, \ldots, \alpha_{l-1}\}$ of $\mathbb{F}_{q^t}$ such that there exists $C \subseteq [0, [t]_q - 1]$ that has the following properties:*

    i. C is a solution to Problem 1 for P, and

    ii. for every l-set P' of primitive elements of $\mathbb{F}_{q^t}$ and for every solution C' to Problem 1 for P', we have that $|C'| \leq |C|$.

```
0 0 1 0 1 2 1 1 2 0 1 1 1
0 1 0 1 2 1 1 2 0 1 1 1 0
1 0 1 2 1 1 2 0 1 1 1 0 0
0 1 2 1 1 2 0 1 1 1 0 0 2
1 2 1 1 2 0 1 1 1 0 0 2 0
2 1 1 2 0 1 1 1 0 0 2 0 2
1 1 2 0 1 1 1 0 0 2 0 2 1
1 2 0 1 1 1 0 0 2 0 2 1 2
2 0 1 1 1 0 0 2 0 2 1 2 2
0 1 1 1 0 0 2 0 2 1 2 2 1
1 1 1 0 0 2 0 2 1 2 2 1 0
1 1 0 0 2 0 2 1 2 2 1 0 2
1 0 0 2 0 2 1 2 2 1 0 2 2
0 0 2 0 2 1 2 2 1 0 2 2 2     A(α)
0 2 0 2 1 2 2 1 0 2 2 2 0
2 0 2 1 2 2 1 0 2 2 2 0 0
0 2 1 2 2 1 0 2 2 2 0 0 1
2 1 2 2 1 0 2 2 2 0 0 1 0
1 2 2 1 0 2 2 2 0 0 1 0 1
2 2 1 0 2 2 2 0 0 1 0 1 2
2 1 0 2 2 2 0 0 1 0 1 2 1
1 0 2 2 2 0 0 1 0 1 2 1 1
0 2 2 2 0 0 1 0 1 2 1 1 2
2 2 2 0 0 1 0 1 2 1 1 2 0
2 2 0 0 1 0 1 2 1 1 2 0 1
2 0 0 1 0 1 2 1 1 2 0 1 1
0 2 1 2 2 2 1 0 0 2 2 0 2
2 1 2 2 2 1 0 0 2 2 0 2 0
1 2 2 2 1 0 0 2 2 0 2 0 1
2 2 2 1 0 0 2 2 0 2 0 1 2
2 2 1 0 0 2 2 0 2 0 1 2 1
2 1 0 0 2 2 0 2 0 1 2 1 1
1 0 0 2 2 0 2 0 1 2 1 1 1
0 0 2 2 0 2 0 1 2 1 1 1 2
0 2 2 0 2 0 1 2 1 1 1 2 0
2 2 0 2 0 1 2 1 1 1 2 0 0
2 0 2 0 1 2 1 1 1 2 0 0 1
0 2 0 1 2 1 1 1 2 0 0 1 1
2 0 1 2 1 1 1 2 0 0 1 1 0
0 1 2 1 1 1 2 0 0 1 1 0 0     A(α^5)
1 2 1 1 1 2 0 0 1 1 0 0 2
2 1 1 1 2 0 0 1 1 0 0 2 1
1 1 1 2 0 0 1 1 0 0 2 1 2
1 1 2 0 0 1 1 0 0 2 1 2 2
1 2 0 0 1 1 0 0 2 1 2 2 2
2 0 0 1 1 0 0 2 1 2 2 2 1
0 0 1 1 0 0 2 1 2 2 2 1 0
0 1 1 0 0 2 1 2 2 2 1 0 0
1 1 0 0 2 1 2 2 2 1 0 0 2
1 0 0 2 1 2 2 2 1 0 0 2 2
0 0 2 1 2 2 2 1 0 0 2 2 0
0 0 0 0 0 0 0 0 0 0 0 0 0     0
```

Table 4.1. The array $\mathcal{A}_0(\{\alpha, \alpha^5\})$ described in Example 4.3.

P	C	$\mathcal{A}_0(P,C)$	Reference
$\{\alpha\}, \alpha \in \mathbb{F}_{q^t}, t \geq 2$	$[0, [t]_q - 1]$	$\mathrm{OA}_{q^{t-2}}(2, [t]_q, q)$	Corollary 3.15
$\{\alpha\}, \alpha \in \mathbb{F}_{q^t}, 4 \mid t$	$\{\alpha^{i+j[t/2]_q} \mid j \in [0, q^{t/2}]\}$	$\mathrm{OA}_{q^{t-3}}(3, q^{t/2} + 1, q)$	Corollary 3.17
$\{\alpha\}, \alpha \in \mathbb{F}_{q^t}$ as in Corollary 3.22	$[0, 2t]$	$\mathrm{OA}_{2^{t-3}}(3, 2t + 1, 2)$	Corollary 3.22
$\{\alpha\}, \alpha \in \mathbb{F}_{q^t}$ as in Corollary 3.24	$[0, 3t - 1]$	$\mathrm{OA}_{3^{t-3}}(3, 3t, 3)$	Corollary 3.24
$\{\alpha, \alpha^{-1}\}, \alpha \in \mathbb{F}_{q^3},$	$[0, q^2 + q]$	$\mathrm{CA}(2q^3 - 1; 3, q^2 + q + 1, q)$	Theorem 3.34

Table 4.2. The orthogonal and covering arrays described in Sections 3.2 and 3.3. In every case, α is a primitive element.

For some values of l and t, these problems have already been addressed. For $l = 1$, Problem 1 is about finding a set of columns of $\mathcal{A}_0(\{\alpha\}) = \mathcal{A}_0(\alpha)$ of maximum size such that the subarray they define is a covering array (in this case, an orthogonal array) of strength t. This is equivalent to the problem of finding arcs of maximum size in $PG(t-1, q)$, as we discuss in Section 3.2.4. Moreover, this is independent of the choice of α and thus Problem 2 is trivial when $l = 1$. For $t = 2$, both problems are trivial since $\mathcal{A}_0(\alpha) = \mathcal{A}_0(\alpha, C)$ for $C = [0, [t]_q - 1]$ is a a a covering array of strength 2. For $t = 3$ and $l \geq 2$, the problems are settled from Proposition 3.10. Indeed, we have that $\mathcal{A}_0(\{\alpha, \alpha^{-1}\})$ is a covering array (in this case, an orthogonal array) of strength 3 for any primitive $\alpha \in \mathbb{F}_{q^3}$, hence the answer to Problem 1 is

$$C = [0, [3]_q - 1] = [0, q^2 + q],$$

which is of the maximum possible size. This also implies that, for any primitive $\alpha \in \mathbb{F}_{q^3}$, the pair $\{\alpha, \alpha^{-1}\}$ is an answer to Problem 2.

From the above we conclude that we can focus on the cases $t \geq 4$ and $l \geq 2$. In this chapter we give algorithmic answers for these cases that rely on finite field theory and combinatorial exhaustive generation. We dedicate Sections 4.2 and 4.3 to Problems 1 and 2, respectively. In Section 4.4 we discuss the computer implementation of our algorithms, which resulted to 38 new covering arrays that improve upon previously best upper bounds for covering array numbers of strength 4, as well as one covering array that improves upon a previously best upper bound [29] of covering arrays of strength 5.

4.2 A backtracking algorithm for Problem 1

4.2.1 Preliminaries

In this section, we present the terminology and minimum background related to backtracking algorithms, which is necessary for Chapter 4.

Algorithm 1 Generic backtracking algorithm with optimal solution saved globally

---

    global X_{best}
    procedure BACKTRACKING$(x_0, \ldots, x_{r-1})$
        if $(x_0, \ldots, x_{r-1})$ is a feasible solution and it is better than X_{best} **then**
            $X_{best} \leftarrow (x_0, \ldots, x_{r-1})$
        Compute $C(x_0, \ldots, x_{r-1})$
        for $x \in C(x_0, \ldots, x_{r-1})$ **do**
            BACKTRACKING$(x_0, \ldots, x_{r-1}, x)$
    Main;
    $X_{best} \leftarrow (x_0)$
    BACKTRACKING(x_0)

An *optimization problem* is one that involves finding an optimal solution among the set of all feasible solutions, which we refer to as the *search space*. Often, the optimal solution can be represented as a list $S = (s_0, s_1, \ldots, s_{n-1})$ in which each s_i is chosen from a finite *possibility set* $\mathcal{P}_i$. A *backtracking algorithm* is a recursive method for solving such problems, that incrementally builds feasible candidate solutions and abandons ("backtracks") the ones that do not lead to an optimal solution, as soon as it determines that this is the case. At every recursion, a backtracking algorithm extends a feasible solution $(s_0, \ldots, s_{r-1})$ to a feasible solution $(s_0, \ldots, s_{r-1}, x)$, where x is restricted to a subset $C(s_0, \ldots, s_{r-1}) \subseteq \mathcal{P}_{r-1}$, according to the problem's constraints. The set $C(s_0, \ldots, s_{r-1})$ is a *set of candidates* (or *choice set*) and its computation is referred to as *pruning*. For all $y \in \mathcal{P}_r \setminus C(s_0, \ldots, s_{r-1})$, the cases $(s_0, \ldots, s_{r-1}, y)$ are not considered.

In Algorithm 1 we show a generic backtracking algorithm where an optimal solution candidate is saved in a global variable X_{best}. The efficiency of this algorithm greatly depends on reducing the size of $C(s_0, \ldots, s_{r-1})$, as well as finding an efficient way of calculating it.

Algorithm 1 gives rise to an ordered tree as follows. The nodes of the tree are all the feasible solutions, where (s_0) is the root of the tree and the children of node $(s_0, \ldots, s_{r-1})$ are precisely the nodes $(s_0, \ldots, s_{r-1}, x)$, for $x \in C(s_0, \ldots, c_{r-1})$, in the order they are processed by the algorithm. A visualization of this is shown in Figure 4.1. We often use this tree terminology for convenience.

Problem 1 can be formulated as an optimization problem. A straightforward way to do this is as follows. Let P be a fixed set of primitive elements of $\mathbb{F}_{q^t}$. A feasible solution to Problem 1 is any subset S of $[0, [t]_q - 1]$ such that $\mathcal{A}_0(P, S)$ is a covering array of strength t. The corresponding candidate set can be defined as

$$C(S) = \left\{ x \mid x > \max(S) \text{ and } \mathcal{A}_0(P, S \cup \{x\}) \text{ is a covering array of strength } t \right\}. \tag{4.1}$$

A feasible solution of the maximum size is an answer to Problem 1. In the following sections we greatly reduce the size of the candidate set in Equation (4.1) and determine an efficient way of computing it.
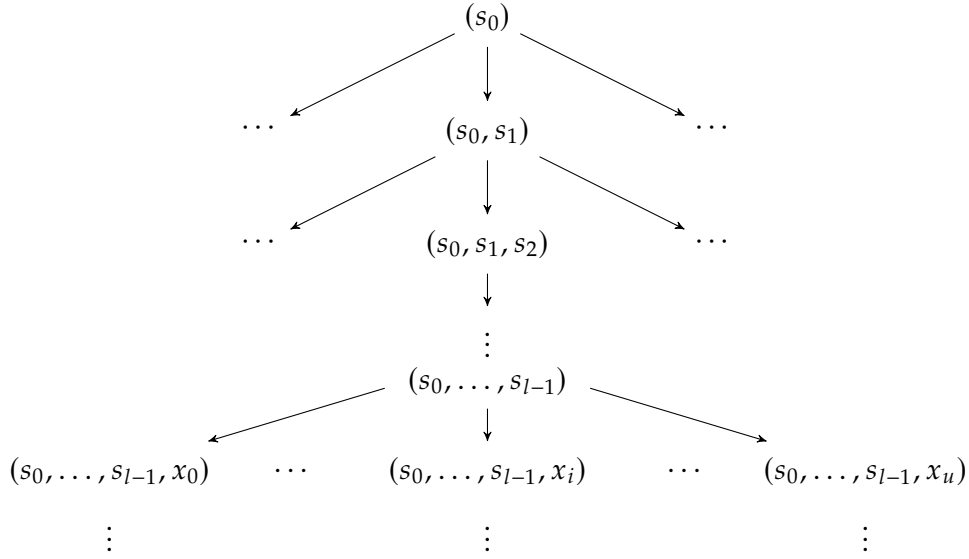
Figure 4.1. A visual representation of the nodes of the tree corresponding to Algorithm 1 that are at distance l from the root, where $C(s_0, \ldots, s_{l-1}) = \{x_0, \ldots, x_u\}$.

4.2.2 Isomorphism pruning for Problem 1

In this section we establish an equivalence relation on sets of positive integers and a criterion for choosing a canonical representative of every equivalence class. For the special case when the sets of integers represent feasible solutions to the optimization problem that we discuss previously, we show that the elements of these equivalence classes yield equivalent feasible solutions. As a result, we can reduce the candidate set in Equation (4.1) by only considering elements that yield canonical feasible solutions.

An equivalence relation on feasible solutions

The equivalence relation that we want to establish relies on the following notion.

Definition 4.5 (Shift of a set modulo n). Let $n \geq 1$ be an integer and $S \subseteq [0, n-1]$. For any integer i, the *shift of S by i modulo n* is the set

$$S +_n i = \{(s + i) \bmod n \mid s \in S\}.$$

Two sets $S, T \subseteq [0, n-1]$ are *shift-equivalent modulo n* if $S = T +_n i$, for some $i \in [0, n-1]$.

The relation shift-equivalence modulo n is an equivalence relation on the power set of $[0, n-1]$. Next, we show that this gives rise to a notion of equivalence of feasible solutions to Problem 1.

Lemma 4.6. *Let q be a prime power, t be an integer with $t \geq 2$ and α be a primitive element of $\mathbb{F}_{q^t}$. Suppose that $I, J \subseteq [0, [t]_q - 1]$ where $|I| = |J| = t$ and I and J are shift-equivalent modulo $[t]_q$. Then, we have that $\mathcal{A}_0(\alpha, I)$ is an $OA(t, t, q)$ if and only if $\mathcal{A}_0(\alpha, J)$ is an $OA(t, t, q)$.*

Proof. From Statements 1 and 2 of Proposition 3.10, it suffices to show that $\{\alpha^i \mid i \in I\}$ is linearly independent if and only if $\{\alpha^j \mid j \in J\}$ is linearly independent. Suppose by means of contradiction that the former is linearly independent but the latter is not. Let $I = \{i_0, \ldots, i_{t-1}\}$ and $J = \{j_0, \ldots, j_{t-1}\}$. From our assumptions, there exist $c_0, \ldots, c_{t-1} \in \mathbb{F}_q$ not all zero such that

$$c_0 \alpha^{j_0} + \cdots + c_{t-1} \alpha^{j_{t-1}} = 0. \tag{4.2}$$

Now, since I and J are shift-equivalent modulo $[t]_q$, then there exists integer k such that

$$j_s = (k + i_s) \bmod [t]_q,$$

for every $s \in [0, t-1]$. In other words, for every $s \in [0, t-1]$ there exists integer l_s such that

$$j_s = k + i_s + l_s[t]_q.$$

Hence, we have that $\alpha^{j_s} = \alpha^k \alpha^{l_s[t]_q} \alpha^{i_s}$ and Equation (4.2) implies that

$$
\begin{aligned}
0 &= c_0 \alpha^k \alpha^{l_0[t]_q} \alpha^{i_0} + \cdots + c_{t-1} \alpha^k \alpha^{l_{t-1}[t]_q} \alpha^{i_{t-1}} \\
&= \alpha^k \left(c_0 \alpha^{l_0[t]_q} \alpha^{i_0} + \cdots + c_{t-1} \alpha^{l_{t-1}[t]_q} \alpha^{i_{t-1}} \right).
\end{aligned}
$$

Thus, denoting $c'_s = c_s \alpha^{l_s[t]_q}$, we have that

$$c'_0 \alpha^{i_0} + \cdots + c'_{t-1} \alpha^{i_{t-1}} = 0. \tag{4.3}$$

From Lemma 2.44, we have that $\alpha^{l_s[t]_q} \in \mathbb{F}_q^\times$, for every s which means that $c'_0, \ldots, c'_{t-1}$ are elements of $\mathbb{F}_q$, not all zero. This, along with Equation (4.3), implies that $\{\alpha^i \mid i \in I\}$ is linearly dependent, contradicting our assumptions. The proof for the other direction is identical. $\quad\square$

For $S \subseteq [0, n-1]$, we denote by $\mathcal{S}_n(S)$ the equivalence class of the shift-equivalence modulo n that contains S. In other words,

$$\mathcal{S}_n(S) = \{S +_n i \mid i \in [0, n-1]\}. \tag{4.4}$$

Proposition 4.7. *Let q be a prime power, t be an integer with $t \geq 2$ and let $\alpha_0, \ldots, \alpha_{l-1}$ be primitive elements of $\mathbb{F}_{q^t}$. Let $S \subseteq [0, [t]_q - 1]$ with the property that, for every $I \subseteq S$ with $|I| = t$, there exists $i \in [0, l-1]$ such that $\mathcal{A}_0(\alpha_i, I)$ is a $OA(t, t, q)$. Then, every $T \in \mathcal{S}_{[t]_q}(S)$ has the same property; that is, for every $I \subseteq T$ with $|I| = t$, there exists $i \in [0, l-1]$ such that $\mathcal{A}_0(\alpha_i, I)$ is a $OA(t, t, q)$.*

Proof. Let $T \in \mathcal{S}_{[t]_q}(S)$ and $J \subseteq T$ with $|T| = t$. Then, J is shift-equivalent modulo $[t]_q$ to some $I \subseteq S$, since S and T are shift-equivalent modulo $[t]_q$ as elements of the same equivalence class

$\mathcal{S}_{[t]_q}(S)$. From the assumptions about S, we have that $\mathcal{A}_0(\alpha_i, I)$ is an OA(t, q, q), by Lemma 4.6, $\mathcal{A}_0(\alpha_i, J)$ is also a covering array of strength t. This is a subarray of $\mathcal{A}_0(P, J)$, and hence the latter is a covering array of strength t. ▫

It follows from Proposition 4.7 that S is a feasible solution to Problem 1 if and only if every set in the equivalence class $\mathcal{S}_{[t]_q}(S)$ is also a feasible solution. Therefore, we can reduce the search space of the problem to only representatives of these canonical sets.

Canonical representatives of the equivalent classes

In the following, we establish a criterion that allows us to choose a unique representative from each class of the shift-equivalence modulo n. We do this using the notion of a binary necklace, which we define next.

> **Definition 4.8 (Necklace).** Let A be an ordered set and $\mathbf{a}$ be a string of elements from A. The *necklace of* $\mathbf{a}$, denoted by neck$(\mathbf{a})$, is the lexicographically smallest of all cyclic shifts of $\mathbf{a}$. If $\mathbf{a} = \text{neck}(\mathbf{a})$, then $\mathbf{a}$ is a necklace. If $A = \{0, 1\}$, then a necklace is a *binary necklace*; we denote $\mathcal{B}_n$ the set of all binary necklaces of length n.

> **Example 4.9.** Let $\mathbf{a} = 10101$. The following are all the cyclic shifts of $\mathbf{a}$, listed in lexicographical order:
>
> $$01011 < 01101 < 10101 < 10110 < 11010,$$
>
> hence, neck$(\mathbf{a}) = 01011$. Let $\mathbf{b} = 101010$. All the (distinct) shifts of $\mathbf{b}$ are 010101 and 101010, therefore neck$(\mathbf{b}) = 010101$.

> **Definition 4.10 (The characteristic vector of a set).** Let n be a positive integer, $S \subseteq [0, n-1]$ and, for every $i \in [0, n-1]$ let
>
> $$b_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise.} \end{cases}$$
>
> Then, the binary string char$_n(S) = b_0 b_1 \ldots b_{n-1}$ is the *characteristic vector of S*.

Let $\mathbf{b} = b_0 \ldots b_{n-1}$ be a binary string. Similarly to Definition 3.5, we denote

$$L^i(\mathbf{b}) = b_i \ldots b_{n-1} b_0 \ldots b_{i-1},$$

and refer to $L^i(\mathbf{b})$ as the left cyclic shift of $\mathbf{b}$ by i. Furthermore, for $b \in \{0, 1\}$, we denote b^n the binary string consisting of the digit b repeated n times. Apart from the characteristic vector, we need to introduce another binary representation for sets.

> **Definition 4.11 (Binary representation of sets).** Let n be a positive integer, S be a nonempty subset of $[0, n-1]$ and, for every $i \in [0, \max(S)]$, let
>
> $$b_i = \begin{cases} 1 & \text{if } i \in S \\ 0 & \text{otherwise.} \end{cases}$$
>
> We define the *binary representation of S*, denoted by $\text{bin}_n(S)$, to be the binary string
>
> $$\text{bin}_n(S) = 0^{n-\max(S)-1} b_0 \ldots b_{\max(S)}$$
> $$= L^{\max(S)+1}(\text{char}_n(S)).$$
>
> Moreover, we define $\text{bin}_n(\emptyset) = 0^n$.

Our focus now becomes to show that we can use the above binary representation and the notion of a binary necklace to choose a unique representative from each class of the shift-equivalence modulo n. We begin with an auxiliary result.

> **Lemma 4.12.** *Let n be a positive integer and $S \subseteq [0, n-1]$. Then,*
>
> $$\{\text{char}_n(T) \mid T \in \mathcal{S}_n(S)\} = \{L^i(\text{char}_n(S)) \mid i \in [0, n-1]\}.$$

Proof. Let $T \subseteq [0, n-1]$; for the rest of the proof, we denote

$$\text{char}_n(S) = b_0 \ldots b_{n-1}$$
$$\text{char}_n(T) = c_0 \ldots c_{n-1}. \tag{4.5}$$

First, we assume that $T \in \mathcal{S}_n(S)$, so that $T = S +_n i$ for some $i \in [0, n-1]$. Then, the following equivalencies hold for all $j \in [0, n-1]$:

$$c_j = 1 \Leftrightarrow j \in T$$
$$\Leftrightarrow j = (s+i) \bmod n, \text{ for some } s \in S$$
$$\Leftrightarrow j = s + i + kn, \text{ for some } s \in S \text{ and } k \in \mathbb{Z}. \tag{4.6}$$

For $j \in [0, i-1]$, we have that Equation (4.6) holds if and only if $k = -1$ and thus $c_j = 1$ is equivalent to $n - i + j \in S$, or $b_{n-i+j} = 1$; this shows that

$$c_0 \ldots c_{i-1} = b_{n-i} \ldots b_{n-1}. \tag{4.7}$$

For $j \in [i, n-1]$, we have that Equation (4.6) holds if and only if $k = 0$ and thus $c_j = 1$ is equivalent to $j - i \in S$, or $b_{j-i} = 1$; this shows that

$$c_i \ldots c_{n-1} = b_0 \ldots b_{n-1-i}. \tag{4.8}$$

From Equations (4.7) and (4.8) we conclude that

$$
\begin{aligned}
\mathrm{char}_n(T) &= c_0 \ldots c_{n-1} \\
&= b_{n-i} \ldots b_{n-1} b_0 \ldots b_{n-1-i} \\
&= L^{n-i}(b_0 \ldots b_{n-1}) \\
&= L^{n-i}(\mathrm{char}_n(S)),
\end{aligned}
$$

which proves that

$$
\{\mathrm{char}_n(T) \mid T \in \mathcal{S}_n(S)\} \subseteq \left\{ L^i(\mathrm{char}_n(S)) \mid i \in [0, n-1] \right\}.
$$

Conversely, we assume that $\mathrm{char}_n(T) = L^i(\mathrm{char}_n(S))$ for some $i \in [0, n-1]$. Then, considering Equation (4.5), we have that

$$
c_0 \ldots c_{n-1} = b_i \ldots b_{n-1} b_0 \ldots b_{i-1}
$$

or, equivalently,

$$
c_j = \begin{cases} b_{i+j} & \text{if } j \in [0, n-1-i] \\ b_{j-n+i} & \text{if } j \in [n-i, n-1]. \end{cases} \tag{4.9}
$$

Equation (4.9) for $j \in [0, n-1-i]$, implies that

$$
\begin{aligned}
j \in T &\Leftrightarrow i + j \in S \\
&\Leftrightarrow j = s - i, \text{ for some } s \in S \\
&\Leftrightarrow j \in S +_n (n-i), \text{ for some } s \in S.
\end{aligned}
$$

For $j \in [n-i, n-1]$, Equation (4.9) implies that

$$
\begin{aligned}
j \in T &\Leftrightarrow j - n + i \in S \\
&\Leftrightarrow j \in S +_n (n-i), \text{ for some } s \in S.
\end{aligned}
$$

We conclude that, for all $j \in [0, n-1]$, we have $j \in T$ if and only if $j \in S +_n (n-i)$, and thus $T = S +_n (n-i)$. $\qquad\blacksquare$

Let $\mathbf{b} = 0^s w$, where w is either a binary string that starts with 1 or the empty string. We define GetSet($\mathbf{b}$) to be the set with characteristic vector $w0^s$.

> **Proposition 4.13.** *Let S be a nonempty subset of $[0, n-1]$. Then, there exists a unique $T \in \mathcal{S}_n(S)$ such that $0 \in T$ and $\mathrm{bin}_n(T)$ is a binary necklace.*

Proof. By Lemma 4.12, the set $\{\mathrm{char}_n(T) \mid T \in \mathcal{S}_n(S)\}$ consists of all the cyclic shifts of $\mathrm{char}_n(S)$, therefore there exists a necklace $\mathbf{b}$ among them. Since there does not exist a lexicographically smaller cyclic shift of $\mathbf{b}$, this must be of the form $\mathbf{b} = 0^s w$, where $s \in [0, n-2]$ and w starts and ends with 1. Let $T = \mathrm{GetSet}(\mathbf{b}) = \mathrm{GetSet}(0^s w)$. Then T is the set with characteristic vector $w0^s$, which implies that $0 \in T$ and that $\mathrm{bin}_n(T) = 0^s w = \mathbf{b}$, so we conclude that $\mathrm{bin}_n(T)$ is a

necklace. Next, we show that $T \in \mathcal{S}_n(S)$. From the definition of $\mathbf{b}$, there exists some $U \in \mathcal{S}_n(S)$ such that

$$\mathrm{char}_n(U) = \mathbf{b} = 0^s w.$$

This implies that the minimum element in U is s and thus

$$\mathrm{char}_n(U +_n (-s)) = w0^s = \mathrm{char}_n(T),$$

which means that

$$T = U +_n (-s). \tag{4.10}$$

Since $U \in \mathcal{S}_n(S)$, by Equation (4.4) there exists some i such that

$$U = S +_n i. \tag{4.11}$$

From Equations (4.10) and (4.11), we conclude that $T = S +_n (i - s) \in \mathcal{S}_n(S)$. We have shown the existence of the set T in question; it remains to show its uniqueness. Let $T' \in \mathcal{S}_n(S)$ such that $0 \in T'$ and $\mathrm{bin}_n(T')$ is a necklace. Since T and T' are in $\mathcal{S}_n(S)$, we have that T' we have that $\mathrm{bin}_n(T)$ and $\mathrm{bin}_n(T')$ are cyclic shifts of each other and since they are both necklaces, we have $\mathrm{bin}_n(T) = \mathrm{bin}_n(T')$ and

$$T' = \mathrm{GetSet}(\mathrm{bin}_n(T')) = \mathrm{GetSet}(\mathrm{bin}_n(T)) = T,$$

which completes the proof ▢

Proposition 4.13 gives a criterion for choosing a unique element from $\mathcal{S}_n(S)$, for every $S \subseteq [0, n-1]$. In other words, it provides a notion of a canonical representative from each equivalent class.

> **Definition 4.14 (Canonical set).** A set $S \subseteq [0, n-1]$ is *canonical* if either $S = \emptyset$, or $0 \in S$ and $\mathrm{bin}_n(S)$ is a necklace. Furthermore, we denote by C_n the set that contains all the canonical subsets of $[0, n-1]$.

Algorithmic generation of canonical representatives

Next, we exploit a correspondence between canonical sets and binary necklaces to efficiently generate all the canonical subsets of $[0, n-1]$. We recall that $\mathcal{B}_n$ is the set of all the binary necklaces of length n.

> **Proposition 4.15.** *The mapping* $\mathrm{bin}_n : C_n \to \mathcal{B}_n$ *is a bijection, and its inverse is the mapping* GetSet.

Proof. We have that $\mathrm{bin}_n(\emptyset) = 0^n$ and $\mathrm{GetSet}(0^n) = \emptyset$, so we only need to examine nonempty canonical subsets $S \subseteq [0, n-1]$. By Definition 4.14, $\mathrm{bin}_n(S)$ is a nonzero necklace of length n, hence bin_n is indeed a mapping from C_n to B_n. Let $\mathbf{b} \in B_n$. Then $\mathbf{b} = 0^s w$, for some $s \in [0, n-2]$ and w starting with 1. Hence $T = \mathrm{GetSet}(\mathbf{b})$ has characteristic vector $w0^s$, which implies that $0 \in T$. Furthermore, we have that $\mathrm{bin}_n(T) = \mathbf{b}$, which is a necklace. We conclude

---

Algorithm 2 Generation of all the nonzero elements in $\mathcal{B}_n$ [82].

1: **procedure** BINARYNECKLACES(**b**)
2:      Output **b**
3:      $done \leftarrow$ **false**
4:      **while** not $done$ **do**
5:          $\mathbf{b} \leftarrow L(\mathbf{b})$
6:          $\mathbf{b}' \leftarrow \tau(\mathbf{b})$
7:          **if** b' is a necklace **then**
8:              BINARYNECKLACES(**b**')
9:          **else**
10:              $done \leftarrow$ **true**
11: **main;**
12: BINARYNECKLACES($0^{n-1}1$)

---

that GetSet is a mapping from B_n to C_n and it is the inverse is bin_n when restricted to C_n.   ∎

We take advantage of Proposition 4.15 to generate the sets in C_n relying on an algorithm for the generation of the binary necklaces of length n due to Ruskey et al. [82], which we present next. For $b \in 0, 1$, let $\bar{b}$ denote the binary complement of b. For a binary string $\mathbf{b} = b_0 \cdots b_{n-1}$ we define

$$\tau(\mathbf{b}) = b_0 \cdots b_{n-2}\overline{b_{n-1}}.$$

In [82], Ruskey et al. consider a tree $T_{\mathcal{B}_n}$ as follows:

- the root of $T_{\mathcal{B}_n}$ is $0^{n-1}1$, and

- for every node **b** of $T_{\mathcal{B}_n}$, its children —if any— are the necklaces

$$\tau(L^i(\mathbf{b})), i \in [1, r],$$

  where $r + 1 \leq n$ is the smallest i such that $L^i(\mathbf{b})$ is not a binary necklace.

From the definition of $T_{\mathcal{B}_n}$, it follows that its nodes are binary necklaces of length n; conversely, every binary necklace is a node of $T_{\mathcal{B}_n}$ [82, Lemma 7]. Furthermore, every necklace appears as a node exactly once [82, Theorem 5]. This is reflected in the fact that a node **b** does not have children among $\tau(L^i(\mathbf{b}))$, $i \in [r, n - 1]$, since it is proven that a string of this form is either not a necklace, or it is a necklace but it is also the child of a previous node.

