2011

Applications of finite geometries to designs and codes

David C. Clark
Michigan Technological University

Follow this and additional works at: https://digitalcommons.mtu.edu/etds
Part of the Mathematics Commons

APPLICATIONS OF FINITE GEOMETRIES TO DESIGNS AND CODES

By

David C. Clark

A DISSERTATION

Submitted in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

(Mathematical Sciences)

MICHIGAN TECHNOLOGICAL UNIVERSITY

2011

This dissertation, "Applications of Finite Geometries to Designs and Codes," is hereby approved in partial fulfillment of the requirements for the Degree of DOCTOR OF PHILOSOPHY IN MATHEMATICAL SCIENCES.

Department of Mathematical Sciences

Signatures:

Dissertation Advisor ______________________________
Dr. Vladimir Tonchev

Committee Member ______________________________
Dr. Donald Kreher

Committee Member ______________________________
Dr. Stefaan De Winter

Committee Member ______________________________
Dr. Steven Seidel

Department Chair ______________________________
Dr. Mark Gockenbach

Date ______________________________

Contents

List of Figures

List of Tables

Preface

Several chapters in this dissertation are the result of collaborative work, and have been published in or submitted to refereed journals. Each paper is written according to the style of the journal in which it was published. The introduction to each paper has been left in place, even though this may repeat definitions which are given in Chapter 1. Several papers have been modified by adding an extended introductory section concerning the history of the paper's topic, as well as minor editorial changes.

Documentation of permission to reprint each article is documented in Appendix C.

- Chapter 2: *Affine geometry designs, polarities, and Hamada's conjecture*. This is joint work with D. Jungnickel and V. D. Tonchev. The topic was suggested by V. D. Tonchev. The author performed the research and wrote the paper, with guidance and editing provided by D. Jungnickel and V. D. Tonchev. It was previously published in the Journal of Combinatorial Theory, Series A.

- Chapter 4: *Nonbinary quantum codes derived from finite geometries*. This is joint work with V. D. Tonchev. The topic was suggested by V. D. Tonchev. The author performed the research and wrote the paper, with guidance and editing provided by V. D. Tonchev. It was previously published in the journal Finite Fields and their Applications.

- Chapter 5: *Entanglement-assisted quantum low-density parity-check codes.* This is joint work with Y. Fujiwara, P. Vandendriessche, M. De Boeck, and V. D. Tonchev. The topic was suggested by Y. Fujiwara. The author performed the research and writing for Section III, except for two theorems concerning minimum distance. The author also performed the simulations and created the plots and tables in Section IV. The author is also responsible for portions of the writing, editing, and figures in all other sections. It was previously published in the journal Physical Review A.

Acknowledgments

My sincere thanks go to my advisor, Vladimir Tonchev. Throughout my graduate career, Professor Tonchev has provided me with an amazing range of opportunities. His encouragement and ideas have directed the course of my research, and I would not be where I am today without his support and guidance. I also owe many thanks to my committee members: Don Kreher, Stefaan De Winter, and Steven Seidel. I very much appreciate the time and effort which you have spent while serving on my committee.

This dissertation would not be possible if not for the help of my collaborators and co-authors. I owe much gratitude to Vladimir Tonchev, Dieter Jungnickel, Yuichiro Fujiwara, Peter Vandendriessche, and Maarten De Boeck for their assistance, support, and encouragement for the work contained in this volume.

I am incredibly grateful to my parents, who have supported me through *many* years of school, and have always believed in me and my goals. Your support, encouragement, love, and patience mean more than I can even begin to say.

Finally, to Sarah: “thank you” isn’t nearly enough. You have provided more support and love than I could have ever imagined, and kept me going through the tough times. Your constant support, wise advice, and quiet comfort mean the world to me.

Abstract

This dissertation concerns the intersection of three areas of discrete mathematics: finite geometries, design theory, and coding theory. The central theme is the power of finite geometry designs, which are constructed from the points and t-dimensional subspaces of a projective or affine geometry. We use these designs to construct and analyze combinatorial objects which inherit their best properties from these geometric structures.

