# Combinatorial Designs for Authentication and Secrecy Codes

By Michael Huber

## Contents

<table>
<thead>
<tr>
<th>1 Introduction</th>
<th>582</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Authentication and Secrecy Model</td>
<td>584</td>
</tr>
<tr>
<td>1.2 Combinatorial Designs: A Brief Historical Account</td>
<td>589</td>
</tr>
<tr>
<td>1.3 Some Group Theory</td>
<td>591</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2 Combinatorial Design Theory</th>
<th>594</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 $t$-Designs and Finite Geometries</td>
<td>595</td>
</tr>
<tr>
<td>2.2 Latin Squares and Perpendicular Arrays</td>
<td>609</td>
</tr>
<tr>
<td>2.3 Authentication Perpendicular Arrays</td>
<td>613</td>
</tr>
<tr>
<td>2.4 Splitting Designs and Others</td>
<td>617</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3 Applications to Authentication and Secrecy Codes</th>
<th>624</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Secrecy Codes</td>
<td>625</td>
</tr>
<tr>
<td>3.2 General Authentication Codes</td>
<td>629</td>
</tr>
<tr>
<td>3.3 Authentication Codes with Secrecy</td>
<td>630</td>
</tr>
<tr>
<td>3.4 Authentication Codes with Secrecy in the Verification Oracle Model</td>
<td>644</td>
</tr>
<tr>
<td>3.5 Authentication Codes with Splitting</td>
<td>648</td>
</tr>
</tbody>
</table>
Combinatorial Designs for Authentication and Secrecy Codes

Michael Huber

Wilhelm Schickard Institute for Computer Science, University of Tuebingen,
Sand 13, D-72076 Tuebingen, Germany, michael.huber@uni-tuebingen.de

Abstract

Combinatorial design theory is a very active area of mathematical research, with many applications in communications and information theory, computer science, statistics, engineering, and life sciences. As one of the fundamental discrete structures, combinatorial designs are used in fields as diverse as error-correcting codes, statistical design of experiments, cryptography and information security, mobile and wireless communications, group testing algorithms in DNA screening, software and hardware testing, and interconnection networks. This monograph provides a tutorial on combinatorial designs, which gives an overview of the theory. Furthermore, the application of combinatorial designs to authentication and secrecy codes is described in depth. This close relationship of designs with cryptography and information security was first revealed in Shannon’s seminal paper on secrecy systems. We bring together in one source foundational and current contributions concerning design-theoretic constructions and characterizations of authentication and secrecy codes.
Introduction

Authentication and secrecy are two crucial concepts in cryptography and information security. Concerning authenticity, typically communicating parties would like to be assured of the integrity of information they obtain via potentially insecure channels. Regarding secrecy, protection of the confidentiality of sensitive information shall be ensured in the presence of eavesdropping. Although independent in their nature, various scenarios require that both aspects hold simultaneously. For information-theoretic, or unconditional, security (i.e. robustness against an attacker that has unlimited computational resources), authentication and secrecy codes can be used to minimize the possibility of an undetected deception. The construction of such codes is of great importance and has been considered by many researchers over the last few decades. Often deep mathematical tools are involved in the constructions, mainly from combinatorics. This close relationship of cryptography and information security with combinatorics has been first revealed in Shannon’s landmark paper “Communication theory of secrecy systems” [182]: a key-minimal secrecy system provides perfect secrecy if and only if the encryption matrix is a Latin square and the keys are used with equal probability. The initial construction
of authentication codes goes back to Gilbert et al. [74], and uses finite projective planes. A more general and systematic theory of authenticity was developed by Simmons (see [183, 184, 185, 186, 187], and [188] for a survey). Further foundational works on authentication and secrecy codes have been carried out by Massey [152] and Stinson et al. [194, 195, 196, 201, 202]. A generalized information-theoretic framework for authentication was introduced by Maurer [157].

The purpose of this monograph is to describe in depth classical and current interconnections between combinatorial designs and authentication and secrecy codes. The latter also include the author’s recent [102, 106, 107] and new contributions (cf. Section 3.4) on multi-fold secure authentication and secrecy codes in various models. Moreover, this issue provides a tutorial overview on the theory of combinatorial designs. These fundamental discrete structures find applications in fields as diverse as error-correcting codes, statistical design of experiments, cryptography and information security, mobile and wireless communications, group testing algorithms in DNA screening, software and hardware testing, and interconnection networks. In particular, the last few years have witnessed an increasing body of work in the communications and information theory literature that makes substantial use of results in combinatorial design theory.

The organization of the monograph is as follows. Section 1.1 introduces the Shannon–Simmons model of information-theoretical authentication and secrecy. We define the important concepts of spoofing attacks and perfect secrecy. A short historical account on combinatorial designs is given in Section 1.2. Since permutation groups often play a crucial role in the construction of combinatorial designs, we introduce basic notions on permutation groups and group actions in Section 1.3. Section 2 provides a tutorial account on combinatorial design theory. We emphasize on the construction of various combinatorial structures including \( t \)-designs, finite geometries, Latin squares, orthogonal arrays, perpendicular and authentication perpendicular arrays, splitting \( t \)-designs, and others. These combinatorial structures provide essential tools for the construction and characterization of authentication and secrecy codes in the following section. A special notice is placed on examples for each type of combinatorial designs. We also briefly
point to the interplay between $t$-designs and error-correcting codes. Section 3 is devoted to various key applications of combinatorial designs to authentication and secrecy codes. Foundational and recent results concerning the construction and characterization of authentication and secrecy codes are exposed. Starting with Shannon’s classical result, we first deal with secrecy codes in Section 3.1. Authentication codes without any secrecy requirements are considered in Section 3.2. In Section 3.3, codes that offer both authenticity and secrecy are discussed in detail. We distinguish between arbitrary and equiprobable source probability distributions. The advantage of the source states being equiprobable distributed is that the number of encoding rules can be reduced. Section 3.4 is devoted to an extended authentication model, where the opponent can act pro-actively by having access to a verification oracle. Authentication codes with splitting are considered in Section 3.5. In such a code, several messages can be used to communicate a particular plaintext (non-deterministic encoding). We briefly mention authentication codes that permit arbitration in Section 3.6. In Section 3.7, further recent applications are highlighted which makes substantial use of combinatorial design theory. Finally, we conclude in Section 3.8 with a synthesis of the work and some directions for future research.

1.1 Authentication and Secrecy Model

We rely on the information-theoretical (or unconditional) secrecy model developed by Shannon [182], and by Simmons [183, 184, 185, 188] including authentication. Information-theoretical security means that the security of the model is not dependent on any complexity assumptions and hence cannot be broken given unlimited computational resources. A well-known practical application of such a perfectly-secure system is the Washington–Moscow Hotline (“red telephone”) during the time of the cold war. Modern applications may include protection of digital data where cryptographic long-term security and/or confidentiality is strongly required, e.g., in archiving official documents, notarial contracts, court records, medical data, state secrets, copyright protection as well as further areas concerning e-government, e-health, e-publication, etc.
1.1 Authentication and Secrecy Model

The reader may be interested in the area of information-theoretical cryptography [156], long-term secure cryptography [33], post-quantum cryptography [15], and in the broad area of cryptography in general [77, 78, 159, 200].

1.1.1 Basic Preliminaries

We introduce the basic model of information-theoretical authentication and secrecy. Our notation follows, for the most part, that of [152, 195]. Figure 1.1 gives an illustration of the model (cf. [152, 195]).

In this basic model of authentication and secrecy three participants are involved: a transmitter, a receiver, and an opponent. The transmitter wants to communicate information to the receiver via a public communications channel. The receiver in return would like to be confident that any received information actually came from the transmitter and not from some opponent (integrity of information). The transmitter and the receiver are assumed to trust each other. Sometimes this is also called an A-code. Variants of this model will be discussed in Sections 3.4, 3.5, and 3.6.

In what follows, let $S$ denote a set of $k$ source states (or plaintexts), $M$ a set of $v$ messages (or ciphertexts), and $E$ a set of $b$ encoding rules (or keys). Using an encoding rule $e \in E$, the transmitter encrypts a source state $s \in S$ to obtain the message $m = e(s)$ to be sent over the

![Fig. 1.1 Shannon–Simmons authentication and secrecy model.](image)
channel. The encoding rule is an injective function from $\mathcal{S}$ to $\mathcal{M}$, and is communicated to the receiver via a secure channel prior to any messages being sent. For a given encoding rule $e \in \mathcal{E}$, let $M(e) := \{e(s) \mid s \in \mathcal{S}\}$ denote the set of valid messages. For an encoding rule $e$ and a set $M^* \subseteq M(e)$ of distinct messages, we define $f_e(M^*) := \{s \in \mathcal{S} \mid e(s) \in M^*\}$, i.e., the set of source states that will be encoded under encoding rule $e$ by a message in $M^*$. Furthermore, we define $E(M^*) := \{e \in \mathcal{E} \mid M^* \subseteq M(e)\}$, i.e., the set of encoding rules under which all the messages in $M^*$ are valid. A received message $m$ will be accepted by the receiver as being authentic if and only if $m \in M(e)$. When this is fulfilled, the receiver decrypts the message $m$ by applying the decoding rule $e^{-1}$, where

$$e^{-1}(m) = s \iff e(s) = m.$$

An authentication code can be represented algebraically by a $(b \times k)$-encoding matrix with the rows indexed by the encoding rules, the columns indexed by the source states, and the entries defined by $a_{es} := e(s) \ (1 \leq e \leq b, 1 \leq s \leq k)$.

### 1.1.2 Protection Against Spoofing Attacks

We introduce the scenario of a spoofing attack of order $i$ (cf. [152]): Suppose that an opponent observes $i \geq 0$ distinct messages, which are sent through the public channel using the same encoding rule. The opponent then inserts a new message $m'$ (being distinct from the $i$ messages already sent), hoping to have it accepted by the receiver as authentic. The cases $i = 0$ and $i = 1$ are called impersonation game and substitution game, respectively. These cases have been studied in detail in recent years (see, for instance, [196, 201, 27, 53, 165]), however less is known for the cases $i \geq 2$. In this monograph, we especially focus on those cases where $i \geq 2$.

For any $i$, we assume that there is some probability distribution on the set of $i$-subsets of source states, so that any set of $i$ source states has a non-zero probability of occurring. For simplification, we ignore the order in which the $i$ source states occur, and assume that no source state occurs more than once. Given this probability distribution $p_S$ on
1.1 Authentication and Secrecy Model

\( S \), the receiver and transmitter choose a probability distribution \( p_E \) on \( E \), called an encoding strategy, with associated independent random variables \( S \) and \( E \), respectively. These distributions are known to all participants and induce a third distribution, \( p_M \), on \( M \) with associated random variable \( M \). The deception probability \( P_{d_i} \) is the probability that the opponent can deceive the receiver with a spoofing attack of order \( i \). The following theorem by Massey provides combinatorial lower bounds (for the proof, we follow \([194, 195]\)).

**Theorem 1.1 (Massey [152]).** In an authentication code with \( k \) source states and \( v \) messages, for every \( 0 \leq i \leq t \), the deception probabilities are bounded below by

\[
P_{d_i} \geq \frac{k - i}{v - i}.
\]

**Proof.** Let \( M^* \subset M \) denote a set of \( i \leq t \) distinct messages. We suppose that an opponent observes the \( i \) messages in the channel, and then sends a message \( m \in M \) not in \( M^* \). Let \( \text{payoff}(m, M^*) \) denote the probability that the message \( m \) would be accepted by the receiver as authentic. Then

\[
\text{payoff}(m, M^*) = \frac{\sum_{e \in E(M^* \cup \{m\})} p(e) \cdot p(S = f_e(M^*))}{\sum_{e \in E(M^*)} p(e) \cdot p(S = f_e(M^*))}.
\]

It follows that

\[
\sum_{m \in M \setminus M^*} \text{payoff}(m, M^*) = k - i.
\]

Hence, there exists some \( m \in M \) not in \( M^* \) such that \( \text{payoff}(m, M^*) \geq (k - i)/(v - i) \). For every set \( M^* \) of \( i \) messages, the opponent can choose such an \( m \). This defines a deception strategy in which the transmitter/receiver can be deceived with probability at least \( (k - i)/(v - i) \).

An authentication code is called \( t_A \)-fold secure against spoofing if \( P_{d_i} = (k - i)/(v - i) \) for all \( 0 \leq i \leq t_A \).
1.1.3 Perfect Secrecy

We address Shannon’s fundamental idea of perfect secrecy (cf. [182]): An authentication code is said to have perfect secrecy if

\[ p_S(s|m) = p_S(s) \]

for every source state \( s \in S \) and every message \( m \in M \).

That is, the \( a \ posteriori \) probability that the source state is \( s \), given that the message \( m \) is observed, is identical to the \( a \ priori \) probability that the source state is \( s \).

It can easily be shown via Bayes’ Theorem that

\[
p_S(s|m) = \frac{p_M(m|s) \cdot p_S(s)}{\sum_{e \in E|e(s) = m} p_E(e) \cdot p_S(s)}.
\]

Moreover, we introduce the concept of perfect multi-fold secrecy established by Stinson [195], which generalizes Shannon’s perfect (one-fold) secrecy. An alternative definition has been given by Godlewski and Mitchell [75]. Instead of assuming that each encoding rule is used to encode only one message, the situation is extended in a natural way: each encoding rule is used to encode up to \( t_S \) messages for some positive integer \( t_S \). More formally, we say that an authentication code has perfect \( t_S \)-fold secrecy if, for every positive integer \( t^* \leq t_S \), for every set \( M^* \) of \( t^* \) messages observed in the channel, and for every set \( S^* \) of \( t^* \) source states, we have

\[ p_S(S^*|M^*) = p_S(S^*). \]

That is, the \( a \ posteriori \) probability distribution on the \( t^* \) source states, given that a set of \( t^* \) messages is observed, is identical to the \( a \ priori \) probability distribution on the \( t^* \) source states. Obviously, for the case \( t_S = 1 \) this coincides with the definition of perfect secrecy.

When clear from the context, we often only write \( t \) instead of \( t_A \) respectively \( t_S \).

As the encoding rules have to be communicated to the receiver via a secure channel, i.e. \( \log_2 b \) bits for \( b \) encoding rules, we want to minimize the number of encoding rules. With respect to the minimal
number, we will deal with the construction and characterization of \textit{optimal} authentication and secrecy codes in Section 3.

\textbf{Remark 1.1.} We note that the term \textit{secrecy code} (sometimes also secrecy system) is customarily used in the above model to describe a cipher that achieves Shannon’s perfect secrecy over \textit{noiseless} channels. This should not be confused with the same expression often used today for describing codes that can achieve both reliable and secure communication over \textit{noisy} channels (also known as wiretap channels). For recent developments on information-theoretic security for noisy channels, we refer to the monograph [142] and the references therein.

\section*{1.2 Combinatorial Designs: A Brief Historical Account}

Combinatorial designs have a long and rich history of work. We briefly highlight three historical examples:

Leonhard Euler considered in 1782 the following problem [64], posed by Catherine the Great according to folklore. This problem came to known as \textit{Euler’s 36 Officers Problem}:

“A very curious question, which has exercised for some time the ingenuity of many people, has involved me in the following studies, which seem to open a new field of analysis, in particular the study of combinations. The question resolves around arranging 36 officers to be drawn from 6 different ranks and also from 6 different regiments so that they are ranged in a square so that in each line (both horizontal and vertical) there are 6 officers of different ranks and different regiments.”
This question asks for finding two orthogonal Latin squares of order 6. Euler correctly conjectured that this was impossible, and a complete proof with an exhaustive search of all Latin squares of order 6 were given in 1900 by Tarry [207, 208]. A short proof is due to Stinson [193].

The Swiss geometer Jakob Steiner posed in 1853 in his classical “Combinatorische Aufgabe” [192] the following question:

“Welche Zahl, \(N\), von Elementen hat die Eigenschaft, dass sich die Elemente so zu dreien ordnen lassen, dass je zwei in einer, aber nur in einer Verbindung vorkommen?”

[Transl.: “For what number, \(N\), of elements is it possible to arrange the elements in triplets, so that every pair of elements is contained in one and only one triplet?”]

Writing \(v\), \(k\), and \(t\) instead of \(N\), 3, and 2, respectively, leads us to the definition of what is now called a Steiner \(t\)-design (or a Steiner system, cf. Definition 2.1). However, there had been earlier work on these combinatorial designs going back to, in particular, Plücker, Woolhouse, and most notably Kirkman.

Thomas Kirkman’s famous 15 Schoolgirl Problem, which he proposed in 1850 in the popular magazine The Lady’s and Gentleman’s Diary [132], states as follows:

“Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily so that no two shall walk twice abreast.”
This is equivalent to the problem of constructing a Steiner 2-design with parameters $k = 3$ and $v = 15$, having the extra requirement that the set of triples can be partitioned into seven ‘parallel classes’. Kirkman’s problem as well as the more general case for other possible values of $v$ attracted great interest among late 19th and early 20th century mathematicians, including contributions by Burnside, Cayley and Sylvester. However, it was not until 1971 that the general problem was completely resolved by Ray-Chaudhuri and Wilson [173], showing that there exists at least one such design for every $v \equiv 3 \pmod{6}$. For $v = 15$, there are seven different solutions to the problem (up to isomorphism). For all other admissible values $v \geq 21$, the number of solutions remains unknown up to the present.

For a detailed account on the history of combinatorial designs, we refer the interested reader, e.g., to [43, Chap. I.2] and [225].

1.3 Some Group Theory

Often permutation groups play a crucial role in the construction of combinatorial designs. We introduce basic notions on permutation groups and group actions in this section. We will restrict ourselves to finite groups, although most of the concepts also make sense for infinite groups.

Let $X$ be a non-empty finite set. The set $\text{Sym}(X)$ of all permutations of $X$ with respect to the composition

$$x^{gh} := (x^g)^h \text{ for } x \in X \text{ and } g, h \in \text{Sym}(X)$$

forms a group, called the symmetric group on $X$. If $X = \{1, \ldots, v\}$, then we write $S_v$ for the symmetric group of degree $v$. Clearly, $\text{Sym}(X) \cong S_v$ if and only if $|X| = v$. 
A group $G$ acts (or operates) on $X$, if to each element $g \in G$ a permutation $x \mapsto x^g$ of $X$ is assigned such that

(i) $x^1 = x$ for all $x \in X$ (where $1 = 1_G$ denotes the identity element of $G$),
(ii) $(x^g)^h = x^{gh}$ for all $x \in X$ and all $g, h \in G$.