The procedure BINARYNECKLACES in Algorithm 2, which is presented in [82], is the algorithmic implementation of the definition of $T_{\mathcal{B}_n}$. The algorithm traverses the tree recursively from the root and outputs every nonzero binary necklace exactly once. While generating the children of a necklace **b** in the tree, at most one is examined which is *not* a necklace. Thus, the total number of nodes examined is at most $2|\mathcal{B}_n|$.

Theorem 4.16 ([82]). *The output of Algorithm 2 consists of all the nonzero binary necklaces of length n, without repetitions.*

Example 4.17 (Algorithm 2 for $n = 6$). The output of BINARYNECKLACES(000001) is

$$000001, 000011, 000111, 001111, 011111, 001101$$
$$011011, 000101, 001011, 010111, 010101, 001001.$$

The tree $T_{\mathcal{B}_6}$ is shown Figure 4.2; the sets underneath the binary strings are discussed in a later example and can be ignored for now. The crossed out strings are *not* nodes of $T_{\mathcal{B}_6}$; they are the strings that were found not to be necklaces in Line 7 of Algorithm 2. When encountering such strings, the algorithm backtracks. We observe that there are 13 binary necklaces of length 6, also counting the all-zero 6-tuple, so $|\mathcal{B}_6| = 13$. A total of 23 checks were performed, so indeed the number of checks is less than $2|\mathcal{B}_6| = 26$.

We now turn our focus on applying Algorithm 2 to generate the sets in C_n uniquely. Since Algorithm 2 generates all the elements in $\mathcal{B}_n$ exactly once and, by Proposition 4.15, GetSet is a bijection between $\mathcal{B}_n$ and C_n, we can simply run Algorithm 2, and for each **b** in the output, obtain the canonical set GetSet(**b**). However, we show a slightly different but equivalent way of achieving our goal that is more useful later in the section. First, we consider a tree T_{C_n} whose nodes are nonempty canonical subsets of $[0, n-1]$, as follows:

- the root is $\{0\}$, and

- for every node S, its children —if any— are the sets

$$S \cup \{i\}, i \in [\max(S) + 1, r] \tag{4.12}$$

where $r + 1$ is the smallest $j \leq n - 1$ such that $S \cup \{i\}$ is not canonical.

We show that the nodes of T_{C_n} are precisely the elements of C_n and that each node appears exactly once.

Lemma 4.18. *Let S be a nonempty subset of $[0, n-1]$. Then, for all $j \in [1, n - \max(S) - 1]$, we have that*

$$S \cup \{\max(S) + j\} = \text{GetSet}(\tau(L^j(\text{bin}_n(S)))). \tag{4.13}$$

Proof. For a nonempty subset $S \subseteq [0, n-1]$, its image under bin_n is given by

$$\text{bin}_n(S) = 0^{n-\max(S)-1} b_0 \cdots b_{\max(S)},$$

where $b_i = 1$ if and only if $i \in S$. Then, for every $j \in [1, n - \max(S) - 1]$, we have that

$$\tau(L^j(S)) = 0^{n-(\max(S)+j)-1} b_0 \cdots b_{\max(S)} 0^{j-1} 1$$
$$= \text{bin}_n(S \cup \{\max(S) + j\}). \tag{4.14}$$

By Proposition 4.15, GetSet is the inverse of bin_n, therefore Equation (4.14) is equivalent to Equation (4.13). $\qquad\blacksquare$
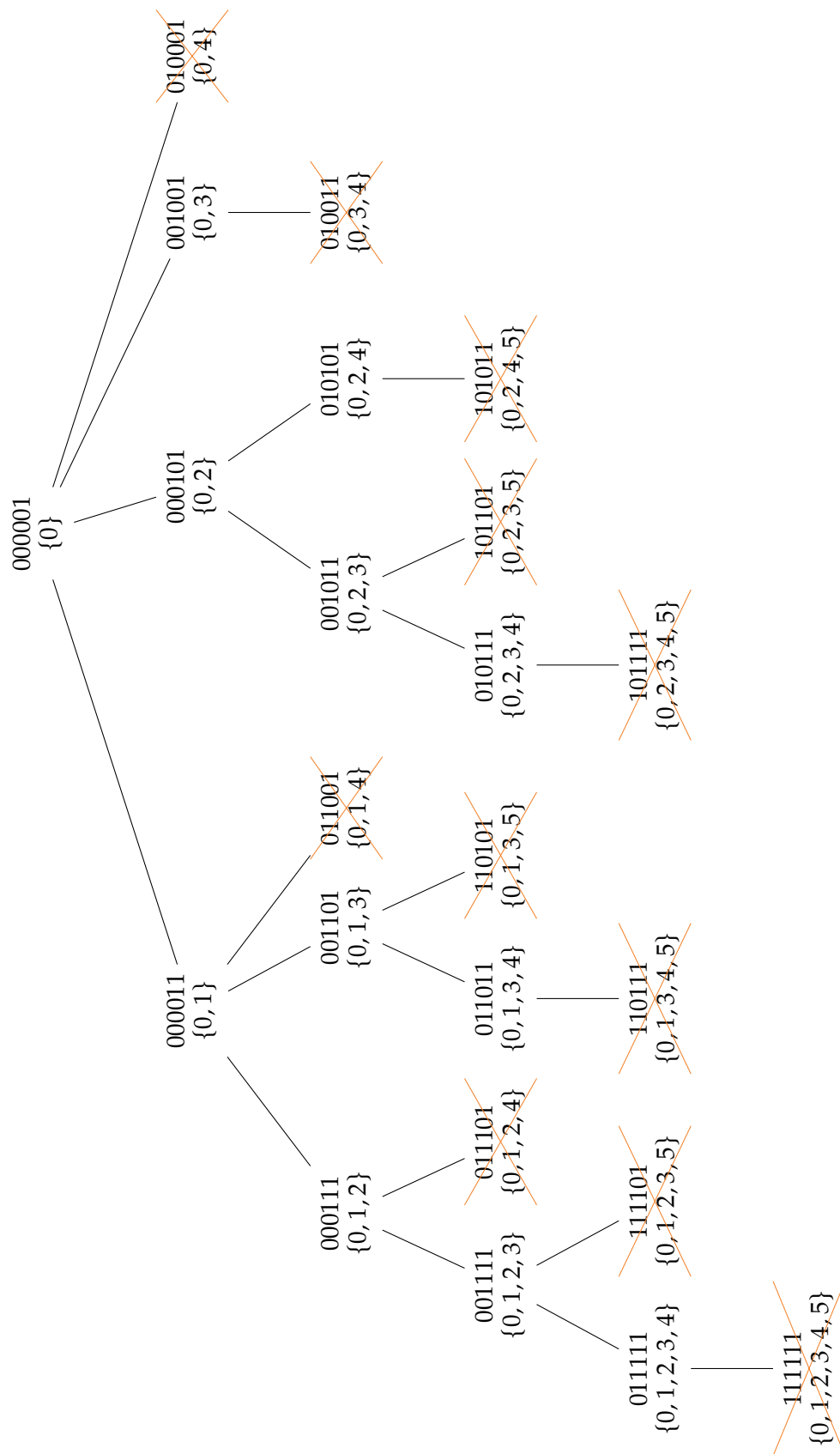
Figure 4.2. The trees $T_{\mathcal{B}_6}$ and T_{C_6}

Algorithm 3 Generation of the nonempty sets in C_n

 1: **procedure** CANONICALSUBSETS(S,n)
 2:     Output S
 3:     *done* $\leftarrow$ False
 4:     $j = \max(S) + 1$
 5:     **while** not *done* and $j \leq n - 1$ **do**
 6:         **if** $\text{bin}(S \cup \{j\})$ is a necklace **then**
 7:             CANONICALSUBSETS($S \cup \{j\}$,n)
 8:             $j \leftarrow j + 1$
 9:         **else**
10:             *done* $\leftarrow$ True
11: **Main;**
12: CANONICALSUBSETS($\{0\}$, n)

The mapping bin_n and its inverse GetSet is a bijection between the nodes of the trees $T_{\mathcal{B}_n}$ and T_{C_n} which, by Lemma 4.18, preserves the parent-child relation of nodes. It follows that, since the nodes of $T_{\mathcal{B}_n}$ are the elements of $\mathcal{B}_n$ without repetitions, then the nodes of T_{C_n} are all the elements of C_n without repetitions.

The procedure CANONICALSUBSETS in Algorithm 3 is the algorithmic implementation of the definition of T_{C_n}. It follows from the above discussion that CANONICALSUBSETS generates all the nonempty elements of S_n exactly once.

The tree $T_{\mathcal{B}_6}$ is shown Figure 4.2; the sets underneath the binary strings are discussed in a later example and can be ignored for now. The crossed out strings are *not* nodes of $T_{\mathcal{B}_6}$; they are the strings that were found not to be necklaces in Line 7 of Algorithm 2. When encountering such strings, the algorithm backtracks.

> ## Example 4.19 (Algorithm 3 for $n = 6$). The output of CANONICALSUBSETS($\{0\}$) is
>
> $$\{0\}, \{0,1\}, \{0,1,2\}, \{0,1,2,3\}, \{0,1,2,3,4\}, \{0,1,3\},$$
> $$\{0,1,3,4\}, \{0,2\}, \{0,2,3\}, \{0,2,3,4\}, \{0,2,4\}, \{0,3\}.$$
>
> The tree T_{C_6} is shown in Figure 4.2, overlapping with the tree $T_{\mathcal{B}_6}$, which demonstrates how bin_6 and GetSet are bijections between the nodes that respect the parent-child relations. The crossed out sets correspond to the sets that are shown not to be canonical in Line 6 of Algorithm 3.

4.2.3 A backtracking algorithm to search for covering subarrays

Overview

It follows from Proposition 4.7 that a subset S of $[0, [t]_q - 1]$ is a feasible solution to Problem 1 if and only if every set in $S_{[t]_q}(S)$ is also a feasible solution. Therefore, considering that all

the sets in an equivalence class have the same size, we have for an optimal solution S that the canonical representative in $\mathcal{S}_{[t]_q}(S)$ is also an optimal solution. We conclude that there exists a solution of Problem 1 in $C_{[t]_q}$. In this section, we use this fact and the framework of Algorithm 3 to give an algorithm that solves Problem 1. To introduce this algorithm we need several auxiliary results.

First, we state the optimization problem that we want to solve. From now on, we fix a set $P = \{\alpha_0, \ldots, \alpha_{l-1}\}$ of primitive elements of $\mathbb{F}_{q^t}$ and use the following terms.

- A *feasible solution* is a set $S \in C_{[t]_q}$ that either has size at most $t-1$, or it has size at least t and for every $I \subseteq S$ with $|I| = t$, there exists $i \in [0, l-1]$ such that $\mathcal{A}_0(\alpha_i, I)$ is an OA(t, t, q).

- An *optimal solution* is a feasible solution of maximum size; this is a solution to Problem 1.

- The *set of candidates* for a feasible solution S, denoted Candidates(S), is given by

$$\text{Candidates}(S) = \left\{ x \in [\max(S) + 1, [t]_q - 1] \mid S \cup \{x\} \text{ is a feasible solution} \right\}.$$

We observe that if S is a feasible solution with size at most $t-2$, then

$$\text{Candidates}(S) = [\max(S) + 1, [t]_q - 1].$$

Calculation of the set of candidates

In order to use a backtracking algorithm to find an optimum solution, we first need to determine a way of calculating efficiently the set Candidates(S), for a feasible solution S. For this, we use a recursive algorithm that is based on Lemma 4.20, that follows. For $I \subset [1, [t]_q - 1]$ we define

$$U_P(I) = \left\{ j \in [\max(I) + 1, [t]_q - 1] \mid I \cup \{0, j\} \text{ is not a feasible solution} \right\}.$$

Furthermore, for a positive integer j, we denote

$$\text{Candidates}(S)_{>j} = \{ i \in \text{Candidates}(S) \mid i > j \}.$$

> **Lemma 4.20.** *Let S be a feasible solution with $|S| \geq t-1$, and $j \in$ Candidates(S). Furthermore, we denote*
>
> $$R(j) = \bigcup_{I \in \binom{S}{t-2}} \left(U_P(I +_{[t]_q} (-j)) +_{[t]_q} j \right).$$
>
> *Then, we have that*
>
> $$\text{Candidates}(S \cup \{j\}) = \text{Candidates}(S)_{>j} \setminus R(j).$$

Proof. "$\subseteq$" Let $d \in$ Candidates$(S \cup \{j\})$. Then, $d > j$ and $S \cup \{j, d\}$ is a feasible solution. Hence, $S \cup \{d\}$ is a feasible solution as a subset of a feasible solution, which means that $d \in$ Candidates$(S)_{>j}$. It remains to show that $d \notin R(j)$; assume by means of contradiction that

this is not the case. Then, there exists $I \subset S$ with $|I| = t - 2$ and $i \in U_P(I +_{[t]_q} (-j))$ such that $d = (i + j) \bmod [t]_q$. Let

$$J = \left(I +_{[t]_q} (-j)\right) \cup \{0, i\}.$$

Then, from the definition of i and U_P we have that J is not a feasible solution. By Proposition 4.7, this implies that $J +_{[t]_q} j$ is not a feasible solution either. However, we have that

$$
\begin{aligned}
J +_{[t]_q} j &= \left(\left(I +_{[t]_q} (-j)\right) \cup \{0, i\}\right) +_{[t]_q} j \\
&= I \cup \{j, (i + j) \bmod [t]_q\} \\
&= I \cup \{j, d\} \\
&\subseteq S \cup \{j, d\},
\end{aligned}
$$

hence $J +_{[t]_q} j$ is a feasible solution as a subset of the feasible solution $S \cup \{j, d\}$, a contradiction.

"$\supseteq$" Let $d \in \text{Candidates}(S)_{>j} \setminus R(j)$, and assume by means of contradiction that $d \notin \text{Candidates}(S \cup \{j\})$. Then, there exists $I \subset S$ with $|I| = t - 2$ such that $I \cup \{j, d\}$ is not a feasible solution. Let

$$
\begin{aligned}
J &= \left(I \cup \{j, d\}\right) +_{[t]_q} (-j) \\
&= \left(I +_{[t]_q} (-j)\right) \cup \{0, d - j\}
\end{aligned}
$$

Since J is shift-equivalent to $I \cup \{j, d\}$, then by Proposition 4.7 it is not a feasible solution either and hence

$$d - j \in U_P(I +_{[t]_q} (-j)),$$

which implies that $d \in R(j)$, contradicting our initial assumption about d. ∎

Lemma 4.20 gives a recursive way of calculating the set of candidates for a feasible solution, which we implement in the procedure COMPUTECAND shown in Algorithm 4. This takes as input a feasible solution S, an element $j \in \text{Candidates}(S)$ as well as the set $\text{Candidates}(S)$ and outputs $\text{Candidates}(S \cup \{j\})$.

The algorithm

We now review Algorithm 5. The procedure FINDCA takes as input $(S, \text{Candidates}(S))$, where S is a feasible solution. It is initiated with input $(\{0\}, [1, [t]_q - 1])$; by the time it terminates, the global variable *Best* holds an optimum solution; this is also the solution to Problem 1. Next, we go through the procedure in more detail.

- In every recursive run, the size of the input S is compared to that of the largest feasible solution found at the time, which is stored in the global variable *Best*. If the size of S is larger, then it is the new best feasible solution and it is stored in the variable *Best*. This is shown in Lines 3 and 4.

- All the successive runs of the procedure with input S have inputs that are subsets of $S \cup \text{Candidates}(S)$ and thus have size at most $|S| + |\text{Candidates}(S)|$. If this is no larger than

---

Algorithm 4 Update of the set Candidates(S) as per Lemma 4.20

1: $j \in$ Candidates(S)
2: Returns Candidates($S \cup \{j\}$)
3: **procedure** COMPUTECAND($S, j,$ Candidates(S))
4:      **if** Candidates(S)$_{>j}$ = $\emptyset$ **then**
5:          **return** $\emptyset$
6:      **if** $|S| < t - 1$ **then**
7:          **return** Candidates(S)$_{>j}$
8:      **else**
9:          $C \leftarrow$ Candidates(S)$_{>j}$
10:         **for** $I \in \binom{S}{t-2}$ **do**
11:             $X \leftarrow \{(i - j) \bmod [t]_q | i \in I\}$ ▷ $X = I +_{[t]_q} (-j)$
12:             $Y \leftarrow \{(u + j) \bmod [t]_q | u \in U_P(X)\}$ ▷ $Y = U_P(X) +_{[t]_q} j$
13:             $C \leftarrow C \setminus Y$
14:             **if** $C = \emptyset$ **then**
15:                 **return** $\emptyset$
16:         **return** C

---

the feasible solution stored in $Best$, then none of the inputs in the successive runs are a better feasible solution and therefore the algorithm backtracks. This is accomplished in Lines 5 and 6.

- In Line 7 we perform pruning as follows. For a feasible solution S with Candidates(S) = $\{s_0, \ldots, s_{r-1}\}$, the algorithm is not run recursively for any of the children $S \cup \{s_i\}$ with

$$i > |S| + |\text{Candidates}(S)| - |Best|.$$

  This is because, for every such i, all the subsequent runs of the procedure with input $S \cup \{s_i\}$ have inputs subsets of $S \cup \{s_{i+1}, \ldots, s_{r-1}\}$ which is no larger than the feasible solution stored in $Best$.

- The check in Line 8 causes the algorithm to recurse only for the children that are canonical. This is done to follow framework of Algorithm 3, which guarantees that the search is restricted to canonical sets.

The results of our experimental runs of the algorithm are discussed in Section 4.4.

We close the section with a rough estimate for the number of candidate solutions that are examined in Algorithm 4. First, we note that for any optimal solution S we have that Candidates(S) = $\emptyset$. Therefore, the nodes of the tree $T_{C_{[t]_q}}$ visited by the algorithm are among the nodes of size up to m, where m is the size of an optimal solution. Let N_i be the number of nodes of size i in $T_{C_{[t]_q}}$ —which is also the number of binary necklaces of length $[t]_q$ and weight i— and let $N_{\leq m} = \sum_{i=0}^{m} N_i$ be the number of nodes with weight at most m. It is known

---

Algorithm 5 Backtracking algorithm for solving Problem 1

1: **procedure** FindCA(S, Candidates(S))   ▷ Let Candidates(S) = $\{s_0, \ldots, s_{r-1}\}$
2:   **global** $Best$
3:   **if** $r > |Best|$ **then**
4:     $Best \leftarrow S$
5:   **if** $|Best| \geq |S| + |$Candidates(S)$|$ **then**
6:     **return**
7:   **while** not $done$ and $i \leq |S| + |$Candidates(S)$| - |Best|$ **do**
8:     **if** bin($S \cup \{s_i\}$) is a necklace **then**
9:       $C \leftarrow$ ComputeCand(S, s_i, Candidates(S))   ▷ $C = $ Candidates($S \cup \{s_i\}$)
10:      FindCA($S \cup \{s_i\}, C$)
11:      $i \leftarrow i + 1$
12:    **else**
13:      $done \leftarrow$ True
14: **global** $Best \leftarrow \{0\}$
15: FindCA($\{0\}, \{1, \ldots, [t]_q - 1\}$)
16: Output $Best$

(see for example [36, 83]) that the number of binary necklaces of length n and weight i is

$$\frac{1}{n} \sum_{j | \gcd(i, n-i)} \varphi(j) \binom{n/j}{i/j},$$

where φ is Euler's phi function, that is, $\varphi(j)$ is the number of integers in $[1, j-1]$ that are coprime to j. It follows that

$$N_{\leq m} = \sum_{i=0}^{m} N_i = \frac{1}{[t]_q} \sum_{j | \gcd(i, [t]_q - i)} \varphi(j) \binom{[t]_q / j}{i/j}. \tag{4.15}$$

This provides an upper bound for the number of candidate solutions in the search space. Since our algorithm follows the framework of Algorithm 2, this implies that at most $2N_{\leq m}$ nodes are visited by Algorithm 5. This bound is not tight since not all nodes are feasible solutions and, furthermore, feasible candidates are also eliminated in Lines 5 and 7 of Algorithm 5. Finally, we note that in comparison a very naive algorithm would require checking $2^{[t]_q}$ subsets of columns, whereas the less naive approach of our algorithm without the isomorphism pruning that uses binary necklaces, would require checking up to $\sum_{i=0}^{m} \binom{[t]_q}{i}$ nodes, where m is the size of an optimal solution.

4.3 The choice of primitive elements

In this section we give an algorithmic answer to Problem 2. A straightforward approach is to consider every possible set $P = \{\alpha_0, \ldots, \alpha_{l-1}\}$ of l distinct primitive elements of $\mathbb{F}_{q^t}$, and run

Algorithm 5 in order to find the solution S_P to Problem 1.Then, for a set S_P with maximum size, we have that P is a solution to Problem 2. By Lemma 2.15 there exist exactly $\phi(q^t - 1)$ distinct primitive elements of $\mathbb{F}_{q^t}$, hence this approach requires running Algorithm 5 for all the $\binom{\phi(q^t-1)}{l}$ choices for the set P.

In this section we show that by considering a particular subset of primitive elements, it suffices to run Algorithm 5 at most $\binom{\phi([t]_q/te)}{l}$ times, where p is a prime such that $q = p^e$. More precisely, we create $\varphi([t]_q/te)$ classes of elements of $\mathbb{F}_{q^t}$ with the property that two primitive elements are in the same class if and only if their corresponding cyclic trace arrays have equivalent coverage properties in a sense that we strictly define later. Then we prove that it suffices to carry out Algorithm 5 only for l-sets of representatives from the classes that contain primitive elements, which means that at most $\binom{\phi([t]_q/te)}{l}$ runs are required. To define these classes and their representatives, we need the notion of cyclotomic cosets.

> **Definition 4.21 (Cyclotomic cosets).** Let p be a prime, w be a positive integer coprime to p, and $i \in \mathbb{Z}_w^\times$. Then, the *cyclotomic coset of p modulo w that contains i* is the set
>
> $$C_{p,w}^i = \left\{ ip^r \bmod w \mid r \in \mathbb{Z}, r \geq 0 \right\}.$$

We can use cyclotomic cosets to partition $\mathbb{Z}_w^\times$ as follows.

> **Lemma 4.22 (Partition of $\mathbb{Z}_w^\times$ using cyclotomic cosets).** *For a prime power p and positive integer w coprime to p, there exists a set $\Gamma_{p,w} \subset \mathbb{Z}_w^\times$ with the property that*
>
> $$\mathbb{Z}_w^\times = \bigcup_{i \in \Gamma_{p,w}} C_{p,w}^i, \tag{4.16}$$
>
> *and $C_{p,w}^i \cap C_{p,w}^j = \emptyset$ for all $i, j \in \Gamma_{p,w}, i \neq j$.*

Proof. First, for any $i \in \mathbb{Z}_w^\times$ and for every nonnegative integer r, we have that $\gcd(ip^r, w) = 1$, since both i and p are coprime to w, which shows that indeed $C_{p,w}^i \subset \mathbb{Z}_w^\times$. Now, let $j \in \mathbb{Z}_w^\times \setminus C_{p,w}^i$ and suppose by means of contradiction that $C_{p,w}^i \cap C_{p,w}^j \neq \emptyset$. Then, there exist nonnegative integers r_1, r_2 such that

$$ip^{r_1} \equiv jp^{r_2} \ (\bmod \ w). \tag{4.17}$$

Without loss of generality, we assume that $r_1 \geq r_2$. Then, Equation (4.17) implies that

$$p^{r_2}(j - ip^{r_1-r_2}) \equiv 0 \ (\bmod \ w),$$

and since $\gcd(p, w) = 1$, it follows that $j \equiv ip^{r_1-r_2} \ (\bmod \ w)$. The latter means that $j \in C_{p,w}^i$, which contradicts our initial assumption about j. $\quad\blacksquare$

> **Definition 4.23 (Cyclotomic coset leaders).** The elements of $\Gamma_{p,w}$ in Lemma 4.22 are *cyclotomic coset leaders of p modulo w.*

Next, we define the notion of equivalent coverage that we mention earlier.

> **Definition 4.24 (Arrays with equivalent coverage).** Let $t \geq 2$, and A_1, A_2 be $N \times k$ arrays with elements from an alphabet of the same finite size. We denote C_i, D_i, $i \in [0, k-1]$ their columns, respectively. Then, A_1 *and* A_2 *have the same t-coverage* if for every $I \subseteq [0, k-1]$ with $|I| = t$, we have that $\{C_i \mid i \in I\}$ is covered if and only if $\{D_i \mid i \in I\}$ is covered.

The main theorem of this section is the following.

> **Theorem 4.25.** *Let q be a power of a prime p, t be a positive integer with $t \geq 2$, and α be a primitive element of $\mathbb{F}_{q^t}$. Then, the following hold.*
>
> 1. *For any primitive element $\beta \in \mathbb{F}_{q^t}$, there exists $i \in \Gamma_{p,[t]_q}$ such that α^i is also primitive and $\mathcal{A}_0(\beta)$ and $\mathcal{A}_0(\alpha^i)$ have the same t-coverage.*
>
> 2. *For all $i, j \in \Gamma_{p,[t]_q}$ with $i \neq j$, we have that $\mathcal{A}_0(\alpha^i)$ and $\mathcal{A}_0(\alpha^j)$ do not have the same t-coverage.*

Remark 4.26. Before we give the proof of Theorem 4.25, we discuss its implications regarding Problem 2. First, we observe that we can write $\Gamma_{p,[t]_q} = X \cup X'$ where

$$X = \{i \in \Gamma_{p,[t]_q} \mid \text{ there exists } j \in C^i_{p,[t]_q} \text{ such that } \alpha^j \text{ is primitive}\}$$
$$= \{i \in \Gamma_{p,[t]_q} \mid \text{ there exists } j \in C^i_{p,[t]_q} \text{ such that } \gcd(j, q^t - 1) = 1\},$$

and $X' = \Gamma_{p,[t]_q} \setminus X$. Without loss of generality, we can choose the elements of $\Gamma_{p,[t]_q}$ so that α^i is primitive for every $i \in X$. Then, it follows from Theorem 4.25 that in order to solve Problem 2, it suffices to run Algorithm 5 for $P = \{\alpha^{i_0}, \ldots, \alpha^{i_{l-1}}\}$, for all the l-sets $\{i_0, \ldots, i_{l-1}\} \in \binom{X}{l}$. From the next proposition we have that $|\Gamma_{p,[t]_q}| = \phi([t]_q)/te$, where $q = p^e$ for a prime p. Hence, we conclude that to solve Problem 2, it suffices to run Algorithm 5 at most $\binom{\phi[t]_q/te}{l}$ times.

> **Proposition 4.27.** *Let p be a prime, and e, q, t be integers with $e > 0$, $q = p^e$, $t \geq 2$. Then, we have that $|C^i_{p,[t]_q}| = te$, for all $i \in \mathbb{Z}^\times_{[t]_q}$.*

Proof. The size of $C^i_{p,[t]_q}$ is equal to the smallest positive integer r such that $ip^r \equiv i \pmod{[t]_q}$, which is equivalent to $[t]_q | p^r - 1$, since $\gcd(i, [t]_q) = 1$. Now, $[t]_q | q^t - 1 = p^{te} - 1$, and thus $p^{te} \equiv 1 \pmod{[t]_q}$. We note that, by its definition, r is the order of p in $\mathbb{Z}^\times_{[t]_q}$ and therefore $p^{te} \equiv 1 \pmod{[t]_q}$ implies that $r | te$, hence $r \leq te$. We assume by means of contradiction that $r < te$. Then, since $r | te$, it must be $r \leq te/2$. On the other hand, since $[t]_q | p^r - 1$, we have that

$$p^r - 1 \geq [t]_q > p^{te-e} - 1,$$

and thus $r > te - e$. Then $te/2 > te - e$ which simplifies to $t < 2$, contradicting our assumption that $t \geq 2$. We conclude that $r = te$. $\qquad\blacksquare$

The rest of the section is dedicated to the proof of Theorem 4.25, which we present after Lemmas 4.28, 4.29, 4.30 and 4.31.

Lemma 4.28. *Let q be a prime power, t be an integer with $t \geq 2$, and α, β primitive elements of $\mathbb{F}_{q^t}$. Then, $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage if and only if there exists $\gamma \in \mathbb{F}_{q^t}$ such that, for all $s \in [0, q^t - 2]$, $\mathrm{Tr}_{q^t/q}(\alpha^s) = 0$ if and only if $\mathrm{Tr}_{q^t/q}(\gamma\beta^s) = 0$.*

Proof. We denote the column vectors of $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ by $A_0, \ldots, A_{[t]_q-1}$, and $B_0, \ldots, B_{[t]_q-1}$, respectively.

"$\Leftarrow$" Let $I \subseteq [0, [t]_q - 1]$ such that $|I| = t$ and $\{A_i \mid i \in I\}$ is covered; we need to show that $\{B_i \mid i \in I\}$ is also covered. We suppose by means of contradiction that this is not the case. Then, by Statement 6 of Proposition 3.10, there exists a row of $\mathcal{A}(\beta)$ that has zeros in the entries corresponding to the columns B_i, $i \in I$. In other words, there exists some $r \in [0, q^t - 2]$ such that

$$\left(\mathcal{A}(\beta)_{r,i}\right)_{i \in I} = \left(\mathrm{Tr}_{q^t/q}(\alpha^r \alpha^i)\right)_{i \in I} = (0, \ldots, 0).$$

From the definition of $\mathcal{A}(\beta)$, the latter means that there exists $\gamma \in \mathbb{F}_{q^t}^*$ such that $\mathrm{Tr}(\gamma\beta^i) = 0$ for all $i \in I$. Setting $\gamma = \alpha^r$, from our assumptions it follows that $\mathrm{Tr}_{q^t/q}(\alpha^i) = 0$ for all $i \in I$, which means that the first row of the columns A_i, $i \in I$ is a row of zeros. Then, by Statement 6 of Proposition 3.10, the columns A_i, $i \in I$ is uncovered; this contradicts our assumptions.

"$\Rightarrow$" By Lemma 2.44, $\alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q^\times$, thus for every $s \in [0, q^t - 2]$ we have that $\alpha^s = c\alpha^u$, where $u \in [0, [t]_q - 1]$, $u \equiv s \pmod{w}$, and $c \in \mathbb{F}_q$. Hence, from the linearity of the trace over $\mathbb{F}_q$, it is sufficient to prove this direction for all $s \in [0, [t]_q - 1]$. Now, $\ker(\mathrm{Tr})$ is a vector space over $\mathbb{F}_q$ with dimension $t - 1$, as implied by Proposition 2.19. Since α is primitive, it follows from the above that there exist $i_1, \ldots, i_{t-1} \in [0, [t]_q - 1]$ such that $\mathcal{B} = \{\alpha^{i_1}, \ldots, \alpha^{i_{t-1}}\}$ is also a basis for $\ker(\mathrm{Tr})$. This means that $\alpha^{i_1}, \ldots, \alpha^{i_{t-1}}$ are linearly independent and the first row of $\mathcal{A}(\alpha)$ has zeros at the columns A_i, $i \in \{i_1, \ldots, i_{t-1}\}$. Then, from Proposition 3.10 and our assumption that $\mathcal{A}(\alpha)$ and $\mathcal{A}(\beta)$ have the same t-coverage, we have that $\beta^{i_1}, \ldots, \beta^{i_{t-1}}$ are also linearly independent, and there exists a row of $M(\beta)$ with zeros at the columns B_i, $i \in \{i_1, \ldots, i_{t-1}\}$. The latter means that there exists $\gamma \in \mathbb{F}_{q^t}^*$ such that $\mathrm{Tr}(\gamma\beta^i) = 0$ for all $i \in \{i_1, \ldots, i_{t-1}\}$. We conclude that $\mathcal{B}' = \{\gamma\beta^{i_1}, \ldots, \gamma\beta^{i_{t-1}}\}$ is a basis for $\ker(\mathrm{Tr})$.