A central question in the study of finite geometry designs is Hamada's conjecture, which proposes that finite geometry designs are the unique designs with minimum p-rank among all designs with the same parameters. In this dissertation, we will examine several questions related to Hamada's conjecture, including the existence of counterexamples. We will also study the applicability of certain decoding methods to known counterexamples.

We begin by constructing an infinite family of counterexamples to Hamada's conjecture. These designs are the first infinite class of counterexamples for the affine case of Hamada's conjecture. We further demonstrate how these designs, along with the projective polarity designs of Jungnickel and Tonchev, admit majority-logic decoding schemes. The codes obtained from these polarity designs attain error-correcting performance which is, in certain cases, equal to that of the finite geometry designs from which they are derived. This further demonstrates the highly geometric structure maintained by these designs.

Finite geometries also help us construct several types of quantum error-correcting codes. We use relatives of finite geometry designs to construct infinite families of q-ary quantum stabilizer codes. We also construct entanglement-assisted quantum error-correcting codes (EAQECCs) which admit a particularly efficient and effective error-correcting scheme, while also providing the first general method for constructing these quantum codes with known parameters and desirable properties. Finite geometry designs are used to give exceptional examples of these codes.

Chapter 1

Designs, codes, and finite geometries

1.1 Introduction

This dissertation will focus on the intersection of three areas of discrete mathematics: finite geometries, design theory, and coding theory. We will use these tools to find counterexamples to a famous conjecture, develop constructions for new designs, and create quantum codes with desirable properties.

The main portion of this work consists of several papers previously published by the author, as well as several chapters containing unpublished work. The central theme will be the power of finite geometry designs. In each chapter, we will use finite geometry designs to construct and analyze new combinatorial objects, including new classes of designs and quantum codes. We will show how the structure of the finite geometries carries through to the new combinatorial objects and provides them with some of their best properties.

In this first chapter, we will give detailed definitions of the fundamental objects of our study, and examine the links between these objects. We will also describe the major contributions of this dissertation. Each other chapter will begin with an introductory section, which describes the history and background of that chapter's particular topic.

1.1.1 Designs

We begin by examining *block designs*, which are one of the central objects in our study. A t-(v,k,λ) *block design* (usually just a *t-design*) is a pair $D = (\mathscr{P}, \mathscr{B})$, where $\mathscr{P}$ is a set of v points, and $\mathscr{B}$ is a collection of k-subsets of $\mathscr{P}$ called *blocks*. These blocks are subject to the condition that every t-subset of $\mathscr{P}$ must be contained in exactly λ blocks. The value λ is sometimes called the *index* of a design. We make the natural assumption that $0 < k < v$ and $t \geq 2$ to avoid trivial designs.

Several invariants of a design can be determined directly from the parameters. The number of blocks in a design is $b = |\mathscr{B}| = \lambda \binom{v}{t} / \binom{k}{t}$. Each point appears in exactly $r = \lambda \binom{v-1}{t-1} / \binom{k-1}{t-1}$ blocks. A t-(v,k,λ) design with $t \geq 2$ is also a $(t-1)$-(v,k,λ_{t-1}) design, where $\lambda_{t-1} = \lambda \frac{v-t+1}{k-t+1}$.

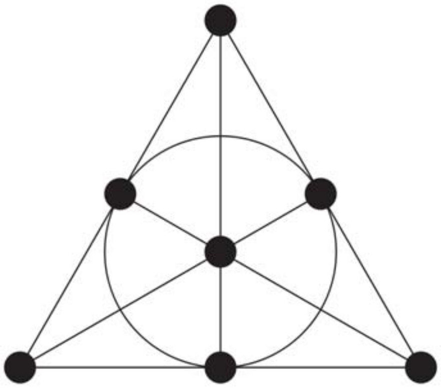


Figure 1.1: The Fano plane, an example of a 2-$(7,3,1)$ design obtained from a finite geometry. It has $b = 7$ blocks, and each point appears in $r = 3$ blocks.