Evidently, these properties are fulfilled if and only if the map

$$\varphi : g \mapsto (x \mapsto x^g)$$

of $G$ into $\text{Sym}(X)$ is a group homomorphism. In general, any homomorphism $\varphi$ of $G$ into $\text{Sym}(X)$ is said to be an action (or a permutation representation) of $G$ on $X$. If $\ker(\varphi) = 1$ for the kernel of $\varphi$, then $G$ acts faithfully on $X$; in this case, $G$ is called a permutation group on $X$. If $\ker(\varphi) = G$, then $G$ operates trivially on $X$. The degree of a permutation group is the size of $X$.

**Example 1.1.** The group of symmetries of a three-dimensional cube (cf. Figure 2.3) acts on various sets including the set of 8 vertices, the set of 6 faces, the set of 12 edges, and the set of 4 principal diagonals. Properties (i) and (ii) are clearly satisfied in each case.

Let $G_1$ and $G_2$ be permutation groups acting on the sets $X_1$ and $X_2$, respectively. Then, $G_1$ and $G_2$ are called permutation isomorphic, if there exists a group isomorphism $\sigma : G_1 \to G_2$ and a bijective map $\tau : X_1 \to X_2$ with

$$(x^g)^\tau = (x^\tau)^{(g^\sigma)}$$

for all $x \in X_1$ and all $g \in G_1$. Essentially, this means that the groups $G_1$ and $G_2$ are “the same” except for the labeling of the points.

Let $G$ be a group acting on $X$. For $x \in X$, the subgroup

$$G_x := \{ g \in G \mid x^g = x \}$$

denotes the (point-)stabilizer of $x$ in $G$ and the set

$$x^G := \{ x^g \mid g \in G \}$$
is the *orbit* of $x$ under $G$ (or the $G$-orbit of $x$). For $B \subseteq X$, let

$$G_B := \{ g \in G \mid B^g = B \}$$

be its *setwise stabilizer*. The *order* of $G$ is denoted by $|G|$.

A group $G$ acting on $X$ is called *transitive* on $X$, if $G$ has only one orbit, i.e. $x^G = X$ for all $x \in X$. Equivalently, $G$ is transitive if for any two points $x, y \in X$ there exists an element $g \in G$ with $x^g = y$. For a positive integer $t \leq |X|$, we call $G$ to be *$t$-transitive*, if for any two injective $t$-tuples $(x_1, x_2, \ldots, x_t)$ and $(y_1, y_2, \ldots, y_t)$ there exists an element $g \in G$ with $x_i^g = y_i$ for all $1 \leq i \leq t$. We say that $G$ is *$t$-homogeneous*, if it is transitive on the set of all $t$-subsets of $X$. Obviously, $t$-transitive implies $t$-homogeneous.

**Example 1.2.** The symmetric group $S_v$ is $v$-transitive, and the alternating group $A_v$ (i.e., the subgroup of $S_v$ consisting of all even permutations) is $(v - 2)$-transitive in their actions on the set $\{1, \ldots, v\}$ ($v \geq 3$).

We will list all finite multiply homogeneous permutation groups in Appendix 4.1. We note that this classification relies on the Classification of the Finite Simple Groups (CFSG), one of the most powerful tools of modern algebra.

For a detailed treatment of finite group theory and permutation groups, we refer the reader to [5, 38, 41, 61, 117, 118, 139, 223].
2

Combinatorial Design Theory

The theory of combinatorial designs is concerned with a crucial problem of combinatorics, that of arranging objects into patterns according to specified rules. It has strong connections with other fields in discrete mathematics. Besides linear and abstract algebra and number theory, we mention especially its links to graph theory [39, 209], finite and incidence geometry [54, 34], and permutation group theory [38, 41, 61, 223]. Fields of applications, among others, include coding and information theory [6, 39, 50, 105, 111, 112, 149], cryptography [170, 197, 200], statistical design of experiments [11, 65, 172, 205], and combinatorial algorithms [129]. Further details on some recent applications are highlighted in Section 3.7.

We give in this section a tutorial overview of combinatorial design theory. We emphasize on the construction of various combinatorial structures including $t$-designs, finite geometries, Latin squares, orthogonal arrays, perpendicular and authentication perpendicular arrays, splitting $t$-designs, and others. These combinatorial structures provide essential tools for the construction and characterization of authentication and secrecy codes in Section 3. A special notice is placed on
examples for each type of combinatorial designs. We also briefly point to the interplay between t-designs and error-correcting codes.

Throughout this section, let \( t \leq k \leq v \) and \( \lambda \) be positive integers, and \( q \) be a prime power. Let \( GF(q) \) denote the finite field with \( q \) elements.

### 2.1 t-Designs and Finite Geometries

We start by introducing combinatorial t-designs.

**Definition 2.1.** A \( t(v,k,\lambda) \) design \( D \) is a pair \((X,\mathcal{B})\), which satisfies the following properties:

1. \( X \) is a set of \( v \) elements, called points,
2. \( \mathcal{B} \) is a family of \( k \)-subsets of \( X \), called blocks,
3. every \( t \)-subset of \( X \) is contained in exactly \( \lambda \) blocks.

We will denote points by lower-case and blocks by upper-case Latin letters. Via convention, let \( b := |\mathcal{B}| \) denote the number of blocks. Throughout this work, ‘repeated blocks’ are not allowed, that is, the same \( k \)-subset of points may not occur twice as a block. If \( t < k < v \) holds, then we speak of a non-trivial t-design. A \( t(v,k,\lambda) \) design with \( \lambda = 1 \) is called a Steiner t-design (or a Steiner system, cf. Section 1.2). The special case of a Steiner design with parameters \( t = 2 \) and \( k = 3 \) is called a Steiner triple system of order \( v \), briefly STS(\( v \)). A Steiner design with parameters \( t = 3 \) and \( k = 4 \) is called a Steiner quadruple system of order \( v \), briefly SQS(\( v \)).

We give some illustrative examples.

**Example 2.1.** We choose as point set

\[
X = \{1,2,3,4,5,6,7\}
\]

and as block set

\[
\mathcal{B} = \{\{1,2,4\}, \{2,3,5\}, \{3,4,6\}, \{4,5,7\}, \{1,5,6\}, \{2,6,7\}, \{1,3,7\}\}.
\]
This yields a Steiner 2-(7, 3, 1) design, the well-known Fano plane, which is the smallest design arising from a projective geometry. The usual representation of this unique projective plane of order 2 is given by the diagram in Figure 2.1.

Combinatorial t-designs can be represented algebraically in terms of incidence matrices: Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-design, and let the points be labeled $\{x_1, \ldots, x_v\}$ and the blocks be labeled $\{B_1, \ldots, B_b\}$. Then, the $b \times v$ matrix $A = (a_{ij})$ ($1 \leq i \leq b$, $1 \leq j \leq v$) defined by

$$a_{ij} := \begin{cases} 1, & \text{if } x_j \in B_i \\ 0, & \text{otherwise} \end{cases} \quad (2.1)$$

is called an incidence matrix of $\mathcal{D}$. Clearly, $A$ depends on the respective labeling, however, it is unique up to column and row permutation.

If a 2-design has, like in Example 2.1, equally many points and blocks, i.e. $v = b$, then we speak of a square design (as its incidence matrix is square). By tradition, square designs are often called symmetric designs, although here the term does not imply any symmetry of the design. For more on these interesting designs, we refer, e.g., to [119].

**Example 2.2.** We take as point set

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

and as block set

$$\mathcal{B} = \{\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}, \{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\},$$

$$\{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}, \{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}\}.$$
This gives a Steiner 2-(9, 3, 1) design, the smallest non-trivial design arising from an affine geometry, which is again unique up to isomorphism. This affine plane of order 3 can be constructed from the array

\[
\begin{array}{ccc}
1 & 2 & 3 \\
4 & 5 & 6 \\
7 & 8 & 9 \\
\end{array}
\]

as illustrated in Figure 2.2.

More generally, we obtain the following examples.

**Example 2.3.** We choose as point set \( X \) the set of one-dimensional subspaces of a vector space \( V = V(d + 1, q) \) of dimension \( d + 1 \geq 3 \) over \( GF(q) \). As block set \( B \) we take the set of two-dimensional subspaces of \( V \). Then there are \( v = \frac{q^{d+1} - 1}{q - 1} \) points and each block \( B \in B \) contains \( k = q + 1 \) points. Since clearly any two one-dimensional subspaces span a single two-dimensional subspace, any two distinct points are contained in a unique block. Hence, the projective space \( PG(d, q) \) is an example of a Steiner 2-(\( \frac{q^{d+1} - 1}{q - 1}, q + 1, 1 \)) design. For \( d = 2 \), the particular designs are projective planes of order \( q \), which are square designs. More generally, for any \( 1 \leq i \leq d - 1 \), the points and \( i \)-dimensional subspaces of \( PG(d, q) \) (i.e., the \( (i + 1) \)-dimensional subspaces of \( V \)) yield a 2-design.

**Example 2.4.** We take as point set \( X \) the set of elements of a vector space \( V = V(d, q) \) of dimension \( d \geq 2 \) over \( GF(q) \). As block set \( B \) we
choose the set of affine lines of $V$ (i.e., the translates of one-dimensional subspaces of $V$). Then there are $v = q^d$ points and each block $B \in \mathcal{B}$ contains $k = q$ points. As obviously any two distinct points lie on exactly one line, they are contained in a unique block. Hence, we obtain the affine space $AG(d,q)$ as an example of a Steiner $2-(q^d, q, 1)$ design. When $d = 2$, these designs are affine planes of order $q$. More generally, for any $1 \leq i \leq d - 1$, the points and $i$-dimensional subspaces of $AG(d,q)$ form a 2-design.

If $\mathcal{D}_1 = (X_1, \mathcal{B}_1)$ and $\mathcal{D}_2 = (X_2, \mathcal{B}_2)$ are two $t$-designs, then a bijective map $\alpha : X_1 \to X_2$ is called an isomorphism of $\mathcal{D}_1$ onto $\mathcal{D}_2$, if

$$B \in \mathcal{B}_1 \iff \alpha(B) \in \mathcal{B}_2.$$ 

In this case, the designs $\mathcal{D}_1$ and $\mathcal{D}_2$ are isomorphic. An isomorphism of a design $\mathcal{D}$ onto itself is called an automorphism of $\mathcal{D}$. Evidently, the set of all automorphisms of a design $\mathcal{D}$ form a group under composition, the full group of automorphisms of $\mathcal{D}$. We call any subgroup of it a group of automorphisms of $\mathcal{D}$.

It is a well-known result that both affine and projective planes of order $n$ exist whenever $n$ is a prime power. The conjecture that no such planes exist with orders other than prime powers is unresolved so far. The classical result of Bruck and Ryser [31] still remains the only general statement: If $n \equiv 1$ or $2 \pmod{4}$ and $n$ is not equal to the sum of two squares of integers, then $n$ does not occur as the order of a finite projective plane. The smallest integer that is not a prime power and not covered by the Bruck–Ryser Theorem is 10. Using substantial computer analysis, Lam et al. [140] proved the non-existence of a projective plane of order 10. The next smallest number is 12, for which neither a positive nor a negative answer has been proved. Likewise the existence problem, the question on the number of different isomorphism types is of fundamental importance. There are, for example, precisely four non-isomorphic projective planes of order 9. For a further discussion, in particular of the rich history of affine and projective planes, the reader may be referred, e.g., to [20, 54, 95, 113, 148, 171].

For our purposes, we are especially interested in $t$-designs with $t \geq 3$. Here is a simple example.
Example 2.5. We take as points the vertices of a three-dimensional cube. As illustrated in Figure 2.3, we can choose three types of blocks:

(i) a face (six of these),
(ii) two opposite edges (six of these),
(iii) an inscribed regular tetrahedron (two of these).

This yields a Steiner 3-(8, 4, 1) design, which is unique up to isomorphism.

More generally, the binary vector space $V(d, 2)$ of dimension $d \geq 2$ with the set $B$ of blocks taken to be the set of all subsets of four distinct elements of $V(d, 2)$ whose vector sum is zero, form a Boolean SQS($2^d$). Geometrically speaking, these SQS($2^d$) consist of the points and planes of the $d$-dimensional binary affine space $AG(d, 2)$ as shown by the next example.

Example 2.6. In $AG(d, q)$ any three distinct points define a plane unless they are collinear (i.e., lie on the same line). If the underlying field is $GF(2)$, then the lines contain only two points and hence any three points cannot be collinear. Therefore, the points and planes of the affine space $AG(d, 2)$ form a Steiner 3-$(2^d, 4, 1)$ design. More generally, for any fixed $i$ with $2 \leq i \leq d - 1$, the points and $i$-dimensional subspaces of $AG(d, 2)$ form a 3-design.

If $\mathcal{D} = (X, B)$ is a $t$-$(v, k, \lambda)$ design with $t \geq 2$, and $x \in X$ arbitrary, then the derived design with respect to $x$ is $\mathcal{D}_x = (X_x, B_x)$, where $X_x = X \setminus \{x\}$, $B_x = \{B \setminus \{x\} \mid x \in B \in B\}$. In this case, $\mathcal{D}$ is also called an extension of $\mathcal{D}_x$. Obviously, $\mathcal{D}_x$ is a $(t - 1)$-$(v - 1, k - 1, \lambda)$ design. The
complementary design $\mathcal{D}$ is obtained by replacing each block of $\mathcal{D}$ by its complement.

We indicate some helpful combinatorial tools.

For the existence of $t$-designs, basic necessary conditions can be obtained via elementary counting arguments.

**Theorem 2.1 (cf., e.g., [16]).** Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-$(v, k, \lambda)$ design. For a positive integer $s \leq t$, let $S \subseteq X$ with $|S| = s$. Then the number $\lambda_s$ of blocks containing all the points of $S$ is given by

$$\lambda_s = \lambda \frac{{v-s \choose t-s}}{{k-s \choose t-s}}.$$

In particular, for $t \geq 2$, a $t$-$(v, k, \lambda)$ design is also an $s$-$(v, k, \lambda_s)$ design.

It is customary to set $r := \lambda_1$ to be the number of blocks containing a given point (referring to the ‘replication number’ from statistical design of experiments, one of the origins of combinatorial design theory). It follows

**Corollary 2.2.** Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-$(v, k, \lambda)$ design. Then the following holds:

(a) $bk = vr$.

(b) ${v \choose t} \lambda = b {k \choose t}$.

(c) $r(k - 1) = \lambda_2(v - 1)$ for $t \geq 2$.

Since in Theorem 2.1 each $\lambda_s$ must be an integer, we obtain moreover the subsequent necessary arithmetic conditions.

**Corollary 2.3.** Let $\mathcal{D} = (X, \mathcal{B})$ be a $t$-$(v, k, \lambda)$ design. Then

$$\lambda \frac{{v-s \choose t-s}}{t-s} \equiv 0 \mod {k-s \choose t-s}$$

for each positive integer $s \leq t$. 


The next theorem is a classical result in the theory of designs, generally known as Fisher’s Inequality.

**Theorem 2.4 (Fisher [66]).** If \( \mathcal{D} = (X, \mathcal{B}) \) is a non-trivial \( t-(v,k,\lambda) \) design with \( t \geq 2 \), then we have \( b \geq v \), that is, there are at least as many blocks as points in \( \mathcal{D} \).

**Proof.** As a non-trivial \( t \)-design with \( t \geq 2 \) is also a non-trivial \( 2-(v,k,\lambda) \) design by Theorem 2.1, it is sufficient to prove the assertion for an arbitrary non-trivial \( 2-(v,k,\lambda) \) design \( \mathcal{D} \). Let \( A \) be an incidence matrix of \( \mathcal{D} \) labeled as in Equation (2.1). Clearly, the \((i,k)\)th entry

\[
(AA^t)_{ik} = \sum_{j=1}^{b} (A)_{ij} (A^t)_{jk} = \sum_{j=1}^{b} a_{ij} a_{kj}
\]

of the \( v \times v \) matrix \( AA^t \) is the number of blocks incident with both \( x_i \) and \( x_k \), and is thus equal to \( r \) if \( i = k \), and to \( \lambda \) if \( i \neq k \). Hence

\[
AA^t = (r - \lambda)I_v + \lambda J_v,
\]

where \( I_v \) denotes the \( v \times v \) unit matrix and \( J_v \) the \( v \times v \) matrix with all entries equal to 1. Using elementary row and column operations, it follows easily that

\[
\det(AA^t) = rk(r - \lambda)^v - 1.
\]

Thus \( AA^t \) is non-singular as \( r = \lambda \) would imply \( v = k \) by Theorem 2.1, yielding that the design is trivial. Therefore, the matrix \( AA^t \) has rank(\( AA^t \)) = \( v \). But, if \( b < v \), then rank(\( A \)) \( \leq b < v \), and thus rank(\( AA^t \)) < \( v \), a contradiction. It follows that \( b \geq v \), proving the claim.

\[\square\]

We note that equality holds exactly for square designs when \( t = 2 \). Obviously, the equality \( v = b \) implies \( r = k \) by Corollary 2.2 (a).

We state an important generalization to arbitrary \( t \)-designs (see also, e.g., [16] for a proof).

**Theorem 2.5 (Ray-Chaudhuri–Wilson [174]).** Let \( \mathcal{D} = (X, \mathcal{B}) \) be a \( t-(v,k,\lambda) \) design. If \( t \) is even, say \( t = 2s \), and \( v \geq k + s \), then \( b \geq \binom{v}{s} \). If \( t \) is odd, say \( t = 2s + 1 \), and \( v - 1 \geq k + s \), then \( b \geq 2\binom{v-1}{s} \).
We will consider now various constructions of $t$-designs. In a very natural way, $t$-designs can be constructed from multiply homogeneous permutations groups.

**Theorem 2.6 (cf., e.g., [16]).** Suppose there is a $t$-homogeneous (in particular, $t$-transitive) permutation group $G$ of degree $v$, and $k \geq t$. Then there is a $t$-$(v,k,\lambda)$ design with

$$\lambda = b \frac{k}{v} = \frac{|G|}{|G_B|} \cdot \frac{k}{v},$$

where $G_B$ is the setwise stabilizer of a block $B \in \mathcal{B}$.