Now, suppose that $\mathrm{Tr}(\alpha^s) = 0$ for some $s \in [0, [t]_q - 1]$. Then, by Proposition 3.10, the set of columns $\{A_{i_1}, \ldots, A_{i_{t-1}}, A_s\}$ of $\mathcal{A}(\alpha)$ is not covered and thus the set of columns $\{B_{i_1}, \ldots, B_{i_{t-1}}, B_s\}$ of $\mathcal{A}(\beta)$ is also not covered, from our assumption that $\mathcal{A}(\alpha)$ and $\mathcal{A}(\beta)$ have the same t-coverage. Hence there exists a row of $\mathcal{A}(\alpha)$ with zeros at the columns $B_{i_1}, \ldots, B_{i_{t-1}}, B_s$, and so there exists $\delta \in \mathbb{F}_{q^t}^*$ such that $\delta\beta^i \in \ker(\mathrm{Tr})$ for all $i \in \{i_1, \ldots, i_{t-1}, s\}$. Since $\mathcal{B}'$ is a basis for $\ker(\mathrm{Tr})$, we have that $\delta = c\gamma$ for some $c \in \mathbb{F}_q^\times$. Then $\delta\beta^s \in \ker(\mathrm{Tr})$ implies that $\gamma\beta^s \in \ker(\mathrm{Tr})$ from the linearity of the trace. $\blacksquare$

Lemma 4.29. *Let p be a prime, q, e, t, l be integers with $e > 0$, $q = p^e$, $t \geq 2$, and $l \in [1, q^t - 2]$. Then, $\mathrm{Tr}_{q^t/q}(x^l) = \mathrm{Tr}_{q^t/q}(x)^l$ for all $x \in \mathbb{F}_{q^t}$ if and only if $l = p^r$ for some $r \in [0, te - 1]$.*

Proof. In this proof we denote $\text{Tr} = \text{Tr}_{q^t/q}$. If $l = p^r, r \in [0, te - 1]$, then $\text{Tr}(x^l) = \text{Tr}(x)^l$ from the properties of the Frobenius automorphism in $\mathbb{F}_q$. Conversely, suppose that $\text{Tr}(x^l) = (\text{Tr}(x))^l$ for all $x \in \mathbb{F}_{q^t}$. For a polynomial f on x, we denote by $[x^n]f(x)$ the coefficient of x^n in f. We observe that

$$[x^{1+(l-1)q}]\text{Tr}(x^l) = \begin{cases} 1, & \text{if } l = 1 \\ 0, & \text{otherwise,} \end{cases} \tag{4.18}$$

and

$$[x^{1+(l-1)q}](\text{Tr}(x))^l = \begin{cases} 1, & \text{if } l = 1 \\ l, & \text{otherwise.} \end{cases} \tag{4.19}$$

If $l = 1$, then $l = p^r$ with $r = 0$. If $l > 1$, then it follows from Equations (4.18) and (4.19), and our assumption that $\text{Tr}(x^l) = \text{Tr}(x)^l$, that $l \equiv 0 \pmod{p}$. Hence $l = kp^r$ for some positive integers k, r, with $0 < r < te$, and $p \nmid k$. We have that, for all $x \in \mathbb{F}_{q^t}$,

$$\left(T(x^k)\right)^{p^r} = \text{Tr}(x^{kp^r}) = \text{Tr}(x^l) = (\text{Tr}(x))^l = \left(\text{Tr}(x)^k\right)^{p^r}. \tag{4.20}$$

Taking p^r-th roots in Equation (4.20) yields that $\text{Tr}(x^k) = (\text{Tr}(x))^k$ for all $x \in \mathbb{F}_{q^t}$. By comparing the coefficients of $\text{Tr}(x^k)$ and $(\text{Tr}(x))^k$ in the same way as we did for $\text{Tr}(x^l)$ and $(\text{Tr}(x))^l$, we have that either $k = 1$, or $k \equiv 0 \pmod{p}$. Since we have assumed that $p \nmid k$, it must be $k = 1$, and thus $l = p^r$. $\qquad\blacksquare$

> **Lemma 4.30.** *Let p be a prime, q, e, t be integers such that $e > 0$, $q = p^e$, $t \geq 2$, and α, β be primitive elements of $\mathbb{F}_{q^t}$. Then $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same coverage if and only if $\beta = \alpha^{p^r}$, for some $r \in [0, te - 1]$.*

Proof. If $\beta = \alpha^{p^r}$ for some $r \in [0, te - 1]$, then for every $s \in [0, q^t - 2]$ we have that $\text{Tr}(\beta^s) = \text{Tr}(\alpha^{sp^r}) = \text{Tr}(\alpha^s)^{p^r}$. Hence, $\text{Tr}(\beta^s) = 0$ if and only if $\text{Tr}(\alpha^s) = 0$, and thus $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage, from Lemma 4.28.

For the converse, we assume that $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage. Since α is primitive, there exists $l \in \mathbb{Z}^*_{q^t-1}$ such that $\beta = \alpha^l$. Then, from Lemma 4.28, there exists $\gamma \in \mathbb{F}_{q^t}$ such that, for all $s \in [0, q^t - 2]$, we have $\text{Tr}(\alpha^s) = 0$ if and only if $\text{Tr}(\gamma\alpha^{ls}) = 0$. Again from the primitivity of α, we have that

$$\mathbb{F}^*_{q^t} = \left\{\alpha^s \mid s \in [0, q^t - 2]\right\},$$

so we conclude from the above that there exists $\gamma \in \mathbb{F}_{q^t}$ such that, for all $x \in \mathbb{F}^*_{q^t}$, we have

$$\text{Tr}(x) = 0 \quad \text{if and only if} \quad \text{Tr}(\gamma x^l) = 0. \tag{4.21}$$

Let y be an element in some extension of $\mathbb{F}_{q^t}$ such that $\text{Tr}(\gamma y^l) = 0$. Then $\gamma y^l = z \in \ker(\text{Tr}) \subseteq \mathbb{F}_{q^t}$, and $y^l = z/\gamma \in \mathbb{F}_{q^t}$. Since $\gcd(l, q^t - 1) = 1$, the l-th root of z/γ exists, and $y = (z/\gamma)^{1/l} \in \mathbb{F}_{q^t}$. We have proved that $\text{Tr}(\gamma x^l)$ splits in $\mathbb{F}_{q^t}$. Now,

$$\text{Tr}(\gamma x^l) = \prod_{a \in \ker(\text{Tr})} \left(\gamma x^l - a\right).$$

Because $\mathrm{Tr}(\gamma x^l)$ splits in $\mathbb{F}_{q^t}$, so does $\gamma x^l - a$ for all $a \in \ker(\mathrm{Tr})$. Furthermore, the only root of $\gamma x^l - a$ is $(a/\gamma)^{1/l}$, and its degree is l; it follows that it must be

$$\gamma x^l - a = \gamma \left(x - (a/\gamma)^{1/l} \right)^l,$$

and hence

$$\mathrm{Tr}(\gamma x^l) = \prod_{a \in \ker(\mathrm{Tr})} \gamma \left(x - (a/\gamma)^{1/l} \right)^l. \tag{4.22}$$

By Equation (4.21) we have that

$$\ker(\mathrm{Tr}) = \left\{ (a/\gamma)^{1/l} \mid a \in \ker(\mathrm{Tr}) \right\},$$

and by Proposition 2.19 we have that $|\ker(\mathrm{Tr})| = q^{t-1}$, hence Equation (4.22) becomes

$$\mathrm{Tr}(\gamma x^l) = \gamma^{q^{t-1}} \prod_{a \in \ker(\mathrm{Tr})} (x - a)^l$$

$$= \gamma^{q^{t-1}} \left(\prod_{a \in \ker(\mathrm{Tr})} (x - a) \right)^l$$

$$= \gamma^{q^{t-1}} \mathrm{Tr}(x)^l. \tag{4.23}$$

By comparing the coefficient of x^l in $\mathrm{Tr}(\gamma x^l)$ and $\gamma^{q^{t-1}}(\mathrm{Tr}(x))^l$, we have that $\gamma = \gamma^{q^{t-1}}$, which means that $\gamma \in \mathbb{F}_{q^{t-1}}$. However $\gamma \in \mathbb{F}_{q^t}$, hence $\gamma \in \mathbb{F}_{q^t} \cap \mathbb{F}_{q^{t-1}} = \mathbb{F}_q$, and from the linearity of the trace over $\mathbb{F}_q$, $\mathrm{Tr}(\gamma x^l) = \gamma \mathrm{Tr}(x^l)$. Equation (4.23) then implies that $\mathrm{Tr}(x^l) = (\mathrm{Tr}(x))^l$, and by Lemma 4.29 we have that $l = p^r$, for some integer r such that $r \in [0, te - 1]$. $\quad\square$

> **Lemma 4.31.** *Let p be prime, and q, e, t integers with $e > 0$ and $q = p^e$. For all $i, j \in \mathbb{Z}^*_{q^t-1}$, we have that $\mathcal{A}_0(\alpha^i)$ and $\mathcal{A}_0(\alpha^j)$ have the same t-coverage if and only if $j \bmod [t]_q \in C^i_{p,[t]_q}$.*

Proof. Suppose that $j \bmod [t]_q \in C^i_{p,[t]_q}$. Then there exist integers r, h such that $j = ip^r + h[t]_q$, and thus $\alpha^j = c\alpha^{ip^r}$ with $c = \alpha^{[t]_q h}$. We have that

$$c^{q-1} = \alpha^{[t]_q(q-1)h} = \alpha^{(q^t-1)h} = 1,$$

which means that $c \in \mathbb{F}_q$. Then, by Theorem 2.17 and the properties of the Frobenius automorphism we have that, for all positive integers s,

$$\mathrm{Tr}(\alpha^{js}) = \mathrm{Tr}(c^s \alpha^{isp^r}) = c^s \mathrm{Tr}(\alpha^{is})^{p^r}.$$

We conclude that $\mathrm{Tr}(\alpha^{js}) = 0$ if and only if $\mathrm{Tr}(\alpha^{is}) = 0$, which implies from Lemma 4.28 that $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage.

Conversely, assume that $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage. Then, from Lemma 4.30 we have that $\alpha^j = \alpha^{ip^r}$ for some $r \in [0, te - 1]$, and thus $j \equiv ip^r \pmod{q^t - 1}$. Since $[t]_q | q^t - 1$, we also have $j \equiv ip^r \pmod{[t]_q}$, which means that $j \bmod [t]_q \in C^i_{p,[t]_q}$. $\quad\square$

We now have the necessary background to give the proof of the main result of this section.

Proof of Theorem 4.25. We begin with the first part. Let β be a primitive element of $\mathbb{F}_{q^t}$. From the primitivity of α, we have that there exists $l \in \mathbb{Z}^*_{q^t-1}$ such that $\beta = \alpha^l$. Let $u = l \bmod [t]_q$. Then $u = l + h[t]_q$ for some integer h, and thus $\alpha^u = c\alpha^l$, with $c = \alpha^{h[t]_q}$. From Lemma 2.44 we have that $c \in \mathbb{F}_q$. Hence, for any positive integer s, we have that $\mathrm{Tr}(\alpha^{us}) = c^s \mathrm{Tr}(\alpha^{ls})$ and therefore $\mathrm{Tr}(\alpha^{ls}) = 0$ if and only if $\mathrm{Tr}(\alpha^{us}) = 0$. It follows from Lemma 4.28 that $\mathcal{A}_0(\alpha)$ and $\mathcal{A}_0(\beta)$ have the same t-coverage. Since $\gcd(l, q^t - 1) = 1$, then also $\gcd(l, [t]_q) = 1$, hence $\gcd(u, [t]_q) = 1$ as well. This means $u \in \mathbb{Z}^\times_{[t]_q}$ and thus, from Equation (4.16) there exists $i \in \Gamma_{p,[t]_q}$ such that $u \in C^i_{p,[t]_q}$. From Lemma 4.31, $\mathcal{A}_0(\alpha^u)$ has the same coverage with $\mathcal{A}_0(\alpha^i)$. Since $\mathcal{A}_0(\alpha^u)$ was shown above to also have the same coverage as $\mathcal{A}_0(\beta)$, we conclude that $\mathcal{A}_0(\beta)$ has the same coverage with $\mathcal{A}_0(\alpha^i)$.

We now prove the second part. Suppose by means of contradiction that $i, j \in \Gamma_{p,[t]_q}$, $i \neq j$, and $\mathcal{A}_0(\alpha^i)$ has the same t-coverage with $\mathcal{A}_0(\alpha^j)$. Then, from Lemma 4.31 we have that $j \in C^i_{p,[t]_q}$. Thus, $C^i_{p,[t]_q} \cap C^j_{p,[t]_q} \neq \emptyset$ which means that $C^i_{p,[t]_q} = C^j_{p,[t]_q}$, as discussed just before Equation (4.16). This contradicts our assumption that $i, j \in \Gamma_{p,[t]_q}$, and we conclude that $\mathcal{A}_0(\alpha^i)$ and $\mathcal{A}_0(\alpha^j)$ do not have the same coverage. $\qquad\blacksquare$

We close this section by giving the steps for solving Problem 2 as a method.

> **Method 4.32 (Solving Problem 2 using Algorithm 5).** *Let p be prime, $q = p^e$ where e is a positive integer, $t \geq 2$, and $l \geq 2$.*
>
> 1. *Calculate the cyclotomic cosets $C^i_{p,[t]_q}$ for all $i \in \mathbb{Z}^\times_{[t]_q}$, and find a set X of coset representatives such that $C^i_{p,[t]_q}$, $i \in X$ are all the distinct cosets with the property that, for every $i \in X$, there exists $j \in C^i_{p,[t]_q}$ with $\gcd(j, q^t - 1)$. Without loss of generality, choose the elements of X so that they are all coprime to $q^t - 1$.*
>
> 2. *Pick* any *primitive polynomial of degree t over $\mathbb{F}_q$ and let α be* any *one of its roots.*
>
> 3. *For every $\{i_0, \ldots, i_{l-1}\} \in \binom{X}{l}$, set $P = \{\alpha^{i_0}, \ldots, \alpha^{i_{l-1}}\}$ and find a solution S_P to Problem 1 for P, using Algorithm 5.*
>
> 4. *Any P in the previous step that corresponds to a set S_P of the maximum size, is a solution to Problem 2.*

As discussed before, this method requires running Algorithm 5 $\binom{|X|}{l}$ times, $|X| \leq \phi([t]_q/te)$.

4.4　Implementation and experimental results

In this section we discuss our implementation of Method 4.32 and present our experimental results. These are explicit constructions of $CA(l(q^t - 1); t, k, q)$ of the form $\mathcal{A}_0(P, S)$, where P is a set of l primitive elements of $\mathbb{F}_{q^t}$, and S is a subset of $[0, [t]_q - 1]$ of size k. Our results are for $t = 4$, with the exception of a few cases for $t = 5$.

We used version 6.8 of the Sage mathematical software [88] for the precomputations that involved finite fields, whereas Algorithm 5 was implemented in version 2.7 of Python using the Cython extension [5] that translates Python code to C for increased speed. We used six computers each with an Intel Xeon CPU E5-2667 processor and 16 GB of memory, running the Scientific linux operating system.

Our experiments were as follows. We ran Method 4.32 for every q and l shown in Table 4.3a. For the cases marked with an asterisk, the method was complete and the entries in the column denoted $CA(N; 4, k, q)$ are the covering array parameters corresponding to the solution of Problem 2. For all the other cases, due to the large search space of the problem, the fourth step was not complete. More precisely, it was not possible to consider all the l-sets in $\binom{X}{l}$ and for the cases that were considered, Algorithm 5 did not terminate. For these cases, we examined up to 30 l-tuples from $\binom{X}{l}$ at random, and for each of them Algorithm 5 ran for up to a month. By the end of that period, for every choice of q and l we compared the results stored in the global variable *Best* for all the l-sets that were tested; the entries in column denoted $CA(N; 4, k, q)$ are the parameters of the corresponding arrays.

Next, we evaluate our results by comparing them with the state of art as of the time of their publication. We recall that the covering array number $CAN(t, k, q)$ is the smallest n such that a $CA(n; t, k, q)$ exists. Hence, a $CA(N; t, k, q)$ implies that N is an upper bound for $CAN(t, k, q)$. In Table 4.3a, the columns labeled PrevN contain the previously smallest known [29] upper bounds for $CAN(4, k, q)$, for the k and q of the corresponding array. Bounds in bold indicate that they are improved by our results, and the numbers of rows of the corresponding arrays, also indicated in bold, are the new smallest known upper bounds for $CAN(4, k, q)$.

More results follow recursively from the fusion operation [25] (see also page 35), where a $CA(N; t, k, q)$, a $CA(N - 2r; t, k, q - r)$ can be constructed for any $r < q$. In several cases, the result of the fusion operation on the arrays in Table 4.3a improve upon the previously best bounds in [29]; we list these cases in Table 4.3b. Although the fusion operation for all possible r was tested, the results that improved upon previous ones were only for r equal to 1 or 2.

In Table 4.5 we give the essential elements for the construction of the 21 arrays displayed in Table 4.3a that improve upon previous results. Every covering array is of the form $\mathcal{A}_0(P, C)$, where C is a subset of $[0, [4]_q - 1]$ and $P = \{\alpha^{i_0}, \ldots, \alpha^{i_{l-1}}\}$, where α and $\alpha^{i_0}, \ldots, \alpha^{i_{l-1}}$ are primitive elements of $\mathbb{F}_{q^4}$. The three columns of Table 4.5 contain the covering array parameters, the powers $i_0, \ldots, i_{l-1}$ and the subset C, respectively. The primitive element $\alpha \in \mathbb{F}_{q^4}$ depends on q; for every q considered in Table 4.5, the primitive element α that is used is the root of the primitive polynomial $P_q(x) \in \mathbb{F}_q[x]$ given in Table 4.4. In the next example we demonstrate how the covering arrays of Table 4.5 can be constructed in practice.

	q	l	CA(N;4,k,q)	PrevN	q	l	CA(N;4,k,q)	PrevN
*	2	2	CA(31;4,6,2)	21	9	2	CA(13121;4,18,9)	13113
*	3	2	CA(161;4,10,3)	159	9	3	CA(**19681**;4,42,9)	**30537**
*	3	3	CA(241;4,12,3)	189	9	4	CA(**26241**;4,50,9)	**30537**
*	3	4	CA(321;4,12,3)	189	9	5	CA(**32801**;4,82,9)	**33129**
*	4	2	CA(**511**;4,17,4)	**760**	11	2	CA(29281;4,21,11)	29271
	4	3	CA(766;4,20,4)	760	11	3	CA(**43921**;4,37,11)	**69091**
	4	4	CA(1021;4,20,4)	760	11	4	CA(**58561**;4,77,11)	**69091**
	5	2	CA(**1249**;4,16,5)	**1865**	11	5	CA(**73201**;4,125,11)	**73931**
	5	3	CA(**1873**;4,25,5)	**2845**	13	2	CA(57121;4,24,13)	57109
	5	4	CA(2497;4,23,5)	1865	13	3	CA(**85681**;4,45,13)	**136045**
	7	2	CA(4801;4,15,7)	4795	13	4	CA(**114241**;4,98,13)	**136045**
	7	3	CA(7201;4,26,7)	7189	13	5	CA(**142801**;4,170,13)	**146185**
	7	4	CA(9601;4,43,7)	9583	16	2	CA(**131071**;4,28,16)	**188401**
	7	5	CA(12001;4,47,7)	9583	16	3	CA(**196606**;4,55,16)	**315136**
	8	2	CA(8191;4,17,8)	8184	16	4	CA(**262141**;4,129,16)	**315136**
	8	3	CA(12286;4,30,8)	12272	17	2	CA(**167041**;4,29,17)	**240721**
	8	4	CA(**16381**;4,48,8)	**18880**	17	3	CA(**250561**;4,61,17)	**402577**
	8	5	CA(20476;4,65,8)	19776	17	4	CA(**334081**;4,141,17)	**402577**
	8	6	CA(24571;4,67,8)	19776	19	2	CA(**260641**;4,30,19)	**377227**
					23	2	CA(**781249**;4,35,23)	**815167**

(a) Overview of our results, where $N = l(q^4 - 1) + 1$. The columns denoted PrevN contain the previous smallest upper bounds for CAN(4, k, v); bold indicates improvement.

q	l	r	CA(N − 2r;4,k,q − r)	PrevN	q	l	r	CA(N − 2r;4,k,q − r)	PrevN
11	3	1	CA(**43919** ;4,37,10)	**57486**	17	3	2	CA(**250560**;4,61,15)	**278181**
11	4	1	CA(**58559** ;4,77,10)	**66545**	16	2	1	CA(**131069**;4,28,15)	**173727**
13	3	1	CA(**85679** ;4,45,12)	**114186**	16	3	1	CA(**196604**;4,55,15)	**277827**
13	4	1	CA(**114239** ;4,98,12)	**129345**	16	4	1	CA(**262139**;4,129,15)	**315134**
16	2	2	CA(**131067** ;4,28,14)	**147753**	17	2	1	CA(**167039**;4,29,16)	**188401**
16	3	2	CA(**196602** ;4,55,14)	**226647**	17	3	1	CA(**250559**;4,61,16)	**315136**
16	4	2	CA(**262137** ;4,129,14)	**283193**	17	4	1	CA(**334079**;4,141,16)	**315136**
17	2	2	CA(**167037** ;4,29,15)	**173800**	19	2	1	CA(**260639**;4,30,18)	**355669**

(b) The results of the fusion operation on the arrays in Table 4.3a, that improve upon previously best bounds [29], where $N = l(q^4 - 1) + 1 - 2r$. For every q and l, the CA(N − 2r;4, k, q − r) is obtained by applying the fusion operation r times to the CA(N;4, k, q) for the corresponding q and l in Table 4.3a.

Table 4.3. Overview of our results

q	Minimal polynomial in $\mathbb{F}_q[x]$ of $\alpha \in \mathbb{F}_{q^4}$	
4	$P_4(x) = x^4 + (\beta + 1)x^3 + \beta x^2 + \beta,$	$\mathbb{F}_4 = \mathbb{F}_2(\beta), \beta^2 = \beta + 1$
5	$P_5(x) = x^4 + x^3 + 2x^2 + 2$	
8	$P_8(x) = x^4 + \beta x^3 + \beta,$	$\mathbb{F}_8 = \mathbb{F}_2(\beta), \beta^3 = \beta + 1$
9	$P_9(x) = x^4 + \beta x^3 + \beta,$	$\mathbb{F}_9 = \mathbb{F}_3(\beta), \beta^2 = \beta + 1$
11	$P_{11}(x) = x^4 + 4x^3 + 2$	
13	$P_{13}(x) = x^4 + 6x^3 + 2x^2 + 2$	
16	$P_{16}(x) = x^4 + \beta^2 x^3 + \beta x^2 + \beta,$	$\mathbb{F}_{16} = \mathbb{F}_2(\beta), \beta^4 = \beta + 1$
17	$P_{17}(x) = x^4 + 6x^3 + 3$	
19	$P_{19}(x) = x^4 + x^3 + 2$	
23	$P_{23}(x) = x^4 + 9x^3 + 5$	

Table 4.4. Minimal polynomials of the primitive elements used in Table 4.5.

Example 4.33 (Construction of CA(1249; 4, 16, 5)). To obtain the CA(1249; 4, 16, 5) in the second row of Table 4.5 we need to construct $\mathcal{A}_0(P, C)$ for $P = \{\alpha, \alpha^7\}$ where α is a root of $P_5(x) = x^4 + x^3 + 2x^2 + 2$ as in Table 4.4, and

$$C = \{0, 6, 9, 15, 39, 45, 48, 54, 78, 84, 87, 93, 117, 123, 126, 132\}.$$

To do that, we construct the $(5^4 - 1) \times 16$ arrays $\mathcal{A}_{5^4/5}(\alpha, C)$ and $\mathcal{A}_{5^4/5}(\alpha^7, C)$. Let $\mathrm{Tr} = \mathrm{Tr}_{5^4/5}$. Then, for every $i \in [0, 5^4 - 2]$, the i-th row of $\mathcal{A}_{5^4/5}(\alpha, C)$ is the vector

$$\left(\mathrm{Tr}(\alpha^{i+c}) \right)_{c \in C},$$

whereas the i-th row of $\mathcal{A}_{5^4/5}(\alpha^7, C)$ is given by

$$\left(\mathrm{Tr}(\alpha^{7(i+c)}) \right)_{c \in C}.$$

The vertical concatenation of these rows and a row of zeros is a CA(1249; 4, 16, 5).

Although the results in Sections 4.2 and 4.3 can be used to search for covering arrays of any strength, the running time increases significantly for strengths $t \geq 5$. We were able to run a few cases of strength $t = 5, 6$ for small q. One notable result was a CA(485; 5, 11, 3) which improves the upper bound of CAN(5, 11, 3) from 546 to 485. This array can be constructed as $\mathcal{A}_0(\{\alpha, \alpha^{17}\}, C)$, where α is a root of $x^5 + 2x^4 + 1 \in \mathbb{F}_3[x]$, and $C = \{11i \mid i = 0, \ldots, 10\}$.

Table 4.5. Components of the new covering arrays.

$\mathcal{A}_0(\{\alpha^{i_1},\ldots,\alpha^{i_l}\},C)$	$i_1,\ldots,i_l$	C
CA(511; 4, 17, 4)	1, 31	$5i, i = 0,1,\ldots,16$
CA(1249; 4, 16, 5)	1, 7	0, 6, 9, 15, 39, 45, 48, 54, 78, 84, 87, 93, 117, 123, 126, 132
CA(1873; 4, 25, 5)	1, 7,17	0, 9, 12, 21, 24, 33, 36, 45, 48, 57, 60, 69, 72, 81, 84, 93, 96, 105, 108, 117, 120, 129, 132, 141, 144
CA(16381; 4, 48, 8)	1, 43, 421, 1324	0-14, 16, 18, 20, 22, 24, 26, 28, 31, 33, 34, 37, 41, 48, 52, 124, 125, 128, 176, 226, 230, 240, 251, 275, 279, 285, 321, 365, 432, 433, 440, 444, 452, 510,
CA(19681; 4, 42, 9)	1, 7,13	$10i, i = 0,1,\ldots,41$
CA(26241; 4, 50, 9)	1, 1129, 1273, 1329	0-3, 5, 6, 8, 9, 11, 13, 15, 16, 18, 19, 22-24, 27-29, 32-34, 38, 43, 46, 49, 54, 56, 57, 60, 65, 67, 70, 80, 97, 102, 117, 168, 201, 226, 310, 335, 358, 367, 369, 391, 458, 468, 482
CA(32801; 4, 82, 9)	1, 29, 43, 47, 139	0-81
CA(43921; 4, 37, 11)	1, 271, 3491	0, 1, 12, 13, 24, 25, 36, 37, 48, 49, 60, 61, 72, 73, 84, 85, 96, 97, 108, 109, 180, 349, 360, 409, 589, 601, 613, 660, 685, 709, 925, 937, 949, 997, 1020, 1189, 1237
CA(58561; 4, 77, 11)	1, 271, 3491, 5861	0-3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, 32, 33, 35, 36, 38, 39, 41, 42, 44, 45, 47, 48, 50, 51, 53, 54, 56, 57, 59, 60, 63, 66, 73, 76, 79, 80, 83, 86, 92, 95, 98, 101, 104, 107, 110, 192, 236, 352, 412, 423, 447, 507, 528, 546, 623, 650, 662, 694, 697, 700, 859, 921, 925, 1078, 1254
CA(73201; 4, 125, 11)	1,119, 181, 245, 397	0-50, 57-62, 69-74, 81-86, 93-107, 111-114, 176, 177, 197, 230-232, 243, 283, 300, 311, 312, 323, 324, 360-362, 418, 419, 443, 455, 469, 539, 566, 603, 673, 674, 675, 798, 824, 945, 1018, 1066, 1174, 1198, 1308, 1339, 1340
CA(85681; 4, 45, 13)	1, 313, 357	0, 1, 14, 15, 28, 29, 42, 43, 56, 57, 70, 71, 84, 85, 98, 99, 112, 113, 126, 127, 140, 141, 154, 168, 182, 238, 336, 532, 574, 686, 714, 742, 798, 1051, 1092, 1162, 1387, 1695, 1737, 1792, 1820, 1862, 1946, 1974, 2030

Continued on the next page

Table 4.5 – *Continued from the previous page*

$\mathcal{A}_0(\{\alpha^{i_1}, \ldots, \alpha^{i_l}\}, C)$	$i_1, \ldots, i_l$	C
CA(114241; 4, 98, 13)	1, 3, 213, 503	0-38, 42-44, 48, 72-74, 79-81, 83, 84, 123-126, 131, 132, 149, 150, 159, 164, 165, 183, 197, 203, 223, 225, 227, 229, 237, 240, 247, 273, 274, 292, 327, 333, 403, 406, 572, 601, 609, 617, 625, 776, 847, 966, 1115, 1288, 1299, 1359, 1386, 1480, 1669, 1750, 1866, 1952, 2098
CA(142801; 4, 170, 13)	1, 79, 109, 171, 421	0-86, 150-169, 243, 245, 247, 264-266, 268, 273, 280, 281, 454, 456, 458-462, 464, 466, 468, 502, 611, 614-619, 642, 773, 782, 797, 803, 810, 811, 828, 829, 965, 975, 977, 979, 983-987, 997, 1158, 1160, 1162, 1163, 1165, 1331, 1447, 1504, 1506, 1643, 1788, 1790, 1792, 2009, 2028, 2152
CA(131071; 4, 28, 16)	1, 601	0-3, 5, 6, 8, 11, 12, 17, 22, 23, 25, 36, 45, 46, 50, 157, 184, 352, 661, 1316, 2236, 2736, 3028, 3102, 3126, 3443
CA(196606; 4, 55, 16)	1, 4636, 11086	0-3, 5, 6, 8, 11, 12, 17, 20, 22, 26, 29, 34, 35, 39, 40, 45, 49, 54, 69, 73, 78, 91, 100, 102, 105, 111, 120, 122, 137, 146, 155, 164, 184, 208, 239, 332, 333, 395, 399, 404, 537, 598, 858, 1746, 1754, 2020, 2279, 2743, 2751, 2810, 2816, 3189
CA(262141; 4, 129, 16)	1, 295, 475, 883	0-53, 87-98, 108-110, 123-125, 129-131, 135-137, 170-173, 182, 185-187, 189-194, 199-201, 210, 223, 308, 337-340, 342, 383, 385, 412, 422, 455, 617, 635, 812, 817, 839, 841, 847, 849, 911, 933, 1438, 1499, 1929, 1938, 1994, 2239, 2758, 2782, 3328, 3383, 3675
CA(167041; 4, 29, 17)	1, 18929	0-3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 23, 24, 27, 35, 36, 134, 252, 367, 877, 952, 1771, 1871, 2171, 2239, 3184, 4154
CA(250561; 4, 61, 17)	1, 6481, 18929	0-3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24, 26, 27, 29, 30, 32, 33, 35, 36, 38, 40, 41, 43, 46, 49, 52, 54, 57, 60, 82, 93, 98, 110, 115, 120, 123, 151, 168, 194, 219, 248, 264, 371, 709, 910, 1220, 1371, 1428, 1778, 2004, 2324, 2446, 2921, 3623

Continued on the next page

Table 4.5 – *Continued from the previous page*

$\mathcal{A}_0(\{\alpha^{i_1},\dots,\alpha^{i_l}\},C)$	$i_1,\dots,i_l$	C
CA(334081; 4, 141, 17)	1, 707, 739, 989	0-61, 63, 65, 67, 69, 71, 73, 102-112, 114, 116, 118, 120, 122, 124, 126, 128, 140, 240, 242, 244, 246, 248, 250, 252, 254, 256-265, 281, 283, 285, 423, 426, 484, 494, 496, 696, 726, 804, 1049, 1127, 1131, 1147, 1149, 1224, 1232, 1237, 1241, 1242, 1245, 1375, 1582, 1913, 2142, 2863, 3061, 3098, 3541, 3576, 3629, 3633, 3863, 3933
CA(260641; 4, 30, 19)	1, 32689	0-3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 43, 51, 53, 62, 72, 248, 357, 1470, 1779, 2660, 3200, 4355, 5378, 5756
CA(781249; 4, 35, 23)	1, 89	0-3, 5, 6, 8, 9, 11, 12, 14, 18, 19, 21, 22, 24, 25, 27, 28, 31, 35, 41, 45, 118, 347, 586, 1397, 2394, 2505, 4479, 5556, 6315, 8126, 9124, 9954

Covering arrays from maximal sequences and character sums

In Chapter 3 we explored the combinatorial properties of arrays constructed from cyclic shifts of maximal sequences over finite fields. We showed that cyclic trace arrays have the property that certain subsets of columns -which we characterize in various ways- are uniformly covered. This is the foundation of several previously established constructions of orthogonal and covering arrays (see Sections 3.2 and 3.3).