For a design D, a set of blocks which partition the points of D is called a *parallel class*. A partition of the blocks of D into parallel classes is called a *resolution*. If a resolution exists, then D is *resolvable*. Note that a design may possess several different resolutions. A design may also possess individual parallel classes without being resolvable.

The designs studied in this work will be *simple*: no block will appear more than once. For simple designs, if $0 < k < v$ and $t \geq 2$, then $b \geq v$ (a result known as Fisher's inequality, which also holds in a variety of other circumstances). A design with $v = b$ is called *symmetric*, in which case any pair of distinct blocks intersect in exactly λ points. A *quasi-symmetric* design is a design in which pairs of distinct blocks intersect in either x or y points, where x and y are distinct integers dependent on the design.

There are special names given to certain classes of designs. A design with $t = 2$ is called a *balanced incomplete block design*, also BIBD or BIB design. A design with index 1 is called a *Steiner* design. The parameters of a Steiner design are sometimes written $S(t,k,v)$. A Steiner design with v points and $k = 3$ is a *Steiner triple system* or *STS(v)*, and a design with $k = 4$ is a *Steiner quadruple system* or *SQS(v)*. These named designs will appear often in our study of geometric designs.

An *incidence matrix* of a design D is a binary $b \times v$ matrix $M = (m_{ij})$ whose rows are indexed by the blocks of D, and columns are indexed by the points. Suppose we label the points of D by $\{1,2,\ldots,v\}$, and arbitrarily label its blocks as $\{B_1,B_2,\ldots,B_b\}$. The entries of the incidence matrix are defined by:

$$m_{ij} = \begin{cases} 1 & \text{if block } B_i \text{ contains point } j, \\ 0 & \text{otherwise} \end{cases}$$

There are many possible incidence matrices for a design, depending on the ordering chosen for points and blocks. However, these matrices are all equivalent up to a permutation of the rows and columns. Thus, we will speak of *the* incidence matrix of a design unless a particular ordering of the rows and columns is essential. The orientation of incidence matrices varies depending on the application: many texts label rows with points and columns with blocks instead. We have chosen to use the block-by-point orientation because we will usually wish for the rows of the incidence matrix to be the incidence vectors of blocks. Note that in Chapter 5, we will make extensive use of *both* orientations of incidence matrices, with important differences. We will specify the orientation of an incidence matrix whenever it may be unclear.

Two designs $D = (\mathscr{P},\mathscr{B})$ and $D' = (\mathscr{P}',\mathscr{B}')$ are said to be *isomorphic* if there exists a bijection $\varphi : \mathscr{P} \to \mathscr{P}'$ which takes $\mathscr{B}$ to $\mathscr{B}'$, that is, for each $B \in \mathscr{B}$, $\varphi(B) \in \mathscr{B}'$. The mapping φ is an *isomorphism* of the designs. An isomorphism of a design onto itself is called an *automorphism*. The group of all automorphisms of a design is called its *automorphism group*. A design is *cyclic* if has an automorphism of order v acting regularly on its v points. Each isomorphism from D to D' corresponds to a point permutation on the incidence matrix of D which produces an incidence matrix for D'. Each automorphism of a design corresponds to a permutation of the columns of an incidence matrix of the design, which preserves the collection of rows.

Other fundamental terms related to designs may be found in [BJL99, Sti04]. The terms defined here emphasize the aspects of designs which will be most useful in this work.

1.1.2 Error-correcting codes

Our second major area of study is *error-correcting codes*. Before giving a formal definition, we require some preliminary terminology. Suppose $x, y \in \mathbb{F}_q^n$. The *Hamming distance* $d(x,y)$ is defined as the number of coordinates in which x and y differ. The *Hamming weight* $\mathrm{wt}(x)$ is defined as the number of nonzero coordinates of x. Note that $d(x,y) = \mathrm{wt}(y-x)$.

An $[n,k,d]_q$ *linear error-correcting code* C is a k-dimensional linear subspace of $\mathbb{F}_q^n$ such that for any $x, y \in C$, $d(x,y) \geq d$. The value d is called the *minimum distance* of C. It is equivalent to specify that $\mathrm{wt}(c) \geq d$ for every nonzero $c \in C$. If the minimum distance d is not known, or if we do not wish to emphasize it, we may use the notation $[n,k]_q$.