**Example 2.7.** Let $d \geq 2$ be an integer. As point set $X$ we choose the elements of the projective line $GF(q^d) \cup \{\infty\}$ over $GF(q^d)$, where $\infty$ denotes a symbol with $\infty \notin GF(q^d)$. The linear fractional group

$$PGL(2,q^d) = \{ g: x \mapsto ax + b/cx + d \mid a, b, c, d \in GF(q^d), ad - bc \neq 0 \}$$

acts on $GF(q^d) \cup \{\infty\}$ in the natural manner (with the usual conventions for $\infty$: $g(\infty) := a/c$, $g(\frac{d}{c}) := \infty$ if $c \neq 0$, and $g(\infty) =: \infty$ if $c = 0$). As block set $\mathcal{B}$ take the images of $GF(q) \cup \{\infty\}$ under $PGL(2,q^d)$. This gives a Steiner 3-$(q^d + 1,q + 1,1)$ design with $PGL(2,q^d)$ as point 3-transitive group of automorphisms. These designs, known as *spherical geometries* (or *circle geometries*), were first described by Witt [227]. For $d = 2$, they are often called *Möbius planes* (or *inversive planes*) of order $q$. Apart from the classical example for each prime power $q$, there is for $q = 2^{2e+1}, e \geq 1$, another Möbius plane with the Suzuki group $Sz(q)$ as a simple point 2-transitive group of automorphisms (cf. Appendix 4.1).

**Example 2.8.** The unique Steiner 2-$(9,3,1)$ design whose points and blocks are the points and lines of the affine plane $AG(2,3)$ is extendable exactly three times to the following designs which are also unique up to isomorphism: the Steiner 3-$(10,4,1)$ design which is the Möbius plane of order 3 with $PGL(2,9)$ as full group of automorphisms, and
the two Mathieu–Witt designs 4-(11,5,1) and 5-(12,6,1) with the sporadic Mathieu groups $M_{11}$ and $M_{12}$ as point 4-transitive and point 5-transitive full groups automorphisms, respectively.

The construction of the ‘large’ Mathieu–Witt designs starts with the Steiner 2-(21,5,1) design whose points and blocks are the points and lines of the projective plane $PG(2,4)$. This is extendable also precisely three times to the following unique designs: the Mathieu–Witt design 3-(22,6,1) with $\text{Aut}(M_{22})$ as point 3-transitive full group of automorphisms as well as the Mathieu–Witt designs 4-(23,7,1) and 5-(24,8,1) with $M_{23}$ and $M_{24}$ as point 4-transitive and point 5-transitive full group of automorphisms, respectively. Further details can be found, e.g., in [4, 147]. However, the easiest way to construct and prove uniqueness of the Mathieu–Witt designs is via coding theory, using the related binary and ternary Golay codes (see, e.g., [149, 50]).

**Historical Note.** The five Mathieu groups were the first examples of sporadic finite simple groups and were discovered over 100 years ago by Mathieu [153, 154]. They are the only finite 4- and 5-transitive permutation groups besides the symmetric or alternating groups. The Steiner designs associated with the Mathieu groups were first constructed by both Carmichael [41] and Witt [226], and their uniqueness, up to isomorphism, proved by Witt [227].

In all the examples above, the group of automorphisms acts transitively on incident point-block pairs, that is, on the flags, of the Steiner $t$-designs. This reveals a high degree of regularity of the combinatorial structure. Basically all flag-transitive Steiner $t$-designs have been determined recently, see [96, 97, 98, 99] and [101] for a monograph. Further recent results about block-transitive and other highly regular $t$-designs are, e.g., [100, 103, 104, 108, 109]. For the numerous interactions between highly regular combinatorial structures and applications in information and coding theory, we refer to the literature given in the application at the end of this section.

**Example 2.9.** A few Steiner 5-$(v,k,1)$ designs have been constructed by combining several orbits of some prescribed group $PSL(2,q)$
Combinatorial Design Theory

on \(k\)-subsets (so-called method of orbiting under a group). Dennis-ton [56] discovered Steiner 5-(24,6,1) designs (with derived Steiner 4-(23,5,1) designs), a Steiner 5-(28,7,1) design (with derived Steiner 4-(27,6,1) and 3-(26,5,1) designs), Steiner 5-(48,6,1) designs (with derived Steiner 4-(47,5,1) designs), and Steiner 5-(84,6,1) designs (with derived Steiner 4-(83,5,1) designs). Mills [160] obtained a Steiner 5-(72,6,1) design (with derived Steiner 4-(71,5,1) design). Several further Steiner 5-(\(v\),6,1) designs have been obtained by this method with the parameters \(v = 36, 108, 132, 168, 244\) (cf. [18, 19, 46, 56, 57, 82, 83, 84, 160]).

The above examples list all presently known Steiner 5-designs. All known Steiner 4-designs are derived from Steiner 5-designs. There are many infinite classes of Steiner 2- and 3-designs. In addition to the examples already given, we mention the following results concerning Steiner triple and quadruple systems.

**Example 2.10.** Recall that a Steiner triple system STS(\(v\)) of order \(v\) is a 2-(\(v\),3,1) design, and a Steiner quadruple system SQS(\(v\)) of order \(v\) is a 3-(\(v\),4,1) design. It is elementary to verify that a STS(\(v\)) of order \(v\) exists if and only if \(v \equiv 1 \text{ or } 3 \pmod{6}\), \(v \geq 3\), as was first proved by Kirkman [131]. The number of non-isomorphic STS(\(v\)) is only known in the following cases: For \(v = 7\) and \(v = 9\) there exists an STS(\(v\)) in each case, unique up to isomorphism. These are the Fano plane \(PG(2,2)\) and the affine plane of order 3. For \(v = 13\) and \(v = 15\) we have exactly 2 and 80 distinct isomorphism types, respectively. For \(v = 19\) there are exactly 11,084,874,829 distinct isomorphism types (cf. [42, 128]).

Using recursive constructions, Hanani [88] showed that a similar condition hold for the existence of a Steiner quadruple system: a SQS(\(v\)) of order \(v\) exists if and only if \(v \equiv 2 \text{ or } 4 \pmod{6}\), \(v \geq 4\). The number of non-isomorphic SQS(\(v\)) is only known in the following cases: For \(v = 8\) and \(v = 10\) there exists an SQS(\(v\)) in each case, unique up to isomorphism. These are the affine space \(AG(3,2)\) and the Möbius plane of order 3. For \(v = 14\) we have exactly four distinct isomorphism
types. For $v = 16$ there are exactly $1,054,163$ distinct isomorphism types (cf. [13, 115, 130]).

We also mention that a Steiner $2-(v, 4, 1)$ design exists if and only if $v \equiv 1$ or $4 \pmod{12}$, and a Steiner $2-(v, 5, 1)$ design exists if and only if $v \equiv 1$ or $5 \pmod{20}$ (cf. [16]).

We give two results due to Hanani on the construction of 3-designs.

**Theorem 2.7 (Hanani [89]).** The following holds:

(a) Suppose there is a $3-(v + 1, q + 1, \lambda)$ design for some prime power $q$. Then there exists a $3-(vq^d + 1, q + 1, \lambda)$ design for all positive integers $d$.

(b) If there is a $3-(v + 1, 6, \lambda)$ design, then there exists a $3-(4v + 2, 6, \lambda)$ design.

Exploration of the construction of $t$-designs for large values of $t$ lead to the following celebrated theorem of Teirlinck.

**Theorem 2.8 (Teirlinck [206]).** For every positive integer value of $t$, there exists a non-trivial $t$-design.

However, although Teirlinck’s recursive methods are constructive, they only produce examples with tremendously large values of $\lambda$. Until now, no non-trivial Steiner $t$-design with $t > 5$ has been constructed. This is one of the most central and long-standing open questions in combinatorial design theory:

**Problem 2.1.** Does there exist any non-trivial Steiner $t$-design with $t \geq 6$?

For recent progress in the case of Steiner $t$-designs for large $t$ with high symmetry properties, see, e.g., [100]. A detailed account
on general Steiner designs can be found, e.g., in [16, 46]. Comprehensive survey articles especially on (Steiner) triple systems and Steiner quadruple systems include [47, 42] and [91, 144], respectively. For a more general treatment of combinatorial \( t \)-designs, the reader is referred to [16, 21, 35, 43, 86, 114, 199]. In particular, [16, 43] provide encyclopedic accounts of key results and existence tables with known parameter sets. DISCRETA [17] and DESIGN [191] are software packages for constructing and classifying combinatorial \( t \)-designs.

**Application: Error-Correcting Codes**

We want to briefly point to the rich and fruitful interplay between coding theory and the theory of \( t \)-designs. For a codeword \( x = (x_1, \ldots, x_d) \), the set

\[
\text{supp}(x) := \{i \mid x_i \neq 0\}
\]

of all coordinate positions with non-zero coordinates is called the support of \( x \). The (support) \( t \)-design of a code can be formed in the following way: given a, usually linear, code of length \( d \) that contains the zero vector, and non-zero weight \( w \), we choose as point set \( X \), the set of \( d \) coordinate positions of the code and as block set \( B \) the supports of all codewords of weight \( w \). As repeated blocks are not allowed, only distinct representatives of supports for codewords with the same supports are taken in the non-binary case.

A simple example is the following.

**Example 2.11.** The matrix

\[
G = \begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1
\end{pmatrix}
\]

is a generator matrix of a binary [7,4,3] Hamming code, which is the smallest non-trivial Hamming code. The seven codewords of weight 3
are exactly the seven rows of the incidence matrix
\[
\begin{pmatrix}
1 & 1 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\]
of the Fano plane $PG(2,2)$ (cf. Example 2.1). The supports of the seven codewords of weight 4 yield the complementary 2-(7,4,2) design, i.e. the biplane of order 2. The matrix $(I_4, J_4 - I_4)$ with $I_4$ the $4 \times 4$ unit matrix and $J_4$ the $4 \times 4$ matrix with all entries equal to 1 generates the extended binary $[8, 4, 4]$ Hamming code. Since any two codewords of weight 4 have distance at least 4, they have at most two ones in common, and hence no codeword of weight 3 appears as a subword of more than one codeword. On the other hand, there are $\binom{8}{3} = 56$ words of weight 3 and each codeword of weight 4 has four subwords of weight 3. Hence each codeword of weight 3 is a subword of precisely one codeword of weight 4. Thus, the supports of the 14 codewords of weight 4 form a Steiner 3-(8,4,1) design (cf. Example 2.5). More generally, in a binary $[2^m - 1, 2^m - 1 - m, 3]$ Hamming code the supports of codewords of weight 3 form an $STS(2^m - 1)$, and the supports of the codewords of weight 4 in the extended code yield an $SQS(2^m)$.

Via multiply homogeneous permutations groups, $t$-designs can be obtained from codes as follows.

**Theorem 2.9 (cf., e.g., [209]).** Let $C$ be a code which admits a group of automorphisms acting $t$-homogeneously (in particular, $t$-transitively) on the set of coordinates. Then the supports of the codewords of any non-zero weight form a $t$-design.

**Example 2.12.** The $r$th order Reed–Muller (RM) code $RM(r,m)$ of length $2^m$ is a binary $[2^m, \sum_{i=0}^{r} \binom{m}{i}, 2^{m-r}]$ code with its codewords
the value-vectors of all Boolean functions in \( m \) variables of degree at most \( r \). For example, the extended binary \([8,4,4]\) Hamming code in Example 2.11 is \( RM(1,3) \). Alternatively, a codeword in \( RM(r,m) \) can be viewed as the sum of characteristic functions of subspaces of dimension at least \( m - r \) of the affine space \( AG(m,2) \). Hence, the full group of automorphisms of \( RM(r,m) \) contains the 3-transitive group \( AGL(m,2) \) of all affine transformations (cf. Appendix 4.1), and so the codewords of any fixed non-zero weight yield a 3-design.

**Historical Note.** These codes were developed by Muller [161] and Reed [175] in 1954.

We also briefly mention the constructions of the Mathieu–Witt designs from the Golay codes.

**Example 2.13.** The supports of codewords of minimum weight 7 in the binary \([23,12,7]\) Golay code form a Steiner 4-(23,7,1) design, and the supports of the codewords of weight 8 in the extended binary \([24,12,8]\) Golay code give a Steiner 5-(24,8,1) design. The supports of codewords of minimum weight 5 in the ternary \([11,6,5]\) Golay code yield a Steiner 4-(11,5,1) design, and that the supports of the codewords of weight 6 in the extended ternary \([12,6,6]\) Golay code give a Steiner 5-(12,6,1) design.

**Historical Note.** The Golay codes were discovered by M. J. E. Golay [76] in 1949 in the process of extending R. W. Hamming’s code constructions [87] from the mid-1940’s.

As the above examples may suggest the interplay between coding theory and \( t \)-designs is most evidently seen in the relationship between perfect linear error-correcting codes and \( t \)-designs (cf. [8]). Another fundamental result in the interplay of coding theory and design theory is the Assmus–Mattson Theorem [9], which gives a sufficient condition for the codewords of constant weight in a linear code to form a \( t \)-design. In the light of this celebrated theorem, a number of new 5-designs have been found in the last decades by considering the codewords of fixed weight in certain codes. For a further discussion of the various
connections of $t$-designs with coding theory, we refer the reader to the large amount of literature [10, 6, 7, 26, 39, 112, 215, 216, 209, 210, 211, 149] as well as a recent up-to-date survey [105] including additional references.

2.2 Latin Squares and Perpendicular Arrays

We recall the definition of a Latin square.

**Definition 2.2.** A Latin square of order $v$ is an $v \times v$ array of $v$ symbols, in which each symbol occurs exactly once in each row and exactly once in each column.

**Example 2.14.** A simple example is given by the following array

\[
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array}
\]

This Latin square of order 3 can be derived from the cyclic group of order 3.

More generally, we have

**Example 2.15.** The multiplication table (Cayley table) of a (quasi-)group on $v$ elements is a Latin square of order $v$.

There are various connections between Latin squares and other types of combinatorial structures (see, e.g., [1]). Exemplarily, we give the following example.

**Example 2.16.** The affine plane of order 3 (see Example 2.2) is equivalent to the two $3 \times 3$ orthogonal Latin squares

\[
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array}
\quad
\begin{array}{ccc}
1 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 2 \\
\end{array}
\]
Combinatorial Design Theory

(Note that two Latin squares of order \( v \) are said to be orthogonal if the \( v^2 \) pairs formed by juxtaposition of the two arrays are all distinct.) More generally, an affine plane, or projective plane, of order \( n \) exists if and only if there are \( n - 1 \) pairwise orthogonal Latin squares of order \( n \).

There is a vast body of research concerning Latin squares. We mention in particular the comprehensive monograph [55] as well as the survey articles in [43] and [12, 124]. Latin squares of small orders are available online [158]; for the number of Latin squares, see sequence A002860 in [190].

For our further purposes, we are interested in a generalization of Latin squares, known as perpendicular arrays.

**Definition 2.3.** A perpendicular array \( PA_\lambda(t,k,v) \) is a \( \lambda \cdot \binom{v}{t} \times k \) array, \( A \), of \( v \) symbols, which satisfies the following properties:

(i) every row of \( A \) contains \( k \) distinct symbols,

(ii) for any \( t \) columns of \( A \), and for any \( t \) distinct symbols, there are precisely \( \lambda \) rows \( r \) of \( A \) such that the \( t \) given symbols all occur in row \( r \) in the given \( t \) columns.

We note that property (i) is implied by (ii), when \( t \geq 2 \).

**Example 2.17.** A Latin square of order \( k \) is a perpendicular array \( PA_1(1,k,k) \). Hence, a \( PA_1(1,k,k) \) exists for all positive integers \( k \).

We prove two helpful assertions on perpendicular arrays.

**Theorem 2.10 (Kramer–Kreher–Rees–Stinson [134, 195]).** For a positive integer \( s \leq t \), let

\[
\binom{k}{t} \geq \binom{k}{s}.
\]

Then a perpendicular array \( PA_\lambda(t,k,v) \) is also a \( PA_\lambda(s,k,v) \) with

\[
\lambda_s = \lambda \frac{\binom{v-s}{t-s}}{\binom{k}{s}}.
\]
Proof. Let $A$ be a $PA_{\lambda}(t,k,v)$, and let the columns be labeled by \{1,\ldots,k\}. Let $S$ be any set of $s$ distinct symbols. For any set $I$ of $s$ columns, define $n(I)$ to be the number of rows of $A$ in which the symbols in $S$ are all contained in the columns in $I$. Then, for any set $J$ of $t$ columns, we obtain the equation

$$\sum_{I \subseteq J, |I| = s} n(I) = \lambda \binom{v-s}{t-s}.$$ 

This gives us $\binom{k}{t}$ linear equations in the $\binom{k}{s}$ unknowns $n(I)$. Now, if we assume that

$$\binom{k}{t} \geq \binom{k}{s},$$

then the system has for each $I$ the unique solution

$$n(I) = \lambda \frac{\binom{v-s}{t-s}}{\binom{t}{s}}.$$

Hence, $A$ is a $PA_{\lambda_s}(s,k,v)$ with $\lambda_s$ as defined above. 

Since each $\lambda_s$ must be an integer, we derive the following necessary arithmetic conditions.

**Corollary 2.11 (Kramer–Kreher–Rees–Stinson [134, 195]).** Let $k \geq 2t - 1$ and suppose that a perpendicular array $PA_{\lambda}(t,k,v)$ exists. Then

$$\lambda \binom{v-s}{t-s} \equiv 0 \pmod{\binom{t}{s}}$$

for each positive integer $s \leq t$.

In the following, we will study several constructions of perpendicular arrays. For $t = 2$, an infinite class can be obtained as follows.

**Example 2.18.** Let $q$ be an odd prime power, and let $a \in GF(q)$ be a primitive element (i.e., a generator of the field’s cyclic multiplicative
Combinatorial Design Theory

For each $0 \leq i \leq \frac{q-3}{2}$ and for each $c \in GF(q)$, we define a row as

$$c \quad c + a^i \quad c + a^{i+1} \quad \cdots \quad c + a^{i+q-2}.$$  

The resulting array is a $PA_1(2,q,q)$. This construction is due to Mullin et al. [162] (see also [195]).

Perpendicular arrays can be obtained in a natural way from multiplying homogeneous permutations groups, by taking the permutations as the rows of an array.

**Theorem 2.12 (Stinson–Teirlinck [202]).** Suppose there is a $t$-homogeneous permutation group $G$ of degree $v$. Then there exists a $PA_\lambda(t,v,v)$ with $\lambda = \frac{|G|}{(v)^t}$.

**Example 2.19.** The group $ASL(1,q)$ is 2-homogeneous of degree $q$, when $q \equiv 3 \pmod{4}$ (cf. Appendix 4.1). Since $|ASL(1,q)| = \frac{q^3-q}{2}$, a $PA_1(2,q,q)$ exists for any prime power $q \equiv 3 \pmod{4}$.