In Chapter 4 we exploited the above-mentioned property to give new covering array constructions using the vertical concatenation of cyclic trace arrays. In this chapter we exploit that property using a different approach: we reduce the alphabet size (and the number of rows) using the discrete logarithm and remainders modulo some integer. We do that by means of character-theoretic arguments and techniques similar to the ones used in the construction of covering arrays from cyclotomy [25]. Our results include new infinite families of covering arrays of strength 3 and 4, as well as an infinite family of covering arrays of arbitrary strength. To the best of our knowledge, the latter and the covering arrays from cyclotomy, are the only currently known direct constructions that provide a $CA(N; t, k, v)$ for arbitrary t, k and v.

The contents of this chapter are as follows. In Section 5.1 we give a brief overview of covering arrays from cyclotomy. In Section 5.2 we present a new type of array that is the result of reducing the alphabet size of a cyclic trace array using the discrete logarithm and taking remainders modulo some integer. We also state the main theorem of this chapter, which gives a sufficient condition for such an array to be a covering array, and we present the new covering array families that follow. Section 5.3 is dedicated to the proof of the main theorem. Finally, in Section 5.4 we evaluate our construction, which includes a comparison of our covering array families to covering arrays from cyclotomy and a comparison between our theoretical results and computer experiments.

The results from this chapter appear in [94].

5.1 Covering arrays from cyclotomy

The new covering array constructions that we present in the next section are established using similar techniques to the ones used by Colbourn in [25]. In this section we give a brief overview of Colbourn's construction.

Let q be a prime power and ω be a primitive element of $\mathbb{F}_q$. Then, for every $x \in \mathbb{F}_q^\times$, there exists a unique $i \in [0, q-1]$ such that $x = \omega^i$. This i is the *discrete logarithm of x with base ω*, denoted $i = \log_\omega(x)$. For a divisor $v \geq 2$ of $q-1$, Colbourn considers the $q \times q$ array $M(q, \omega, v)$

whose (i, j)-th element is given by

$$M(q, \omega, v)_{ij} = \begin{cases} \log_\omega(j - i) \,(\mathrm{mod}\ v) & \text{if } j \neq i, \\ 0 & \text{otherwise,} \end{cases}$$

where $(i, j) \in [0, q - 1] \times [0, q - 1]$. This is the *cyclotomic matrix associated to q, v and ω*. We note that, for a different primitive element ω', the matrix $M(q, \omega', v)$ is either identical to $M(q, \omega, v)$, or it is the result of multiplying $M(q, \omega, v)$ by some m coprime to v and then reducing modulo v. For the purposes of constructing covering arrays, such arrays are equivalent; thus the choice of the primitive element ω is irrelevant and we simply write $M(q, v)$ instead of $M(q, \omega, v)$.

Cyclotomic matrices are a special case of a type of array with interesting statistical properties. Let $X = (X_1, \ldots, X_k)$ be a random variable over a set $\Omega \subseteq \mathbb{Z}_v^k$. Then, for any vector $A = (a_1, \ldots, a_k) \in \mathbb{Z}_v^k$, the bias of A is

$$\mathrm{bias}(A) = \frac{1}{g} \max_{0 \leq l < v/g} \left| \Pr\left[\sum_{i=1}^{k} a_i X_i \equiv lg \,(\mathrm{mod}\ v) \right] - \frac{g}{v} \right|,$$

where $g = \gcd(a_1, \ldots, a_k, v)$. For $0 \leq \varepsilon \leq 1$, a set $\Omega \subseteq \mathbb{Z}_v^k$ is ε-*biased* if the random variable $X = (X_1, \ldots, X_k)$ has the properties that

1. for all $i \in [1, k]$, X_i is distributed uniformly over $\mathbb{Z}_v$, and

2. $\mathrm{bias}(A) \leq \varepsilon$ for all $A \in \mathbb{Z}_v^k$.

Then, an ε-*based array* is one whose rows are the elements of Ω. The connection to covering arrays is that a $(2/v^{2t})$-biased array is also a covering array of strength t [25]. It turns out that when

$$q > t^2 v^{4t}, \tag{5.1}$$

then $M(q, v)$ is a $(2/v^{2t})$-biased array, and thus a $\mathrm{CA}(q; t, q, v)$ [4].

A stronger result is known for the binary case: $M(q, 2)$ is a *Paley matrix* which is known to be a $\mathrm{CA}(q; t, q, 2)$ when $q > t^2 2^{2t-2}$ [3, 6, 7, 43]. This weaker condition is due to the fact that the proof does not rely on $M(q, v)$ being an ε-biased array, which is an object with more restrictions than a covering array; instead, different character-theoretic arguments are used. Similarly, Colbourn employs characters over finite fields to give a sufficient condition for $M(q, v)$ to be a covering array of strength t that is better (weaker) than Equation (5.1).

> **Theorem 5.1 (Covering arrays from cyclotomy [25, Theorem 3.3.]).** *Let q be a prime power and $v \geq 2$ be a divisor of $q - 1$. If $q > t^2 v^{2t}$, then $M(q, v)$ is a $\mathrm{CA}(q; t, q, v)$.*

In the proof of Theorem 5.1, Colbourn provides a character sum which, if larger than a target value, guarantees that a cyclotomic matrix is a covering array. He then uses a standard technique that uses Weil's theorem (see [56, Theorem 5.38]) to give a lower bound for that sum. Comparing that lower bound with the target value yields the sufficient condition of Theorem 5.1.

In the following sections we adapt this method by constructing similar arrays, built using discrete logarithms of selected elements from maximal sequences and finding lower bounds for character sums that imply the covering array property. Using the balanced nature of tuples of elements of maximal sequences, we are able to make connections to Jacobi sums for which we know exact values (cf. Theorem 2.27). This results in constructions of covering arrays of strength 3 and 4, as well as an infinite family of general strength covering arrays.

5.2 New covering array constructions

5.2.1 Reducing the alphabet size of cyclic trace arrays

In this chapter we study arrays that resemble those in Definition 3.3, and which we describe in the next definition. Before we state the definition we recall that, as per Lemma 2.44, if α is a primitive element of $\mathbb{F}_{q^t}$, then $\omega = \alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q$. Thus, for every nonzero $x \in \mathbb{F}_q^\times$, there exists some $i \in [0, q-2]$ such that $\omega^i = x$. This i is the *discrete logarithm of x with base ω*, denoted $\log_\omega x$.

> **Definition 5.2 (Cyclic trace array modulo v).** Let t, k be positive integers, α be a primitive element of $\mathbb{F}_{q^t}$, $\omega = \alpha^{[t]_q}$, and $C = \{c_0, \ldots, c_{k-1}\}$ be an ordered subset of $[0, q^t - 2]$. Then, the *cyclic trace array modulo v corresponding to α and C*, denoted $\mathcal{A}_{q^t/q}(\alpha, C; v)$, is the $v[t]_q \times k$ array with elements
>
> $$\mathcal{A}_{q^t/q}(\alpha, C; v)_{ij}, \quad (i, j) \in [0, v[t]_q - 1] \times [0, k-1]$$
>
> given by
>
> $$\mathcal{A}_{q^t/q}(\alpha, C; v)_{ij} = \begin{cases} \log_\omega \left(\mathcal{A}_{q^t/q}(\alpha, C)_{ij} \right) \bmod v, & \text{if } \mathcal{A}_{q^t/q}(\alpha, C)_{ij} \neq 0; \\ 0, & \text{otherwise;} \end{cases} \tag{5.2}$$
>
> $$= \begin{cases} \log_\omega \left(\mathrm{Tr}_{q^t/q}(\alpha^{i+c_j}) \right) \bmod v, & \text{if } \mathrm{Tr}_{q^t/q}(\alpha^{i+c_j}) \neq 0; \\ 0, & \text{otherwise.} \end{cases} \tag{5.3}$$
>
> Furthermore, we simply write $\mathcal{A}_{q^t/q}(\alpha; v)$ to denote $\mathcal{A}_{q^t/q}(\alpha, [0, [t]_q - 1]; v)$.

The construction of $\mathcal{A}_{q^t/q}(\alpha, C; v)$ in Definition 5.2 essentially gives a method for reducing the alphabet size of $\mathcal{A}_{q^t/q}(\alpha, C)$ from q to v. Indeed, the discrete logarithm in Equations (5.2) and (5.3) maps $\mathbb{F}_q^\times$ to $[0, q-2]$, which is then reduced to $[0, v-1]$ by considering remainders modulo v. As we see in this chapter, this reduction of the alphabet size preserves some of the properties of the cyclic trace arrays. Apart from the alphabet size, another difference between the arrays in Definition 3.3 and Definition 5.2 is their dimensions; while $\mathcal{A}_{q^t/q}(\alpha, C)$ has $q^t - 1$ rows, $\mathcal{A}_{q^t/q}(\alpha, C; v)$ has $v[t]_q$ rows. To justify the choice for this number of rows in our definition, we make a connection between cyclic trace arrays modulo v and a new type of sequence.

Lemma 5.3. *Let m be a positive integer, α be a primitive element of $\mathbb{F}_{q^t}$, $v \geq 2$ be a divisor of $q - 1$, and let $\omega = \alpha^{[t]_q}$. Then, the sequence $\mathrm{Seq}_{q^t/q}(\alpha; v) = (\mathrm{Seq}_{q^t/q}(\alpha; v)_i)_{i \geq 0}$ defined below, has period $v[t]_q$:*

$$\mathrm{Seq}_{q^t/q}(\alpha; v)_i = \begin{cases} \log_\omega \left(\mathrm{Seq}_{q^t/q}(\alpha)_i \right) \bmod v, & \text{if } \mathrm{Seq}_{q^t/q}(\alpha)_i \neq 0; \\ 0, & \text{otherwise}; \end{cases}$$

$$= \begin{cases} \log_\omega \left(\mathrm{Tr}_{q^t/q}(\alpha^i) \right) \bmod v, & \text{if } \mathrm{Tr}_{q^t/q}(\alpha^i) \neq 0; \\ 0, & \text{otherwise}. \end{cases} \tag{5.4}$$

Proof. We denote $\mathrm{Tr} = \mathrm{Tr}_{q^t/q}$. Let i be a positive integer and $j = i \bmod v[t]_q$; we need to prove that $\mathrm{Seq}_{q^t/q}(\alpha; v)_i = \mathrm{Seq}_{q^t/q}(\alpha; v)_j$. Let n be an integer such that $i = j + nv[t]_q$. Then, $\mathrm{Tr}(\alpha^i) = \mathrm{Tr}(\alpha^j \alpha^{nv[t]_q})$. By Lemma 2.44, we have that $\omega = \alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q$, hence $\alpha^{[t]_q nv} = \omega^{nv} \in \mathbb{F}_q$. From the linearity of the trace over $\mathbb{F}_q$, as per Theorem 2.17, we have

$$\mathrm{Tr}(\alpha^i) = \alpha^{[t]_q nv} \mathrm{Tr}(\alpha^j) = \omega^{nv} \mathrm{Tr}(\alpha^j). \tag{5.5}$$

It follows from Equation (5.5) that

$$\mathrm{Tr}(\alpha^i) = 0 \text{ if and only if } \mathrm{Tr}(\alpha^j) = 0. \tag{5.6}$$

For the case when $\mathrm{Tr}(\alpha^i)$ and $\mathrm{Tr}(\alpha^j)$ are nonzero, applying $\log_\omega$ in Equation (5.5) yields

$$\log_\omega(\mathrm{Tr}(\alpha^i)) = \log_\omega(\omega^{nv} \mathrm{Tr}(\alpha^j)) = nv + \log_\omega(\mathrm{Tr}(\alpha^j)).$$

Now, considering remainders modulo v in the above, we have

$$\log_\omega(\mathrm{Tr}(\alpha^i)) \bmod v = \log_\omega(\mathrm{Tr}(\alpha^j)) \bmod v. \tag{5.7}$$

We recall that $\mathrm{Tr}(\alpha^i)$ is the i-th element $\mathrm{Seq}_{q^t/q}(\alpha)_i$ of $\mathrm{Seq}_{q^t/q}(\alpha)$, therefore it follows from Definition 5.4 and Equations (5.6) and (5.7) that $\mathrm{Seq}_{q^t/q}(\alpha; v)_i = \mathrm{Seq}_{q^t/q}(\alpha; v)_j$. $\blacksquare$

Definition 5.4 (Maximal sequence modulo v). The sequence $\mathrm{Seq}_{q^t/q}(\alpha; v)$ described in Lemma 5.3 is the *maximal sequence modulo v corresponding to α*.

Example 5.5. Let $q = 4$, $t = 2$ and β be a primitive element of $\mathbb{F}_{q^t}$. We recall that in Example 2.14 we construct the finite field with 16 elements as follows.

- We first identify $\mathbb{F}_4$ as $\mathbb{F}_2(\alpha)$, where α is a root of the (primitive) polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$.

- We then identify $\mathbb{F}_{16}$ as $\mathbb{F}_4(\beta)$, where β is a root of the (primitive) polynomial $x^2 + x + \alpha \in \mathbb{F}_4[x]$.

i	0	1	2	3	4
$\mathrm{Tr}_{q^t/q}(\beta^i)$	ω	ω	1	ω	0
$\log_\omega(\mathrm{Tr}_{q^t/q}(\beta^i))$	1	1	0	1	–
$\mathrm{Seq}_{q^t/q}(\beta;v)_i$	1	1	0	1	**0**
i	5	6	7	8	9
$\mathrm{Tr}_{q^t/q}(\beta^i)$	$\omega+1$	$\omega+1$	ω	$\omega+1$	0
$\log_\omega(\mathrm{Tr}_{q^t/q}(\beta^i))$	2	2	1	2	–
$\mathrm{Seq}_{q^t/q}(\beta;v)_i$	2	2	1	2	**0**
i	10	11	12	13	14
$\mathrm{Tr}_{q^t/q}(\beta^i)$	1	1	$\omega+1$	1	0
$\log_\omega(\mathrm{Tr}_{q^t/q}(\beta^i))$	0	0	2	0	–
$\mathrm{Seq}_{q^t/q}(\beta;v)_i$	0	0	2	0	**0**

Table 5.1. Demonstration of the sequences in Example 5.5

- We list the nonzero elements of $\mathbb{F}_{q^t} = \mathbb{F}_4(\beta)$ in Table 2.1.

Now, we have

$$[t]_q = [2]_4 = \frac{2^4 - 1}{4 - 1} = 5,$$

so $\omega = \beta^{[t]_q} = \beta^5$ is a primitive element of $\mathbb{F}_q$. In Table 2.1 we see that $\beta^5 = \alpha$, which is indeed primitive as mentioned previously. We have that

$$\mathrm{Tr}_{q^t/q}(\beta^i) = \beta^i + \beta^{4i} \in \mathbb{F}_q,$$

for all integers i. We calculate these values for $i \in [0, 15]$ using Table 2.1 and we list them in the row labeled $\mathrm{Tr}_{q^t/q}(\beta^i)$ in Table 5.1. Since $\omega = \alpha$ is a root of $x^2 + x + 1$, we have that $\omega^2 = \omega + 1$ thus $\log_\omega(\omega + 1) = 2$; furthermore, $\log_\omega(\omega) = 1$ and $\log_\omega(1) = 0$. Using the above, we list the values of $\log_\omega(\mathrm{Tr}_{q^t/q}(\beta^i))$ for $i \in [0, 15]$ in Table 5.1 when $\mathrm{Tr}(\beta^i)$ is nonzero. Then, setting $v = 3$, which is a divisor of $q - 1$, we also show the corresponding values of $\mathrm{Seq}_{q^t/q}(\beta;v)_i$ for $i \in [0, 15]$, where the zeros in bold are the zeros that are correspond to i such that $\mathrm{Tr}_{q^t/q}(\beta^i) = 0$. Furthermore, $\mathrm{Seq}_{q^t/q}(\beta;v)$ has period $v[t]_q = 3 \cdot 5 = 15$; we compare the elements in a period of the two sequences below, omitting the parentheses and commas in the sequence notation:

$$\begin{array}{lcccccccccccccc}
\mathrm{Seq}_{q^t/q}(\beta): & \omega & \omega & 1 & \omega & 0 & \omega+1 & \omega+1 & \omega & \omega+1 & 0 & 1 & 1 & \omega+1 & 1 & 0 \\
\mathrm{Seq}_{q^t/q}(\beta;v): & 1 & 1 & 0 & 1 & \mathbf{0} & 2 & 2 & 1 & 2 & \mathbf{0} & 1 & 1 & 2 & 1 & \mathbf{0}
\end{array}$$

In Example 5.5, $\mathrm{Seq}_{q^t/q}(\beta;v)$ and $\mathrm{Seq}_{q^t/q}(\beta)$ have the same period. This is not always the case, as we show in the following less detailed example.

i	0	1	2	3	4	5	6	7
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	2	1	2	6	0	3	3	1
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	2	0	2	3	–	1	1	0
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	2	0	2	0	**0**	1	1	0
i	8	9	10	11	12	13	14	15
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	6	3	6	4	0	2	2	3
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	3	1	3	4	–	2	2	1
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	0	1	0	1	**0**	2	2	1
i	16	17	18	19	20	21	22	23
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	4	2	4	5	0	6	6	2
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	4	2	4	5	–	3	3	2
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	1	2	1	2	**0**	0	0	2
i	24	25	26	27	28	29	30	31
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	5	6	5	1	0	4	4	6
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	5	3	5	0	–	4	4	3
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	2	0	2	0	**0**	1	1	0
i	32	33	34	35	36	37	38	39
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	1	4	1	3	0	5	5	4
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	0	4	0	1	–	5	5	4
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	0	1	0	1	**0**	2	2	1
i	40	41	42	43	44	45	46	47
$\mathrm{Seq}_{q^t/q}(\alpha)_i$	3	5	3	2	0	1	1	5
$\log_\omega(\mathrm{Seq}_{q^t/q}(\alpha)_i)$	1	5	1	2	–	0	0	5
$\mathrm{Seq}_{q^t/q}(\alpha;v)_i$	1	2	1	2	**0**	0	0	2

Table 5.2. Demonstration of the sequences in Example 5.6

Example 5.6. Let $q = 7$, $t = 2$, and α be a root of the primitive polynomial $x^2 + 6x + 3 \in \mathbb{F}_7[x]$. Then, $\mathrm{Seq}_{q^t/q}(\alpha)$ is a maximal sequence with period $7^2 - 1 = 48$; we list the first 48 elements in Table 5.2. Let $v = 3$, which is a divisor of $q - 1$. We calculate $[t]_q = [2]_7 = (7^2 - 1)/(7 - 1) = 8$, so we have that $\omega = \alpha^8 = 3$ is a primitive element of $\mathbb{F}_7$. We have that $3^2 = 2$, $3^3 = 6$, $3^4 = 4$, $3^5 = 5$, and $3^6 = 1$; using this information we list the first 48 elements of $\mathrm{Seq}_{q^t/q}(\alpha;v)$ in Table 5.2. As before, the zeros in bold correspond to zero elements of $\mathrm{Seq}_{q^t/q}(\alpha)$. Furthermore, by Lemma 5.3, $\mathrm{Seq}_{q^t/q}(\alpha;v)$ has period $v[t]_q = 3 \cdot 8 = 24$, which is indeed reflected in the table.

The reader may have noticed that in Tables 5.1 and 5.2, the rows labeled $\mathrm{Seq}_{q^t/q}(\alpha)_i$ are nonzero constant multiples of each other. This pattern is due to the projective property of

$$
\mathcal{A}_{q^t/q}(\alpha) =
\begin{array}{ccccc}
\omega & \omega & 1 & \omega & 0 \\
\omega & 1 & \omega & 0 & \omega+1 \\
1 & \omega & 0 & \omega+1 & \omega+1 \\
\omega & 0 & \omega+1 & \omega+1 & \omega \\
0 & \omega+1 & \omega+1 & \omega & \omega+1 \\
\omega+1 & \omega+1 & \omega & \omega+1 & 0 \\
\omega+1 & \omega & \omega+1 & 0 & 1 \\
\omega & \omega+1 & 0 & 1 & 1 \\
\omega+1 & 0 & 1 & 1 & \omega+1 \\
0 & 1 & 1 & \omega+1 & 1 \\
1 & 1 & \omega+1 & 1 & 0 \\
1 & \omega+1 & 1 & 0 & \omega \\
\omega+1 & 1 & 0 & \omega & \omega \\
1 & 0 & \omega & \omega & 1 \\
0 & \omega & \omega & 1 & \omega
\end{array}
\qquad
\mathcal{A}_{q^t/q}(\alpha;v) =
\begin{array}{ccccc}
1 & 1 & 0 & 1 & 0 \\
1 & 0 & 1 & 0 & 2 \\
0 & 1 & 0 & 2 & 2 \\
1 & 0 & 2 & 2 & 1 \\
0 & 2 & 2 & 1 & 2 \\
2 & 2 & 1 & 2 & 0 \\
2 & 1 & 2 & 0 & 0 \\
1 & 2 & 0 & 0 & 0 \\
2 & 0 & 0 & 0 & 2 \\
0 & 0 & 0 & 2 & 0 \\
0 & 0 & 2 & 0 & 0 \\
0 & 2 & 0 & 0 & 1 \\
2 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 1 & 0 \\
0 & 1 & 1 & 0 & 1
\end{array}
$$

Table 5.3. The arrays $\mathcal{A}_{q^t/q}(\alpha)$ and $\mathcal{A}_{q^t/q}(\alpha;v)$ for $q = t = 4$, $v = 3$ and α as in Example 5.5.

maximal sequences, that we describe in Proposition 2.45.

We recall that, as per Definition 3.5, for integers j, n, we denote

$$
L_n^j \left(\mathrm{Seq}_{q^t/q}(\alpha;v) \right) = \left(\mathrm{Seq}_{q^t/q}(\alpha;v)_{i+j} \right)_{i=0}^{n-1} .
$$

Remark 5.7. The following analogues of the statements in Remark 3.6 are straightforward implications of Definitions 5.2 and 5.4.

1. The columns of $\mathcal{A}_{q^t/q}(\alpha, C;v)$ are the left cyclic shifts of $\mathrm{Seq}_{q^t/q}(\alpha;v)$ by the elements in C, as follows:

$$
\mathcal{A}_{q^t/q}(\alpha, C;v) = \left[L_{v[t]_q}^{c_0} \left(\mathrm{Seq}_{q^t/q}(\alpha;v) \right) \mid \cdots \mid L_{v[t]_q}^{c_{k-1}} \left(\mathrm{Seq}_{q^t/q}(\alpha;v) \right) \right] .
$$

2. If $C = \{c_0, \ldots, c_{k-1}\}$, then for $(i, j) \in [0, v[t]_q - 1] \times [0, k - 1]$, the (i, j)-th element of $\mathcal{A}_{q^t/q}(\alpha, C;v)$ is

$$
\mathcal{A}_{q^t/q}(\alpha, C;v)_{i,j} = \mathrm{Seq}_{q^t/q}(\alpha;v)_{i+c_j} . \tag{5.8}
$$

3. The rows of $\mathcal{A}_{q^t/q}(\alpha;v)$ are the vectors $L_{[t]_q}^i(\mathrm{Seq}_{q^t/q}(\alpha;v))$, $i \in [0, v[t]_q - 1]$.

4. For $C \subseteq C'$, we have that $\mathcal{A}_{q^t/q}(\alpha, C;v)$ is a subarray of $\mathcal{A}_{q^t/q}(\alpha, C';v)$.

In Tables 5.3 and 5.4, we give $\mathcal{A}_{q^t/q}(\alpha)$ and $\mathcal{A}_{q^t/q}(\alpha;v)$ for q, t, v and α as in Examples 5.5 and 5.6, respectively; the statements in Remark 5.7 can be verified for these arrays using Tables 5.1 and 5.2.

We close this section commenting on the choice of the number of rows in Definition 5.2. Let j be a positive integer with $j \geq v[t]_q$ and $i = j \bmod v[t]_q$. Since $\mathrm{Seq}_{q^t/q}(\alpha;v)$ has period

$$
\mathcal{A}_{q^t/q}(\alpha) =
\begin{array}{cccccccc}
2 & 1 & 2 & 6 & 0 & 3 & 3 & 1 \\
1 & 2 & 6 & 0 & 3 & 3 & 1 & 6 \\
2 & 6 & 0 & 3 & 3 & 1 & 6 & 3 \\
6 & 0 & 3 & 3 & 1 & 6 & 3 & 6 \\
0 & 3 & 3 & 1 & 6 & 3 & 6 & 4 \\
3 & 3 & 1 & 6 & 3 & 6 & 4 & 0 \\
3 & 1 & 6 & 3 & 6 & 4 & 0 & 2 \\
1 & 6 & 3 & 6 & 4 & 0 & 2 & 2 \\
6 & 3 & 6 & 4 & 0 & 2 & 2 & 3 \\
3 & 6 & 4 & 0 & 2 & 2 & 3 & 4 \\
6 & 4 & 0 & 2 & 2 & 3 & 4 & 2 \\
4 & 0 & 2 & 2 & 3 & 4 & 2 & 4 \\
0 & 2 & 2 & 3 & 4 & 2 & 4 & 5 \\
2 & 2 & 3 & 4 & 2 & 4 & 5 & 0 \\
2 & 3 & 4 & 2 & 4 & 5 & 0 & 6 \\
3 & 4 & 2 & 4 & 5 & 0 & 6 & 6 \\
4 & 2 & 4 & 5 & 0 & 6 & 6 & 2 \\
2 & 4 & 5 & 0 & 6 & 6 & 2 & 5 \\
4 & 5 & 0 & 6 & 6 & 2 & 5 & 6 \\
5 & 0 & 6 & 6 & 2 & 5 & 6 & 5 \\
0 & 6 & 6 & 2 & 5 & 6 & 5 & 1 \\
6 & 6 & 2 & 5 & 6 & 5 & 1 & 0 \\
6 & 2 & 5 & 6 & 5 & 1 & 0 & 4 \\
2 & 5 & 6 & 5 & 1 & 0 & 4 & 4 \\
5 & 6 & 5 & 1 & 0 & 4 & 4 & 6 \\
6 & 5 & 1 & 0 & 4 & 4 & 6 & 1 \\
5 & 1 & 0 & 4 & 4 & 6 & 1 & 4 \\
1 & 0 & 4 & 4 & 6 & 1 & 4 & 1 \\
0 & 4 & 4 & 6 & 1 & 4 & 1 & 3 \\
4 & 4 & 6 & 1 & 4 & 1 & 3 & 0 \\
4 & 6 & 1 & 4 & 1 & 3 & 0 & 5 \\
6 & 1 & 4 & 1 & 3 & 0 & 5 & 5 \\
1 & 4 & 1 & 3 & 0 & 5 & 5 & 4 \\
4 & 1 & 3 & 0 & 5 & 5 & 4 & 3 \\
1 & 3 & 0 & 5 & 5 & 4 & 3 & 5 \\
3 & 0 & 5 & 5 & 4 & 3 & 5 & 3 \\
0 & 5 & 5 & 4 & 3 & 5 & 3 & 2 \\
5 & 5 & 4 & 3 & 5 & 3 & 2 & 0 \\
5 & 4 & 3 & 5 & 3 & 2 & 0 & 1 \\
4 & 3 & 5 & 3 & 2 & 0 & 1 & 1 \\
3 & 5 & 3 & 2 & 0 & 1 & 1 & 5 \\
5 & 3 & 2 & 0 & 1 & 1 & 5 & 2 \\
3 & 2 & 0 & 1 & 1 & 5 & 2 & 1 \\
2 & 0 & 1 & 1 & 5 & 2 & 1 & 2 \\
0 & 1 & 1 & 5 & 2 & 1 & 2 & 6 \\
1 & 1 & 5 & 2 & 1 & 2 & 6 & 0 \\
1 & 5 & 2 & 1 & 2 & 6 & 0 & 3 \\
5 & 2 & 1 & 2 & 6 & 0 & 3 & 3 \\
\end{array}
$$

$$
\mathcal{A}_{q^t/q}(\alpha;v) =
\begin{array}{cccccccc}
2 & 0 & 2 & 0 & \mathbf{0} & 1 & 1 & 0 \\
0 & 2 & 0 & \mathbf{0} & 1 & 1 & 0 & 0 \\
2 & 0 & \mathbf{0} & 1 & 1 & 0 & 0 & 1 \\
0 & \mathbf{0} & 1 & 1 & 0 & 0 & 1 & 0 \\
\mathbf{0} & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
1 & 1 & 0 & 0 & 1 & 0 & 1 & \mathbf{0} \\
1 & 0 & 0 & 1 & 0 & 1 & \mathbf{0} & 2 \\
0 & 0 & 1 & 0 & 1 & \mathbf{0} & 2 & 2 \\
0 & 1 & 0 & 1 & \mathbf{0} & 2 & 2 & 1 \\
1 & 0 & 1 & \mathbf{0} & 2 & 2 & 1 & 1 \\
0 & 1 & \mathbf{0} & 2 & 2 & 1 & 1 & 2 \\
1 & \mathbf{0} & 2 & 2 & 1 & 1 & 2 & 1 \\
\mathbf{0} & 2 & 2 & 1 & 1 & 2 & 1 & 2 \\
2 & 2 & 1 & 1 & 2 & 1 & 2 & \mathbf{0} \\
2 & 1 & 1 & 2 & 1 & 2 & \mathbf{0} & 0 \\
1 & 1 & 2 & 1 & 2 & \mathbf{0} & 0 & 0 \\
1 & 2 & 1 & 2 & \mathbf{0} & 0 & 0 & 2 \\
2 & 1 & 2 & \mathbf{0} & 0 & 0 & 2 & 2 \\
1 & 2 & \mathbf{0} & 0 & 0 & 2 & 2 & 0 \\
2 & \mathbf{0} & 0 & 0 & 2 & 2 & 0 & 2 \\
\mathbf{0} & 0 & 0 & 2 & 2 & 0 & 2 & 0 \\
0 & 0 & 2 & 2 & 0 & 2 & 0 & \mathbf{0} \\
0 & 2 & 2 & 0 & 2 & 0 & \mathbf{0} & 1 \\
2 & 2 & 0 & 2 & 0 & \mathbf{0} & 1 & 1 \\
\end{array}
$$

Table 5.4. The arrays $\mathcal{A}_{q^t/q}(\alpha)$ and $\mathcal{A}_{q^t/q}(\alpha;v)$ for $q = 7$, $t = 2$, $v = 3$, and α as in Example 5.6.