We are often interested in more than just the minimum distance of a code. The *weight distribution* of a code is an ordered list $\{A_0, A_1, \ldots, A_n\}$ in which A_i is the number of words of weight i. Note that $A_0 = 1$, and $A_i = 0$ for all $0 < i < d$.

Every linear code C may be represented by a *generator matrix* whose rows span C. *Any* matrix whose rows span the code (whether the rows are linearly independent or not) may be called a generator matrix. Thus, there are typically many generator matrices for a given code.

For a code C, the *dual* code $C^\perp$ is defined as the set of vectors orthogonal to every vector in C. In this work, orthogonality is always with respect to the Euclidean dot product. The code $C^\perp$ is a linear $[n, n-k]_q$ code. Any generator matrix for $C^\perp$ is called a *parity check matrix* for C. The minimum distance of $d^\perp$ of $C^\perp$ is not necessarily related to the minimum distance d of C in any simple way. However, the minimum distance d of C is equal to the size of the smallest set of linearly dependent columns in a generator matrix for $C^\perp$. This follows from the fact that any nonzero word $c \in C$ must be orthogonal to each row of a generator matrix of $C^\perp$.

If $C \subseteq C^\perp$, then the code C is said to be *self orthogonal*. If $C = C^\perp$, then C is *self-dual*. Self-orthogonality is a frequently studied property of codes. It is especially useful in constructing certain types of quantum error-correcting codes, such as those described in Chapter 4.

For additional terms related to coding theory, the reader is referred to [HP03]. The definitions given here have been chosen to emphasize the aspects of codes which will be most useful in this dissertation.

1.1.3 The codes of a design and p-ranks

Designs and codes are closely related. Here, we will examine the links between these two fundamental structures.

Let D be a design, and M be its incidence matrix. The rows of M are the incidence vectors of the blocks of the design. For a prime power q, the span of these vectors over $\mathbb{F}_q$ forms a subspace of $\mathbb{F}_q^n$ called the q-ary *block code* of D, denoted $C_q(D)$. This is the most commonly studied code associated with a design, and so we will often call it *the* code of a design.

The rows of a transposed incidence matrix (that is, one which has v rows and b columns) also span a code, usually called the *point code* (see for example [BLT96] and [TW97]). However, other than in Chapter 5, our work will generally focus on the block codes of designs.

Because the incidence matrix of a design D is a $(0,1)$ matrix, the block code of D may be constructed over any finite field $\mathbb{F}_q$. The parameters of $C_q(D)$ depend on the parameters and structure of the design D, as well as the prime power q. In particular, the dimension of $C_q(D)$ is given by the rank of M over $\mathbb{F}_q$, denoted $\operatorname{rank}_q M$ and called the "q-rank" of the matrix. Because all incidence matrices of D have the same q-rank, we will use the shorthand notation $\operatorname{rank}_q D$ to indicate this dimension. Because M is a $(0,1)$ matrix, $\operatorname{rank}_{\mathrm{p}} D = \operatorname{rank}_{p^n} D$ for each prime p and integer $n \geq 1$. Thus it is customary to study only the *p-rank* of D, denoted $\operatorname{rank}_{\mathrm{p}} D$ for a specified prime p.

The structure and parameters of a design dictates many of the properties of its block code. As we have seen, the p-rank of a design gives the dimension of the associated block code, and the length of the $C_p(D)$ is exactly the number of points of the design. However, the minimum distance of $C_p(D)$ may be much more difficult to determine. In the best cases, the minimum weight vectors of $C_p(D)$ are exactly scalar multiples of the incidence vectors of the blocks of D. Although this is not always the case, it is true for many codes which we will study in this work. In the following section, we will describe the codes obtained from finite geometry designs, which give rise to particularly interesting codes.