**Example 2.20.** The group $PSL(2,q)$ is 3-homogeneous of degree $q + 1$, when $q \equiv 3 \pmod{4}$ (cf. Appendix 4.1). Note that $|PSL(2,q)| = \frac{q^3-q}{2}$. Hence a $PA_3(3,q+1,q+1)$ exists for any prime power $q \equiv 3 \pmod{4}$.

For $t > 3$, only a finite number of perpendicular arrays are presently known. We summarize in Table 2.1 all perpendicular arrays that arise from finite $t$-homogeneous but not $t$-transitive permutation groups for $t \geq 2$ (cf. [126] and the list of finite multiply homogeneous permutation groups in Appendix 4.1).

Sometimes perpendicular arrays can be constructed from other perpendicular arrays via recursive constructions.
Table 2.1. Perpendicular arrays $PA_\lambda(t,v,v)$ from finite $t$-homogeneous but not $t$-transitive permutation groups $G$, $t \geq 2$.

\[
\begin{array}{cccc}
\lambda & t & v & G \\
1 & 2 & q & ASL(1,q) \\
1 & 3 & 8 & AGL(1,8) \\
1 & 3 & 32 & A\Gamma L(1,32) \\
3 & 3 & q + 1 & PSL(2,q) \\
4 & 4 & 9 & PGL(2,8) \\
4 & 4 & 33 & P\Gamma L(2,32) \\
\end{array}
\]

**Theorem 2.13 (Kramer–Magliveras–van Trung–Wu [135]).** If there is an $PA_\lambda(t,k,k)$ which is also a $PA_{\lambda-1}(t-1,k,k)$, then there is a $PA_{\lambda(k+1-t)}(t,k+1,k+1)$.

Concerning the existence of perpendicular arrays, we state two important and long-standing open problems (cf. [195]):

**Problem 2.2.** Is there an infinite class of a $PA_1(3,k,k)$ with $k \geq 5$? (As necessary condition, $k \equiv 2 \pmod{3}$ must hold by Corollary 2.11.)

**Problem 2.3.** Does there exist any $PA_1(t,k,v)$ with $t \geq 4$?

### 2.3 Authentication Perpendicular Arrays

We introduce a further class of combinatorial designs, known as *authentication perpendicular arrays*. These are natural extensions of perpendicular arrays, which were defined by Stinson and Teirlinck [202] in order to endow secrecy codes with an authentication capacity (cf. Section 3.3).

**Definition 2.4.** An *authentication perpendicular array* $APA_\lambda(t,k,v)$ is a $PA_\lambda(t,k,v)$, $A$, such that, for any $s \leq t - 1$ and for any $s + 1$
distinct symbols \( \{x_i\}_{i=1}^{s+1} \), it holds that among all the rows of \( A \) that contain all the symbols \( \{x_i\}_{i=1}^{s+1} \), the \( s \) symbols \( \{x_i\}_{i=1}^{s} \) occur in all possible subsets of \( s \) columns equally often.

We note that perpendicular arrays and authentication perpendicular arrays may be regarded as generalizations of \( t \)-designs with an additional ordering on the blocks.

We present a simple example (due to van Rees, cf. [194]).

**Example 2.21.** A \( 55 \times 3 \) array \( A \) can be constructed by developing the five rows

\[
\begin{array}{ccc}
0 & 1 & 2 \\
0 & 9 & 7 \\
0 & 3 & 6 \\
0 & 4 & 8 \\
0 & 5 & 10 \\
\end{array}
\]

modulo 11. Every pair \( \{x_1, x_2\} \) occurs in three rows of \( A \). Within these three rows, \( x_1 \) occurs once in each of the three columns, as does \( x_2 \). This gives an \( APA_1(2,3,11) \).

For authentication perpendicular arrays, we have the following assertions.

**Theorem 2.14 (Stinson–Teirlinck [202]).** If \( k \geq 2t - 1 \), then a perpendicular array \( PA_\lambda(t,k,k) \) is an authentication perpendicular array \( APA_\lambda(t,k,k) \).

**Proof.** Let \( A \) be a \( PA_\lambda(t,k,k) \). Then every subset of \( \{1, \ldots, k\} \) appears in all rows of \( A \). Thus, \( A \) is an \( APA_\lambda(t,k,k) \) if and only if \( A \) is a \( PA_{\lambda_s}(s,k,k) \) for all positive integers \( s \leq t \). Hence, by Theorem 2.10, the claim follows. \( \square \)

**Example 2.22.** Each example of the \( PA_\lambda(t,k,k) \) given above is also an example of an \( APA_\lambda(t,k,k) \) (except for \( q = 3 \) in Example 2.20).
Theorem 2.15 (Stinson–Teirlinck [202]). For a positive integer \( s \leq t \), an authentication perpendicular array \( APA_\lambda(t,k,v) \) is also an \( APA_\lambda(s,k,v) \).

Proof. Let \( A \) be an \( APA_\lambda(t,k,v) \). The case \( s = t \) is trivial. Therefore, let us assume that \( s < t \) and that it has already been proven that \( A \) is an \( APA_\lambda(s+1,k,v) \). Let \( S \) denote a set of \( s \) columns of \( A \) and \( \{x_i\}_{i=1}^{s} \) a set of \( s \) distinct symbols. For each symbol \( y \notin \{x_i\}_{i=1}^{s} \), we have \( \lambda_{s+1} \binom{k}{s+1} \) rows containing \( \{y\} \cup \{x_i\}_{i=1}^{s} \). Of these,

\[
\lambda_{s+1} \binom{k}{s+1} \binom{k}{s} \tag{2.2}
\]

will contain \( \{x_i\}_{i=1}^{s} \) in the columns in \( S \). Let \( \lambda_0 \) denote the number of rows containing \( \{x_i\}_{i=1}^{s} \) in the columns in \( S \). We now count triples \((c,x_{s+1},r)\), where \( c \notin S \), \( x_{s+1} \notin \{x_i\}_{i=1}^{s} \), and row \( r \) contains \( \{x_i\}_{i=1}^{s} \) in the columns in \( S \) and \( x_{s+1} \) in column \( c \). It follows

\[
(k - s)\lambda_0 = (v - s)\lambda_{s+1} \binom{k}{s+1} \binom{k}{s},
\]

and hence \( \lambda_0 = \lambda_s \). Therefore, \( A \) is a \( PA_\lambda(s,k,v) \), and hence an \( APA_\lambda(s,k,v) \) in view of Theorem 2.14. \qed

As we can see from Equation (2.2), the following necessary arithmetic conditions must hold.

Corollary 2.16 (Stinson–Teirlinck [202]). Suppose that an authentication perpendicular array \( APA_\lambda(t,k,v) \) exists. Then

\[
\lambda_{s+1} \binom{k}{s+1} \equiv 0 \left( \mod \binom{k}{s} \right)
\]

for each positive integer \( s \leq t - 1 \).

We present an infinite class of authentication perpendicular arrays.
Example 2.23. Let $a \in GF(q)$ be a primitive element, and set $b := a^{q-1}$. For each $1 \leq i \leq \frac{q-1}{2k}$, for each $0 \leq j \leq k - 1$, and for each $c \in GF(q)$, we define a row as

$$c + a^ib^j \quad c + a^ib^{j+1} \quad \cdots \quad c + a^ib^{k-1+j}.$$ 

The resulting array is an APA$_1(2,k,q)$. This construction is due to Granville et al. [85] (see also [195]).

We also mention that there always exists an APA$_1(1,k,v)$ for all positive integers $k \leq v$ (see [195]). There also exists an APA$_1(2,3,v)$ if and only if $v \geq 7$ is odd (see [194]), and an APA$_1(2,5,v)$ if $v \equiv 1$ or 5 (mod 10), $v \geq 11$, $v \neq 15$ (see [145]).

Sometimes it is possible to construct authentication perpendicular arrays by combining different classes of combinatorial designs, as we can see from the following result.

**Theorem 2.17 (Stinson–Teirlinck [202]).** Suppose there is a $t$-$(v,k,\lambda)$ design and an authentication perpendicular array APA$\lambda'(t,k,k)$, then there is an APA$_{\lambda \cdot \lambda'}(t,k,v)$.

**Proof.** We construct an APA$\lambda'(t,k,k)$ for each block in the $t$-$(v,k,\lambda)$ design. The union of these authentication perpendicular arrays yields an APA$_{\lambda \cdot \lambda'}(t,k,v)$. \qed

Example 2.24. Using spherical geometries from Example 2.7, we obtain from Example 2.22 an APA$_3(3,q+1,q^d+1)$ for all prime powers $q \equiv 3$ (mod 4), $q \geq 7$, and all integers $d \geq 2$. Moreover, there is an APA$_1(3,q+1,q^d+1)$ for all integers $d \geq 2$, when $q = 7$ or 31 (cf. [202]).

Further recursive constructions of authentication perpendicular arrays which make use of $t$-designs or other authentication perpendicular arrays have been obtained. We list some of them without proofs.
Theorem 2.18 (van Trung [219]). We have the following:

(a) Suppose there is a $t$-$(v, l, \lambda)$ design and an $APA_\lambda(t, k, l)$, then there is an $APA_{\lambda, \lambda}(t, k, v)$.
(b) If there is an $APA_\lambda(t, k, k)$, then there is an $APA_{\lambda(k+1-t)}(t, k + 1, k + 1)$.
(c) Suppose there is a $t$-$(v, k, \lambda)$ design and an $APA_\lambda(t, k, k)$, then there is an $APA_{\lambda, \lambda(v-k)}(t, k + 1, v)$.

For further constructions (in particular when the underlying set of permutations is not a group) as well as existence tables of known $PA_\lambda(t,k,v)$ resp. $APA_\lambda(t,k,v)$ for small values of $\lambda$ and $t$, we refer the reader to [24, 25, 23, 22, 219].

We close this section by mentioning two long-standing open problems concerning the existence of authentication perpendicular arrays (cf. [202]):

**Problem 2.4.** Does there exist any $APA_1(3, k, v)$ for arbitrarily large values of $k$?

**Problem 2.5.** Is there any $APA_1(t, k, v)$ with $t \geq 4$?

We note that sometimes the transposed orthogonal (perpendicular, authentication perpendicular) array is used.

### 2.4 Splitting Designs and Others

We introduce a new type of combinatorial designs, called *splitting t-designs* (cf. [106]). This extends the notion of a *splitting balanced incomplete block design*, introduced by Ogata et al. [165], to the general case for arbitrary $t$.

**Definition 2.5.** For positive integers $t, v, b, c, u, \lambda$ with $t \leq u$ and $cu \leq v$, a $t$-$(v,b,l = cu, \lambda)$ *splitting design* $D$ is a pair $(X, \mathcal{B})$, which
satisfies the following properties:

(i) $X$ is a set of $v$ elements, called *points*.
(ii) $\mathcal{B}$ is a family of $l$-subsets of $X$, called *blocks*, such that every block $B_i \in \mathcal{B}$ ($1 \leq i \leq b := |\mathcal{B}|$) is expressed as a disjoint union

$$B_i = B_{i,1} \cup \cdots \cup B_{i,u}$$

with $|B_{i,1}| = \cdots = |B_{i,u}| = c$ and $|B_i| = l = cu$,

(iii) every $t$-subset $\{x_m\}_{m=1}^t$ of $X$ is contained in exactly $\lambda$ blocks $B_i = B_{i,1} \cup \cdots \cup B_{i,u}$ such that

$$x_m \in B_{i,j_m} \quad (j_m \text{ between } 1 \text{ and } u)$$

for each $1 \leq m \leq t$, and $j_1, \ldots, j_t$ are mutually distinct.

---

**Example 2.25.** As a simple example, take as point set

$$X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

and as block set

$$\mathcal{B} = \{B_1, \ldots, B_9\}$$

with

$$B_1 = \{\{1,2\}, \{3,5\}\}$$
$$B_2 = \{\{2,3\}, \{4,6\}\}$$
$$B_3 = \{\{3,4\}, \{5,7\}\}$$
$$B_4 = \{\{4,5\}, \{6,8\}\}$$
$$B_5 = \{\{5,6\}, \{7,9\}\}$$
$$B_6 = \{\{6,7\}, \{8,1\}\}$$
$$B_7 = \{\{7,8\}, \{9,2\}\}$$
$$B_8 = \{\{8,9\}, \{1,3\}\}$$
$$B_9 = \{\{9,1\}, \{2,4\}\}.$$

This gives a $2$-(9,9,4 = 2 × 2,1) splitting design (cf. [165]).
Example 2.26. A \(3-(10,15,6=2 \times 3,1)\) splitting design can be obtained by taking as point set

\[ X = \{1,2,3,4,5,6,7,8,9,0\} \]

and as block set

\[ B = \{B_1,\ldots,B_{15}\} \]

with

\[
\begin{align*}
B_1 &= \{\{1,2\}, \{4,0\}, \{5,9\}\} \\
B_2 &= \{\{1,3\}, \{2,8\}, \{5,0\}\} \\
B_3 &= \{\{1,4\}, \{3,8\}, \{6,9\}\} \\
B_4 &= \{\{1,5\}, \{4,7\}, \{6,8\}\} \\
B_5 &= \{\{1,7\}, \{2,3\}, \{4,8\}\} \\
B_6 &= \{\{1,8\}, \{2,5\}, \{6,9\}\} \\
B_7 &= \{\{1,8\}, \{6,7\}, \{9,0\}\} \\
B_8 &= \{\{1,9\}, \{2,5\}, \{3,7\}\} \\
B_9 &= \{\{1,9\}, \{3,4\}, \{7,0\}\} \\
B_{10} &= \{\{2,4\}, \{5,6\}, \{7,9\}\} \\
B_{11} &= \{\{2,5\}, \{4,7\}, \{3,0\}\} \\
B_{12} &= \{\{2,9\}, \{6,8\}, \{3,0\}\} \\
B_{13} &= \{\{2,0\}, \{4,5\}, \{6,8\}\} \\
B_{14} &= \{\{3,7\}, \{4,6\}, \{8,0\}\} \\
B_{15} &= \{\{3,9\}, \{5,7\}, \{6,0\}\}.
\end{align*}
\]

We prove some basic necessary conditions for the existence of splitting designs.

**Theorem 2.19 (Huber [106]).** Suppose that \(\mathcal{D} = (X, B)\) is a \(t-(v,b,l = cu,\lambda)\) splitting design, and for a positive integer \(s \leq t\), let
Combinatorial Design Theory

$S \subseteq X$ with $|S| = s$. Then the number of blocks containing each element of $S$ as per Definition 2.5 is given by

$$\lambda_s = \lambda \frac{(v-s)_{t-s}}{l-s(l-s)}.$$ 

In particular, for $t \geq 2$, a $t$-$(v,b,l = cu,\lambda)$ splitting design is also an $s$-$(v,b,l = cu,\lambda_s)$ splitting design.

Proof. We count in two ways the number of pairs $(T,B_i)$, where $T := \{ x_m \}_{m=1}^t \subseteq X$ and $B_i = \bigcup_{j=1}^u B_{i,j} \in \mathcal{B}$ such that

$$x_m \in B_{i,j_m}$$

for each $1 \leq m \leq t$ with $j_1, \ldots, j_t$ mutually distinct, and $S := \{ \tilde{x}_m \}_{m=1}^s \subseteq T$. First, each of the $\lambda_s$ blocks $B_i = \bigcup_{j=1}^u B_{i,j}$ such that

$$\tilde{x}_m \in B_{i,j_m}$$

for each $1 \leq m \leq s$ with $j_1, \ldots, j_s$ mutually distinct gives

$$\prod_{i=s}^{t-1}(l-ic) \over (t-s)! = c^{t-s} \begin{pmatrix} u-s \\ t-s \end{pmatrix}$$

such pairs. Second, there are

$$\begin{pmatrix} v-s \\ t-s \end{pmatrix}$$

such subsets $T \subseteq X$ with $S \subseteq T$, each giving $\lambda$ pairs by Definition 2.5.

As it is customary for $t$-designs, we also set $r := \lambda_1$ denoting the number of blocks containing a given point. The above elementary counting arguments give the following assertions.

Corollary 2.20 (Huber [106]). Let $\mathcal{D} = (X,\mathcal{B})$ be a $t$-$(v,b,l = cu,\lambda)$ splitting design. Then the following holds:

(a) $bl = vr$. 

2.4 Splitting Designs and Others  621

(b) \( \begin{pmatrix} v \\ t \end{pmatrix} \lambda = bc^t \begin{pmatrix} u \\ t \end{pmatrix} \).

(c) \( r c^{t-1} (u - 1) = \lambda_2 (v - 1) \) for \( t \geq 2 \).

The assertions (b) and (c) have been proved in [165] for the case when \( t = 2 \). Since in Theorem 2.19 each \( \lambda_s \) must be an integer, we obtain furthermore the subsequent necessary arithmetic conditions.

**Corollary 2.21 (Huber [106]).** Let \( D = (X, B) \) be a \( t-(v, b, l = cu, \lambda) \) splitting design. Then

\[
\lambda \begin{pmatrix} v - s \\ t - s \end{pmatrix} \equiv 0 \pmod{c^{t-s} \begin{pmatrix} u - s \\ t - s \end{pmatrix}}
\]

for each positive integer \( s \leq t \).

Ogata et al. [165] proved a Fisher-type inequality for splitting \( t \)-designs when \( t = 2 \). Since a splitting \( t \)-design with \( t \geq 2 \) is also a splitting 2-design in view of Theorem 2.19, we obtain the following theorem.

**Theorem 2.22 (Ogata–Kurosawa–Stinson–Saido–Huber [106, 165]).** If \( D = (X, B) \) is a \( t-(v, b, l = cu, \lambda) \) splitting design with \( t \geq 2 \), then

\[
b \geq \frac{v}{u}.
\]

We shortly mention two further types of combinatorial designs. For more details, we refer to [16, 43, 200].

**Definition 2.6.** An orthogonal array \( OA_{\lambda}(t, k, v) \) is a \( \lambda v^t \times k \) array, \( A \), of \( v \) symbols, such that for any injective \( t \)-tuple \( (x_1, \ldots, x_t) \) of symbols and any \( t \) columns \( c_1, \ldots, c_t \) of \( A \), there are precisely \( \lambda \) rows of \( A \) in which the entry \( x_{i} \) occurs in column \( c_{i} \) for all \( 1 \leq i \leq t \).
Example 2.27. The Latin square given in Example 2.2 can represented by the following orthogonal array \( OA_1(2,3,v) \)

\[
\begin{array}{ccc}
1 & 1 & 1 \\
1 & 2 & 2 \\
1 & 3 & 3 \\
2 & 1 & 2 \\
2 & 2 & 3 \\
2 & 3 & 1 \\
3 & 1 & 3 \\
3 & 2 & 1 \\
3 & 3 & 2 \\
\end{array}
\]

More generally, a Latin square of order \( v \) is equivalent to an \( OA_1(2,3,v) \).