$v[t]_q$, then, for any positive integer n, we have that

$$L_n^j \left(\text{Seq}_{q^t/q}(\alpha; v) \right) = L_n^i \left(\text{Seq}_{q^t/q}(\alpha; v) \right).$$

In view of the second statement of Remark 5.7, this means that if $\mathcal{A}_{q^t/q}(\alpha; v)$ had been defined with more than $v[t]_q$ rows, the rows with indexes greater than $v[t]_q$ would be identical to some rows with indexes less than $v[t]_q$. For the purpose of constructing covering arrays, such rows are redundant.

5.2.2 Main results

In this section we state the main theorem of Chapter 5 and present the implied results. The main theorem's proof relies on several lengthy results and is the topic of Section 5.3.

Theorem 5.8 (Main theorem of Chapter 5). *Let q be a prime power, $t \geq 2$, α be a primitive element of $\mathbb{F}_{q^t}$, and v be a positive divisor of $q - 1$. Let $C \subseteq [0, q^t - 2]$, such that the following equivalent (cf. Theorem 3.13 for $s = t - 1$) statements hold:*

1. *The $q^t \times |C|$ array $\mathcal{A}_0(\alpha, C)$ is a linear $\text{OA}_q(t - 1, |C|, q)$.*

2. *The set $\{\alpha^c \mid c \in C\}$ is a $(|C|, t - 1)$-set over $\mathbb{F}_q$.*

3. *The set $\{L_{q^t-1}^c(\text{Seq}_{q^t/q}(\alpha)) \mid c \in C\}$ is a $(|C|, t - 1)$-set over $\mathbb{F}_q$.*

4. *For every $c_0, \ldots, c_{t-2} \in C$ and $d_0, \ldots, d_{t-2} \in \mathbb{F}_q$ not all zero, the minimal polynomial of α does not divide $\sum_{j=0}^{t-2} d_j x^{c_j}$.*

5. *For every $t - 1$ points in $\{[\alpha^c] \mid c \in C\}$, there is no $(t - 3)$-flat in $\text{PG}(t - 1, q)$ that contains them.*

If furthermore

$$q^{\frac{t}{2}-2}(q - tv) \geq v^{t-1}, \tag{5.9}$$

then $\mathcal{A}_{q^t/q}(\alpha, C; v)$ is a $\text{CA}(v[t]_q; t, |C|, v)$.

Remark 5.9. The bound on q improves with respect to the number of columns as t increases. Indeed, in Equation (5.9) it is required that $q > tv$, so a sufficient condition for Equation (5.9) to hold is $q^{\frac{t}{2}-2} \geq v^{t-1}$, which is equivalent to $q \geq v^{2+\frac{6}{t-4}}$. We conclude that a sufficient condition for Theorem 5.8 is

$$q > \max\{tv, v^{2+\frac{6}{t-4}}\},$$

which means that q needs to be larger than tv.

We now focus on special cases of t in the main theorem. We consider some of the orthogonal arrays that we present in Chapter 3, of strength $t - 1$ for the cases when t is equal to 3, 4, or it is arbitrary. Then, for each case, we give a corollary of the main theorem that describes a family of covering arrays of strength t.

Corollary 5.10 (Covering arrays of strength 3). *Let q be a prime power, α be a primitive element of $\mathbb{F}_{q^3}$, and v be a positive divisor of $q - 1$, such that $q \geq v^4 + 6v^3 + 9v^2$. Then, $\mathcal{A}_{q^3/q}(\alpha; v)$ is a $\mathrm{CA}(v(q^2 + q + 1); 3, q^2 + q + 1, v)$.*

Proof. Let $C = [0, [3]_q - 1] = [0, q^2 + q]$. By Corollary 3.15, we have that $\mathcal{A}_{q^3/q,0}(\alpha, C)$ is an $\mathrm{OA}_{q^{3-2}}(2, [3]_q, q) = \mathrm{OA}_q(2, q^2 + q + 1, q)$. Hence the second statement of Theorem 5.8 holds for $t = 3$. Furthermore, we claim that Equation (5.9) holds for $t = 3$. Indeed, substituting $t = 3$ in Equation (5.9), we have that an equivalent condition in that case is $q^{3/2-2}(q - 3v) \geq v^2$, which is equivalent to $q^{1/2} \geq v^2 + 3v/\sqrt{q}$. A sufficient condition for the latter to hold is $q^{1/2} \geq v^2 + 3v$; squaring both sides gives $q \geq (v^2 + 3v)^2 = v^4 + 6v^3 + 9v^2$, which holds by our assumptions. We conclude that all the conditions of Theorem 5.8 hold for $t = 3$, and thus $\mathcal{A}_{q^t/q}(\alpha, C; v) = \mathcal{A}_{q^t/q}(\alpha; v)$ is a $\mathrm{CA}(v[t]_q; t, |C|, v)$ for $t = 3$, i.e. a $\mathrm{CA}(v(q^2 + q + 1); 3, q^2 + q + 1, v)$. ∎

We note that the bound in Corollary 5.10 can be improved to $q \geq v^4 + 6v^3$ using the better but more complicated conditions used in the proofs in Section 5.3. We discuss the details in the end of that section.

Corollary 5.11 (Covering arrays of strength 4). *Let q be a prime power, α be a primitive element of $\mathbb{F}_{q^4}$, and*

$$C = \left\{ j(q + 1) \mid j \in [0, q^2] \right\}.$$

Furthermore, let v be a positive divisor of $q - 1$, such that $q \geq v^3 + 4v$. Then, $\mathcal{A}_{q^4/q}(\alpha, C; v)$ is a $\mathrm{CA}(v(q^3 + q^2 + q + 1); 4, q^2 + 1, v)$.

Proof. By Corollary 3.17 we have that $\mathcal{A}_{q^4/q}(\alpha, C)$ is an $\mathrm{OA}_{q^{4-3}}(3, q^2 + 1, q) = \mathrm{OA}_q(3, q^2 + 1, q)$. Hence, the second statement of Theorem 5.8 holds for $t = 4$. Furthermore, we claim that Equation (5.9) holds for $t = 4$. Indeed, substituting $t = 4$ in Equation (5.9), we have that an equivalent condition in that case is $q \geq v^3 - 4v$. We conclude that all the conditions of Theorem 5.8 hold for $t = 4$, and thus $\mathcal{A}_{q^t/q}(\alpha, C; v)$ is a $\mathrm{CA}(v[t]_q; t, |C|, v)$ for $t = 4$, i.e. a $\mathrm{CA}(v(q^3 + q^2 + q + 1); 4, q^2 + 1, v)$. ∎

Suppose that $q = p^r$, for a prime p and some positive integer r. We recall that in Equation (3.7), we define

$$N_q = \begin{cases} q + \lfloor 2\sqrt{q} \rfloor, & \text{if } p \mid 2\sqrt{q} \text{ and } r \geq 3, r \text{ odd}; \\ q + \lfloor 2\sqrt{q} \rfloor + 1, & \text{otherwise.} \end{cases}$$

Corollary 5.12 (Covering arrays of strength t). *Let q be a prime power, $t \geq 2$, α be a primitive element of $\mathbb{F}_{q^t}$, and v be a positive divisor of $q - 1$, such that*

$$q^{t/2-2}(q - tv) \geq v^t - 1.$$

Then, there exists $C \subset [0, [t]_q - 1]$ with $|C| = N_q$, such that $\mathcal{A}_{q^t/q}(\alpha, C; v)$ is a $\mathrm{CA}(v[t]_q; t, N_q, v)$.

Proof. By Corollary 3.30, there exists $C \subset [0, [t]_q - 1]$ with $|C| = N_q$, such that $\mathcal{A}_{q^t/q}(\alpha, C)$ is an $OA_q(t - 1, N_q, q)$. Hence, the second statement of Theorem 5.8 holds. From our assumptions, Equation (5.9) also holds. We conclude that all the conditions of Theorem 5.8 are satisfied, and hence $\mathcal{A}_{q^t/q}(\alpha, C; v)$ is a $CA(v[q]_q; t, N_q, v)$. $\blacksquare$

5.3 Proof of the main theorem

5.3.1 Overview

As we mention earlier, the proof of Theorem 5.8 relies on several results; before we delve into this, we give an overview of the strategy of our proof. For convenience, we denote

$$S_i = S_i(\alpha, q, v, t) = L^i_{v[t]_q}\left(\text{Seq}_{q^t/q}(\alpha; q; v)\right), \quad i \in [0, [t]_q - 1]. \tag{5.10}$$

Let $C \subseteq [0, [t]_q - 1]$. By Remark 5.7, the $v[t]_q \times |C|$ array $\mathcal{A}_{q^t/q}(\alpha, C; v)$ consists of precisely the columns $S_c, c \in C$. Thus, to prove that this is a covering array of strength t, we need to show that, for every $I \subseteq C$ with $|I| = t$, the set $\{S_i \mid i \in I\}$ is covered. In view of that, we establish the following two results:

- **Proposition 5.14:** For every t-set I, if $\{\alpha^i \mid i \in I\}$ is linearly independent, then $\{S_i \mid i \in I\}$ is covered.

- **Proposition 5.20:** For every t-set I, if $\{\alpha^i \mid i \in I\}$ is a linearly dependent $(t, t-1)$-set and Equation (5.9) is satisfied, then $\{S_i \mid i \in I\}$ is covered.

We claim that establishing the above two propositions essentially proves Theorem 5.8. Indeed, assume that the five equivalent statements of Theorem 5.8 hold. Then, in particular, $\{\alpha^c \mid c \in C\}$ is a $(|C|, t-1)$-set. This implies that for every $I \subseteq C$, since $\{\alpha^i \mid i \in I\}$ is a subset of a $(|C|, t-1)$-set, there are two cases:

1. $\{\alpha^i \mid i \in I\}$ is linearly independent over $\mathbb{F}_q$, or

2. $\{\alpha^i \mid i \in I\}$ is a linearly dependent $(t, t-1)$-set over $\mathbb{F}_q$.

If we further assume that Equation (5.9) holds, then in either case we have from Propositions 5.14 and 5.20 that the set $\{S_i \mid i \in I\}$ is covered, which shows that $\mathcal{A}_{q^t/q}(\alpha, q; v)$ is a covering array of strength t.

The next sections are as follows: In Section 5.3.2 we prove an auxiliary result that we need often. In Section 5.3.3, we prove Proposition 5.14, which is the first (and most straightforward) part of the proof of Theorem 5.8. In Section 5.3.4, we give the second part of the proof, that consists of some preliminary results on multiplicative characters, and the proof of Proposition 5.20, that relies on them.

5.3.2 A preliminary result

We state a corollary of Proposition 3.10 that comes in handy throughout the rest of this chapter.

Corollary 5.13. *Let α be a primitive element of $\mathbb{F}_{q^t}$, $i_0, \ldots, i_{t-1} \in [0, [t]_q - 1]$ and $b_0, \ldots, b_{t-1} \in \mathbb{F}_q$. We denote by R the number of elements $r \in [0, q^t - 2]$ such that*

$$\left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_0}), \mathrm{Tr}_{q^t/q}(\alpha^{r+i_1}), \ldots, \mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-1}}) \right) = (b_0, b_1, \ldots, b_{t-1}). \tag{5.11}$$

Then, we have the following values for R.

1. *If $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is linearly independent, then*

$$R = \begin{cases} 1 & \text{if } (b_0, \ldots, b_{t-1}) \neq (0, \ldots, 0) \\ 0 & \text{otherwise.} \end{cases}$$

2. *If $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is a linearly dependent $(t, t-1)$-set, then there exist $y_0, \ldots, y_{t-1} \in \mathbb{F}_q^\times$ such that $\sum_{k=0}^{t-1} \alpha^{i_k} = 0$ and*

$$R = \begin{cases} q & \text{if } \sum_{k=0}^{t-1} y_k b_k = 0 \text{ and } (b_0, \ldots, b_{t-1}) \neq (0, \ldots, 0) \\ q - 1 & \text{if } (b_0, \ldots, b_{t-1}) = (0, \ldots, 0) \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We prove each case separately.

1. If $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is linearly independent, then by Proposition 3.10 we have that $\mathcal{A} = \mathcal{A}_0(\alpha, \{i_0, \ldots, i_{t-1}\})$ is an $\mathrm{OA}_\lambda(t, t, q)$ with $\lambda = q^{t-t} = 1$. This means that, for every $b_0, \ldots, b_{t-1} \in \mathbb{F}_q$ there exists a unique row of $\mathcal{A}$ equal to $(b_0, \ldots, b_{t-1})$. Indexing the rows of $\mathcal{A}$ by $[0, q^t - 1]$ and considering Definition 3.3, we have that the row of index $r \in [0, q^t - 2]$ is given by the left hand side of Equation (5.11), while the row with index $r = q^t - 1$ is the last row that contains only zeros. Therefore, if $(b_0, \ldots, b_{t-1})$ is not the zero t-tuple, then there exists a unique $r \in [0, q^t - 2]$ such that Equation (5.11) holds; otherwise, such an r does not exist.

2. If $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is a linearly dependent $(t, t-1)$-set, then from its linear dependence we have that there exist $y_0, \ldots, y_{t-1} \in \mathbb{F}_q$ not all zero such that $\sum_{k=0}^{t-1} y_k \alpha^{i_k} = 0$. Suppose by means of contradiction that the coefficients are not all nonzero and, without loss of generality, assume that $y_{t-1} = 0$. Then, we have that $\sum_{k=0}^{t-2} y_k \alpha^{i_k} = 0$, which means that $\alpha^{i_0}, \ldots, \alpha^{i_{t-2}}$ is a linearly dependent subset of $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ of size $t - 1$, contradicting the fact that the latter is a $(t, t-1)$-set. We conclude that $y_0, \ldots, y_{t-1}$ are all nonzero, i.e. $y_0, \ldots, y_{t-1} \in \mathbb{F}_q^\times$.

   Indexing the rows of $\mathcal{A}'$ by $[0, q^t - 1]$, we have two cases:

   (a) If $(b_0, \ldots, b_{t-2}) \neq (0, \ldots, 0)$, these q rows are among the ones with indexes in $[0, q^t - 2]$, as the last row is the all-zero row. In other words, by Definition 3.3, there exist exactly q elements $r \in [0, q^t - 2]$ such that

   $$\left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_0}), \mathrm{Tr}_{q^t/q}(\alpha^{r+i_1}), \ldots, \mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-2}}) \right) = (b_0, b_1, \ldots, b_{t-2}). \tag{5.12}$$

(b) If $(b_0, \ldots, b_{t-2}) = (0, \ldots, 0)$, one among these q rows is the last, with index $q^t - 1$, while the remaining $q - 1$ rows are among those with indexes in $[0, q^t - 2]$. Hence, there exist exactly $q - 1$ elements $r \in [0, q^t - 2]$ such that Equation (5.12) holds.

Multiplying the equation $\sum_{k=0}^{t-1} y_k \alpha^{i_k} = 0$ by α^r and solving for $\alpha^r \alpha^{i_{t-1}} = \alpha^{r+i_{t-1}}$ yields

$$\alpha^{r+i_{t-1}} = -\sum_{k=0}^{t-2} \frac{y_k}{y_{t-1}} \alpha^{r+i_k}. \tag{5.13}$$

For all $r \in [0, q^t - 2]$ satisfying Equation (5.12) in any of the above cases, we have that Equation (5.11) holds if and only if

$$b_{t-1} = \mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-1}}) = \mathrm{Tr}_{q^t/q}\left(-\sum_{k=0}^{t-2} \frac{y_k}{y_{t-1}} \alpha^{r+i_k}\right) = -\sum_{k=0}^{t-2} \frac{y_i}{y_{t-1}} \mathrm{Tr}(\alpha^{r+i_k}) = -\sum_{k=0}^{t-2} \frac{y_i}{y_{t-1}} b_k,$$

that is, $\sum_{k=0}^{t-1} y_k b_k = 0$. We conclude that if this last equation holds, the number of $r \in [0, q^t - 2]$ satisfying Equation (5.11) is q if $(b_0, \ldots, b_{t-1})$ is not the all-zero t-tuple, and $q - 1$ if it is. If that equation does not hold, then there are no such r.

$\blacksquare$

5.3.3 First part of the proof: the linear independence case

Proposition 5.14. *Let t be a positive integer, α be a primitive element of $\mathbb{F}_{q^t}$, $v \geq 2$ be a divisor of $q - 1$, and $S_i = S_i(\alpha, q, v, t)$, $i \in [0, [q]_q - 1]$ as defined in Equation (5.10). For $I \subseteq [0, [t]_q - 1]$ such that $\{\alpha^i \mid i \in I\}$ is linearly independent over $\mathbb{F}_q$, we have that $\{S_i \mid i \in I\}$ is covered.*

Proof. Let $I = \{i_0, \ldots, i_{t-1}\} \subseteq [0, [t]_q - 1]$, such that $\{\alpha^i \mid i \in I\}$ is linearly independent. We recall that, for $i \in I$, S_i is a vector of length $v[t]_q$ and elements from $[0, v - 1]$. By Definition 2.62, in order to show that $\{S_i \mid i \in I\}$ is covered, we need to prove that, for every $(l_0, \ldots, l_{t-1}) \in [0, v - 1]^t$, there exists some row of the $v[t]_q \times t$ array with columns S_i, $i \in I$, that is equal to $(l_0, \ldots, l_{t-1})$.

Let $(l_0, \ldots, l_{t-1}) \in [0, v - 1]^t$. By Lemma 2.44, we have that $\omega = \alpha^{[t]_q}$ is a primitive element of $\mathbb{F}_q$. We observe that, since $v \mid q - 1$, then for every $l \in [0, v - 1]$ there exists some $y \in [0, q - 2]$ such that $l = y \bmod v$. Furthermore, since $x \mapsto \log_\omega(x)$ is a bijection between $\mathbb{F}_q^\times$ and $[0, q - 2]$, we have that, for every $y \in [0, q - 2]$, there exists $b \in \mathbb{F}_q^\times$ such that $\log_\omega(b) = y$. We conclude that, for every $l \in [0, v - 1]$, there exists $b \in \mathbb{F}_q^\times$ such that $l = \log_\omega(b) \bmod v$. In particular, there exist $b_0, \ldots, b_{t-1} \in \mathbb{F}_q^\times$ such that

$$(l_0, \ldots, l_{t-1}) = \left(\log_\omega(b_0) \bmod v, \ldots, \log_\omega(b_{t-1}) \bmod v\right). \tag{5.14}$$

Now, since $\{\alpha^i \mid i \in I\}$ is linearly independent, and $(b_0, \ldots, b_{t-1})$ is not the zero t-tuple, then,

by Corollary 5.13 we have that there exists $r \in [0, q^t - 2]$ such that

$$(b_0, \ldots, b_{t-1}) = \left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_0}), \ldots, \mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-1}}) \right).$$

Since $b_0, \ldots, b_{t-1} \in \mathbb{F}_q^\times$, there are no zeros among the elements of the t-tuples in the last equation and thus we can apply $\log_\omega$, which yields

$$(\log_\omega(b_0), \ldots, \log_\omega(b_{t-1})) = \left(\log_\omega(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_0})), \ldots, \log_\omega(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-1}})) \right).$$

Taking remainders modulo v, we have

$$(\log_\omega(b_0) \bmod v, \ldots, \log_\omega(b_{t-1}) \bmod v)$$
$$= \left(\log_\omega(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_0})) \bmod v, \ldots, \log_\omega(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_{t-1}})) \bmod v \right),$$

and from Equations (5.4) and (5.14), we have

$$(l_0, \ldots, l_{t-1}) = \left(\mathrm{Seq}_{q^t/q}(\alpha; v)_{r+i_0}, \ldots, \mathrm{Seq}_{q^t/q}(\alpha; v)_{r+i_{t-1}} \right). \tag{5.15}$$

Now, let $s \in [0, v[t]_q - 1]$ such that $s = r \bmod v[t]_q$. By Lemma 5.3, we know that $\mathrm{Seq}_{q^t/q}(\alpha; v)$ has period $v[t]_q$, and therefore $\mathrm{Seq}_{q^t/q}(\alpha; v)_{r+i} = \mathrm{Seq}_{q^t/q}(\alpha; v)_{s+i}$ for all positive integers i. This, along with Equation (5.15), implies that

$$(l_0, \ldots, l_{t-1}) = \left(\mathrm{Seq}_{q^t/q}(\alpha; v)_{s+i_0}, \ldots, \mathrm{Seq}_{q^t/q}(\alpha; v)_{s+i_{t-1}} \right).$$

The right hand side is the row with index s of the $v[t]_q \times t$ array with columns $S_i, i \in I$; from our discussion in the beginning, this completes the proof. ∎

5.3.4 Second part of the proof: the linear dependence case

Preliminaries on characters

We start with the study of some useful character sums that the proof of Proposition 5.20 relies on. Let q be a prime power, ω be a primitive element of $\mathbb{F}_q$ and v be a positive divisor of $q - 1$. We denote by $\chi_{\omega,v}$, or simply χ_v when ω is clear from the context, the multiplicative character of $\mathbb{F}_q$ defined by

$$\chi_v(\omega^j) = \chi_{\omega,v}(\omega^j) = e^{\frac{2\pi i}{v} j}, \quad j \in \mathbb{Z}.$$

We know from Corollary 2.24 that the set $\widehat{\mathbb{F}_q^\times}$ of multiplicative characters of $\mathbb{F}_q$ is a cyclic group of order $q - 1$ and generator χ, defined by

$$\chi(\omega^j) = e^{\frac{2\pi i}{q-1} j}, \quad j \in \mathbb{Z}. \tag{5.16}$$

Lemma 5.15. *For a prime power q and v a positive divisor of $q - 1$, the order of χ_v in $\widehat{\mathbb{F}_q^\times}$ is v.*

Proof. The order of χ_v is the smallest positive integer s such that χ_v^s is the identity mapping, that is, such that for every integer k we have

$$\chi_v^s(\omega^k) = e^{\frac{2\pi i}{v} sk} = 1.$$

This is satisfied for $s = v$, but not for $s \in [1, v-1]$, hence the order of χ_v is indeed v. ◻

Lemma 5.16. *Let q be a prime power, v be a divisor of $q-1$ and ω be a primitive element of $\mathbb{F}_q$. Then, for $y \in \mathbb{F}_q^\times$ and integer l, we have that*

$$\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l})\chi_v^j(y) = \begin{cases} v & \text{if } \log_\omega(y) \equiv l \pmod{v}; \\ 0 & \text{otherwise.} \end{cases}$$

Proof. We have that

$$\chi_v^j(\omega^{v-l})\chi_v^j(y) = \chi_v^j(\omega^{v-l})\chi_v^j(\omega^{\log_\omega(y)}) = \chi_v^j(\omega^{v-l+\log_\omega(y)}).$$

Let $s = v - l + \log_\omega(y)$ and

$$S = \sum_{j=0}^{v-1} \chi_v^j(\omega^s) = \sum_{j=0}^{v-1} e^{\frac{2\pi i}{v} sj}.$$

If $s \equiv 0 \pmod{v}$ then $e^{\frac{2\pi i}{v} sj} = 1$ and $S = v$. Otherwise, we have that $e^{\frac{2\pi i}{v} sj} \neq 1$ and thus we can apply the formula for a finite geometric sum, which yields

$$S = \sum_{j=0}^{v-1} e^{\frac{2\pi i}{v} sj} = \frac{(e^{\frac{2\pi i}{v} s})^v - 1}{e^{\frac{2\pi i}{v} s} - 1} = \frac{1 - 1}{e^{\frac{2\pi i}{v} s} - 1} = 0.$$

◻

A useful function

We now introduce a function that is used to indicate when a given set of column vectors of a cyclic trace array modulo v is covered. Let α be a primitive element of $\mathbb{F}_{q^t}$, v be a positive divisor of $q-1$, $\omega = \alpha^{[t]_q}$, and $I = \{i_0, \ldots, i_{t-1}\} \subseteq [0, [t]_q - 1]$. For $L = (l_0, \ldots, l_{t-1}) \in [0, v-1]^t$ and $r \in [0, q^t - 2]$, we define

$$h(\alpha, I, v, L; r) = \prod_{k=0}^{t-1} \left(\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k})\chi_v^j\left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_k})\right) \right). \tag{5.17}$$

The values of this function, which we give in the next lemma, can be expressed using the set

$$N_r(\alpha, I) = \left\{ k \in [0, t-1] \mid \mathrm{Tr}_{q^t/q}(\alpha^{r+i_k}) \neq 0 \right\}. \tag{5.18}$$

Lemma 5.17. *Let q be a prime power, v a positive divisor of $q - 1$, $\omega = \alpha^{[t]_q}$, $I = \{i_0, \ldots, i_{t-1}\}$, $L = (l_0, \ldots, l_{t-1})$, and $r \in [0, q^t - 2]$. Then, we have*

$$h(\alpha, I, v, L; r) = \begin{cases} v^{|N_r(\alpha, I)|} & \text{if } \log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \equiv l_k \pmod{v}, \text{ for all } k \in N_r(\alpha, I); \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if $N_r(\alpha, I) = \emptyset$ then $h(\alpha, I, v, L; r) = 1$.

Proof. We denote $\mathrm{Tr} = \mathrm{Tr}_{q^t/q}$. For $k \in [0, t - 1]$, we show that

$$\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j \left(\mathrm{Tr}(\alpha^{r+i_k}) \right) = \begin{cases} v & \text{if } \mathrm{Tr}(\alpha^{r+i_k}) \neq 0 \text{ and } \log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \equiv l_k \pmod{v}; \\ 0 & \text{if } \mathrm{Tr}(\alpha^{r+i_k}) \neq 0 \text{ and } \log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \not\equiv l_k \pmod{v}; \quad (5.19) \\ 1 & \text{if } \mathrm{Tr}(\alpha^{r+i_k}) = 0. \end{cases}$$

The first two cases are a straightforward application of Lemma 5.16 for $l = l_k$ and $y = \mathrm{Tr}(\alpha^{r+i_k})$. For the case when $\mathrm{Tr}(\alpha^{r+i_k}) = 0$ we recall that, by Definition 2.23, we have

$$\chi_v^j(0) = \begin{cases} 0 & \text{if } j \not\equiv 0 \pmod{v}; \\ 1 & \text{otherwise,} \end{cases}$$

and thus

$$\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j \left(\mathrm{Tr}(\alpha^{r+i_k}) \right) = \sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j(0) = \chi_v^0(\omega^{v-l_k}) \chi_v^0(0) = 1,$$

which proves the third case of Equation (5.19). Now, denoting $N_r = N_r(\alpha, I)$, we have

$$h(\alpha, I, v, L; r) = \prod_{\substack{k=0 \\ k \notin N_r}}^{t-1} \left(\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j \left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_k}) \right) \right) \prod_{\substack{k=0 \\ k \in N_r}}^{t-1} \left(\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j \left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_k}) \right) \right).$$

By Equation (5.19), the terms of the first product are all equal to 1, therefore,

$$h(\alpha, I, v, L; r) = \prod_{\substack{k=0 \\ k \in N_r}}^{t-1} \left(\sum_{j=0}^{v-1} \chi_v^j(\omega^{v-l_k}) \chi_v^j \left(\mathrm{Tr}_{q^t/q}(\alpha^{r+i_k}) \right) \right).$$

If for every $k \in N_r(\alpha, I)$ we have $\log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \equiv l_k \pmod{v}$, then, by Equation (5.19), every term of the product is equal to v and hence $h(\alpha, I, v, L; r) = v^{|N_r(\alpha, I)|}$. Otherwise, if for some $k \in N_r(\alpha, I)$ we have $\log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \not\equiv l_k \pmod{v}$, then, again by Equation (5.19), the corresponding term of the product is equal to 0 and hence $h(\alpha, I, v, L; r) = 0$. $\blacksquare$

The proof of Proposition 5.20

It follows from Lemma 5.17 that the values of $h(\alpha, I, v, L; r)$ are nonnegative integers. Next, we show that a specific value implies that one of the rows of $\mathcal{A}_{q^t/q}(\alpha, I; v)$ is equal to L.