Designs may also be found within codes. A code is said to *support* a design if there exists a collection of words in the code whose nonzero positions correspond to the points in blocks of a design. Note that such vectors need not be binary. A code obtained from the incidence matrix of a design necessarily supports the original design, but other designs may be found within the same code. The major result in this area is the *Assmus-Mattson Theorem* [AM69], which guarantees the existence of designs in many codes.

1.2 Finite geometry designs and codes

We have now developed the tools which will allow us to introduce the central combinatorial objects in this dissertation. Finite geometry designs are a class of designs obtained from affine and projective geometries. These designs and their block codes have a great deal of structure and important combinatorial properties, which has lead to their use in many fields of study. In this section, we will give constructions and parameters for these designs, and also identify the codes spanned by their incidence matrices.

We will approach the construction of finite geometries and designs from the point of view of vector spaces. Throughout, let $q = p^e$ be a prime power with $e \geq 1$. As a result of our focus on vector spaces, we will frequently make use of the Gaussian coefficient $\left[{m \atop i} \right]_q$, which counts the number of i-dimensional subspaces of an m-dimensional vector space over $\mathbb{F}_q$:

$$\begin{bmatrix} m \\ i \end{bmatrix}_q = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

Here $0 \leq i \leq m$. Note that by convention, $\left[{m \atop 0} \right]_q = 1$.

We will examine finite geometry designs obtained from projective and affine geometries. While we will introduce each separately, they share fundamental links which will be described below. We will also be interested in designs which have the same parameters as a finite geometry design, but which are not isomorphic to that design. These designs are called *pseudo-geometric designs*.

1.2.1 Projective Geometry Designs

We begin by defining the *projective geometry of dimension m over* $\mathbb{F}_q$, denoted $PG(m,q)$. The points of $PG(m,q)$ are the 1-dimensional subspaces of $\mathbb{F}_q^{m+1}$, excluding the zero vector. The t-dimensional subspaces of $PG(m,q)$ $(1 \leq t \leq m-1)$ are the $(t+1)$-dimensional vector subspaces of $\mathbb{F}_q^{m+1}$, excluding the zero vector. Note that, when speaking of projective geometries or designs, the *projective dimension t* of a subspace is always one lower than the *vector dimension* $t+1$ of the same subspace. We will always use the projective dimension unless otherwise specified. For consistency, we will frequently speak of $PG(m-1,q)$, because its underlying vector space has dimension m.

The designs derived from this space are defined as follows.

Definition 1. *The* projective geometry design $PG_t(m,q)$ *is the design whose points are the points of $PG(m,q)$, and whose blocks are the t-dimensional projective subspaces of $PG(m,q)$.*

The design $PG_t(m,q)$ has parameters

$$2-\left(\frac{q^{m+1}-1}{q-1},\frac{q^{t+1}-1}{q-1},\begin{bmatrix} m-1 \\ t-1 \end{bmatrix}_q\right).$$

This design has $b=\begin{bmatrix} m+1 \\ t+1 \end{bmatrix}_q$ blocks, and each point appears in $r=\begin{bmatrix} m \\ t \end{bmatrix}_q$ blocks.

Some authors refer to the projective designs with the notation $PG(m,q):t$ or $PG_{m,t}(q)$.

Projective geometries and projective geometry designs have been extensively studied. The designs which have received the most attention are those at the extreme limits of the block sizes: $t=1$ and $t=m-1$. A design with the same parameters as $PG_1(2,q)$ is called a *projective plane of order q*. Note that the finite geometry design is typically not the only projective plane of a given order. This is related to the question of the existence of designs with the same parameters as a geometric design. All projective planes of order q are Steiner designs with parameters $2-(q^2+q+1,q+1,1)$.

Projective planes are a special case of *hyperplane designs*, which are designs with the same parameters as $PG_{m-1}(m,q)$. These well-studied designs are symmetric designs with parameters $2-(\frac{q^{m+1}-1}{q-1},\frac{q^m-1}{q-1},\frac{q^{m-1}-1}{q-1})$. Again, there are typically many pseudo-geometric designs with these parameters.