Example 2.28. An \( OA_1(2,q,q) \) can be constructed for any prime power \( q \). The well-known construction is essentially obtained from an affine plane of order \( q \), yielding the property that each of the \( q \) distinct rows contains precisely one symbol \( q \)-times (cf., e.g., [195, 200]).

A comprehensive reference on the theory of orthogonal arrays and their applications is [92]. An electronic library of orthogonal arrays is given in [189].

Definition 2.7. A transversal design \( TD_\lambda(t,k,v) \) is a triple \( (X,G,A) \), which satisfies the following properties:

(i) \( X \) is a set of \( kv \) elements, called points,
(ii) \( G \) is a partition of \( X \) into \( k \) classes, called groups, each of size \( v \),
(iii) \( A \) is a family of \( \lambda v^t \) blocks, each of which meets each group in a point,
(iv) every \( t \)-subset of points from distinct groups is contained in exactly \( \lambda \) blocks.
Example 2.29. A Latin square of order $v$ is equivalent to a $TD_1(2,3,v)$.

Further types of combinatorial designs including difference sets and group divisible designs can be found in [16, 43, 200]. For the reader interested in the broad area of combinatorics in general, we recommend [2, 37, 81, 86, 176, 217].
This section is devoted to various key applications of combinatorial designs to authentication and secrecy codes. Foundational and current results concerning the construction and characterization of authentication and secrecy codes are exposed. Starting with Shannon’s classical result [182] on secrecy systems, we first deal with secrecy codes in Section 3.1. Authentication codes without any secrecy requirements are considered in Section 3.2. In Section 3.3, codes that offer both authenticity and secrecy are discussed in detail. We distinguish between arbitrary and equiprobable source probability distributions. The advantage of the source states being equiprobable distributed is that the number of encoding rules can be reduced. Section 3.4 is devoted to an extended authentication model, where the opponent can act pro-actively by having access to a verification oracle (V-oracle). Authentication codes with splitting are considered in Section 3.5. In such a code, several messages can be used to communicate a particular plaintext (non-deterministic encoding). We briefly mention authentication codes that permit arbitration in Section 3.6. In Section 3.7, further recent applications are highlighted which makes substantial use of combinatorial design theory. Finally, we conclude in Section 3.8 with a synthesis of the work and some directions for future research.
3.1 Secrecy Codes

We first study codes which provide solely secrecy. Recall that the formal definition of perfect (multi-fold) secrecy is given in Subsection 1.1.3. As combinatorial tools, we will make use of Latin squares and perpendicular arrays (cf. Section 2.2).

As a starting point, we state Shannon’s fundamental result, which gives the first link between information-theoretical cryptography and combinatorial designs (see also, e.g., [200] for a proof).

Theorem 3.1 (Shannon [182]). If a secrecy code provides perfect secrecy, then \( b \geq k \), that is, there are at least as many encoding rules as source states. Moreover, equality occurs if and only if the encoding matrix is a Latin square of order \( k \) and the encoding rules are used with equal probability.

Presumably the most prominent example of an information-theoretically secure secrecy code is the One-time Pad of Vernam [221, 222].

Example 3.1. Let \( S = M = E = V(d, 2) \), \( d \geq 1 \). Each encoding rule is used with equal probability \( 1/2^d \). For a given \( u \in V(d, 2) \), we define an encoding rule

\[
e_u(s) := (s_1 + u_1, \ldots, s_d + u_d) \mod 2
\]

as the vector sum modulo 2 of \( u \) and \( s \). A message \( m \) will be decoded analogously. The encoding matrix is a Latin square of order \( 2^d \). Therefore, the One-time Pad has perfect secrecy.

A close connection between secrecy codes and perpendicular arrays has been established by Stinson.

Theorem 3.2 (Stinson [195]). Suppose there is a perpendicular array \( PA_\lambda(t, k, v) \) with \( k \geq 2t - 1 \). Then there is a secrecy code for \( k \) source states, having \( v \) messages and \( \lambda(v^t) \) encoding rules, that provides perfect \( t \)-fold secrecy.
Proof. Let $A$ be a $PA_{\lambda}(t,k,v)$. An encoding rule can be constructed from each row $r$ of $A$ by defining

$$e_r(s) := x_s$$

for each row $r = (x_1,\ldots,x_k)$ and for each source state $1 \leq s \leq k$. Each encoding rule is used with probability $1/(\lambda(v^t))$. It remains to show that perfect $t^*$-fold secrecy can be achieved for every $t^* \leq t$; as $k \geq 2t - 1$ by assumption, we have

$$\binom{k}{t} \geq \binom{k}{t^*}.$$

Thus, $A$ is a $PA_{\lambda^*}(t^*,k,v)$ in view of Theorem 2.10. It follows that any set of $t^*$ messages corresponds equally often to every possible set of $t^*$ source states. We conclude now by showing via Bayes’ Theorem that

$$p_S(S^*|M^*) = \frac{p_M(M^*|S^*) \cdot p_S(S^*)}{p_M(M^*)} = \frac{(\lambda_{t^*}/b) \cdot p_S(S^*)}{\sum_{\{e \in E | M^* \subseteq M(e)\}} p_E(e) \cdot p_S(f_e(M^*))}$$

$$= \frac{(\lambda_{t^*}/b) \cdot p_S(S^*)}{\sum_{\{S \subseteq S | |S| = t^*\}} \sum_{\{e \in E | S = f_e(M^*)\}} (1/b) \cdot p_S(S)}$$

$$= \frac{(\lambda_{t^*}/b) \cdot p_S(S^*)}{p_S(S^*)}$$

for every set $M^*$ of $t^*$ messages observed in the channel, and for every set $S^*$ of $t^*$ source states.

The condition $k \geq 2t - 1$ is necessary as demonstrated by the following example (cf. [195]).

Example 3.2. The array

$$\begin{array}{cccc}
1 & 2 & 3 & 4 \\
2 & 1 & 4 & 3 \\
3 & 4 & 1 & 2 \\
4 & 3 & 2 & 1
\end{array}$$
3.1 Secrecy Codes

is a \( PA_1(1,4,4) \) as well as a \( PA_1(3,4,4) \). However, it is not a \( PA_\lambda(2,4,4) \) for any \( \lambda \). Thus, perfect one-fold secrecy is achieved, but not perfect two-fold secrecy.

The next theorem generalizes Shannon’s result (Theorem 3.1). It also gives a partial converse to Theorem 3.2.

**Theorem 3.3 (Godlewski–Mitchell–Stinson [75, 195]).** If a secrecy code provides perfect \( t \)-fold secrecy and \( k \geq 2t - 1 \), then

\[
b \geq \binom{k}{t}.
\]

Moreover, equality occurs if and only if the encoding matrix is a perpendicular array \( PA_1(t,k,k) \) and the encoding rules are used with equal probability.

**Proof.** For an arbitrary encoding rule \( e_1 \in \mathcal{E} \), let \( M^* \subseteq M(e_1) \) with \( |M^*| = t \). Let \( S^* \subseteq S \) with \( |S^*| = t \). We first prove that the lower bound on the number of encoding rules holds if a secrecy code achieves perfect \( t \)-fold secrecy. We assume that there is no encoding rule \( e_2 \in \mathcal{E} \) such that \( S^* = f_{e_2}(M^*) \). It follows that \( p_S(S^*|M^*) = 0 \neq p_S(S^*) \), and thus perfect \( t \)-fold secrecy cannot hold by definition. Therefore, there are at least \( \binom{k}{t} \) encoding rules under which all the messages in \( M^* \) are valid. This establishes the bound

\[
b \geq \binom{k}{t}.
\]

For the second part of the theorem, observe that for secrecy codes constructed from a \( PA_\lambda(t,k,v) \) with \( k \geq 2t - 1 \) via Theorem 3.2 this bound is attained if and only if \( \lambda = 1 \) and \( k = v \). To prove the other direction, recall from above that there is at least one encoding rule \( e_2 \in \mathcal{E} \) such that \( S^* = f_{e_2}(M^*) \). Hence, for the bound on the number of encoding rules to be met with equality, there must be exactly one such encoding rule. This implies that all the messages in \( M^* \) are valid under all \( b = \binom{k}{t} \) encoding rules. Clearly, we have \( \binom{k}{t} \) different \( t \)-subsets of messages which are contained in \( M(e_1) \), and each of
these occurs in $\binom{k}{t}$ encoding rules. On the other hand, each of the $\binom{k}{t}$ encoding rules contains $\binom{k}{t}$ different $t$-subsets of messages. Therefore, $M(e_1) = M(e)$ must hold for every encoding rule $e \in \mathcal{E}$. Furthermore, the encoding matrix is a perpendicular array $PA_1(t, k, k)$ of the symbols in $M(e_1)$.

A secrecy code is called \textit{optimal} if the number of encoding rules meets the lower bound with equality. As an example, the One-time Pad (Example 3.1) is an optimal secrecy codes providing perfect one-fold secrecy. Relying on Theorem 3.2, we can give in the following further constructions of optimal secrecy codes with perfect multi-fold secrecy:

As noted in Example 2.17, a $PA_1(1, k, k)$ exists for all positive integers $k$. Hence, we have

\begin{theorem}[Stinson \cite{195}] For all positive integers $k$, there is an optimal secrecy code for $k$ source states that achieves perfect one-fold secrecy.
\end{theorem}

In view of Example 2.18, we obtain

\begin{theorem}[Stinson \cite{195}] For all odd prime powers $q$, there is an optimal secrecy code for $q$ source states that achieves perfect two-fold secrecy.
\end{theorem}

From Table 2.1, we have

\begin{theorem}[Stinson \cite{195}] For $v = 8$ and $32$, there is an optimal secrecy code for $v$ source states that achieves perfect three-fold secrecy. For $v = 9$ and $33$, there is an optimal secrecy code for $v$ source states that achieves perfect four-fold secrecy.
\end{theorem}

We remark that with respect to optimal secrecy codes, no infinite class having perfect $t$-fold secrecy is known for $t = 3$, and no example for $t > 3$ (cf. Section 2.2).
3.2 General Authentication Codes

For general authentication codes, no secrecy requirements are specified. The following theorem gives a combinatorial lower bound on the number of encoding rules for multi-fold secure authentication codes.

**Theorem 3.7 (Massey–Schöbi [152, 181]).** If an authentication code is \((t - 1)\)-fold secure against spoofing, then the number of encoding rules is bounded below by

\[
b \geq \binom{v}{t} \binom{k}{t}.
\]

**Proof.** Let \(M^* \subseteq M\) be a set of \(i \leq t - 1\) distinct messages that are valid under a particular encoding rule. Let \(x \in M\) be any message not in \(M^*\). We assume that there is no encoding rule \(e \in \mathcal{E}\) under which all messages in \(M^* \cup \{x\}\) are valid. Following the proof of Theorem 1.1, mutatis mutandis, yields

\[
P_{d_i} > (k - i)/(v - i),
\]

a contradiction. Therefore, any set of \(t\) distinct messages is valid under at least one encoding rule. Now, the bound follows by counting in two ways the number of pairs \((e, M^*)\), where \(e \in \mathcal{E}\) and \(M^* \subseteq M\) with \(|M^*| = t\): first choosing \(e\) and then \(M^*\), gives \(b \binom{k}{t}\) such pairs. On the other hand, there are \(\binom{v}{t}\) subsets \(M^* \subseteq M\), each giving at least one pair by the above observation.

An authentication code is called *optimal* if the number of encoding rules meets the lower bound with equality.

When the source states are known to be independent and equiprobable, optimal authentication codes which are \((t - 1)\)-fold secure against spoofing can be constructed via \(t\)-designs.

**Theorem 3.8 (De Soete–Schöbi–Stinson [52, 181, 195]).** Suppose there is a \(t-(v,k,\lambda)\) design. Then there is an authentication code
for $k$ equiprobable source states, having $v$ messages and $\lambda \cdot \binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t - 1)$-fold secure against spoofing. Conversely, if there is an authentication code for $k$ equiprobable source states, having $v$ messages and $\binom{v}{t}/\binom{k}{t}$ encoding rules, that is $(t - 1)$-fold secure against spoofing, then there is a Steiner $t$-$(v,k,1)$ design.

Proof. Let $\mathcal{D} = (X,\mathcal{B})$ be a $t$-$(v,k,\lambda)$ design. We order each block $B \in \mathcal{B}$ arbitrarily, and take these ordered blocks as encoding rules. We prove first that $P_{d_{t-1}} = (k - t + 1)/(v - t + 1)$: Let $\{m_i\}_{i=1}^{t-1}$ be a set of distinct messages. We suppose that an opponent observes the $t - 1$ messages $\{m_i\}_{i=1}^{t-1}$ in the channel, and then sends the message $m_t$. The probability payoff($m_t,\{m_i\}_{i=1}^{t-1}$) that the message $m_t$ is accepted by the receiver as authentic is

$$\text{payoff}(m_t,\{m_i\}_{i=1}^{t-1}) = \frac{\sum_{e \in E(\{m_i\}_{i=1}^{t-1})} p(e) \cdot p(\{s_i\}_{i=1}^{t-1} = f_e(\{m_i\}_{i=1}^{t-1}))}{\sum_{e \in E(\{m_i\}_{i=1}^{t-1})} p(e) \cdot p(\{s_i\}_{i=1}^{t-1} = f_e(\{m_i\}_{i=1}^{t-1}))}.$$ 

Since $p(e)$ is constant and the source states are known to be equiprobable, it follows that

$$\text{payoff}(m_t,\{m_i\}_{i=1}^{t-1}) = \frac{|\{e \in E(\{m_i\}_{i=1}^{t-1})\}|}{|\{e \in E(\{m_i\}_{i=1}^{t-1})\}|} = \frac{k - t + 1}{v - t + 1},$$

as desired. To establish that $P_{d_i} = (k - i)/(v - i)$ for all $0 \leq i \leq t - 2$, we make use of the fact that a $t$-$(v,k,\lambda)$ design with $t \geq 2$ is also an $t^*$-$(v,k,\lambda_{t^*})$ design for every $t^* \leq t$ in view of Theorem 2.1.

Conversely, in order to meet the lower bound in Theorem 3.7 with equality, every set of $t$ distinct messages must be valid under precisely one encoding rule.

### 3.3 Authentication Codes with Secrecy

We study now codes that offer both authenticity and secrecy. For authentication codes without secrecy, there exist numerous constructions for quite some time. Combinatorial constructions (see, e.g., [79, 170, 196, 197, 201]) rely on configurations including orthogonal arrays and transversal designs (cf. Section 2.4). However, if we wish that the authentication codes simultaneously provide for secrecy, then only a
few constructions have been known until recently. These constructions are primarily of combinatorial nature. An algebraic approach by Ding et al. [60, 59] is based on (non-)linear functions between finite Abelian groups.

We will distinguish between equiprobable and arbitrary source probability distributions. The advantage of the source states being equiprobable distributed is that the number of encoding rules can be reduced.

3.3.1 Equiprobable source probability distribution

In the first part, we assume that the source states are equiprobable distributed. Our approach relies on various \( t \)-designs and finite geometries (cf. Section 2.1).

As a consequence of Equation (1.1), we obtain the following useful observation.

Lemma 3.9 (Stinson [201]). An authentication code has perfect secrecy if and only if

\[
\sum_{\{e \in \mathcal{E} | s(e) = m\}} p_e(e) = \sum_{\{e \in \mathcal{E} | m \in \mathcal{M}(e)\}} p_e(e) \cdot p_s(e^{-1}(m))
\]

for every source state \( s \in \mathcal{S} \) and every message \( m \in \mathcal{M} \).

Thus, if the encoding rules in a code are used with equal probability, then a given message \( m \) occurs with the same frequency in each column of the encoding matrix.

The first optimal authentication codes that are one-fold secure against spoofing and simultaneously achieve perfect secrecy were constructed by Stinson in 1990. The constructions rely on Steiner 2-designs and assume that the source states are equiprobably distributed.

Theorem 3.10 (Stinson [195]). Suppose there is a Steiner \( 2-(v,k,1) \) design, where \( v \) divides the number of blocks \( b \). Then there is an optimal authentication code for \( k \) equiprobable source states, having \( v \) messages and \( v(v - 1)/k(k - 1) \) encoding rules, that is one-fold secure against spoofing and provides perfect secrecy.
We will give a proof of the more general case for arbitrary $t$ in Theorem 3.12.

Relying on Steiner $2-(\frac{q^{d+1}-1}{q-1}, q+1, 1)$ designs from projective geometries (cf. Example 2.3), an infinite class of authentication and secrecy codes can be constructed as follows.

**Theorem 3.11 (Stinson [195]).** For all prime powers $q$ and for all even integers $d \geq 2$, there is an optimal authentication code for an equiprobable source probability distribution with $q + 1$ source states, having $(q^{d+1} - 1)/(q - 1)$ messages, that is one-fold secure against spoofing and provides perfect secrecy.

We give the smallest example (cf. [195]).

**Example 3.3.** An optimal authentication code for $k = 3$ equiprobable source states, having $v = 7$ messages, and $b = 7$ encoding rules, that is one-fold secure against spoofing and provides perfect secrecy can be constructed from a Steiner $2-(7, 3, 1)$ design, i.e. the unique Fano plane (cf. Example 2.1). Each encoding rule is used with probability $1/7$. An encoding matrix is given in Table 3.1.

Theorem 3.10 have been extended recently. Optimal multi-fold secure authentication codes which simultaneously achieve perfect secrecy can be obtained by means of Steiner $t$-designs for larger $t$.

| Table 3.1. Authentication code from the Fano plane. |
|---------|-----|-----|
| $s_1$  | $s_2$ | $s_3$ |
| $e_1$  | 1    | 2    | 4    |
| $e_2$  | 2    | 3    | 5    |
| $e_3$  | 3    | 4    | 6    |
| $e_4$  | 4    | 5    | 7    |
| $e_5$  | 5    | 6    | 1    |
| $e_6$  | 6    | 7    | 2    |
| $e_7$  | 7    | 1    | 3    |
**Theorem 3.12 (Huber [102]).** Suppose there is a Steiner $t$-$(v,k,1)$ design with $t \geq 2$, where $v$ divides the number of blocks $b$. Then there is an optimal authentication code for $k$ equiprobable source states, having $v$ messages and $\binom{v}{t} / \binom{k}{t}$ encoding rules, that is $(t - 1)$-fold secure against spoofing and provides perfect secrecy.