> **Lemma 5.18.** *Let q be a prime power, v be a positive divisor of $q - 1$, $I \subseteq [0, [t]_q - 1]$ with $|I| = t$, and $L \in [0, v - 1]^t$. If $h(\alpha, I, v, L; r) = v^t$ for some $r \in [0, q^t - 2]$, then there exists a row of $\mathcal{A}_{q^t/q}(\alpha, I; v)$ equal to L.*

Proof. We denote $\mathrm{Seq}(\alpha; v) = \mathrm{Seq}_{q^t/q}(\alpha; v)$ and $\mathrm{Tr} = \mathrm{Tr}_{q^t/q}$. Let $r \in [0, q^t - 2]$ so that $h(\alpha, I, v, L; r) = v^t$. We index the rows of $\mathcal{A}_{q^t/q}(\alpha, I; v)$ by $[0, v[t]_q - 1]$ and let $s = r \bmod v[t]_q$. We show that the row of $\mathcal{A}_{q^t/q}(\alpha, I; v)$ with index s is equal to L; in other words, if $I = \{i_0, \dots, i_{t-1}\}$ and $L = \{l_0, \dots, l_{t-1}\}$, we show that

$$\left(\mathrm{Seq}(\alpha; v)_{s+i_0}, \dots, \mathrm{Seq}(\alpha; v)_{s+i_{t-1}}\right) = (l_0, \dots, l_{t-1}).$$

By Lemma 5.3, $\mathrm{Seq}(\alpha; v)$ has period $v[t]_q$, which implies that $\mathrm{Seq}(\alpha; v)_{s+i} = \mathrm{Seq}(\alpha; v)_{r+i}$ for every i, therefore we can equivalently show that

$$\left(\mathrm{Seq}(\alpha; v)_{r+i_0}, \dots, \mathrm{Seq}(\alpha; v)_{r+i_{t-1}}\right) = (l_0, \dots, l_{t-1}).$$

Since $h(r) = v^t$, by Lemma 5.17, we can make two deductions: first, $|N_r(\alpha, I)| = t$, and therefore $N_r(\alpha, I) = [0, t - 1]$; secondly,

$$\log_\omega(\mathrm{Tr}(\alpha^{r+i_k})) \equiv l_k \pmod{v}, \quad \text{for all } k \in [0, t - 1]. \tag{5.20}$$

By the definition of $N_r(\alpha, I)$ in Equation (5.18), the fact that $N_r(\alpha, I) = [0, t - 1]$ means that $\mathrm{Tr}(\alpha^{r+i_k}) \neq 0$, for all $k \in [0, t - 1]$. By Equation (5.4), this in turn implies that

$$\mathrm{Seq}(\alpha; v)_{r+i_k} = \log_\omega(\mathrm{Tr}(\alpha^{r+i_k})), \quad \text{for all } k \in [0, t - 1]. \tag{5.21}$$

Combining Equations (5.20) and (5.21), we conclude that $\mathrm{Seq}(\alpha; v)_{r+i_k} = l_k$, for all $k \in [0, t-1]$; from our previous discussion, this completes the proof. $\blacksquare$

> **Lemma 5.19.** *Let q be a prime power, v be a positive divisor of $q - 1$, $I \subseteq [0, [t]_q - 1]$ with $|I| = t$, and $S_i = S_i(\alpha, q, v, t)$, $i \in [0, [t]_q - 1]$ as defined in Equation (5.10). Furthermore, we denote*
>
> $$\sigma(\alpha, I, v, L) = \sum_{r=0}^{q^t-2} h(\alpha, I, v, L; r).$$
>
> *If for every $L \in [0, v - 1]^t$ we have that*
>
> $$\sigma(\alpha, I, v, L) \geq tvq^{t-1} - 1, \tag{5.22}$$
>
> *then the set $\{S_i \mid i \in I\}$ is covered.*

Proof. Let $I \subseteq [0, [t]_q - 1]$, $|I| = t$. By Definition 2.62, the set $\{S_i \mid i \in I\}$ is covered if, for every $L \in [0, v - 1]^t$, there exists a row of the $v[t]_q \times t$ array with columns S_i, $i \in I$, that is equal to L. However, by Remark 5.7 and the definition of S_i, this array is $\mathcal{A}_{q^t/q}(\alpha, I; v)$. Hence, by Lemma 5.18, a sufficient condition for $\{S_i \mid i \in I\}$ to be covered is that, for every L, there exists some r with $h(\alpha, I, v, L; r) = v^t$. Let

$$\sigma_n(\alpha, I, v, L) = \sum_{\substack{r=0 \\ |N_r(\alpha, I)| = n}}^{q^t - 2} h(\alpha, I, v, L; r), \quad n \in [0, t]. \tag{5.23}$$

We observe that if $|N_r(\alpha, I)| = t$ for some r, then by Lemma 5.17 we have that $h(\alpha, I, v, L; r)$ is equal to either 0 or v^t. Therefore, if $\sigma_t(\alpha, I, v, L) > 0$, then there exists r such that $h(\alpha, I, v, L; r) = v^t$. It follows from the above discussion that, to prove this lemma, it is sufficient to show for arbitrary L that, if Equation (5.22) holds, then $\sigma_t(\alpha, I, v, L) > 0$.

Let $I = \{i_0, \ldots, i_{t-1}\} \subseteq [0, [t]_q - 1]$, and $L = (l_0, \ldots, l_{t-1}) \in [0, v - 1]^t$. For the rest of the proof, we fix α, I, v and L, and we denote $h(r) = h(\alpha, I, v, L; r)$, $N_r = N_r(\alpha, I)$, $\sigma = \sigma(\alpha, I, v, L)$, and $\sigma_n = \sigma_n(\alpha, I, v, L)$. We observe that $\sigma = \sum_{n=0}^{t} \sigma_n$, and hence

$$\sigma_t = \sigma - \sum_{n=0}^{t-1} \sigma_n.$$

We evaluate the terms of the right hand side. First, for every r such that $|N_r| = 0$, we have that $N_r = \emptyset$ and thus $h(r) = 1$, by Lemma 5.17. This implies that σ_0 is equal to the number of r such that $N_r = \emptyset$ or, equivalently, the number of r such that

$$\left(\mathrm{Tr}(\alpha^{r+i_0}), \ldots, \mathrm{Tr}(\alpha^{r+i_{t-1}}) \right) = (0, \ldots, 0),$$

which is $q - 1$, by Corollary 5.13. We conclude that $\sigma_0 = q - 1$.

Next we examine σ_n for $n \in [1, t]$. We rewrite σ_n as

$$\sigma_n = \sum_{\substack{r=0 \\ |N_r| = n}}^{q^t - 2} h(r) = \sum_{\substack{J \subseteq [0, t-1] \\ |J| = n}} \sum_{\substack{r=0 \\ N_r = J}}^{q^t - 2} h(r). \tag{5.24}$$

We focus on the inner sum of the right hand side; for clarity, we assume without loss of generality that $J = [0, n - 1]$. Then,

$$\sum_{\substack{r=0 \\ N_r = J}}^{q^t - 2} h(r) = \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k}) \neq 0, \text{ all } k \in J \\ \mathrm{Tr}(\alpha^{r+i_k}) = 0, \text{ all } k \notin J}}^{q^t - 2} h(r) = \sum_{b_0, \ldots, b_{n-1} \in \mathbb{F}_q^\times} \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k}) = b_i, \text{ all } k \in I \\ \mathrm{Tr}(\alpha^{r+i_k}) = 0, \text{ all } k \notin I}}^{q^t - 2} h(r).$$

Since $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is a linearly dependent $(t, t-1)$-set, there exist $y_i \in \mathbb{F}_q^\times$ such that $\sum_{k=0}^{t-1} y_k \alpha^{i_k} = 0$ (see Corollary 5.13). Defining $b_k = 0$ for $k \in [n, t-1]$, we have from Corollary 5.13 that there are no r satisfying the conditions of the inner sum unless

$$\sum_{k=0}^{t-1} y_k b_k = \sum_{k=0}^{n-1} y_k b_k = 0. \tag{5.25}$$

Now, since $J = [0, n-1]$ and $n \geq 1$, we have that $b_0 \neq 0$; since y_0 is also nonzero, Equation (5.25) does not hold when $n = 1$. We conclude that there are no r satisfying the condition of the inner sum of the right hand side of Equation (5.24), and hence $\sigma_1 = 0$.

We have shown that $\sigma_0 = q - 1$ and $\sigma_1 = 0$; next, we consider the case $n \in [2, t]$. We have

$$\sum_{\substack{r=0 \\ N_r = J}}^{q^t-2} h(r) = \sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \sum_{k=0}^{n-1} y_k b_k = 0}} \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k})=b_k,\, \text{all } k\in J \\ \mathrm{Tr}(\alpha^{r+i_k})=0,\, \text{all } k\notin J}}^{q^t-2} h(r).$$

We can break the sum on the right hand side as

$$\sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \sum_{k=0}^{n-1} y_k b_k = 0 \\ \text{and} \\ \log_\omega(b_k)\equiv l_k(\mathrm{mod}\ v) \\ \text{for all } k\in[0,n-1]}} \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k})=b_k,\, \text{all } k\in J \\ \mathrm{Tr}(\alpha^{r+i_k})=0,\, \text{all } k\notin J}}^{q^t-2} h(r) + \sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \sum_{k=0}^{n-1} y_k b_k = 0 \\ \text{and} \\ \log_\omega(b_k)\not\equiv l_k(\mathrm{mod}\ v) \\ \text{for some } k\in[0,n-1]}} \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k})=b_k,\, \text{all } k\in J \\ \mathrm{Tr}(\alpha^{r+i_k})=0,\, \text{all } k\notin J}}^{q^t-2} h(r).$$

From Lemma 5.17, we have that $h(r) = v^n$ for all r in the first double sum, and $h(r) = 0$ for all r in the second double sum. Therefore

$$\sum_{\substack{r=0 \\ N_r = J}}^{q^t-2} h(r) = \sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \sum_{k=0}^{n-1} y_k b_k = 0 \\ \text{and} \\ \log_\omega(b_k)\equiv l_k(\mathrm{mod}\ v) \\ \text{for all } k\in[0,n-1]}} \sum_{\substack{r=0 \\ \mathrm{Tr}(\alpha^{r+i_k})=b_k,\, \text{all } k\in J \\ \mathrm{Tr}(\alpha^{r+i_k})=0,\, \text{all } k\notin J}}^{q^t-2} v^n.$$

It follows from Corollary 5.13 that there exist exactly q elements $r \in [0, q^t - 2]$ that satisfy the conditions of the inner sum, and therefore the equality becomes

$$\sum_{\substack{r=0 \\ N_r = J}}^{q^t-2} h(r) = \sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \sum_{k=0}^{n-1} y_k b_k = 0 \\ \text{and} \\ \log_\omega(b_k)\equiv l_k(\mathrm{mod}\ v) \\ \text{for all } k\in[0,n-1]}} q v^n. \tag{5.26}$$

We claim that there are at most $((q-1)/v)^{n-1}$ n-tuples $(b_0, \ldots, b_{n-1})$ satisfying the conditions of the sum on the right hand side. Since $v | q - 1$, for every $l \in [0, v-1]$ there exist exactly $(q-1)/v$ elements $y \in [0, q-2]$ such that $y = l \bmod v$. For each such y, there exists a unique $b \in \mathbb{F}_q^\times$ such that $\log_\omega(b) = y$. From the above, we conclude that for every $l \in [0, v-1]$ there exist precisely $(q-1)/v$ elements $b \in \mathbb{F}_q^\times$ such that $l = \log_\omega(b) \bmod v$. Thus, there exist $((q-1)/v)^{n-1}$ choices of $b_0, \ldots, b_{n-2} \in \mathbb{F}_q^\times$ such that

$$(l_0, \ldots, l_{n-2}) = \left(\log_\omega(b_0) \bmod v, \ldots, \log_\omega(b_{n-2}) \bmod v\right). \tag{5.27}$$

For every such choice, consider the unique $b_{n-1} \in \mathbb{F}_q^{\times}$ such that $\sum_{k=0}^{n-1} y_k b_k = 0$. Then, the condition of the outer sum is satisfied if and only if $\log_{\omega}(b_{n-1}) \equiv l_{n-1} \pmod{v}$, which holds if and only if

$$\log_{\omega}(b_{n-1})\log_{\omega}\left(-\sum_{k=0}^{n-2} \frac{y_k}{y_{n-1}} b_k\right) \equiv l_{n-1} \pmod{v}.$$

This does not necessarily hold for all $((q-1)/v)^{n-1}$ choices of $b_0, \ldots, b_{n-2}$, therefore there are indeed at most that many choices of n-tuples $(b_0, \ldots, b_{n-1})$ satisfying the conditions of the last sum, as we claimed. It follows from the above and Equation (5.26) that

$$\sum_{\substack{r=0 \\ N_r=J}}^{q^t-2} h(r) \leq \left(\frac{q-1}{v}\right)^{n-1} q v^n.$$

From this and Equation (5.24) we conclude that, for all $n \in [2, t-1]$, we have

$$\sigma_n \leq \sum_{\substack{J \subseteq [0,t-1] \\ |J|=n}} \left(\frac{q-1}{v}\right)^{n-1} q v^n = \binom{t}{n}(q-1)^{n-1} q v.$$

Now, solving for σ_t in $\sigma = \sum_{n=0}^t \sigma_n$, yields

$$\sigma_t = \sigma - \sigma_0 - \sigma_1 - \sum_{n=2}^{t-1} \sigma_n$$

$$= \sigma - (q-1) - 0 - \sum_{n=2}^{t-1} \sigma_n$$

$$\geq \sigma - (q-1) - \sum_{n=2}^{t-1} \binom{t}{n}(q-1)^{n-1} q v.$$

Thus, a sufficient condition for $\sigma_t > 0$ to hold is for the last expression to be positive, or equivalently

$$\sigma > q - 1 + \sum_{n=2}^{t-1} \binom{t}{n}(q-1)^{n-1} q v$$

$$= q - 1 + q v \left(\frac{q^t - 1}{q - 1} - (q-1)^{t-1} - t\right).$$

We observe that $tvq^{t-1} - 1 > q - 1 + qv(\frac{q^t-1}{q-1} - (q-1)^{t-1} - t)$, so a simpler sufficient condition for σ_t to be positive is $\sigma \geq tvq^{t-1} - 1$ as given in Equation (5.22). From the discussion in the beginning, this completes the proof.

We now have everything we need in order to prove the analogue of Proposition 5.14 for the case of a linearly dependent $(t, t-1)$-set.

Proposition 5.20. *Let t be a positive integer, α be a primitive element of $\mathbb{F}_{q^t}$, $v \geq 2$ be a divisor of $q-1$, and $S_i = S_i(\alpha, q, v, t)$, $i \in [0, [t]_q - 1]$ as defined in Equation (5.10). For $I \subseteq [0, [t]_q - 1]$ with $|I| = t$ such that $\{\alpha^i \mid i \in I\}$ is a linearly dependent $(t, t-1)$-set. If furthermore*

$$q^{\frac{t}{2}-2}(q - tv) > v^{t-1}, \tag{5.28}$$

then the set $\{S_i \mid i \in I\}$ is covered.

Proof. To prove this proposition, it is sufficient to show that if Equation (5.28) holds, then Equation (5.22) holds for every $L \in [0, v-1]^t$; the proof then is complete by Lemma 5.19. Throughout the proof we fix $\alpha, v, I = \{i_0, \ldots, i_{t-1}\}$, $L = (l_0, \ldots, l_{t-1})$, and we denote $\sigma = \sigma(\alpha, I, v, L)$, $h(r) = h(\alpha, I, v, L; r)$, $\text{Tr} = \text{Tr}_{q^t/q}$, and $\omega_k = \omega^{v-l_k}$ where, as usual, $\omega = \alpha^{[t]_q}$. We rewrite σ as

$$\sigma = \sum_{r=0}^{q^t-2} h(r) = \sum_{r=0}^{q^t-2} \prod_{k=0}^{t-1} \left(\sum_{j=0}^{v-1} \chi_v^j(\omega_k) \chi_v^j \left(\text{Tr}(\alpha^{r+i_k}) \right) \right)$$

$$= \sum_{r=0}^{q^t-2} \prod_{k=0}^{t-1} \left(1 + \sum_{j=1}^{v-1} \chi_v^j(\omega_k) \chi_v^j \left(\text{Tr}(\alpha^{r+i_k}) \right) \right)$$

$$= q^t - 1 + \sum_{\substack{U \subseteq [0,t-1] \\ U \neq \emptyset}} \sum_{r=0}^{q^t-2} \prod_{u \in U} \sum_{j=1}^{v-1} \chi_v^j(\omega_u) \chi_v^j \left(\text{Tr}(\alpha^{r+i_u}) \right)$$

$$= q^t - 1 + \sum_{n=1}^{t} \sum_{\substack{U \subseteq [0,t-1] \\ U = \{u_0, \ldots, u_{n-1}\}}} \sum_{r=0}^{q^t-2} \prod_{s=0}^{n-1} \sum_{j=1}^{v-1} \chi_v^j(\omega_{u_s}) \chi_v^j(\alpha^{r+i_{u_s}})$$

$$= q^t - 1 + \sum_{n=1}^{t} \sum_{\substack{U \subseteq [0,t-1] \\ U = \{u_0, \ldots, u_{n-1}\}}} \sum_{\substack{j_0, \ldots, j_{n-1} \\ \in [1, v-1]}} \sum_{r=0}^{q^t-2} \prod_{s=0}^{n-1} \chi_v^{j_s}(\omega_{u_s}) \chi_v^{j_s} (\text{Tr}(\alpha^{r+u_s}))$$

$$= q^t - 1 + \sum_{n=1}^{t} \sum_{\substack{U \subseteq [0,t-1] \\ U = \{u_0, \ldots, u_{n-1}\}}} \sum_{\substack{j_0, \ldots, j_{n-1} \\ \in [1, v-1]}} \prod_{s=0}^{n-1} \chi_v^{j_s}(\omega_{u_s}) \sum_{r=0}^{q^t-2} \prod_{s=0}^{n-1} \chi_v^{j_s} (\text{Tr}(\alpha^{r+u_s})) \tag{5.29}$$

We first examine the terms of the expression in Equation (5.29) corresponding to $n \leq t - 1$. We focus on the last sum of the right hand side of Equation (5.29). Let $N(b_0, \ldots, b_{n-1})$ be the number of $r \in [0, q^t - 2]$ such that

$$\left(\text{Tr}(\alpha^{r+i_{u_0}}), \ldots, \text{Tr}(\alpha^{r+i_{u_{n-1}}}) \right) = (b_0, \ldots, b_{n-1}). \tag{5.30}$$

Then, we can rewrite the right hand side of Equation (5.29) as

$$\sum_{r=0}^{q^t-2}\prod_{s=0}^{n-1}\chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_{u_s}})\right) = \sum_{r=0}^{q^t-2}\chi_v^{j_0}\left(\mathrm{Tr}(\alpha^{r+i_{u_0}})\right)\cdots\chi_v^{j_{n-1}}\left(\mathrm{Tr}(\alpha^{r+i_{u_{n-1}}})\right)$$

$$= N(b_0,\ldots,b_{n-1})\sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q \\ \text{Eq. (5.30), some } r}}\chi_v^{j_0}(b_0)\cdots\chi_v^{j_{n-1}}(b_{n-1}),\qquad(5.31)$$

where the sum runs over all $b_0,\ldots,b_{n-1}\in\mathbb{F}_q$ for which there exists some $r\in[0,q^t-2]$ such that Equation (5.30) holds.

Since $\chi_v^j(0)=0$ for all $j\in[1,v-1]$, all the sum terms in Equation (5.31) where any of $b_0,\ldots,b_{n-1}$ is zero, vanish. Hence, we have that

$$\sum_{r=0}^{q^t-2}\prod_{s=0}^{n-1}\chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_{u_s}})\right) = N(b_0,\ldots,b_{n-1})\sum_{\substack{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times \\ \text{Eq. (5.30)}}}\chi_v^{j_0}(b_0)\cdots\chi_v^{j_{n-1}}(b_{n-1}),\qquad(5.32)$$

where the sum runs over all $b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times$ for which there exists $r\in[0,q^t-2]$ such that Equation (5.30) holds. Now, we observe that the left hand side of Equation (5.30) is the row of index r of $\mathcal{A}_{q^t/q}(\alpha,\{i_{u_0},\ldots,i_{u_{n-1}}\})$. This is an $\mathrm{OA}_{q^{t-n}}(n,n,q)$ by Proposition 3.10, since $\{\alpha^{i_{u_0}},\ldots,\alpha^{i_{u_{n-1}}}\}$ is linearly independent as a subset of size $n\le t-1$ of $\{\alpha^{i_0},\ldots,\alpha^{i_{t-1}}\}$, which is a $(t,t-1)$-set from our assumptions. We conclude that, for every $b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times$, there exist precisely $N(b_0,\ldots,b_{n-1})=q^{n-t}$ elements $r\in[0,q^t-2]$ such that Equation (5.30) holds, and therefore Equation (5.32) becomes

$$\sum_{r=0}^{q^t-2}\prod_{s=0}^{n-1}\chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_{u_s}})\right) = q^{n-t}\sum_{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times}\chi_v^{j_0}(b_0)\cdots\chi_v^{j_{n-1}}(b_{n-1}),\qquad(5.33)$$

where this time the sum runs over all elements $b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times$. By Lemma 2.25, we have

$$\sum_{b_0,\ldots,b_{n-1}\in\mathbb{F}_q^\times}\chi_v^{j_0}(b_0)\cdots\chi_v^{j_{n-1}}(b_{n-1})=0,\qquad(5.34)$$

hence, from Equations (5.33) and (5.34) we have that, for all $n\in[1,t-1]$,

$$\sum_{r=0}^{q^t-2}\prod_{s=0}^{n-1}\chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_{u_s}})\right)=0.$$

This shows that the terms corresponding to $n\in[1,t-1]$ of the sum in Equation (5.29) vanish. Therefore, the only term remaining is for $n=t$, which means that $U=[0,t-1]$, and

$$\sigma = q^t-1+\sum_{\substack{j_0,\ldots,j_{t-1} \\ \in[1,v-1]}}\prod_{s=0}^{t-1}\chi_v^{j_s}(\omega_{i_s})\sum_{r=0}^{q^t-2}\prod_{s=0}^{t-1}\chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_s})\right).\qquad(5.35)$$

Now, since $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$ is a linearly dependent $(t, t-1)$-set, there exist $y_0, \ldots, y_{t-1} \in \mathbb{F}_q^\times$ such that $\sum_{s=0}^{t-1} y_s \alpha^{i_s} = 0$ (see Corollary 5.13). Multiplying the equation by α^r yields $\sum_{s=0}^{t-1} y_s \alpha^{r+i_s} = 0$, and applying the trace, which is linear over $\mathbb{F}_q$, yields $\sum_{s=0}^{t-1} y_s \mathrm{Tr}(\alpha^r \alpha^{i_s}) = 0$. Solving for the term corresponding to $s = t-1$, we get

$$\mathrm{Tr}(\alpha^{r+i_{t-1}}) = -\sum_{s=0}^{t-2} \frac{y_s}{y_{t-1}} \mathrm{Tr}(\alpha^{r+i_s}). \tag{5.36}$$

Hence, Equation (5.35) becomes

$$\sigma - q^t + 1 = \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in [1,v-1]}} \prod_{s=0}^{t-1} \chi_v^{j_s}(\omega_s) \sum_{r=0}^{q^t-2} \chi_v^{j_{t-1}}\left(\mathrm{Tr}\left(\alpha^{r+i_{t-1}}\right)\right) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_s})\right),$$

and by

$$\sigma - q^t + 1 = \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in [1,v-1]}} \prod_{s=0}^{t-1} \chi_v^{j_s}(\omega_s) \sum_{r=0}^{q^t-2} \chi_v^{j_{t-1}}\left(-\sum_{s=0}^{t-2} \frac{y_s}{y_{t-1}} \mathrm{Tr}(\alpha^{r+i_s})\right) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\mathrm{Tr}(\alpha^{r+i_s})\right).$$

We note that $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-2}}\}$ is linearly independent as a subset of size $t-1$ of the $(t, t-1)$-set $\{\alpha^{i_0}, \ldots, \alpha^{i_{t-1}}\}$. Hence, by Proposition 3.10, $\mathcal{A}_0(\alpha, \{i_0, \ldots, i_{t-1}\})$ is an $\mathrm{OA}_q(t-1, t-1, q)$. This implies that, for every $b_0, \ldots, b_{t-2} \in \mathbb{F}_q^\times$, there exist exactly q rows equal to $(b_0, \ldots, b_{t-2})$, i.e. there exist exactly exactly q values of $r \in [0, q^t - 2]$ such that

$$\left(\mathrm{Tr}(\alpha^{r+i_0}), \ldots, \mathrm{Tr}(\alpha^{r+i_{t-2}})\right) = (b_0, \ldots, b_{t-2}).$$

Thus, we have that

$$\sigma - q^t + 1 = \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in [1,v-1]}} \prod_{s=0}^{t-1} \chi_v^{j_s}(\omega_s) \; q \sum_{b_0,\ldots,b_{t-2}\in\mathbb{F}_q^\times} \chi_v^{j_{t-1}}\left(-\sum_{s=0}^{t-2} \frac{y_s}{y_{t-1}} b_s\right) \prod_{s=0}^{t-2} \chi_v^{j_s}(b_s)$$

$$= \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in [1,v-1]}} \prod_{s=0}^{t-1} \chi_v^{j_s}(\omega_s) \; q \sum_{z\in\mathbb{F}_q^\times} \chi_v^{j_{t-1}}(z) \sum_{\substack{b_0,\ldots,b_{t-2}\in\mathbb{F}_q^\times \\ z=-\sum_{s=0}^{t-2}\frac{y_s}{y_{t-1}} b_s}} \prod_{s=0}^{t-2} \chi_v^{j_s}(b_s).$$

We recall that $y_s \neq 0$ for all s, so we can normalize the last sum by substituting b_s with $-\frac{z y_{t-1}}{y_s} b_s$. This yields

$$\sigma - q^t + 1 = \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in [1,v-1]}} \prod_{s=0}^{t-1} \chi_v^{j_s}(\omega_s) \; q \sum_{z\in\mathbb{F}_q^\times} \chi_v^{j_{t-1}}(z) \sum_{\substack{b_0,\ldots,b_{t-2}\in\mathbb{F}_q^\times \\ b_0+\cdots+b_{t-2}=1}} \prod_{s=0}^{t-2} \chi_v^{j_s}\left(-\frac{z y_{t-1}}{y_s} b_s\right). \tag{5.37}$$

Since the characters are multiplicative, we have that

$$\prod_{s=0}^{t-2} \chi_v^{j_s}\left(-\frac{z y_{t-1}}{y_s} b_s\right) = \prod_{s=0}^{t-2} \chi_v^{j_s}(z) \chi_v^{j_s}\left(\frac{-y_t}{y_s}\right) \chi_v^{j_s}(b_s)$$

$$= \chi_v^{j_0+\cdots+j_{t-2}}(z) \prod_{s=0}^{t-2} \chi_v^{j_s} \left(\frac{-y_{t-2}}{y_s}\right) \chi_v^{j_s}(b_s),$$

Substituting this in Equation (5.37), we get

$$\sigma - q^t + 1 = q \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in[1,v-1]}} \chi_v^{j_{t-1}}(\omega_{t-1}) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\frac{-y_{t-1}\omega_s}{y_s}\right) \sum_{z\in\mathbb{F}_q^\times} \chi_v^{j_0+\cdots+j_{t-1}}(z) \sum_{\substack{b_0,\ldots,b_{t-2}\in\mathbb{F}_q^\times \\ b_0+\cdots+b_{t-2}=1}} \prod_{s=0}^{t-2} \chi_v^{j_s}(b_s).$$

By Definition 2.26, the last sum is a Jacobi sum and we have

$$\sigma - q^t + 1 = q \sum_{\substack{j_0,\ldots,j_{t-1} \\ \in[1,v-1]}} \chi_v^{j_{t-1}}(\omega_{t-1}) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\frac{-y_{t-1}\omega_s}{y_s}\right) \sum_{z\in\mathbb{F}_q^\times} \chi_v^{j_0+\cdots+j_{t-1}}(z) \mathcal{J}(\chi_v^{j_0},\ldots,\chi_v^{j_{t-2}}).$$

Since χ_v is a character of order v, we have that χ_v^n is the trivial character if and only if $n \equiv 0 \pmod{v}$. Thus, from Theorem 2.22 we have that

$$\sum_{z\in\mathbb{F}_q^\times} \chi_v^{j_0+\cdots+j_{t-1}}(z) = \begin{cases} q-1 & \text{if } j_0+\cdots+j_{t-1} \equiv 0 \pmod{v}; \\ 0 & \text{otherwise.} \end{cases}$$

Therefore our equation becomes

$$\sigma - q^t + 1 = q(q-1) \sum_{\substack{j_0,\ldots,j_{t-1}\in[1,v-1] \\ j_0+\cdots+j_{t-1}\equiv 0(\text{mod } v)}} \chi_v^{j_{t-1}}(\omega_{t-1}) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\frac{-y_{t-1}\omega_s}{y_s}\right) \mathcal{J}(\chi_v^{j_0},\ldots,\chi_v^{j_{t-2}}). \quad (5.38)$$

For all $1 \le j_0,\ldots,j_{t-1} \le v-1$ such that $j_0+\cdots+j_{t-1} \equiv 0 \pmod{v}$, we have

$$j_0+\cdots+j_{t-2} \equiv -j_{t-1} \not\equiv 0 \pmod{v},$$

since $j_{t-1} \in [1,v-1]$. Hence $\prod_{i=0}^{t-1} \chi_v^{j_i}$ is a nontrivial character, and by Theorem 2.27 we have that $|\mathcal{J}(\chi_v^{j_0},\ldots,\chi_v^{j_{t-2}})| = q^{\frac{t}{2}-1}$. Furthermore, the codomain of characters is $\mathbb{C}^\times$, so they are absolutely bounded by 1 and hence

$$\left|\chi_v^{j_{t-1}}(\omega_{t-1}) \prod_{s=0}^{t-2} \chi_v^{j_s}\left(\frac{-y_{t-1}\omega_s}{y_s}\right)\right| \le 1.$$

Thus, applying absolute values to Equation (5.38) yields

$$\left|\sigma - q^t + 1\right| \le q(q-1) \sum_{\substack{j_0,\ldots,j_{t-1}\in[1,v-1] \\ j_0+\cdots+j_{t-1}\equiv 0 \ (\text{mod } v)}} q^{\frac{t}{2}-1}.$$

Using inclusion-exclusion we deduce that the number of $j_0,\ldots,j_{t-1}$ satisfying the conditions of the sum above is

$$S = \sum_{n=1}^{t-1} (-1)^{t-n-1}(v-1)^n.$$

Thus

$$|\sigma - q^t + 1| \leq q(q-1)q^{\frac{t}{2}-1}S$$

$$\leq q^{\frac{t}{2}}(q-1)\sum_{n=1}^{t-1}(-1)^{t-n-1}(v-1)^n$$

$$= q^{\frac{t}{2}}(q-1)\frac{(v-1)^t + (-1)^t(v-1)}{v},$$

which implies that

$$\sigma \geq q^t - 1 - q^{\frac{t}{2}}(q-1)\frac{(v-1)^t + (-1)^t(v-1)}{v}. \tag{5.39}$$

From the lower bound for σ in Equation (5.39), it follows that Equation (5.22) is satisfied if

$$q^t - 1 - q^{\frac{t}{2}}(q-1)\frac{(v-1)^t + (-1)^t(v-1)}{v} \geq tvq^{t-1} - 1.$$

Using the fact that

$$v^{t-1} \geq \frac{(v-1)^t + (-1)^t(v-1)}{v},$$

we have that a simpler sufficient condition is $q^{\frac{t}{2}-1}(q-tv) \geq v^{t-1}$. Equation (5.22) is satisfied. From the discussion in the beginning, this completes the proof. □

5.4 Evaluation of our construction

5.4.1 Comparison with covering arrays from cyclotomy

Colbourn [25] constructs covering arrays using cyclotomic generators over finite fields. These are CA$(q; t, q, v)$ for t, q, v satisfying $v|q - 1$ and $q > t^2 v^{2t}$, and are referred to as *covering arrays from cyclotomy*. The techniques used to provide covering arrays from cyclotomy and *covering arrays from maximal sequences* are similar and, as far as we know, they are the only direct constructions that provide a CA$(N; t, k, v)$ for any arbitrary t, k and v.

The main similarity of the two constructions is that they start with a function whose values are uniformly distributed over the field, and take the logarithm. Furthermore, in both constructions, the conditions that guarantee the covering array property rely on the evaluation of similar character sums. On the other hand, the resulting arrays have different dimensions and existence conditions.