1.2.2 Affine Geometry Designs

Our second class of finite geometry designs are constructed from the *affine geometry of dimension m over* $\mathbb{F}_q$, denoted by $AG(m,q)$. The points of $AG(m,q)$ are the vectors of $\mathbb{F}_q^m$. The t-dimensional affine subspaces of the geometry are the t-dimensional vector subspaces of $\mathbb{F}_q^m$ and their cosets. These subspaces are sometimes referred to as *t-flats*.

Definition 2. *The* affine geometry design of $AG_t(m,q)$ *is the design whose points are the points of $AG(m,q)$, and whose blocks are the t-dimensional affine subspaces of $AG(m,q)$.*

The parameters of $AG_t(m,q)$ are

$$2-\left(q^m, q^t, \begin{bmatrix} m-1 \\ t-1 \end{bmatrix}_q\right).$$

This design has $b = q^{m-t}\begin{bmatrix} m \\ t \end{bmatrix}_q$ blocks, and each point appears in $r = \begin{bmatrix} m \\ t \end{bmatrix}_q$ points. In the binary case, $AG_t(m,2)$ is also a 3-design, with parameters:

$$3-\left(2^m, 2^t, \begin{bmatrix} m-2 \\ t-2 \end{bmatrix}_2\right).$$

The set of cosets of a fixed vector subspace of dimension t in $AG(m,q)$ form a natural parallel class of blocks in $AG_t(m,q)$. Each parallel class in $AG_t(m,q)$ contains q^{m-t} blocks. The design $AG_t(m,q)$ is resolvable, with the sets of natural parallel classes forming the resolution.

Some authors refer to the affine geometry designs with the notation $AG(m,q):t$, $AG_{m,t}(q)$, or $EG(m,q):t$, where EG stands for "Euclidean Geometry". In some works, $EG_t(m,q)$ denotes the design derived from $AG_t(m,q)$ by taking all points except the origin and all blocks not containing the origin. These structures may assist in proving results for the full affine geometry design, and are sometimes interesting in their own right. We will study Euclidean Geometry designs in Chapter 5.

A design with the same parameters as $AG_1(2,q)$ (that is, a 2-$(q^2,q,1)$ design) is referred to as an *affine plane of order q*. The designs created from points and hyperplanes, that is, $AG_{m-1}(m,q)$, are referred to as hyperplane designs. As in the projective case, affine hyperplane designs have been extensively studied – much more so than designs created from subspaces of other dimensions.

Affine geometry designs are closely related to projective geometry designs by the following well-known construction:

Construction 1. *Let H be any hyperplane of $PG(m,q)$. Let $\mathscr{B}$ be the blocks of $PG_t(m,q)$. Then the structure with point set $\mathscr{P}\setminus H$ and block set $\{B\setminus H : B\in\mathscr{B}$ and $B\not\subseteq H\}$ is isomorphic to $AG_t(m,q)$.*

Thus each projective geometry design comes with a "built in" affine geometry design. This result is very helpful in proving results for both projective and affine designs.

1.2.3 The finite geometry codes and their duals

The block codes of finite geometry designs – usually termed the *finite geometry codes* – have many desirable qualities. They are very closely related to generalized Reed-Muller codes. For a more detailed discussion of the links between generalized Reed-Muller codes and the finite geometry codes, see Assmus and Key's seminal book, "Designs and their Codes" [AK92, Chapter 5]. In particular Theorem 5.3.3 (p. 151) and Theorem 5.7.9 (p. 192) give the exact links between generalized Reed-Muller codes and finite geometry codes. A different method of construction is given in [HP03]. In this section, we will only present results which apply directly to the finite geometry codes.

The block codes of $PG_t(m,q)$ and $AG_t(m,q)$ are traditionally taken over $\mathbb{F}_p$, the prime subfield of $\mathbb{F}_q$. The duals of these finite geometry codes are also frequently studied, although their parameters are not as well-known.