*Proof.* Let $\mathcal{D} = (X, B)$ be a Steiner $t$-$(v,k,1)$ design with $t \geq 2$, where $v$ divides $b$. Clearly, the authentication capacity of the code follows via Theorem 3.8. To establish perfect secrecy under the assumption that the encoding rules are used with equal probability, it is necessary in view of Lemma 3.9 that a given message occurs with the same frequency in each column of the resulting encoding matrix. This can be done by ordering every block of $\mathcal{D}$ in such a way that every point occurs in each possible position in precisely $b/v$ blocks. Since every point occurs in exactly $r = \binom{v-1}{t-1} / \binom{k-1}{t-1}$ blocks due to Corollary 2.2 (c), necessarily $k$ must divide $r$, or equivalently, $v$ divides $b$ by Corollary 2.2 (b). To show that the condition is also sufficient, we consider the bipartite point-block incidence graph of $\mathcal{D}$ with vertex set $X \cup B$, where $(x, B)$ is an edge if and only if $x \in B$ for $x \in X$ and $B \in B$. An ordering on each block of $\mathcal{D}$ can be obtained via an edge-coloring of this graph using $k$ colors in such a way that each vertex $B \in B$ is adjacent to one edge of each color, and each vertex $x \in X$ is adjacent to $b/v$ edges of each color. Technically, this can be achieved by first splitting up each vertex $x$ into $b/v$ copies, each having degree $k$, and then by finding an appropriate edge-coloring of the resulting $k$-regular bipartite graph using $k$ colors. Taking the ordered blocks as encoding rules, each used with equal probability, establishes the claim. \[\square\]

Relying on spherical geometries from Example 2.7, we can construct a new infinite class of optimal codes which are two-fold secure against spoofing and achieve perfect secrecy.

**Theorem 3.13 (Huber [102]).** For all prime powers $q$ and for all even integers $d \geq 2$, there is an optimal authentication code for an equiprobable source probability distribution with $q + 1$ source states,
Applications to Authentication and Secrecy Codes

having \( q^d + 1 \) messages, that is two-fold secure against spoofing and provides perfect secrecy.

\[ q^2 - 1 \mid q^d - 1 \]

and hence

\[ (q + 1)(q - 1) \mid q^d(q^d - 1). \]

Therefore, \( v \) divides \( b \), and the claim follows by applying Theorem 3.12.

We present the smallest example (cf. [102]).

**Example 3.4.** An optimal authentication code for \( k = 4 \) equiprobable source states, having \( v = 10 \) messages, and \( b = 30 \) encoding rules, that is two-fold secure against spoofing and provides perfect secrecy can be constructed from a Steiner 3-(10, 4, 1) design, i.e. the unique Möbius plane of order 3 (cf. Example 2.7). Each encoding rule is used with probability \( 1/30 \). We give an encoding matrix in Table 3.2.

We can construct several further new optimal authentication codes for equiprobable source distributions, which are \( (t - 1) \)-fold secure against spoofing and simultaneously achieve perfect secrecy:

By Theorem 3.12, we have to examine whether the parameters of known Steiner \( t-(v,k,1) \) designs satisfy the condition that \( v \) divides the number of blocks \( b = \binom{v}{t}/\binom{k}{t} \). We recall that there are two infinite classes of optimal authentication codes, one arises from projective geometries (Theorem 3.11) and the other from spherical geometries (Theorem 3.13). In view of Example 2.10, further infinite classes of optimal codes for a fixed number of source states can be constructed as follows (cf. [102]).

- A Steiner 2-(\( v, 3, 1 \)) design exists if and only if \( v \equiv 1 \) or \( 3 \) (mod 6). Hence, if \( v \equiv 1 \) (mod 6), then an optimal authentication
3.3 Authentication Codes with Secrecy

Table 3.2. Authentication code from the Möbius plane of order 3.

<table>
<thead>
<tr>
<th></th>
<th>$s_1$</th>
<th>$s_2$</th>
<th>$s_3$</th>
<th>$s_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$e_1$</td>
<td>1</td>
<td>2</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>$e_2$</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>$e_3$</td>
<td>3</td>
<td>4</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>$e_4$</td>
<td>4</td>
<td>5</td>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>$e_5$</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>$e_6$</td>
<td>6</td>
<td>7</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>$e_7$</td>
<td>7</td>
<td>8</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$e_8$</td>
<td>8</td>
<td>9</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$e_9$</td>
<td>9</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>$e_{10}$</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>$e_{11}$</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>$e_{12}$</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>$e_{13}$</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>9</td>
</tr>
<tr>
<td>$e_{14}$</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>$e_{15}$</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>$e_{16}$</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>$e_{17}$</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>3</td>
</tr>
<tr>
<td>$e_{18}$</td>
<td>8</td>
<td>9</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>$e_{19}$</td>
<td>9</td>
<td>0</td>
<td>1</td>
<td>5</td>
</tr>
<tr>
<td>$e_{20}$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>6</td>
</tr>
<tr>
<td>$e_{21}$</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>8</td>
</tr>
<tr>
<td>$e_{22}$</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>$e_{23}$</td>
<td>3</td>
<td>5</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td>$e_{24}$</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>1</td>
</tr>
<tr>
<td>$e_{25}$</td>
<td>5</td>
<td>7</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>$e_{26}$</td>
<td>6</td>
<td>8</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>$e_{27}$</td>
<td>7</td>
<td>9</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>$e_{28}$</td>
<td>8</td>
<td>0</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>$e_{29}$</td>
<td>9</td>
<td>1</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>$e_{30}$</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>7</td>
</tr>
</tbody>
</table>

code can be constructed for $k = 3$ equiprobable source states, having $v$ messages, and $v(v - 1)/6$ encoding rules, that is one-fold secure against spoofing and provides perfect secrecy.
• A Steiner 2-(v,4,1) design exists if and only if \( v \equiv 1 \) or 4 (mod 12). Hence, if \( v \equiv 1 \) (mod 12), then an optimal authentication code can be constructed for \( k = 4 \) equiprobable source states, having \( v \) messages, and \( v(v-1)/12 \) encoding rules, that is one-fold secure against spoofing and provides perfect secrecy.

• A Steiner 2-(v,5,1) design exists if and only if \( v \equiv 1 \) or 5 (mod 20). Hence, if \( v \equiv 1 \) (mod 20), then an optimal authentication code can be constructed for \( k = 5 \) equiprobable source states, having \( v \) messages, and \( v(v-1)/20 \) encoding rules, that is one-fold secure against spoofing and provides perfect secrecy.

• A Steiner 3-(v,4,1) design exists if and only if \( v \equiv 2 \) or 4 (mod 6). Hence, if \( v \equiv 2 \) or 10 (mod 24), then an optimal authentication code can be constructed for \( k = 4 \) equiprobable source states, having \( v \) messages, and \( v(v-1)/(v-2) \) encoding rules, that is two-fold secure against spoofing and provides perfect secrecy.

We summarize in Table 3.3 the infinite classes of optimal codes constructed in this subsection. Moreover, we present further optimal codes with these properties in Table 3.4. Here, all presently known Steiner 4-designs and 5-designs have been examined; for Steiner 2-designs and 3-designs only the cases up to \( v = 30 \) have been investigated (cf. [102]).

We give the parameters of the codes as well as of the respective Steiner

<table>
<thead>
<tr>
<th>( t_A )</th>
<th>( t_S )</th>
<th>( k )</th>
<th>( v )</th>
<th>( b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{k(k-1)} )</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{6} )</td>
</tr>
<tr>
<td>1</td>
<td>4</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{12} )</td>
</tr>
<tr>
<td>1</td>
<td>5</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{20} )</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( t_A )</th>
<th>( t_S )</th>
<th>( k )</th>
<th>( v )</th>
<th>( b )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{k(k-1)(k-2)} )</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>( q + 1 )</td>
<td>( \frac{q^d + 1}{q-1} )</td>
<td>( \frac{v(v-1)}{24} )</td>
</tr>
</tbody>
</table>
### 3.3 Authentication Codes with Secrecy

<table>
<thead>
<tr>
<th>$t_A$</th>
<th>$t_S$</th>
<th>$k$</th>
<th>$v$</th>
<th>$b$</th>
<th>Design parameters</th>
<th>Design ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>5</td>
<td>26</td>
<td>260</td>
<td>3-$(26,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>5</td>
<td>11</td>
<td>66</td>
<td>4-$(11,5,1)$</td>
<td>Ex. 2.8</td>
</tr>
<tr>
<td>7</td>
<td>23</td>
<td>253</td>
<td></td>
<td></td>
<td>4-$(23,7,1)$</td>
<td>Ex. 2.8</td>
</tr>
<tr>
<td>5</td>
<td>23</td>
<td>1,771</td>
<td></td>
<td></td>
<td>4-$(23,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>47</td>
<td>35,673</td>
<td></td>
<td></td>
<td>4-$(47,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>83</td>
<td>367,524</td>
<td></td>
<td></td>
<td>4-$(83,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>71</td>
<td>194,327</td>
<td></td>
<td></td>
<td>4-$(71,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>107</td>
<td>1,032,122</td>
<td></td>
<td></td>
<td>4-$(107,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>131</td>
<td>2,343,328</td>
<td></td>
<td></td>
<td>4-$(131,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>167</td>
<td>6,251,311</td>
<td></td>
<td></td>
<td>4-$(167,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>5</td>
<td>243</td>
<td>28,344,492</td>
<td></td>
<td></td>
<td>4-$(243,5,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>6</td>
<td>12</td>
<td>132</td>
<td>5-$(12,6,1)$</td>
<td>Ex. 2.8</td>
</tr>
<tr>
<td>6</td>
<td>84</td>
<td>5,145,336</td>
<td></td>
<td></td>
<td>5-$(84,6,1)$</td>
<td>Ex. 2.9</td>
</tr>
<tr>
<td>6</td>
<td>244</td>
<td>1,152,676,008</td>
<td></td>
<td></td>
<td>5-$(244,6,1)$</td>
<td>Ex. 2.9</td>
</tr>
</tbody>
</table>

$t$-designs (cf. Section 2.1). Both tables lists all presently known optimal authentication codes with perfect secrecy.

We consider now authentication codes that are $(t-1)$-fold secure against spoofing and achieves perfect $(t-1)$-fold secrecy:

Starting from the condition of perfect $t$-fold secrecy, we obtain via Bayes’ Theorem that

$$p_S(S^*|M^*) = \frac{p_M(M^*|S^*) \cdot p_S(S^*)}{p_M(M^*)}$$

$$= \frac{\sum_{e \in E|S^* = f_e(M^*)} P_E(e) \cdot p_S(S^*)}{\sum_{e \in E|M^* \subseteq M(e)} P_E(e) \cdot p_S(f_e(M^*))}$$

This yields

**Lemma 3.14 (Huber [107]).** An authentication code has perfect $t$-fold secrecy if and only if, for every positive integer $t^* \leq t$, for every set $M^*$ of $t^*$ messages observed in the channel and for every set $S^*$ of $t^*$
source states, we have

$$
\sum_{\{e \in E | S^* = f_e(M^*)\}} p_E(e) = \sum_{\{e \in E | M^* \subseteq M(e)\}} p_E(e) \cdot p_S(f_e(M^*)).
$$

Hence, if the encoding rules in a code are used with equal probability, then for every \(t^* \leq t\), a given set of \(t^*\) messages occurs with the same frequency in each \(t^*\) columns of the encoding matrix.

We can now establish an extension of Theorem 3.12. Our construction yields optimal authentication codes which are multi-fold secure against spoofing and provide perfect multi-fold secrecy.

**Theorem 3.15 (Huber [107]).** Suppose there is a Steiner \(t-(v,k,1)\) design with \(t \geq 2\), where \(\binom{v}{t^*}\) divides the number of blocks \(b\) for every positive integer \(t^* \leq t - 1\). Then there is an optimal authentication code for \(k\) equiprobable source states, having \(v\) messages and \(\binom{v}{t^*}/\binom{k}{t^*}\) encoding rules, that is \((t-1)\)-fold secure against spoofing and provides perfect \((t-1)\)-fold secrecy.

**Proof.** Let \(\mathcal{D} = (X, B)\) be a Steiner \(t-(v,k,1)\) design with \(t \geq 2\), where \(\binom{v}{t^*}\) divides \(b\) for every positive integer \(t^* \leq t - 1\). By Theorem 3.8, the authentication code has \((t-1)\)-fold security against spoofing attacks. Hence, it remains to prove that the code also achieves perfect \((t-1)\)-fold secrecy under the assumption that the encoding rules are used with equal probability. With respect to Lemma 3.14, we have to show that, for every \(t^* \leq t - 1\), a given set of \(t^*\) messages occurs with the same frequency in each \(t^*\) columns of the resulting encoding matrix. This can be accomplished by ordering, for each \(t^* \leq t - 1\), every block of \(\mathcal{D}\) in such a way that every \(t^*\)-subset of \(X\) occurs in each possible choice in precisely \(b/\binom{v}{t^*}\) blocks. Since every \(t^*\)-subset of \(X\) occurs in exactly \(\lambda_t = \binom{v-t^*}{t-t^*}/\binom{k-t^*}{t-t^*}\) blocks due to Theorem 2.1, necessarily \(\binom{k}{t^*}\) must divide \(\lambda_t\). By Corollary 2.2 (b), this is equivalent to saying that \(\binom{v}{t^*}\) divides \(b\). To show that the condition is also sufficient, we consider the bipartite \((t^*\)-subset, block) incidence graph of \(\mathcal{D}\) with vertex set \(\binom{X}{t^*} \cup B\), where \(\{x_i\}_{i=1}^{t^*}, B\) is an edge if and only if \(x_i \in B\) \((1 \leq i \leq t^*)\) for \(\{x_i\}_{i=1}^{t^*} \in \binom{X}{t^*}\) and \(B \in B\). An ordering on each block of \(\mathcal{D}\) can be
3.3 Authentication Codes with Secrecy

obtained via an edge-coloring of this graph using \( \binom{k}{t} \) colors in such a way that each vertex \( B \in \mathcal{B} \) is adjacent to one edge of each color, and each vertex \( \{x_i\}_{i=1}^{t^*} \in \binom{X}{t^*} \) is adjacent to \( b/\binom{v}{t^*} \) edges of each color. Specifically, this can be done by first splitting up each vertex \( \{x_i\}_{i=1}^{t^*} \) into \( b/\binom{v}{t^*} \) copies, each having degree \( \binom{k}{t^*} \), and then by finding an appropriate edge-coloring of the resulting \( \binom{k}{t^*} \)-regular bipartite graph using \( \binom{k}{t} \) colors. The claim follows now by taking the ordered blocks as encoding rules, each used with equal probability.

\[ \square \]

Remark 3.1. It follows from the proof that we may obtain optimal authentication codes that provide \((t - 1)\)-fold security against spoofing and at the same time perfect \((t' - 1)\)-fold secrecy for \( t' \leq t \), when the assumption of the above theorem holds with \( \binom{v}{t^*} \) divides \( b \) for every positive integer \( t^* \leq t' - 1 \).

As an application, we give an infinite class of optimal codes which are two-fold secure against spoofing and achieve perfect two-fold secrecy. This appears to be the first infinite class of authentication and secrecy codes with these properties.

Theorem 3.16 (Huber [107]). For all positive integers \( v \equiv 2 \pmod{24} \), there is an optimal authentication code for \( k = 4 \) equiprobable source states, having \( v \) messages, and \( v(v - 1)(v - 2)/24 \) encoding rules, that is two-fold secure against spoofing and provides perfect two-fold secrecy.

Proof. By Example 2.10, a Steiner quadruple system \( \text{SQS}(v) \) exists if and only if \( v \equiv 2 \) or \( 4 \pmod{6} \) \((v \geq 4)\). Hence, the condition \( v \mid b \) is fulfilled when \( v \equiv 2 \) or \( 10 \pmod{24} \) and the condition \( \binom{v}{2} \mid b \) when \( v \equiv 2 \pmod{12} \) in view of Corollary 2.2 (b). Therefore, if we assume that \( v \equiv 2 \pmod{24} \), then we can apply Theorem 3.15 to establish the claim.

\[ \square \]

We present the smallest example (cf. [107]).
Example 3.5. An optimal authentication code for $k = 4$ equiprobable source states, having $v = 26$ messages, and $b = 650$ encoding rules, that is two-fold secure against spoofing and provides perfect two-fold secrecy can be constructed from a Steiner quadruple system SQS(26). Each encoding rule is used with probability $1/650$.

Historical Note. The first SQS($v$) for $v = 26$ was constructed by Fitting [67], admitting a $v$-cycle as an automorphism (a cyclic SQS($v$)).

3.3.2 Arbitrary Source Probability Distribution

In this part, let us assume that we have arbitrary source probability distributions. As combinatorial tools, we will use primarily authentication perpendicular arrays (cf. Section 2.3).

We first consider authentication codes that are $(t - 1)$-fold secure against spoofing and simultaneously achieves perfect $t$-fold secrecy:

For these codes, a combinatorial lower bound on the number of encoding rules can be given as follows.

Theorem 3.17 (Stinson [194]). If an authentication code is $(t - 1)$-fold secure against spoofing and provides perfect $t$-fold secrecy, then the number of encoding rules is bounded below by

$$b \geq \binom{v}{t}.$$ 

Proof. Assuming that the authentication code is $(t - 1)$-fold secure against spoofing, we may establish analogously as in the proof of Theorem 3.7 that any set of $t$ distinct messages is valid under at least one encoding rule. Under the further assumption that the code provides perfect $t$-fold secrecy, we obtain as in the proof of the bound in Theorem 3.3 that any such set of $t$ distinct messages must be valid under at least $\binom{t}{1}$ encoding rules. Now, counting pairs analogously as in the proof of Theorem 3.7 establishes the claim.

We call such a code optimal if the number of encoding rules meets the lower bound with equality.
Theorem 3.18 (Stinson–Teirlinck [202]). Suppose there is an authentication perpendicular array \( APA_\lambda(t,k,v) \). Then there is an authentication code for \( k \) source states, having \( v \) messages and \( \lambda \cdot \binom{v}{t} \) encoding rules, that is \((t - 1)\)-fold secure against spoofing and achieves perfect \( t \)-fold secrecy. Moreover, the code is optimal if and only if \( \lambda = 1 \).