In what follows, we consider v and t fixed and analyze when maximal sequences yield "better" covering arrays than covering arrays from cyclotomy. Let $k_{t,v}(q)$ and $N_{t,v}(q)$ be the number of columns and number of rows in the maximal sequence construction, respectively,
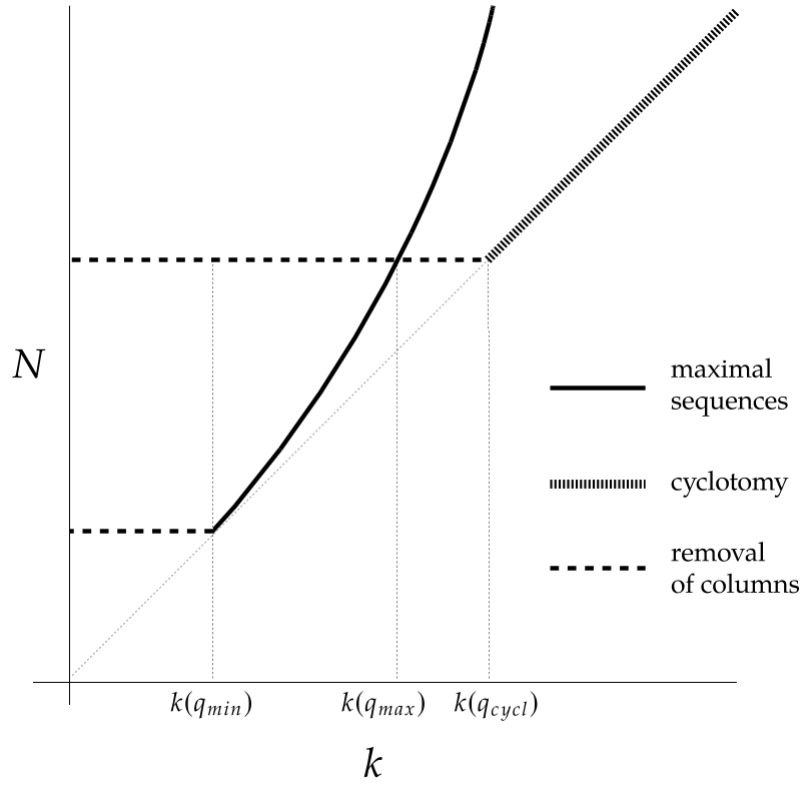
Figure 5.1. Comparison of the sizes of covering arrays from maximal sequences and covering arrays from cyclotomy, for fixed t and v.

that is

$$
k_{t,v}(q) = \begin{cases} q^2 + q + 1 & \text{if } t = 3, \\ q^2 + 1 & \text{if } t = 4, \\ \sim q + \lfloor \sqrt{2q} \rfloor & \text{if } t \geq 5, \end{cases} \quad \text{and} \quad N_{t,v}(q) = v\frac{q^t - 1}{q - 1}.
$$

We define

$q_{min}(t, v) = \min \{q \mid \text{ a CA}(N_{t,v}(q); t, k_{t,v}(q), v) \text{ can be constructed from maximal sequences}\}$,

$q_{cycl}(t, v) = \min \{q \mid \text{ a CA}(q; t, q, v) \text{ can be constructed from cyclotomy}\}$.

If $N_{t,v}(q_{min}(t, v)) < q_{cycl}(t, v)$, we further define

$$
q_{max}(t, v) = \max \{q \mid q \geq q_{min}(t, v) \text{ and } N_{t,v}(q) < q_{cycl}(t, v)\}.
$$

and note that for all prime powers q such that $q_{min}(t, v) \leq q \leq q_{max}(t, v)$, covering arrays from maximal sequences have fewer rows than covering arrays from cyclotomy for the same number of columns.

In Figure 5.1, we give the graph of N as a function of k for the CA$(N; t, k, v)$ that can be constructed from cyclotomy and maximal sequences. The horizontal doted lines are justified since when we remove some columns from a covering array we obtain another covering array.

v	t	q_{min}	q_{max}	v	t	q_{min}	q_{max}	v	t	q_{min}	q_{max}
3	3	16	16	12	8	313	337	12	9	277	313
4	4	37	37	12	9	277	313	12	10	277	289
4	5	37	37	12	10	277	289	13	7	443	443
4	6	29	29	13	7	443	443	13	10	313	313
5	5	61	61	13	10	313	313	14	8	449	463
6	5	97	97	14	8	449	463	14	9	421	421
6	6	73	79	14	9	421	421	14	10	379	379
6	7	67	79	14	10	379	379	15	7	601	601
6	8	67	73	15	7	601	601	15	8	541	541
6	9	67	67	15	8	541	541	15	10	421	421
6	10	67	67	15	10	421	421	16	8	593	641
7	6	113	127	16	8	593	641	16	9	529	593
7	7	113	113	16	9	529	593	16	10	529	529
8	5	193	193	16	10	529	529	17	9	613	647
8	6	169	169	17	9	613	647	17	10	613	613
8	7	137	137	17	10	613	613	18	8	811	829
8	8	121	137	18	8	811	829	18	9	739	757
8	9	113	121	18	9	739	757	18	10	631	631
8	10	113	121	18	10	631	631	19	10	761	761
9	7	181	199	19	10	761	761	20	8	1021	1021
9	8	163	181	20	8	1021	1021	20	9	881	961
9	9	163	163	20	9	881	961	20	10	821	881
9	10	163	163	20	10	821	881	21	9	1009	1051
10	6	271	281	21	9	1009	1051	21	10	967	967
10	7	241	251	21	10	967	967	22	8	1277	1277
10	8	211	211	22	8	1277	1277	22	9	1123	1123
10	9	181	211	22	9	1123	1123	22	10	1013	1013
10	10	181	191	22	10	1013	1013	23	9	1289	1289
11	6	353	353	23	9	1289	1289	23	10	1151	1151
11	8	243	243	23	10	1151	1151	24	9	1369	1369
11	9	243	243	24	9	1369	1369	24	10	1249	1321
11	10	243	243	24	10	1249	1321				
12	7	349	373	12	8	313	337				

Table 5.5. A sample of values of v, t where $v \leq 24$, $t \leq 10$, and the corresponding $q_{min} = q_{min}(v, t)$ and $q_{max} = q_{max}(v, t)$. For any prime power q such that $q | v - 1$ and $q_{min} \leq q \leq q_{max}$, covering arrays from maximal sequences can be constructed with fewer rows than covering arrays from cyclotomy with the same number of columns.

In Table 5.5, we list for $2 \leq v \leq 25$ and $2 \leq t \leq 10$, the nonempty intervals $q_{min}(v, t) \leq q \leq q_{max}(v, t)$, q a prime power, where a covering array from maximal sequences yields fewer rows than the corresponding covering array from cyclotomy. We note that both in this work and in [25], the conditions that guarantee the existence of the covering arrays can be replaced with slightly better (weaker) but more complicated conditions found in the proofs. The compilation of Table 5.5 was done by taking into account these better conditions for both constructions.

5.4.2 *Experimental results*

Equation (5.9) gives a theoretical lower bound on q to guarantee the existence of a covering array. Values of q smaller than this theoretical bound can yield covering arrays. To test this, we created the arrays described in Corollaries 5.10 and 5.11 for values of q and v, $v|q - 1$, for which experiments were computationally feasible and checked if they were covering arrays. This was often true for values of q smaller than the required condition, as demonstrated in Tables 5.6a and 5.6b. As before, the theoretical guarantee is calculated using the weaker, more complicated conditions for q that follow from the proofs in Section 5.3, rather than the conditions in Corollaries 5.10 and 5.11.

v	Successful q below theoretical guarantee	Values of q tested	Theoretical guarantee
2	None	$q < 7$	$q \geq 7$
3	None	$q < 19$	$q \geq 19$
4	$q \geq 37$, except 41	$q < 61$	$q \geq 61$
5	$q \geq 81$, except 101	$q < 181$	$q \geq 181$
6	$q \geq 103$, except $109, 139, 157, 223, 277$	$q < 439$	$q \geq 439$
7	$q \geq 169$	$q \leq 379$	$q \geq 953$
8	$193, 241, 281, 313$	$q \leq 337$	$q \geq 1849$
9	289	$q \leq 523$	$q \geq 3259$
10	361	$q \leq 491$	$q \geq 5261$
11	$243, 397$	$q \leq 463$	$q \geq 8273$
12	None	$q \leq 457$	$q \geq 12241$

(a) Ranges for q such that $v|q-1$ and q being a prime power is sufficient for the construction of a $CA(v(q^2 + q + 1); 3, q^2 + q + 1, v)$ as per Corollary 5.10

v	Successful q below theoretical guarantee	Values of q tested	Theoretical guarantee
2	$q \geq 5$	$q < 9$	$q \geq 9$
3	$q \geq 13$	$q < 19$	$q \geq 19$
4	$q \geq 25$	$q < 37$	$q \geq 37$
5	$31 \leq q \leq 61$	$q \leq 61$	$q \geq 81$
6	49	$q \leq 49$	$q \geq 139$
7	None	$q \leq 43$	$q \geq 239$
8	None	$q \leq 49$	$q \geq 337$

(b) Ranges for q such that $v|q-1$ and q being a prime power is sufficient for the construction of a $CA(v(q^3 + q^2 + q + 1); 4, q^2 + 1, v)$ as per Corollary 5.11.

Table 5.6. Experimental results and comparison with theoretical guarantee

A preliminary computation of the number of t-tuples in cyclic trace arrays modulo v

LET q BE A PRIME POWER, $t > 2$ be an integer, $v \geq 2$ be a divisor of $q - 1$, α be a primitive element of $\mathbb{F}_{q^t}$, and $C \subseteq [0, [t]_q - 1]$ such that $\{\alpha^c \mid c \in C\}$ is a $(|C|, t - 1)$-set. In Chapter 5 we showed by means of a character sum argument that when

$$q^{\frac{t}{2}-2}(q - tv) \geq v^{t-1}, \tag{6.1}$$

then $\mathcal{A}_{q^t/q}(\alpha, C; v)$ is a $\mathrm{CA}(v[t]_q; t, |C|, v)$. As we demonstrated in Section 5.4.2, the bound in Equation (6.1) appears to be weak, that is, covering arrays are produced for q smaller than this bound. In this chapter, we develop another approach to determine when covering arrays are obtained, based on bounding the number of rows that contain different t-tuples. In Section 6.1 we give the necessary preliminaries and in Section 6.2 we give upper and lower bounds for this number, that we express as the solutions of a linear program.

The contents of this chapter are preliminary work which has also been submitted as an extended abstract [69].

6.1 Preliminaries

For the rest of the chapter, we fix the notation of q, t, v and α as in the introduction and let $\omega = \alpha^{[t]_q}$, which is a primitive element of $\mathbb{F}_q$ as shown in Lemma 2.44. Furthermore, we define M to be the $(q - 1) \times (q - 1)$ array, whose (i, j)-th element for $(i, j) \in [0, q^t - 2]^2$ is given by

$$M_{ij} = \begin{cases} \log_\omega(\mathrm{Tr}_{q^t/q}(\alpha^{i+j})) \bmod v, & \text{if } \mathrm{Tr}_{q^t/q}(\alpha^{i+j}) \neq 0; \\ 0, & \text{otherwise.} \end{cases}$$

We index the rows and columns of M by $[0, q^t - 2]$.

We start with some preliminary observations. Let $I \subseteq [0, q^t - 2]$ with $|I| = s$ and let M_I be the $(q^t - 1) \times s$ subarray of M defined by the columns with indexes in I. For $\mathbf{b} \in \mathbb{Z}_v^s$, let $\lambda_{\mathbf{b}}$ denote the number of rows in M_I equal to $\mathbf{b}$. From a similar argument as the one we used for Equation (5.27) we observe that, if there are r zeros in $\mathbf{b}$, then there are $(\frac{q-1}{v})^{s-r}(\frac{q+v-1}{v})^r$ pre-images under the $\log_\omega$. It follows that

$$\lambda_{\mathbf{b}} = \left(\frac{1}{v}\right)^s (q - 1)^{s-r}(q + v - 1)^r \tag{6.2}$$

if $\{\alpha^i \mid i \in I\}$ is linearly independent, and

$$0 \leq \lambda_{\mathbf{b}} \leq q \left(\frac{1}{v}\right)^s (q-1)^{s-r}(q+v-1)^r$$

otherwise. Our goal is to improve these bounds. Let $C \subseteq [0, q^t - 2]$ such that $\{\alpha^c \mid c \in C\}$ is a $(t, t-1)$-set. We recall that $d(\mathbf{x}, \mathbf{y})$ denotes the Hamming distance between the vectors $\mathbf{x}$ and $\mathbf{y}$.

Lemma 6.1. *Let q be a prime power, $v \mid q - 1$, and $\mathbf{b} = (b_1, \dots, b_t) \in \mathbb{Z}_v^t$ with r 0-entries. Let $\lambda_{\mathbf{b}}$ be the number of rows equal to $(b_1, \dots, b_t)$ of the subarray of M defined by the columns in C. Then, we have*

$$\lambda_{\mathbf{b}} = \left(\frac{1}{v}\right)^t (q-1)^{t-r}(v+q-1)^r$$

$$- (-1)^t \left(\frac{1}{v}\right)^t (q-1)^r (v-1)^r \left(v + (q-1)(v-1)\right)^{t-r}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b}, \mathbf{c}) = t}} \lambda_{\mathbf{c}'}. \tag{6.3}$$

Proof. We start by computing $\lambda_{\mathbf{b}}$ using an inclusion-exclusion argument.

$$\lambda_{\mathbf{b}} = \sum_{s=0}^{t} (-1)^s \sum_{\substack{C' \subseteq C \\ |C'| = s}} \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^s \\ d(\mathbf{c}, \mathbf{b}|_{C'}) = s}} \lambda_{\mathbf{c}}$$

Now we use the fact that if $C' \subsetneq C$ then C' is a linearly independent set of columns and therefore Equation (6.2) allows us to explicitly compute this sum for all but $C' = C$. To use Equation (6.2) to compute $\lambda_{\mathbf{c}}$, with $d(\mathbf{c}, \mathbf{b}|_{C'}) = s$ we need to know the number of zero entries in $\mathbf{c}$. We count these by supposing that $\mathbf{b}$ has j zero entries and i non-zero entries among the C' with $i + j = s \leq t$. If $\mathbf{c}$ disagrees everywhere with $\mathbf{b}|_{C'}$ then for all the zero entries in $\mathbf{b}|_{C'}$, $\mathbf{c}$ can be any of the $v - 1$ non-zero elements of $\mathbb{Z}_v$. For a position where $\mathbf{b}|_{C'}$ is non-zero, say z, $\mathbf{c}$ could have a zero entry or one of the $v - 2$ other non-zero entries of $\mathbb{Z}_v \setminus \{z\}$. We count the number of zero entries in $\mathbf{c}$ with $k \leq i$. Thus

$$\lambda_{\mathbf{b}} = \sum_{\substack{0 \leq j \leq r \\ 0 \leq i \leq t-r \\ i+j < t}} \binom{r}{j}\binom{t-r}{i}(-1)^{i+j}$$

$$\sum_{k=0}^{i} \binom{i}{k}(v-1)^j(v-2)^{i-k}\left(\frac{q-1}{v}\right)^{i+j-k}\left(\frac{q+v-1}{v}\right)^k q^{t-i-j}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b}, \mathbf{c}) = t}} \lambda_{\mathbf{c}}$$

To simplify the first sum we include $i + j = t$ in the sum and remove it afterwards.

$$\lambda_{\mathbf{b}} = \sum_{j=0}^{r} \sum_{i=0}^{t-r} \binom{r}{j} \binom{t-r}{i} (-1)^{i+j}$$

$$\sum_{k=0}^{i} \binom{i}{k} (v-1)^j (v-2)^{i-k} \left(\frac{q-1}{v}\right)^{i+j-k} \left(\frac{q+v-1}{v}\right)^{k} q^{t-i-j}$$

$$- (-1)^t \sum_{k=0}^{t-r} \binom{t-r}{k} (v-1)^r (v-2)^{t-r-k} \left(\frac{q-1}{v}\right)^{t-k} \left(\frac{q+v-1}{v}\right)^{k}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_{\mathbf{c}}$$

Manipulating the above expression we get

$$\lambda_{\mathbf{b}} = \sum_{j=0}^{r} \sum_{i=0}^{t-r} \binom{r}{j} \binom{t-r}{i} (-1)^{i+j} (v-1)^j \left(\frac{q-1}{v}\right)^{i+j} q^{t-i-j}$$

$$\sum_{k=0}^{i} \binom{i}{k} (v-2)^{i-k} \left(\frac{q-1}{v}\right)^{-k} \left(\frac{q+v-1}{v}\right)^{k}$$

$$- (-1)^t \left(\frac{1}{v}\right)^t (q-1)^t (v-1)^r (v-2)^{t-r} \sum_{k=0}^{t-r} \binom{t-r}{k} \left(\frac{q+v-1}{(q-1)(v-2)}\right)^{k}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_{\mathbf{c}}$$

$$= \sum_{j=0}^{r} \sum_{i=0}^{t-r} \binom{r}{j} \binom{t-r}{i} (-1)^{i+j} (v-1)^j \left(\frac{q-1}{v}\right)^{i+j} q^{t-i-j} \left(\frac{qv}{q-1} - 1\right)^{i}$$

$$- (-1)^t \left(\frac{1}{v}\right)^t (q-1)^t (v-1)^r (v-2)^{t-r} \left(1 + \frac{q+v-1}{(q-1)(v-2)}\right)^{t-r}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_{\mathbf{c}}$$

$$= q^t \sum_{i=0}^{t-r} \binom{t-r}{i} (-1)^i \left(1 - \frac{q-1}{qv}\right)^{i} \sum_{j=0}^{r} \binom{r}{j} (-1)^j (v-1)^j \left(\frac{q-1}{qv}\right)^{j}$$

$$- (-1)^t \left(\frac{1}{v}\right)^t (q-1)^t (v-1)^r (v-2)^{t-r} \left(\frac{v + (q-1)(v-1)}{(q-1)(v-2)}\right)^{t-r}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_{\mathbf{c}}$$

Finally we obtain

$$\lambda_{\mathbf{b}} = \left(\frac{1}{v}\right)^t (q-1)^{t-r}(v+q-1)^r$$

$$- (-1)^t \left(\frac{1}{v}\right)^t (q-1)^r(v-1)^r \left(v+(q-1)(v-1)\right)^{t-r}$$

$$+ (-1)^t \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c})=t}} \lambda_{\mathbf{c}}.$$

$\square$

To simplify our expression in the remainder of the paper we define

$$c_r = \left(\frac{1}{v}\right)^t (q-1)^{t-r}(v+q-1)^r, \tag{6.4}$$

$$c_{r,t-1} = (-1)^{t-1} q \left(\frac{1}{v}\right)^{t-1} ((v-1)(q-1))^{r-1}(qv-q+1)^{t-r-1}$$

$$(tvq - tq - tv + t + rv), \tag{6.5}$$

$$c_{r,t} = (-1)^t \left(\frac{1}{v}\right)^t (q-1)^r(v-1)^r \left(v+(q-1)(v-1)\right)^{t-r}, \tag{6.6}$$

$$d_{r,k} = (-1)^t \binom{t-r}{k}(v-1)^r(v-2)^{t-r-k}. \tag{6.7}$$

Note that $c_{r,t-1}$ and $c_{r,t}$ are the $i+j=t-1$ and $i+j=t$ summands of c_r respectively.

6.2 Upper and lower bounds on λ

In this section we compute more precise upper lower and upper bounds on $\lambda_{\mathbf{b}}$. We define

$$\lambda_r^- = \min\{\lambda_{\mathbf{b}} : \mathbf{b} \in \mathbb{Z}_v^t, \mathbf{b} \text{ has } r \text{ zeros}\}$$

and

$$\lambda_r^+ = \max\{\lambda_{\mathbf{b}} : \mathbf{b} \in \mathbb{Z}_v^t, \mathbf{b} \text{ has } r \text{ zeros}\}.$$

The very simplest bounds we know when $\mathbf{b}$ has r zeros, are

$$0 \le \lambda_r^- \le \lambda_{\mathbf{b}} \le \lambda_r^+ \le qc_r.$$

One improvement on this is to take advantage of the fact that the successive terms of a inclusion-exclusion computation are each upper and lower bounds depending on the sign of the last term in the summation. We use the fact that truncating before the last and before the second-to-last terms are the best possible of these upper and lower bounds.

Lemma 6.2. *Let* $\{A_i : i \in I\}$ *be subsets of* U *with* $|I| = t$ *and for* $0 \leq s \leq t$, *define*

$$c_s = \sum_{i=0}^{s} \sum_{\substack{S \subseteq I \\ |S| = i}} \left| \bigcap_{i \in S} A_i \right|$$

Then for any $0 \leq j \leq t$ *we have*

$$(-1)^{t-j} c_t \leq (-1)^{t-j} c_{t-j}, \tag{6.8}$$

for all odd $1 \leq j \leq t$ *we have*

$$(-1)^{t-1} c_{t-1} \leq (-1)^{t-j} c_{t-j}, \tag{6.9}$$

and for all even $2 \leq j < t$ *we have*

$$(-1)^{t-2} c_{t-2} \leq (-1)^{t-j} c_{t-j}. \tag{6.10}$$

Proof. We observe that $c_0 = |U|$ and $c_t = |U \setminus \bigcup_{i \in I} A_i|$ and c_s is just the computation of $|U \setminus \bigcup_{i \in I} A_i|$ by inclusion-exclusion truncated at step s. The first conclusion of the theorem is simply that the successive truncations are upper and lower bounds depending on the sign of the last summand. It is proven by considering the contribution of any single point of U to each side of the equation. If a point x is in none of the A_i then it contributes 1 to the computation of c_s for all $0 \leq s \leq t$ and thus contributes equally to both sides of Inequality (6.8). If a point x is in exactly $r > 0$ of the subsets then its contribution to c_s is

$$\sum_{i=0}^{s} (-1)^i \binom{r}{i} = (-1)^s \binom{r-1}{s}.$$

This last equality is easily established. (Also recall that $(-1)^s \binom{-1}{s} = 1$.) Then Inequality (6.8) is established by noting that the contribution of a point in $\bigcup_{i \in I} A_i$ (and thus $r \geq 1$) is

$$(-1)^{t-j}(-1)^t \binom{r-1}{t} = 0 \leq \binom{r-1}{t-j} = (-1)^{t-j}(-1)^{t-j} \binom{r-1}{t-j}$$

since $t > r - 1 \geq 0$.

Now we prove Inequality (6.9). Again the contribution of any point x in none of the A_i is 1 to both c_{t-1} and to c_{t-j}, so we can restrict our attention to points that belong to $r > 0$ of the A_i. If point x is in $0 < r < t$ of the A_i then its contribution to c_{t-1} is

$$(-1)^{t-1} \binom{r-1}{t-1} = 0$$

and its contribution to c_{t-j} is

$$(-1)^{t-j} \binom{r-1}{t-j}.$$

The needed inequality follows from

$$(-1)^{t-1}0 = 0 \leq \binom{r-1}{t-j} = (-1)^{t-j}(-1)^{t-j}\binom{r-1}{t-j}.$$

If x is a point in all t of the A_i then its contribution to c_{t-1} is

$$(-1)^{t-1}\binom{t-1}{t-1} = (-1)^{t-1}$$

and it contribution to c_{t-j} is

$$(-1)^{t-j}\binom{t-1}{t-j}.$$

The needed inequality follows from

$$(-1)^{t-1}(-1)^{t-1} = 1 \leq \binom{t-1}{t-j} = (-1)^{t-j}(-1)^{t-j}\binom{t-1}{t-j},$$

unless $t - j < 0$, that is $j > t$, or $j < 1$ which are not possible.

Now we prove Inequality (6.10). Again the contribution of any point x in none of the A_i is 1 to both c_{t-1} and to c_{t-j}, so we can restrict our attention to points that belong to $r > 0$ of the A_i. If point x is in $0 < r < t - 1$ of the A_i then its contribution to c_{t-2} is

$$(-1)^{t-2}\binom{r-1}{t-2} = 0$$

and its contribution to c_{t-j} is

$$(-1)^{t-j}\binom{r-1}{t-j}.$$

The needed inequality follows from

$$(-1)^{t-1}0 = 0 \leq \binom{r-1}{t-j} = (-1)^{t-j}(-1)^{t-j}\binom{r-1}{t-j}.$$

If x is a point in $t - 1$ of the A_i then its contribution to c_{t-2} is

$$(-1)^{t-2}\binom{t-2}{t-2} = (-1)^{t-2}$$

and its contribution to c_{t-j} is

$$(-1)^{t-j}\binom{t-2}{t-j}.$$

The needed inequality follows from

$$(-1)^{t-2}(-1)^{t-2} = 1 \leq \binom{t-2}{t-j} = (-1)^{t-j}(-1)^{t-j}\binom{t-2}{t-j},$$

unless j is out of range ($j > t$ or $j < 2$). If x is a point in all t of the A_i then its contribution to c_{t-2} is

$$(-1)^{t-2}\binom{t-1}{t-2} = (-1)^{t-2}(t-1)$$

and its contribution to c_{t-j} is

$$(-1)^{t-j}\binom{t-1}{t-j}.$$

The needed inequality follows from

$$(-1)^{t-2}(-1)^{t-2}(t-1) = t - 1 \le \binom{t-1}{t-j} = (-1)^{t-j}(-1)^{t-j}\binom{t-1}{t-j},$$

unless j is out of range ($j < 2$, $j \ge t$). When $j = t$ this inequality can be violated indicating that our method does not prove the bound in Inequality (6.10). However when $j = t$ and even, and letting n_i be the number of points that appear in exactly i of the A, we get that Inequality (6.10) holds except when

$$n_t(t-2) > \sum_{i=1}^{t-2} n_i.$$

It is also worth noting that when $j = t$, $c_{t-j} = |U|$ and so the only time that c_{t-2} is a worse upper bound for c_t than c_0 is when $c_{t-2} > |U|$. ◻

This lemma implies that the best bounds obtainable by truncating an inclusion-exclusion computation are obtained by the last two truncations, except possibly in the case that t is even and there exist points in every A_i, when it might be the case that

$$c_t < c_0 = |U| < c_{t-2}.$$

Thus when t is even and $\mathbf{b}$ has r zeros,

$$c_r - c_{r,t} \le \lambda_\mathbf{b} \le \min(c_r - c_{r,t} - c_{r,t-1}, q^t) \tag{6.11}$$

and when t is odd and $\mathbf{b}$ has r zeros,

$$c_r - c_{r,t} - c_{r,t-1} \le \lambda_\mathbf{b} \le c_r - c_{r,t}. \tag{6.12}$$

To derive even more precise bounds on $\lambda_\mathbf{b}$ we use Linear Programming by substituting λ_r^- and λ_r^+ for $\lambda_\mathbf{c}$ in Equation (6.3). How we do so will again depend on the sign of the last term which depends on the parity of t.

6.2.1 Bounds on $\lambda_\mathbf{b}$ when t is even

When $t \bmod 2 = 0$ Equation (6.3) is

$$\lambda_\mathbf{b} = \left(\frac{1}{v}\right)^t (q-1)^{t-r}(v+q-1)^r - \left(\frac{1}{v}\right)^t (q-1)^r(v-1)^r \left(v+(q-1)(v-1)\right)^{t-r} + \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_\mathbf{c},$$

Since $\lambda_k^- \leq \lambda_\mathbf{c} \leq \lambda_k^+$ for any $\mathbf{c}$ with k zeros we have that

$$c_r - c_{r,t} + \sum_{k=0}^{t-r} \binom{t-r}{k}(v-1)^r(v-2)^{t-r-k}\lambda_k^- \leq \lambda_\mathbf{b} \leq c_r - c_{r,t} + \sum_{k=0}^{t-r} \binom{t-r}{k}(v-1)^r(v-2)^{t-r-k}\lambda_k^+,$$

for any $\mathbf{b}$ with r zeros, and thus

$$c_r - c_{r,t} \quad \leq \quad \lambda_r^- - \sum_{k=0}^{t-r} d_{r,k}\lambda_k^-, \qquad 0 \leq r \leq t$$

$$-c_r + c_{r,t} \quad \leq \quad -\lambda_r^+ + \sum_{k=0}^{t-r} d_{r,k}\lambda_k^+, \qquad 0 \leq r \leq t$$

$$0 \quad \leq \quad \lambda_r^- \leq \lambda_r^+ \leq qc_r, \qquad 0 \leq r \leq t.$$

Let $\lambda \in \mathbb{Z}^{2t+2}$, $\mathbf{C} \in \mathbb{Z}^{5t+5}$ and $D \in \mathbb{Z}^{(t-1)\times(t+1)}$ defined by

$$\lambda = \left(-\lambda_0^-, \dots, -\lambda_t^-, \lambda_0^+, \dots, \lambda_t^+\right)$$

$$\mathbf{C} = \left(c_0 - c_{0,t}, \dots, c_t - c_{t,t}, -c_0 + c_{0,t}, \dots, -c_t + c_{t,t}, 0_1, \dots, 0_{2t+2}, -qc_0, \dots, -qc_t\right)$$

$$D_{i,j} = d_{i,j} = \binom{t-i}{j}(v-1)^i(v-2)^{t-i-j},$$

and $B \in \mathbb{Z}^{5t+5\times2t+1}$ defined in $(t+1) \times (t+1)$ blocks as

$$B = \left(\begin{array}{c|c} D - I_{t+1} & \mathbf{0} \\ \hline \mathbf{0} & D - I_{t+1} \\ \hline I_{t+1} & I_{t+1} \\ \hline -I_{t+1} & \mathbf{0} \\ \hline \mathbf{0} & -I_{t+1} \end{array}\right),$$

We have the linear program

$$B\lambda \geq \mathbf{C}. \tag{6.13}$$

6.2.2 Bounds on $\lambda_\mathbf{b}$ when t is odd

When $t \bmod 2 = 1$ Equation (6.3) is

$$\lambda_\mathbf{b} = \left(\frac{1}{v}\right)^t (q-1)^{t-r}(v+q-1)^r + \left(\frac{1}{v}\right)^t (q-1)^r(v-1)^r \left(v + (q-1)(v-1)\right)^{t-r} - \sum_{\substack{\mathbf{c} \in \mathbb{Z}_v^t \\ d(\mathbf{b},\mathbf{c}) = t}} \lambda_\mathbf{c},$$

Substituting in the bounds for $\lambda_\mathbf{c}$, we get

$$c_r - c_{r,t} - \sum_{k=0}^{t-r} \binom{t-r}{k}(v-1)^r(v-2)^{t-r-k}\lambda_k^+ \leq \lambda_\mathbf{b} \leq c_r - c_{r,t} - \sum_{k=0}^{t-r} \binom{t-r}{k}(v-1)^r(v-2)^{t-r-k}\lambda_k^-,$$

and thus

$$
c_r - c_{r,t} \;\leq\; \lambda_r^- + \sum_{k=0}^{t-r} d_{r,k}\lambda_k^+, \qquad 0 \leq r \leq t
$$

$$
-c_r + c_{r,t} \;\leq\; -\lambda_r^+ - \sum_{k=0}^{t-r} d_{r,k}\lambda_k^-, \qquad 0 \leq r \leq t
$$

$$
0 \;\leq\; \lambda_r^- \leq \lambda_r^+ \leq q c_r, \qquad 0 \leq r \leq t.
$$

Let $\lambda \in \mathbb{Z}^{2t+2}$, $\mathbf{C} \in \mathbb{Z}^{5t+5}$ and $D \in \mathbb{Z}^{(t-1)\times(t+1)}$ defined by

$$
\lambda = \left(-\lambda_0^-, \ldots, -\lambda_t^-, \lambda_0^+, \ldots, \lambda_t^+\right)
$$

$$
\mathbf{C} = \left(c_0 - c_{0,t}, \ldots, c_t - c_{t,t}, -c_0 + c_{0,t}, \ldots, -c_t + c_{t,t}, 0_1, \ldots, 0_{2t+2}, -qc_0, \ldots, -qc_t\right)
$$

$$
D_{i,j} = d_{i,j} = \binom{t-i}{j}(v-1)^i(v-2)^{t-i-j},
$$

and $B \in \mathbb{Z}^{5t+5\times 2t+1}$ defined in $(t+1) \times (t+1)$ blocks as

$$
B = \left(
\begin{array}{c|c}
-I_{t+1} & D \\
\hline
D & -I_{t+1} \\
\hline
I_{t+1} & I_{t+1} \\
\hline
-I_{t+1} & \mathbf{0} \\
\hline
\mathbf{0} & -I_{t+1}
\end{array}
\right),
$$

We have the linear program

$$
B\lambda \geq \mathbf{C}. \tag{6.14}
$$

As we discuss in Chapter 7, we plan to implement a computer program to solve the above linear program.