Proof. Let \( A \) be an \( APA_\lambda(t,k,v) \). We construct the code as in Theorem 3.2, which gives immediately the desired secrecy capacity. To establish that the code is also \((t - 1)\)-fold secure against spoofing, we have to prove that \( P_{d_i} = (k - i)/(v - i) \) for all \( 0 \leq i \leq t - 1 \). Let \( \{m_i\}_{i=1}^{t*+1} \) be a set of distinct messages \( 0 \leq t^* \leq t - 1 \). We assume that an opponent observes the \( t^* \) messages \( \{m_i\}_{i=1}^{t^*} \) in the channel, and then sends the message \( m_{t^*+1} \). The probability payoff\((m_{t^*+1}, \{m_i\}_{i=1}^{t*})\) that the message \( m_{t^*+1} \) is accepted by the receiver as authentic is

\[
\text{payoff}(m_{t^*+1}, \{m_i\}_{i=1}^{t*}) = \frac{\sum_{e \in E(\{m_i\}_{i=1}^{t^*+1})} p(e) \cdot p(\{s_i\}_{i=1}^{t*} = f_e(\{m_i\}_{i=1}^{t}))}{\sum_{e \in E(\{m_i\}_{i=1}^{t^*})} p(e) \cdot p(\{s_i\}_{i=1}^{t^*} = f_e(\{m_i\}_{i=1}^{t}))}
\]

and as \( p(e) \) is constant, it follows that

\[
\text{payoff}(m_{t^*+1}, \{m_i\}_{i=1}^{t^*}) = \frac{\lambda_{t^*+1} \binom{k}{t^*+1}}{\lambda_{t^*} \binom{k}{t^*}}.
\]

As \( \frac{\lambda_{t^*+1}}{\lambda_{t^*}} = \frac{t^*+1}{v-t^*} \) due to Theorem 2.10, we obtain

\[
\text{payoff}(m_{t^*+1}, \{m_i\}_{i=1}^{t^*}) = \frac{(t^*+1) \binom{k}{t^*+1}}{(v-t^*) \binom{k}{t^*}} = \frac{k - t^*}{v - t^*}.
\]

So, we have \( P_{d_i} = (k - i)/(v - i) \) for all \( 0 \leq i \leq t - 1 \), as desired. Obviously, optimality holds if and only if \( \lambda = 1 \) in view of Theorem 3.17, completing the proof.

In view of Examples 2.23 and 2.24, we hence obtain the subsequent results.
Theorem 3.19 (Stinson–Teirlinck [202]). The following holds:

(a) For all odd positive integers $k$ and all prime powers $q \equiv 1 \pmod{2k}$, there is an optimal authentication code with $k$ source states and $q$ messages, that is one-fold secure against spoofing and provides perfect two-fold secrecy.

(b) For all prime powers $q \equiv 3 \pmod{4}$ ($q \geq 7$) and all integers $d \geq 2$, there is a (non-optimal) authentication code for $q + 1$ source states, having $q^d + 1$ messages and $\frac{(d-1)q^d}{2}$ encoding rules, that is two-fold secure against spoofing and provides perfect three-fold secrecy. Furthermore, there is an optimal code for $q + 1$ source states and $q^d + 1$ messages achieving these capacities, when $q = 7$ or 31.

Further authentication codes with these properties can be constructed from the other examples of authentication perpendicular arrays given in Section 2.3.

We state without proof the following result, which gives a partial converse to Theorem 3.18.

Theorem 3.20 (Stinson [195]). Suppose there is an authentication code for $k$ source states, having $v$ messages and $\binom{v}{t}$ encoding rules, that is $(t-1)$-fold secure against spoofing and achieves perfect $t$-fold secrecy, and $k \geq 2t - 1$. Then there exists an authentication perpendicular array $APA_1(t,k,v)$.

We consider now authentication codes that are $t$-fold secure against spoofing and simultaneously achieves perfect $t$-fold secrecy:

A combinatorial lower bound on the number of encoding rules as well as a characterization of these codes can be obtained similarly as before.

Theorem 3.21 (Stinson [195]). If an authentication code is $t$-fold secure against spoofing and provides perfect $t$-fold secrecy, then the
number of encoding rules is bounded below by

\[ b \geq \binom{v}{t} \frac{v - t}{k - t}. \]

Again, we call such a code *optimal* when equality is achieved.

**Theorem 3.22 (Stinson [195]).** Suppose there is a perpendicular array \( PA_\lambda(t, k, k) \) and a \((t + 1)\)-\((v, k, \lambda')\) design with \( k \geq 2t - 1 \). Then there is an authentication code for \( k \) source states, having \( v \) messages and \( \frac{\lambda\lambda'(v-t)}{k-t} \binom{v}{t} \) encoding rules, that is \( t \)-fold secure against spoofing and achieves perfect \( t \)-fold secrecy. Moreover, the code is optimal if and only if \( \lambda = \lambda' = 1 \).

Using Example 2.17 and Steiner 2-\( 2^{d+1}-1 \), \( q+1,1 \) designs from projective geometries (cf. Example 2.3) yields the following theorem.

**Theorem 3.23 (Stinson [195]).** The following holds:

(a) Suppose there is a Steiner 2-\((v, k, 1)\) design. Then there is an optimal authentication code with \( k \) source states and \( v \) messages, that is one-fold secure against spoofing and provides perfect one-fold secrecy.

(b) For all prime powers \( q \) and all positive integers \( d \geq 2 \), there is an optimal authentication code for \( q+1 \) source states, having \( \frac{2^{d+1}-1}{q-1} \) messages, that is one-fold secure against spoofing and provides perfect one-fold secrecy.

We obtain from Theorem 3.22 furthermore the next results.

**Theorem 3.24 (Stinson [195]).** The following holds:

(a) For all Mersenne primes \( q = 2^a - 1 \) and for all integers \( d \geq 2 \), there is a (non-optimal) authentication code for \( q+1 \) source states, having \( q^d + 1 \) messages and \( \frac{(q^d+1)q^d(q^d-1)}{q-1} \) encoding rules, that is two-fold secure against spoofing and provides perfect two-fold secrecy.
(b) For all Fermat primes \( q = 2^a + 1 \) and for all integers \( d \geq 2 \), there is an optimal authentication code for \( q \) source states, having \((q - 1)^d + 1\) messages, that is two-fold secure against spoofing and provides perfect two-fold secrecy.

**Proof.** Since \( q + 1 = 2^a \) is a prime power, there is an \( OA_1(2, q + 1, q + 1) \) in view of Example 2.28. Using spherical geometries from Example 2.7 establishes assertion (a).

By Example 2.18, there is a \( PA_1(2, q, q) \). As \( q - 1 = 2^a \) is a prime power, a Steiner 3-\((q - 1)^d + 1, q, 1)\) design exists due to Example 2.7. This proves (b).

We remark that presently only five Fermat primes are known (3 = \( 2^1 + 1 \), 5 = \( 2^2 + 1 \), 17 = \( 2^4 + 1 \), 257 = \( 2^8 + 1 \), and 65,537 = \( 2^{16} + 1 \)). For Mersenne primes, only 47 prime numbers are known (the largest known Mersenne prime \( 2^{243,112,609} - 1 \) is indeed the largest known prime number up to the time of writing; for the list of known Mersenne primes, see sequence A000668 in [190].)

A partial converse to Theorem 3.22 can be stated (without proof) as follows.

**Theorem 3.25 (Stinson [195]).** Suppose there is an authentication code for \( k \) source states, having \( v \) messages and \( \binom{v}{t} \frac{v-t}{k-t} \) encoding rules, that is \( t \)-fold secure against spoofing and achieves perfect \( t \)-fold secrecy. Then there is a \( (t + 1)-(v, k, \lambda) \) design with \( \lambda = \binom{k}{t} \).

We summarize the results in this subsection in Table 3.5 (cf. [195]).

### 3.4 Authentication Codes with Secrecy in the Verification Oracle Model

Using the same notation as in the basic model (cf. Section 1.1), we consider in this section an extended authentication model, where the opponent has access to a verification oracle (V-oracle). In this model,
we assume that the opponent is no longer restricted to passively observing messages transmitted by the sender to the receiver. The opponent may send a message of the opponent’s choice to the receiver and observe the receiver’s response whether or not the receiver accepts it as authentic. This more powerful, pro-active attack scenario can be modeled in terms of a V-oracle that provides a response (accept or reject) to a query message in the same way as the message would be accepted or not by the legitimate receiver. This attack model was recently introduced in [14, 177]. Further details on this model can be found in [14, 177, 213, 214].

Two types of attacks, an online and an offline attack, are considered in [213]. In the online attack, the receiver is supposed to response to each incoming query message, and thus the opponent is successful as soon as the receiver accepts a message as authentic. Thus, every query message is at the same time a spoofing message. In the offline attack, the query and the spoofing phase are separated. First, the opponent makes all his queries to the oracle, and then uses this collected (state) information to construct a spoofing message. In both scenarios, the opponent is assumed to be adaptive. The online attack models an opponent’s interaction with a verification oracle such as an ATM,
while in the offline attack the opponent may have captured an offline verification box. Often, the offline attack model is used as an intermediate model for analyzing the online scenario.

We speak in each scenario of a spoofing attack of order \( i \) in the V-oracle model if the opponent has access to \( i \) verification queries. The opponent’s strategy can be modeled via probability distributions on the query set \( \mathcal{M} \) of verification queries. The online deception probability \( P_{d_i}^{\text{online}} \), respectively offline deception probability \( P_{d_i}^{\text{offline}} \), denotes the probability that the opponent can deceive the receiver with a spoofing attack of order \( i \).

We indicate lower bounds on the deception probabilities in the V-oracle model.

**Theorem 3.26 (Tonien–Safavi-Naini–Wild [213]).** In an authentication code with \( k \) source states and \( v \) messages, the offline and online deception probabilities in the V-oracle model are bounded below by

\[
P_{d_i}^{\text{offline}} \geq \frac{k}{v} \quad \text{and} \quad P_{d_i}^{\text{online}} \geq 1 - \frac{(v-k)}{(i+1)}
\]

Moreover, it follows that

\[
P_{d_i}^{\text{offline}} = \frac{k}{v} \quad \text{if and only if} \quad P_{d_i}^{\text{online}} = 1 - \frac{(v-k)}{(i+1)}.
\]

Hence, an authentication code that attains the bound in the offline attack is the same as in the online attack, and vice versa. Clearly, \( P_{d_i}^{\text{offline}} \) is independent of \( i \). If the bound for \( P_{d_i}^{\text{offline}} \) is satisfied with equality, then also the bound for \( P_{d_{i-1}}^{\text{offline}} \) is satisfied with equality for \( i > 1 \) (cf. [213]). Thus, a code is called \( t \)-fold secure against spoofing in the V-oracle model (in either scenario) if \( t = i \).

An analogue to Theorem 3.7 has been derived for the V-oracle model.

**Theorem 3.27 (Tonien–Safavi-Naini–Wild [213]).** If an authentication code is \((t - 1)\)-fold secure against spoofing in the V-oracle model,
then the number of encoding rules is bounded below by
\[ b \geq \frac{\binom{v}{t}}{\binom{k}{t}}. \]

Again, we call a code *optimal* when the lower bound holds with equality.

For equiprobable source states, optimal authentication codes which are \((t - 1)\)-fold secure against spoofing in the V-oracle model have been characterized recently. We present the result in a slightly more generalized form, which can be deduced from the original proof.

**Theorem 3.28 (Tonien–Safavi-Naini–Wild [213]).** Suppose there is a \(t-(v,k,\lambda)\) design. Then there is an authentication code for \(k\) equiprobable source states, having \(v\) messages and \(\lambda \cdot \frac{\binom{v}{t}}{\binom{k}{t}}\) encoding rules, that is \((t - 1)\)-fold secure against spoofing in the V-oracle model. Conversely, if there is an authentication code for \(k\) equiprobable source states, having \(v\) messages and \(\frac{\binom{v}{t}}{\binom{k}{t}}\) encoding rules, that is \((t - 1)\)-fold secure against spoofing in the V-oracle model, then there is a Steiner \(t-(v,k,1)\) design.

We will now proceed as in Theorem 3.12 to construct optimal authentication codes which are multi-fold secure against spoofing in the V-oracle model and simultaneously achieve perfect secrecy.

**Theorem 3.29 (Huber).** Suppose there is a Steiner \(t-(v,k,1)\) design with \(t \geq 2\), where \(v\) divides the number of blocks \(b\). Then there is an optimal authentication code for \(k\) equiprobable source states, having \(v\) messages and \(\frac{\binom{v}{t}}{\binom{k}{t}}\) encoding rules, that is \((t - 1)\)-fold secure against spoofing in the V-oracle model and provides perfect secrecy.

*Proof.* The authentication capacity of the code follows from Theorem 3.28. Under the assumption that the encoding rules are used with equal probability, we may proceed as in the proof of Theorem 3.12 to establish perfect secrecy. \(\square\)
Clearly, our constructions in Theorem 3.13 and the subsequent tables also work for authentication codes in the V-oracle model. Exemplarily, we state:

**Theorem 3.30 (Huber).** For all prime powers $q$ and for all even integers $d \geq 2$, there is an optimal authentication code for an equiprobable source probability distribution with $q + 1$ source states, having $q^d + 1$ messages, that is two-fold secure against spoofing in the V-oracle model and provides perfect secrecy.

Moreover, Theorem 3.15 and all the other results obtained in Subsection 3.3.1 can be transferred accordingly.

We close with an interesting open question:

**Problem 3.1.** Addressing a further variant of an extended authentication model, where the opponent has access to an authentication oracle that provides the authenticated message corresponding to a query source state in the same way as the legitimate sender would (cf. [14, 177]): Is it possible to give combinatorial characterizations as well as constructions of optimal codes (with and without secrecy requirements)?

### 3.5 Authentication Codes with Splitting

We study authentication codes with splitting in this section. In such a code, several messages can be used to communicate a particular plaintext (*non-deterministic encoding*). These codes were first introduced by Simmons [183]. The concept plays an important role, for instance, in the context of authentication codes that permit arbitration (cf. Section 3.6). We will make use of splitting $t$-designs, which we introduced in Section 2.4 and for which we gave basic necessary conditions regarding their existence.

Let $\mathcal{S}$ again denote a finite set of *source states*, $\mathcal{M}$ a finite set of *messages*, and $\mathcal{E}$ a finite set of *encoding rules*. In addition to the
notion of the basic model in Section 1.1, we introduce the following definitions: When it is possible that more than one message can be used to communicate a particular source state \( s \in S \) under the same encoding rule \( e \in E \), then the authentication code is said to have splitting. In this case, a message \( m \in M \) is computed as \( m = e(s,r) \), where \( r \) denotes a random number chosen from some specified finite set \( R \). If we define

\[
e(s) := \{ m \in M \mid m = e(s,r) \text{ for some } r \in R \},
\]

for each encoding rule \( e \in E \) and each source state \( s \in S \), then splitting means that \( |e(s)| > 1 \) for some \( e \in E \) and some \( s \in S \). In order to ensure that the receiver can decrypt the message being sent, it is required for any \( e \in E \) that \( e(s) \cap e(s') = \emptyset \) if \( s \neq s' \). For a given encoding rule \( e \in E \), let

\[
M(e) := \bigcup_{s \in S} e(s)
\]

denote the set of valid messages. For an encoding rule \( e \) and a set \( M^* \subseteq M(e) \) of distinct messages, we define

\[
f_e(M^*) := \{ s \in S \mid e(s) \cap M^* \neq \emptyset \},
\]

i.e., the set of source states that will be encoded under encoding rule \( e \) by a message in \( M^* \). A received message \( m \) will be accepted by the receiver as being authentic if and only if \( m \in M(e) \). When this is fulfilled, the receiver decrypts the message \( m \) by applying the decoding rule \( e^{-1} \), where

\[
e^{-1}(m) = s \text{ if } m = e(s,r) \text{ for some } r \in R.
\]

A splitting authentication code is called \( c \)-splitting if

\[
|e(s)| = c
\]

for every encoding rule \( e \in E \) and every source state \( s \in S \). When splitting occurs, the receiver and transmitter will also choose a splitting strategy to determine \( m \in M \), given \( s \in S \) and \( e \in E \).

We first state lower bounds on deception probabilities for splitting authentication codes.
Theorem 3.31 (De Soete–Blundo–De Santis–Kurosawa–Ogata [27, 53]). In a splitting authentication code, for every \(0 \leq i \leq t\), the deception probabilities are bounded below by

\[
P_{d_i} \geq \min_{e \in \mathcal{E}} \frac{|M(e)| - i \cdot \max_{s \in S} |e(s)|}{|\mathcal{M}| - i}.
\]

A splitting authentication code is called \(t\)-fold secure against spoofing if

\[
P_{d_i} = \min_{e \in \mathcal{E}} \frac{|M(e)| - i \cdot \max_{s \in S} |e(s)|}{|\mathcal{M}| - i}
\]

for all \(0 \leq i \leq t\).

For splitting authentication codes that are one-fold secure against spoofing attacks, Brickell [30] and Simmons [187] have established a combinatorial lower bound on the number of encoding rules. A combinatorial lower bound accordingly for multi-fold secure splitting authentication codes has been obtained lately.

Theorem 3.32 (Huber [106]). If a splitting authentication code is \((t-1)\)-fold secure against spoofing, then the number of encoding rules is bounded below by

\[
|\mathcal{E}| \geq \prod_{i=0}^{t-1} \frac{|\mathcal{M}| - i}{|M(e)| - i \cdot \max_{s \in S} |e(s)|}.
\]

Proof. Let \(M^* \subseteq \mathcal{M}\) be a set of \(i \leq t - 1\) distinct messages that are valid under a particular encoding rule, in such a way that they define \(i\) different source states. Let \(x \in \mathcal{M}\) be any message not in \(M^*\). We assume that there is no encoding rule \(e \in \mathcal{E}\) under which all messages in \(M^* \cup \{x\}\) are valid and for which \(f_e(x) \notin f_e(M^*)\). Following the proof of Theorem 3.31, mutatis mutandis, yields

\[
P_{d_i} > \min_{e \in \mathcal{E}} \frac{|M(e)| - i \cdot \max_{s \in S} |e(s)|}{|\mathcal{M}| - i},
\]
3.5 Authentication Codes with Splitting

A contradiction. Therefore, any set of \( t \) distinct messages is valid under at least one encoding rule such that they define different source states. The bound follows now by counting in two ways the number of \( t \)-subsets of messages that are valid under some encoding rule such that they correspond to different source states.

Analogously, we call a splitting authentication code \textit{optimal} if the number of encoding rules meets the lower bound with equality.

As a consequence, we obtain for \( c \)-splitting authentication codes the following lower bounds:

**Corollary 3.33 (Huber [106]).** In a \( c \)-splitting authentication code,

\[
P_{d_i} \geq \frac{c(|S| - i)}{|M| - i}
\]

for every \( 0 \leq i \leq t \).