Future directions

WE CONCLUDE with a number of directions for future research related to our thesis.

Concatenation of cyclic trace arrays and finite geometry

In Chapter 4 we consider the vertical concatenation of cyclic trace arrays and we search for subarrays of columns that are covering arrays. Here we restate the problem in terms of finite geometry, we analyze some of our experimental results from this point of view and conclude with some questions that naturally arise.

For simplicity, let us assume the case of vertically concatenating two cyclic trace arrays. The problem is the following: let α be a primitive element of $\mathbb{F}_{q^t}$ and let j be coprime to $q^t - 1$, which means that α^j is also primitive. We want to find $S \subseteq [0, [t]_q - 1]$ with the property that, for every $I \subseteq S$ with $|I| = t$, we have that $\mathcal{A}_0(\alpha, I)$ or $\mathcal{A}_0(\alpha^j, I)$ is an OA(t, t, q). For such S, we have that $\mathcal{A}_0(\{\alpha, \alpha^j\}, S)$ is a CA($2(q^t - 1) + 1; t, |S|, q$). This problem is studied in Chapter 4 in more generality, and our results are presented in Section 4.4.

We now restate the problem in terms of finite geometry. First, we note that as discussed in Section 2.1.4, we consider the points of $PG(t - 1, q)$ to be

$$PG(t - 1, q) = \{[\alpha^i] \mid i \in [0, [t]_q - 1]\}.$$

However, since α^j is also a primitive element of $\mathbb{F}_{q^t}$, we also have that

$$PG(t - 1, q) = \{[\alpha^{ji}] \mid i \in [0, [t]_q - 1]\},$$

which means that the mapping

$$\phi_j : \begin{array}{l} PG(t - 1, q) \to PG(t - 1, q) \\ [\alpha^i] \mapsto [\alpha^{ji}] \end{array}$$

is a permutation of the points of $PG(t-1, q)$. Furthermore, we note that, by Statements 1 and 5 of Proposition 3.10, $\mathcal{A}_0(\alpha, I)$ (respectively $\mathcal{A}_0(\alpha^j, I)$) is an OA($t, t, q$) if and only if $\{[\alpha^i] \mid i \in I\}$ (respectively $\{[\alpha^{ij}] \mid i \in I\}$) is a set of points of $PG(t - 1, q)$ that are not contained in a hyperplane. Hence, we can restate our problem as follows: we want to find a permutation ϕ_j of the points of $PG(t-1, q)$ and a subset $S \subseteq PG(t-1, q)$ with the property that, for every $I \subseteq S$ with $|I| = t$, we have that I or $\phi_j(I)$ is a set of points that are not contained in a hyperplane.

From the above point of view, some of the experimental results of Chapter 4 are of particular interest. We define $I(q) = \{i(q + 1) \mid i \in [0, q^2]\}$. From our discussion after Corollary 3.17,

q	P	S	$\mathcal{A}_0(P, S)$	Ovoids
3	$\{\alpha, \alpha^{17}\}$	$I_2(3) \cup (I_2(3) + 1)$	CA(161; 4, 10, 3)	Two halfs
4	$\{\alpha, \alpha^{31}\}$	$I(4)$	CA(511; 4, 17, 4)	Ovoid
5	$\{\alpha, \alpha^{37}\}$	$I_2(5)$	CA(1249; 4, 13, 5)	Half
5	$\{\alpha, \alpha^{37}, \alpha^{71}\}$	$I_2(5) \cup (I_2(5) + 3)$	CA(1873; 4, 26, 5)	Two half
7	$\{\alpha, \alpha^{223}\}$	$I_{10}(7) \cup (I_{10}(7) + 1) \cup (I_{10}(7) + 3)$	CA(4801; 4, 15, 7)	Three tenths
7	$\{\alpha, \alpha^{37}, \alpha^{223}\}$	$I_2(7)$	CA(7201; 4, 25, 7)	Half
8	$\{\alpha, \alpha^{43}\}$	$I_5(8) \cup (I_5(8) + 1) \cup (I_5(8) + 3)$	CA(8191; 4, 39, 8)	Three fifths
9	$\{\alpha, \alpha^{7}, \alpha^{13}\}$	$I_2(9)$	CA(19681; 4, 41, 9)	Half

Table 7.1. Strength 4 covering arrays from vertical concatenation of cyclic trace arrays and parts of ovoids.

for a primitive element $\alpha \in \mathbb{F}_{q^4}$ the set $\Omega(\alpha, q) = \{[\alpha^i] \mid i \in I(q)\}$ is an ovoid in $PG(3, q)$, which means that every three points from the set are not colinear. For $q = 4$, we have that $I(4) = \{5i \mid i \in [0, 16]\}$. We observe that the first experimental result in Table 4.5 is the array $\mathcal{A}_0(\{\alpha, \alpha^{31}\}, I(4))$, where α is given in Table 4.4. From the geometrical interpretation above, we have that ϕ_{31} is a permutation of the points of $PG(3, 4)$ that maps the ovoid $\Omega(\alpha, 4)$ to the ovoid $\Omega(\alpha^{31}, 4)$ and, moreover, for every set I of points in $\Omega(\alpha, 4)$ with $|I| = 4$, we have that I or $\phi_{31}(I)$ is a set of points that are not contained in the same plane (that is the same as a hyperplane in $PG(3, q)$).

Another interesting experimental result can be described in similar terms. For $d \in [1, q]$ such that $d | q^2 + 1$ we define $I_d(q) = \{id(q + 1) \mid i \in [0, q^2]\}$. One of our experimental results is the CA(161; 4, 10, 3) shown in Table 4.3a. This is constructed as a $\mathcal{A}_0(\{\alpha, \alpha^{17}\}, S)$, where

$$S = \{0, 1, 8, 9, 16, 17, 24, 25, 32, 33\}$$
$$= \{0, 8, 16, 24, 32\} \cup \{1, 9, 17, 25, 33\}$$
$$= I_2(3) \cup (I_2(3) + 1).$$

This could be described as a construction using two *half ovoids*.

Inspired by the above, we constructed arrays $\mathcal{A}_0(P, S)$ where P is a set of primitive elements of $\mathbb{F}_{q^4}$ and S is an ovoid or the union of fractions of an ovoid. Our tests were for q up to 11. The successful cases are listed in Table 7.1. We note that the cases for $q = 3$ and $q = 4$ were found using Algorithm 5, whereas in all the other cases the covering array definition was tested directly.

We propose investigating the above constructions in the context of finite geometry. One aspect of this research would be to find permutations of the points of $PG(3, q)$ such that they map 4-sets of coplanar points to 4-sets of non-coplanar points, when restricted to parts of ovoids. For support in this direction, we suggest studying two previous works for possible connections: Ebert [32] describes the partitioning of $PG(3, q)$ into disjoint ovoids, and Wilson and Qing [96] use half ovoids for the construction of a family of linear codes.

Alternative algorithmic search for covering arrays from concatenation of cyclic trace arrays

In Chapter 4 we consider the problem of vertically concatenating cyclic trace arrays and finding subarrays of columns that yield covering arrays as an optimization problem to which we give an algorithmic solution that uses backtracking. One problem with the backtracking approach is that, for large values of q such as $q \geq 15$, due to the increased size of the search space, Algorithm 5 takes a very long time to fully traverse branches of the tree corresponding to the search space. We suggest adapting Algorithm 5 so that branches with more potential have higher probability of being examined first. This could be done by ranking the nodes of the tree according to the size of the corresponding candidate set. Another option would be to use this type of ranking with metaheuristics such as tabu search or simulated annealing.

Other covering array constructions from character sums

In Chapter 5 we establish a criterion for cyclic trace arrays using a character sum argument. A crucial part of this is bound a character sum that involves the function h, defined in Equation (5.17). A similar function is used by Colbourn [25] in order to construct covering arrays from cyclotomy, where instead of values of the trace function, linear shifts of the base field elements are used. We propose extending this idea further by substituting the trace function in h with some other function that distributes the values uniformly over the field, and examine whether this yields another covering array construction.

Randomness properties of maximal sequences modulo v

In Chapter 5 we introduce the sequence $\mathrm{Seq}_{q^t/q}(\alpha; v)$. To the best of our knowledge, this type of sequence has not been studied before. We propose researching these sequences further for randomness criteria similar to the ones studied in [41] for LFSR sequences. For example, examine their autocorrelation and crosscorrelation properties and, if v is prime, find values or bounds for their linear complexity.

Counting the rows of cyclic trace arrays modulo v by linear programming.

In Chapter 6 we consider arrays constructed by applying the discrete logarithm modulo v to the nonzero elements of maximal sequences, similar to the cyclic trace arrays of Chapter 5. We provide bounds for the number of occurrences of the different rows in subarrays of columns, by expressing this number as the solution of a linear program, as shown in Equations (6.13) and (6.14). We propose investigating this further by solving these linear program for some feasible cases, and compare the lower bounds to the conditions established in Chapter 5 for cyclic trace arrays modulo v to be covering arrays.

List of Figures

List of Tables

List of Algorithms

Nomenclature

Symbols that appear only in a restricted context are not listed. Wherever appropriate, a page reference is given.

0^n	The binary string consisting of the digit 0 repeated n times, 65
1^n	The binary string consisting of the digit 1 repeated n times, 65
$\mathcal{A}_{q^t/q}(\alpha, C)$	Cyclic trace array for primitive $\alpha \in \mathbb{F}_{q^t}$ and $C \subseteq [0, [t]_q - 1]$, 38
$\mathcal{A}(\alpha, C)$	Simplified notation for $\mathcal{A}_{q^t/q}(\alpha, C)$, 38
$\mathcal{A}_{q^t/q}(\alpha)$	The cyclic trace array $\mathcal{A}_{q^t/q}(\alpha, [0, [t]_q - 1])$, 38
$\mathcal{A}(\alpha)$	Simplified notation for $\mathcal{A}_{q^t/q}(\alpha)$, 38
$\mathcal{A}_{q^t/q,\mathbf{0}}(\alpha, C)$	The array $\mathcal{A}_{q^t/q}(\alpha, C)$ with a row of zeros appended, 38
$\mathcal{A}_{\mathbf{0}}(\alpha, C)$	Simplified notation for $\mathcal{A}_{q^t/q,\mathbf{0}}(\alpha, C)$, 38
$\mathcal{A}_{q^t/q,\mathbf{0}}(\alpha)$	The cyclic trace array $\mathcal{A}_{q^t/q,\mathbf{0}}(\alpha, [0, [t]_q - 1])$, 38
$\mathcal{A}_{\mathbf{0}}(\alpha)$	Simplified notation for $\mathcal{A}_{q^t/q,\mathbf{0}}(\alpha)$, 38
$\mathcal{A}_{q^t/q}(\alpha, C; v)$	Cyclic trace array modulo v corresponding to $\alpha \in \mathbb{F}_{q^t}$, 91
$\mathcal{A}_{q^t/q}(\alpha; v)$	Simplified notation for $\mathcal{A}_{q^t/q}(\alpha, [0, [t]_q - 1]; v)$, 91
$\mathcal{B}_n$	Set of all the binary necklaces of length n 64
c_r	See Equation (6.4), 122
$c_{r,t-1}$	See Equation (6.5), 122
$c_{r,t}$	See Equation (6.6), 122
$\mathrm{char}_n(S)$	Characteristic vector of set S, 64
$d_{r,k}$	See Equation (6.7), 122
$d(\mathbf{x}, \mathbf{y})$	The Hamming distance of the vector $\mathbf{x}$ and $\mathbf{y}$, 26
$C_{p,w}^i$	Cyclotomic coset of p modulo w that contains i, 76
C_n	Set containing all canonical subsets of $[0, n-1]$, 67
$\mathrm{CA}_\lambda(N; t, k, v)$	A covering array of index λ, 28
$\mathrm{CA}(N; t, k, v)$	A covering array $\mathrm{CA}_1(N; t, k, v)$, 28
$\mathrm{CAN}(t, k, v)$	The covering array number for t, k and v, 31
$\textsc{Candidates}(S)$	The set of candidates for a feasible solution S, 72

ϕ	Euler's function, 11
χ_0	The trivial character of a group, 12
χ_v	Multiplicative character of $\mathbb{F}_q$ of order v, 102
$\overline{b}$	The binary complement of b, 68
$\overline{\chi}$	The conjugate of a character χ, 12
$\overline{(s_0, \dots, s_{r-1})}$	Infinite periodic sequence with period r, 15
$\widehat{G}$	The group of the characters of a group G
$C^{\perp}$	The dual code of the code C, 26
(v, s, λ)-BIBD	A balanced incomplete block design, 23
(k, s)-set	Set of k vectors, every s of them linearly independent, 45
$x = y \bmod n$	x is the remainder of the Euclidean division of y by n
$x \equiv y \pmod{n}$	Congruence of integers x and y modulo n
$S +_n i$	Shift of the set S modulo n, 62
$[v]$	The point of a projective space represented by the vector v, 22
$[t]_q$	$(q^t - 1)/(q - 1)$ 19
$\lceil x \rceil$	The smallest integer that is greater or equal to x
$\lfloor x \rfloor$	The largest integer that is smaller or equal to x
$[a, b]$	The set $\{a, a+1, \dots, b\}$ where a, b are integers such that $a < b$
$[n, k, d]_q$	A linear code over $\mathbb{F}_q$ of length n, dimension k and minimum distance d, 26
$\binom{a}{b}$	The binomial coefficient $\frac{a!}{(a-b)!b!}$
$\begin{bmatrix} a \\ b \end{bmatrix}_q$	Gaussian binomial coefficient, 23
AMDS	Almost maximum distance separable code, 52
BIBD	Balance incomplete block design, 23
LFSR	Linear Feedback Shift Registers
MDS	maximum distance separable code, 52
NMDS	near maximum distance separable code, 52

Bibliography

[1] S. Addelman and O. Kempthorne. "Some main-effect plans and orthogonal arrays of strength two." *The Annals of Mathematical Statistics* (1961), pp. 1167–1176.

[2] N. Alon and J. H. Spencer. "The probabilistic method." In: *Wiley interscience series in discrete mathematics and optimization*. 3rd ed. Wiley Online Library, 2008, pp. 353–354.

[3] W. Ananchuen and L. Caccetta. "On the adjacency properties of Paley graphs." *Networks* 23.4 (1993), pp. 227–236.

[4] Y. Azar, R. Motwani, and J. S. Naor. "Approximating probability distributions using small sample spaces." *Combinatorica* 18.2 (1998), pp. 151–171.

[5] S. Behnel, R. Bradshaw, C. Citro, L. Dalcin, D. S. Seljebotn, and K. Smith. "Cython: The best of both worlds." *Computing in Science & Engineering* 13.2 (2011), pp. 31–39.

[6] A. Blass, G. Exoo, and F. Harary. "Paley graphs satisfy all first-order adjacency axioms." *Journal of Graph Theory* 5.4 (1981), pp. 435–439.

[7] B. Bollobás. "Random graphs." In: In *Modern Graph Theory*. Springer, 1998, pp. 215–252.

[8] S. Y. Boroday. "Determining essential arguments of Boolean functions." *Proceedings of the Conference on Industrial Mathematics, Taganrog*. Vol. 59. Citeseer. 1998, p. 61.

[9] R. C. Bose. "Mathematical theory of the symmetrical factorial design." *Sankhyā: The Indian Journal of Statistics* (1947), pp. 107–166.

[10] R. Bose. "On some connections between the design of experiments and information theory." *Bull. Inst. Inter. Statist.* 38 (1961), pp. 257–271.

[11] R. C. Bryce and C. J. Colbourn. "A density-based greedy algorithm for higher strength covering arrays." *Software Testing, Verification and Reliability* 19.1 (2009), pp. 37–53.

[12] R. C. Bryce and C. J. Colbourn. "The density algorithm for pairwise interaction testing." *Software Testing Verification and Reliability* 17.3 (2007), pp. 159–182.

[13] K. A. Bush. "Orthogonal arrays of index unity." *The Annals of Mathematical Statistics* 23.3 (1952), pp. 426–434.

[14] M Chateauneuf and D. L. Kreher. "On the state of strength-three covering arrays." *Journal of Combinatorial Designs* 10.4 (2002), pp. 217–238.

[15] M. Chateauneuf, C. J. Colbourn, and D. L. Kreher. "Covering arrays of strength three." *Designs, Codes and Cryptography* 16.3 (1999), pp. 235–242.

[16] D. M. Cohen and M. L. Fredman. "New techniques for designing qualitatively independent systems." *Journal of Combinatorial Designs* 6.6 (1998), pp. 411–416.

[17] D. M. Cohen, S. R. Dalal, M. L. Fredman, and G. C. Patton. "The AETG system: An approach to testing based on combinatorial design." *IEEE Transactions on Software Engineering* 23.7 (1997), pp. 437–444.

[18] D. M. Cohen, S. R. Dalal, J. Parelius, and G. C. Patton. "The combinatorial design approach to automatic test generation." *IEEE Software* 13.5 (1996), p. 83.

[19] M. B. Cohen. "Designing Test Suites for Software Interaction Testing." PhD thesis, University of Auckland, 2004.

[20] M. B. Cohen, C. J. Colbourn, and A. C. Ling. "Augmenting simulated annealing to build interaction test suites." *Software Reliability Engineering, 2003. ISSRE 2003. 14th International Symposium on*. IEEE. 2003, pp. 394–405.

[21] M. B. Cohen, C. J. Colbourn, and A. C. Ling. "Constructing strength three covering arrays with augmented annealing." *Discrete Mathematics* 308.13 (2008), pp. 2709–2722.

[22] M. B. Cohen, P. B. Gibbons, W. B. Mugridge, C. J. Colbourn, and J. S. Collofello. "A variable strength interaction testing of components." *Computer Software and Applications Conference, 2003. COMPSAC 2003. Proceedings. 27th Annual International*. IEEE. 2003, pp. 413–418.

[23] M. B. Cohen, P. B. Gibbons, W. B. Mugridge, and C. J. Colbourn. "Constructing test suites for interaction testing." *Software Engineering, 2003. Proceedings. 25th International Conference on*. IEEE. 2003, pp. 38–48.

[24] C. J. Colbourn. "Combinatorial aspects of covering arrays." *Le Matematiche (Catania)* 58.121-167 (2004), pp. 0–10.

[25] C. J. Colbourn. "Covering arrays from cyclotomy." *Designs, Codes and Cryptography* 55.2-3 (2010), pp. 201–219.

[26] C. J. Colbourn. "Strength two covering arrays: Existence tables and projection." *Discrete Mathematics* 308.5 (2008), pp. 772–786.

[27] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs*. CRC press, 2006.

[28] C. J. Colbourn, G. Kéri, P. R. Soriano, and J.-C. Schlage-Puchta. "Covering and radius-covering arrays: constructions and classification." *Discrete Applied Mathematics* 158.11 (2010), pp. 1158–1180.

[29] C. Colbourn. *Covering array tables*. URL: `http://www.public.asu.edu/~ccolbou/src/tabby/catable.html` (visited on 06/03/2017).

[30] P. Delsarte. "An algebraic approach to the association schemes of coding theory." *Philips research reports supplements* 10 (1973), p. 103.

[31] M. Dewar, L. Moura, D. Panario, B. Stevens, and Q. Wang. "Division of trinomials by pentanomials and orthogonal arrays." *Designs, Codes and Cryptography* 45.1 (2007), pp. 1–17.

[32] G. L. Ebert. "Partitioning projective geometries into caps." *Canad. J. Math* 37.6 (1985), pp. 1163–1175.

[33] L. Gargano, J. Körner, and U. Vaccaro. "Capacities: from information theory to extremal set theory." *Journal of Combinatorial Theory, Series A* 68.2 (1994), pp. 296–316.

[34] L. Gargano, J. Körner, and U. Vaccaro. "Sperner capacities." *Graphs and combinatorics* 9.1 (1993), pp. 31–46.

[35] H. A. George. "Constructing Covering Arrays using Parallel Computing and Grid Computing." PhD thesis, Universitat Politecnica de Valencia, 2012.

[36] E. Gilbert and J. Riordan. "Symmetry types of periodic sequences." *Illinois Journal of Mathematics* 5.4 (1961), pp. 657–665.

[37] M. Giulietti. "On near-MDS elliptic codes." *arXiv preprint math/0211107* (2002).

[38] A. P. Godbole, D. E. Skipper, and R. A. Sunley. "t-covering arrays: upper bounds and Poisson approximations." *Combinatorics, Probability and Computing* 5.02 (1996), pp. 105–117.

[39] S. W. Golomb. *Shift Register Sequences*. Aegean Park Press, 1982.

[40] S. W. Golomb. "Shift Register Sequences Holden-Day." *San Francisco* (1967).

[41] S. W. Golomb and G. Gong. *Signal Design for Good Correlation: for Wireless Communication, Cryptography, and Radar*. Cambridge University Press, 2005.

[42] S. W. Golomb. *Sequences with randomness properties*. Glenn L. Martin Company, 1955.

[43] R. L. Graham and J. H. Spencer. "A constructive solution to a tournament problem." *Canad. Math. Bull* 14.1 (1971), pp. 45–48.

[44] A. Hartman. "Software and hardware testing using combinatorial covering suites." In: *Graph theory, combinatorics and algorithms*. Springer, 2005, pp. 237–266.

[45] A. Hartman and L. Raskin. "Problems and algorithms for covering arrays." *Discrete Mathematics* 284.1 (2004), pp. 149–156.

[46] A. S. Hedayat, N. J. A. Sloane, and J. Stufken. *Orthogonal Arrays: Theory and Applications*. Springer Science & Business Media, 2012.

[47] J. W. Hirschfeld and L. Storme. "The packing problem in statistics, coding theory and finite projective spaces: update 2001." In: *Finite geometries*. Springer, 2001, pp. 201–246.

[48] D. S. Johnson. "Approximation algorithms for combinatorial problems." *Journal of computer and system sciences* 9.3 (1974), pp. 256–278.

[49] G. O. Katona. "Two applications (for search theory and truth functions) of Sperner type theorems." *Periodica Mathematica Hungarica* 3.1-2 (1973), pp. 19–26.

[50]   O Kempthorne. "A simple approach to confounding and fractional replication in factorial experiments." *Biometrika* 34.3/4 (1947), pp. 255–272.

[51]   R. Kim, O.-H. Song, and M.-H. Ri. "Division of tetranomials by type II pentanomials and orthogonal arrays." *Vietnam Journal of Mathematics* 44.4 (2016), pp. 697–708.

[52]   D. J. Kleitman and J. Spencer. "Families of k-independent sets." *Discrete Mathematics* 6.3 (1973), pp. 255–262.

[53]   D. R. Kuhn, D. R. Wallace, and A. M. Gallo. "Software fault interactions and implications for software testing." *IEEE Transactions on Software Engineering* 30.6 (2004), pp. 418–421.

[54]   V. V. Kuliamin and A. Petukhov. "A survey of methods for constructing covering arrays." *Programming and Computer Software* 37.3 (2011), pp. 121–146.

[55]   Y. Lei and K.-C. Tai. "In-parameter-order: A test generation strategy for pairwise testing." *High-Assurance Systems Engineering Symposium, 1998. Proceedings. Third IEEE International*. IEEE. 1998, pp. 254–261.

[56]   R. Lidl and H. Niederreiter. *Finite Fields*. Vol. 20. Cambridge University Press, 1997.

[57]   J. R. Lobb, C. J. Colbourn, P. Danziger, B. Stevens, and J. Torres-Jimenez. "Cover starters for covering arrays of strength two." *Discrete Mathematics* 312.5 (2012), pp. 943–956.

[58]   L. Lovász. "On the ratio of optimal integral and fractional covers." *Discrete mathematics* 13.4 (1975), pp. 383–390.

[59]   S. Martirosyan. "On t-covering arrays." *Designs, Codes and Cryptography* 32.1-3 (2004), pp. 323–339.

[60]   K. Meagher and B. Stevens. "Group construction of covering arrays." *Journal of Combinatorial Designs* 13.1 (2005), pp. 70–77.

[61]   A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC press, 1996.

[62]   L. Moura, G. L. Mullen, and D. Panario. "Finite field constructions of combinatorial arrays." *Designs, Codes and Cryptography* 78.1 (2016), pp. 197–219.

[63]   G. L. Mullen and D. Panario. *Handbook of Finite Fields*. CRC Press, 2013.

[64]   A. Munemasa. "Orthogonal arrays, primitive trinomials, and shift-register sequences." *Finite Fields and Their Applications* 4.3 (1998), pp. 252–260.

[65]   J. Naor and M. Naor. "Small-bias probability spaces: Efficient constructions and applications." *SIAM Journal on Computing* 22.4 (1993), pp. 838–856.

[66]   M. Naor, L. J. Schulman, and A. Srinivasan. "Splitters and near-optimal derandomization." *Foundations of Computer Science, 1995. Proceedings., 36th Annual Symposium on*. IEEE. 1995, pp. 182–191.

[67]   *NIST Covering Array Tables*. http://math.nist.gov/coveringarrays.

[68]   K. J. Nurmela. "Upper bounds for covering arrays by tabu search." *Discrete Applied Mathematics* 138.1 (2004), pp. 143–152.

[69]   D. Panario, B. Stevens, and G. Tzanakis. "Number of t-tuples in arrays from LFSRs." International conference on algebraic informatics. June 2017. URL: http://www.cargo.wlu.ca/CAI2017/.

[70]   D. Panario, O. Sosnovski, B. Stevens, and Q. Wang. "Divisibility of polynomials over finite fields and combinatorial applications." *Designs, Codes and Cryptography* 63.3 (2012), pp. 425–445.

[71]   S. Poljak, A. Pultr, and V. Rödl. "On qualitatively independent partitions and related problems." *Discrete Applied Mathematics* 6.2 (1983), pp. 193–205.

[72]   S. Poljak and Z. Tuza. "On the maximum number of qualitatively independent partitions." *Journal of Combinatorial Theory, Series A* 51.1 (1989), pp. 111–116.

[73]   B. Qvist. *Some remarks concerning curves of the second degree in a finite plane*. Suomalainen Tiedeakatemia, 1952.

[74]   S. Raaphorst. "Variable Strength Covering Arrays." PhD thesis, University of Ottawa, 2013.

[75]   S. Raaphorst, L. Moura, and B. Stevens. "A construction for strength-3 covering arrays from linear feedback shift register sequences." *Designs, Codes and Cryptography* 73.3 (2014), pp. 949–968.

[76]   C. R. Rao. "Factorial experiments derivable from combinatorial arrangements of arrays." *Supplement to the Journal of the Royal Statistical Society* 9.1 (1947), pp. 128–139.

[77]   C. R. Rao. "Hypercubes of strength d leading to confounded designs in factorial experiments." *Bull. Calcutta Math. Soc* 38 (1946), pp. 67–78.

[78]   C. R. Rao. "On a class of arrangements." *Proceedings of the Edinburgh Mathematical Society (Series 2)* 8.03 (1949), pp. 119–125.

[79]   A. Rényi. *Foundations of Probability*. Holden-Day Inc., 1970.

[80]   A. H. Ronneseth and C. J. Colbourn. "Merging covering arrays and compressing multiple sequence alignments." *Discrete Applied Mathematics* 157.9 (2009), pp. 2177–2190.

[81]   G. Roux. "k-propriétés dans des tableaux de n colonnes: cas particulier de la k-surjectivité et de la k-permutivité." PhD thesis, Paris 6, 1987.

[82]   F. Ruskey, C. Savage, and T. M. Y. Wang. "Generating necklaces." *Journal of Algorithms* 13.3 (1992), pp. 414–430.

[83]   F. Ruskey and J. Sawada. "An efficient algorithm for generating necklaces with fixed density." *SIAM Journal on Computing* 29.2 (1999), pp. 671–684.

[84]   K. Sarkar and C. J. Colbourn. "Upper bounds on the size of covering arrays." *arXiv preprint arXiv:1603.07809* (2016).

[85]   R. Singleton. "Maximum distance q-nary codes." *IEEE Transactions on Information Theory* 10.2 (1964), pp. 116–118.

[86]   J. Stardom. "Metaheuristics and the Search for Covering and Packing Arrays." PhD thesis, Simon Fraser University, 2001.

[87] S. K. Stein. "Two combinatorial covering theorems." *Journal of Combinatorial Theory, Series A* 16.3 (1974), pp. 391–397.

[88] W. Stein et al. "Sage: Open source mathematical software." *7 December 2009* (2008).

[89] B. Stevens. "Transversal covers and packings." PhD thesis, University of Toronto, 1998.

[90] B. Stevens and E. Mendelsohn. "New recursive methods for transversal covers." *Journal of Combinatorial Designs* 7.3 (1999), pp. 185–203.

[91] M. Tsfasman and S. G. Vlădut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.

[92] Y.-W. Tung and W. S. Aldiwan. "Automating test case generation for the new generation mission software system." *Aerospace Conference Proceedings, 2000 IEEE*. Vol. 1. IEEE. 2000, pp. 431–437.

[93] G. Tzanakis, L. Moura, D. Panario, and B. Stevens. "Constructing new covering arrays from LFSR sequences over finite fields." *Discrete Mathematics* 339.3 (2016), pp. 1158–1171.

[94] G. Tzanakis, L. Moura, D. Panario, and B. Stevens. "Covering arrays from m-sequences and character sums." *Designs, Codes and Cryptography* (2016), pp. 1–20. issn: 1573-7586. url: http://dx.doi.org/10.1007/s10623-016-0316-2.

[95] D. R. Wallace and D. R. Kuhn. "Failure modes in medical device software: an analysis of 15 years of recall data." *International Journal of Reliability, Quality and Safety Engineering* 8.04 (2001), pp. 351–371.

[96] R. M. Wilson and Q. Xiang. "Cyclotomy, half ovoids and two-weight codes." *Unpublished preprint* (1997).

Index