\textbf{Proof.} We set \( l := |M(e)| = c|S|. \) Then Theorem 3.31 yields

\[
P_{d_i} \geq \frac{l - i \cdot c}{|M| - i} = \frac{c(|S| - i)}{|M| - i}.
\]

**Corollary 3.34 (Huber [106]).** If a \( c \)-splitting authentication code is \( (t-1) \)-fold secure against spoofing, then

\[
|\mathcal{E}| \geq \frac{{|M| \choose t}}{c^t \cdot {S| \choose i}}.
\]

\textbf{Proof.} Using Theorem 3.32, we may proceed as for Corollary 3.33.

Ogata et al. characterized in 2004 optimal splitting authentication codes that are one-fold secure against spoofing. Their combinatorial result is based on splitting 2-designs.

**Theorem 3.35 (Ogata–Kurosawa–Stinson–Saido [165]).** Suppose there is a \( 2-(v, b, l = cu, 1) \) splitting design. Then there is an optimal \( c \)-splitting authentication code for \( u \) equiprobable source states,
having \( v \) messages and \( \binom{v}{2}/[c^2 \binom{v}{2}] \) encoding rules, that is one-fold secure against spoofing. Conversely, if there is an optimal \( c \)-splitting authentication code for \( u \) source states, having \( v \) messages and \( \binom{v}{2}/[c^2 \binom{v}{2}] \) encoding rules, that is one-fold secure against spoofing, then there is a 2-(\( v,b,l = cu,1 \)) splitting design.

A simple example is as follows (cf. [165]).

**Example 3.6.** An optimal 2-splitting authentication code for \( u = 2 \) equiprobable source states, having \( v = 9 \) messages and \( b = 9 \) encoding rules, that is one-fold secure against spoofing can be constructed from the 2-(9,9,4 = 2 \( \times \) 2,1) splitting design in Example 2.25. Each encoding rule is used with probability \( 1/9 \). An encoding matrix is given in Table 3.6.

A natural extension of Theorem 3.35 has been obtained recently. Optimal splitting authentication codes that are multi-fold secure against spoofing can be characterized in terms of splitting \( t \)-designs.

**Theorem 3.36 (Huber [106]).** Suppose there is a \( t-(v,b,l = cu,1) \) splitting design with \( t \geq 2 \). Then there is an optimal \( c \)-splitting

<table>
<thead>
<tr>
<th>( s_1 )</th>
<th>( s_2 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( e_1 )</td>
<td>{1,2}</td>
</tr>
<tr>
<td>( e_2 )</td>
<td>{2,3}</td>
</tr>
<tr>
<td>( e_3 )</td>
<td>{3,4}</td>
</tr>
<tr>
<td>( e_4 )</td>
<td>{4,5}</td>
</tr>
<tr>
<td>( e_5 )</td>
<td>{5,6}</td>
</tr>
<tr>
<td>( e_6 )</td>
<td>{6,7}</td>
</tr>
<tr>
<td>( e_7 )</td>
<td>{7,8}</td>
</tr>
<tr>
<td>( e_8 )</td>
<td>{8,9}</td>
</tr>
<tr>
<td>( e_9 )</td>
<td>{9,1}</td>
</tr>
</tbody>
</table>

Table 3.6. Splitting authentication code from a 2-(9,9,4 = 2 \( \times \) 2,1) splitting design.
authentication code for \( u \) equiprobable source states, having \( v \) messages and \( \binom{v}{c}/c^t(u) \) encoding rules, that is \((t-1)\)-fold secure against spoofing. Conversely, if there is an optimal \( c \)-splitting authentication code for \( u \) source states, having \( v \) messages and \( \binom{v}{c}/c^t(u) \) encoding rules, that is \((t-1)\)-fold secure against spoofing, then there is a \( t-(v,b,l = cu,1) \) splitting design.

Proof. Let us first assume that there is an optimal \( c \)-splitting authentication code for \(|S| := u \) source states, having \(|\mathcal{M}| := v \) messages and \(|\mathcal{E}| := \binom{v}{c}/c^t(u) \) encoding rules, that is \((t-1)\)-fold secure against spoofing. In order to meet the lower bound in Theorem 3.32 with equality, every set of \( t \) distinct messages must be valid under precisely one encoding rule, in such a way that they define different source states. For \( e \in \mathcal{E} \), let us define a block \( B_e \in \mathcal{B} \) as disjoint union

\[
B_e := \bigcup_{j=1}^{u} e(s_j).
\]

Then \((X, \mathcal{B}) = (\mathcal{M}, \{B_e \mid e \in \mathcal{E}\})\) is a \( t-(v,b,l = cu,1) \) splitting design in view of Definition 2.5.

To prove the other direction, let \(|\mathcal{M}| := v \). For every block \( B_i \in \mathcal{B} \) with

\[
B_i = \bigcup_{j=1}^{u} B_{i,j},
\]

we arbitrarily define an encoding rule \( e_{B_i} \) via

\[
e_{B_i}(s_j) := B_{i,j}
\]

for each \( 1 \leq j \leq u \). Using every encoding rule with equal probability \( 1/b \) establishes the claim.

We give a simple example (cf. [106]).

**Example 3.7.** An optimal 2-splitting authentication code for \( u = 3 \) equiprobable source states, having \( v = 10 \) messages and \( b = 15 \) encoding
rules, that is two-fold secure against spoofing can be constructed from the 3-(10, 15, 6 = 2 × 3, 1) splitting design in Example 2.26. Each encoding rule is used with probability $1/15$. An encoding matrix is given in Table 3.7.

We close this section by indicating two interesting questions concerning future research.

**Problem 3.2.** We pose the following problems (cf. [106]):

(i) Construction of multi-fold secure splitting authentication codes: Using Theorem 3.36, this asks for systematically constructing $t$-$(v, b, l = cu, 1)$ splitting design for $t > 2$. We remark that in the case when $t = 2$, various combinatorial constructions have been obtained recently, e.g., in [71] via recursive and direct constructions by the method of differences.
(ii) Including the aspect of perfect secrecy: Is it possible to give a characterization of optimal splitting authentication codes that are multi-fold secure against spoofing and simultaneously achieve perfect (multi-fold) secrecy?

3.6 Authentication Codes with Arbitration

We only briefly mention authentication codes that permit arbitration. To our best knowledge, no secrecy aspects have been incorporated so far. In this scenario, the two communicating parties do not trust each other, and hence disputes between them may occur. Hence, a trusted person (i.e., the arbiter) is also involved in this model. The arbiter chooses an encoding rule $e_K$ which is distributed only to the transmitter and a verification rule $f_K$ which is distributed only to the receiver. The arbiter is only present to resolve possible disputes and does not take part in any communication activities. The arbiter is assumed to be honest. Sometimes such a code is also called an $A_2$-code. These codes were introduced by Simmons [186, 187]. Further important work include [73, 120, 121, 136, 137, 138, 170].

We generally remark that further constructions and characterizations of authentication codes from combinatorial designs can be obtained by using entropy bounds, instead of combinatorial bounds, on deception probabilities and encoding rules. For this different approach, see [170] and the references therein.

We also mention that there are various other constructions of different types of authentication codes, using, e.g., algebraic curves [228], Galois rings [168], rational normal curves [170], generalized quadrangles [52, 180], coding theory [218], universal hashing [198], and many more. A bibliography on early publications (until 1998) on authentication and secrecy codes is online available [204].

3.7 Other Applications

We highlight in this section some further applications of combinatorial designs which we have not discussed so far. Particularly the last few years have witnessed an increasing body of work in the communications
and information theory, cryptography, and computer science literature that makes substantial use of combinatorial designs. General surveys are [43, 44, 48, 197, 200]. Specific areas of recent applications include:

- **Secret sharing schemes.** There are several constructions and characterizations of secret sharing schemes based on combinatorial designs. These include combinatorial characterizations of ideal threshold schemes via orthogonal arrays, anonymous threshold schemes via partitionable and resolvable Steiner designs, and optimum secret sharing schemes secure against cheating via difference sets, amongst others. There are also combinatorial constructions for non-perfect threshold schemes. Cf., e.g., [164, 165, 197, 203].

- **Visual cryptography.** Visual threshold schemes have been obtained based on 2-designs. In particular, schemes with optimal relative contrast have been constructed via 2-designs obtained from Hadamard matrices, depending on the famous Hadamard Matrix Conjecture (1893). Cf., e.g., [28, 29, 63].

- **Key predistribution for distributed wireless sensor networks.** A variety of combinatorial designs have found applications for different types of cryptographic key establishment schemes. In particular, key predistribution schemes suitable for distributed wireless sensor networks have been constructed via 2-designs, 3-designs, transversal designs and strongly-regular graphs. Cf., e.g., [141, 151, 224].

- **Powerline communication (PCL).** Permutation arrays offer a way of encoding data which allows the noise problems experienced in PLCs to be overcome. These combinatorial structures are closely related to mutually orthogonal Latin squares (MOLS). Cf., e.g., [45, 110, 169].

- **Frequency-hopping (FH) sequences.** Various FH sequences have been constructed by means of combinatorial structures such as affine geometries, cyclic designs, difference families and difference packings, which are useful for frequency-hopping spread-spectrum (FHSS) communication
systems and ultra-wide-band (UWB) communication systems. Cf., e.g., [40, 68, 70, 72].

- **Low-density parity-check (LDPC) codes.** Finite geometries (also partial geometries) and Steiner 2-designs (particularly when resolvable or cyclic) have been used for the design of regular LDPC codes. One of the main advantages of these structured LDPC codes is that they can lend themselves to very low-complexity encoding, as opposed to random-like LDPC codes. Experimental results show that the proposed codes perform well with iterative decoding. Cf., e.g., [3, 122, 123, 133, 220].

- **Software and hardware testing.** Orthogonal arrays and combinatorial structures known as covering arrays have found applications as efficient test suites in the testing of software and hardware. Cf., e.g., [32, 90, 155].

- **Group testing algorithms in DNA screening.** Steiner $t$-designs, in particular resolvable Steiner 2-designs and 2-resolvable Steiner 3-designs, provide useful structures to achieve a minimal number of individual tests in a two-stage disjunctive testing algorithm. Transversal designs have also been used for one- and two-stage group testing algorithms. Cf., e.g., [62, 212].

### 3.8 Synthesis and Discussion

We have discussed applications of combinatorial designs for the construction and characterization of authentication and secrecy codes. We have considered different attack scenarios in the classical Shannon-Simmons model and in extended models, such as with oracle access or in case of non-deterministic encoding. Moreover, we have given a tutorial overview of combinatorial designs and we pointed to further applications of combinatorial designs in various other fields.

Several challenging open problems have been stated throughout the text. Another direction for future work may concern applications of the proposed codes with regard to authentication and secrecy aspects in group communication. Moving from point-to-point communication
to point-to-multipoint communication, the concept of multi-receiver (or group-based, broadcast) authentication codes was introduced by Desmedt et al. [58] and extended in [69, 163, 178, 179, 177]. Multi-receiver authentication codes have found recent applications in network coding [166, 167], amongst others. In such a multi-receiver authentication code, a trusted sender constructs an authenticated message for a group of receivers such that each receiver can individually verify the authenticity of the received message. The receivers are not trusted and may try to construct fraudulent messages on behalf of the transmitter. If the fraudulent message is accepted by even one receiver the attack has been successful. Often, constructions of multi-receiver authentication codes are obtained by combining conventional authentication codes with further building blocks, including combinatorial designs such as orthogonal arrays and cover-free families, finite geometries, perfect hash families, secret sharing schemes, etc. It is therefore interesting to investigate further applications of the proposed codes in this framework (with and without secrecy constraints).
4

Appendix

4.1 Multiply Homogeneous Permutation Groups

We list all finite multiply homogeneous permutation groups. We remark that besides the symmetric or alternating groups, the sporadic simple Mathieu groups $M_v$ with $v = 11$, 23 and $v = 12$, 24 are the only finite 4- and 5-transitive permutation groups, respectively.

Let $G$ be a group acting 2-homogeneously on a finite set $X$ of $v \geq 3$ points. If $G$ is not 2-transitive on $X$, then $G \leq AGL(1, q)$ with $v = q \equiv 3 \pmod{4}$ by a result of Kantor [125]. On the other hand, relying on the Classification of the Finite Simple Groups (CFSG), all 2-transitive groups on $X$ are known (cf. [51, 80, 93, 94, 116, 127, 143, 150]). By a classical result of Burnside, they split into two types of groups. The list of groups is as follows: A finite 2-transitive permutation group $G$ on $X$ is either of

(A) Affine Type: $G$ contains a regular normal subgroup $T$ which is elementary Abelian of order $v = p^d$, where $p$ is a prime. If $a$ divides $d$, and if we identify $G$ with a group of affine transformations

$$x \mapsto x^g + u$$
of $V = V(d, p)$, where $g \in G_0$ and $u \in V$, then particularly one of the following occurs:

1. $G \leq AGL(1, p^d)$
2. $G_0 \succeq SL(\frac{d}{a}, p^a)$, $d \geq 2a$
3. $G_0 \succeq Sp(\frac{2d}{a}, p^a)$, $d \geq 2a$
4. $G_0 \succeq G_2(2^a)$, $d = 6a$
5. $G_0 \cong A_6$ or $A_7$, $v = 2^4$
6. $G_0 \supseteq SL(2, 3)$ or $SL(2, 5)$, $v = p^2$, $p = 5, 7, 11, 19, 23, 29$ or $59$, or $v = 3^4$
7. $G_0$ contains a normal extraspecial subgroup $E$ of order $2^5$, and $G_0/E$ is isomorphic to a subgroup of $S_5$, $v = 3^4$
8. $G_0 \cong SL(2, 13)$, $v = 3^6$

or

(B) Almost Simple Type: $G$ contains a simple normal subgroup $N$, and $N \leq G \leq \text{Aut}(N)$. In particular, one of the following holds, where $N$ and $v = |X|$ are given as follows:

1. $A_v$, $v \geq 5$
2. $PSL(d, q)$, $d \geq 2$, $v = \frac{2^d-1}{q-1}$, where $(d, q) \neq (2, 2), (2, 3)$
3. $PSU(3, q^2)$, $v = q^3 + 1$, $q > 2$
4. $Sz(q)$, $v = q^2 + 1$, $q = 2^{2e+1} > 2$ (Suzuki groups)
5. $Re(q)$, $v = q^3 + 1$, $q = 3^{2e+1} > 3$ (Ree groups)
6. $Sp(2d, 2)$, $d \geq 3$, $v = 2^{2d-1} \pm 2^{d-1}$
7. $PSL(2, 11)$, $v = 11$
8. $PSL(2, 8)$, $v = 28$ ($N$ is not 2-transitive)
9. $M_v$, $v = 11, 12, 22, 23, 24$ (Mathieu groups)
10. $M_{11}$, $v = 12$
11. $A_7$, $v = 15$
12. $HS$, $v = 176$ (Higman–Sims group)
13. $Co_3$, $v = 276$. (smallest Conway group)

We also state the classification of all finite 3-homogeneous permutation groups, again relying on CFSG (cf. [36, 80, 126, 143, 146]). The list of groups is as follows: Let $G$ be a finite 3-homogeneous permutation
4.1 Multiply Homogeneous Permutation Groups

A group on a finite set $X$ of $v \geq 4$ points. Then $G$ is either of

A **Affine Type**: $G$ contains a regular normal subgroup $T$ which is elementary Abelian of order $v = 2^d$. If we identify $G$ with a group of affine transformations

$$x \mapsto x^g + u$$

of $V = V(d, 2)$, where $g \in G_0$ and $u \in V$, then particularly one of the following occurs:

1. $G \cong AGL(1, 8), A\Gamma L(1, 8)$ or $A\Gamma L(1, 32)$
2. $G_0 \cong SL(d, 2), d \geq 2$
3. $G_0 \cong A_7, v = 2^4$

or

B **Almost Simple Type**: $G$ contains a simple normal subgroup $N$, and $N \leq G \leq \text{Aut}(N)$. In particular, one of the following holds, where $N$ and $v = |X|$ are given as follows:

1. $A_v, v \geq 5$
2. $PSL(2, q), q > 3, v = q + 1$
3. $M_v, v = 11, 12, 22, 23, 24$
4. $M_{11}, v = 12$

It is elementary that if $q$ is odd, then $PSL(2, q)$ is 3-homogeneous for $q \equiv 3 \pmod{4}$, but not for $q \equiv 1 \pmod{4}$, and hence not every group $G$ of almost simple type satisfying (2) is 3-homogeneous on $X$.

For further properties of the listed groups, we refer, e.g., to [38, 49, 61, 117, 118].
Acknowledgments

I thank Prof. Douglas Stinson, University of Waterloo, for an inspiring conversation on this topic. I am also indebted to the Editor-in-Chief Prof. Sergio Verdú, Princeton University, and Mike Casey from Now Publishers for their interest and encouragement to write this Foundations and Trends issue as well as to an anonymous reviewer for insightful comments. This work was supported by the Deutsche Forschungsgemeinschaft (DFG) via a Heisenberg grant (Hu954/4) and a Heinz Maier-Leibnitz Prize grant (Hu954/5). Last but certainly not least, special thanks to my wife Susanne and our two daughters Lynn-Scharon and Sheila-Ann.
References


References


References

References


References


[142] Y. Liang, H. V. Poor, and S. Shamai (Shitz), “Information theoretic security,” 
*Foundations and Trends in Communications and Information Theory*, vol. 5, 

[143] M. W. Liebeck, “The affine permutation groups of rank three,” 


[146] D. Livingstone and A. Wagner, “Transitivity of finite permutation groups on 


symétriques ou alternés,” *Journal de Mathématiques Pures et Appliquées*, 
vol. 1, pp. 5–34, 1895.

[151] K. M. Martin, “On the applicability of combinatorial designs to key predis-
tribution for wireless sensor networks,” in *International Workshop on Coding 
and Cryptology — IWCC 2009*, Lecture Notes in Computer Science, vol. 5557, 

(E. Biglieri and G. Prati, eds.), pp. 3–21, Amsterdam, New York, 

[153] E. Mathieu, “Mémoire sur l’étude des fonctions de plusieurs quantités,” 
*Journal de Mathématiques Pures et Appliquées*, vol. 6, pp. 241–323, 1861.

[154] E. Mathieu, “Sur la fonction cinq fois transitive de 24 quantités,” 
*Journal de Mathématiques Pures et Appliquées*, vol. 18, pp. 25–46, 1873.

2008.


[161] D. E. Muller, “Application of boolean algebra to switching circuit design and 
References


References