We first consider the block codes of projective geometry designs. Let $D = PG_t(m,q)$. Then $C_p(D)$ is a linear code with parameters

$$\left[\frac{q^{m+1}-1}{q-1}, \operatorname{rank}_{\mathrm{p}} D, \frac{q^{t+1}-1}{q-1}\right]_p$$

where $\operatorname{rank}_{\mathrm{p}} D$ denotes the p-rank of the projective geometry design. This rank can be calculated by using an extensive summation formula of Hamada [Ham68] or one of its many simplifications (which will be presented in Chapter 2), but in general there is not a simple formula for $\operatorname{rank}_{\mathrm{p}} D$. The minimum weight words are exactly scalar multiples of the incidence vectors of blocks of D.

The dual projective geometry code $C_p(D)^{\perp}$ has a minimum distance $d^{\perp}$ which is bounded as follows [AK92]:

$$(q+p)q^{m-t-1} \leq d^{\perp} \leq 2q^{m-t} \tag{1.1}$$

The bounds are equal (and thus tight) when $q = p$. This bound has been improved by K. L. Clark and J. D. Key [CK99], for fields of odd characteristic and prime-power order:

$$\frac{4(q^m-1)}{3(q^t-1)} + \frac{2}{3} \leq d^{\perp} \leq 2q^{m-t}. \tag{1.2}$$

If additionally $p \neq 3$, then

$$\frac{3(q^m-1)}{2(q^t-1)} + \frac{1}{2} \leq d^{\perp} \leq 2q^{m-t}. \tag{1.3}$$

When $q = 2^e$ is a power of 2, Calkin, Key, and de Resmini give an exact value [CKdR99]:

$$d^{\perp} = (q+2)q^{m-t-1}. \tag{1.4}$$

A great deal of work has also been done on finding gaps in the weight distribution of $C_p(D)^{\perp}$.

The block codes of affine geometry designs are very similar. Let $D = AG_t(m,q)$. Then $C_p(D)$ is a linear code with parameters

$$\left[q^m, \mathrm{rank_p}\, D, q^t\right]_p$$

As before, $\mathrm{rank_p}\, D$ can be calculated using Hamada's formula [Ham68]. The minimum weight words are exactly scalar multiples of the incidence vectors of blocks of D.

The dual affine geometry code $C_p(D)^{\perp}$ has minimum distance $d^{\perp}$ which is bounded by exactly the same bounds in Equations (1.1) through (1.4). The exact formula for the p-ranks of finite geometry designs will be given in Chapter 2, along with several simplified rank formulas which apply in special cases.

1.2.4 Decoding schemes

Among the reasons for studying the finite geometry codes and their duals are the encoding and decoding schemes associated with them. Suppose that a codeword c has been transmitted over a noisy channel, such that the value of each coordinate in c is changed independently with probability p. When words are transmitted over this *binary symmetric channel*, it is highly likely that errors introduced by the channel could transform the codeword into a vector which is not a codeword. The challenge is then to determine the codeword which was most likely transmitted, given the received word.

Finite geometry codes and their duals admit two particularly good decoding algorithms. Finite geometry codes are particularly amenable to an easy-to-implement decoding method known as *majority logic decoding*. These codes also provide some of the best examples of *low-density parity-check* (or LDPC) codes, which can be decoded by a fast and efficient decoding scheme known as the *sum-product algorithm*. These algorithms both rely on the structure of a code's dual. Thus, to take advantage of the geometric structure of finite geometry codes, we must interpret each finite geometry code as the dual of the code to be decoded. For this reason, the dual of a finite geometry code is often known as a *geometric code*. (See, for example, [AK92].)

The details of majority-logic and sum-product decoding will be described in detail in Chapters 3 and 5, respectively. Here, we briefly describe the history and importance of these algorithms. We first describe a decoding method which defines a baseline of comparison for other decoding algorithms. The traditional decoding method known as *nearest-neighbor decoding* depends on the minimum distance d of a code. If at most $\lfloor (d-1)/2 \rfloor$ errors have occurred in a received vector z, then there is a unique codeword which is "nearest" (in Hamming distance) to z. This guarantees correction of at most $\lfloor (d-1)/2 \rfloor$ errors, and detection of up to $d-1$ errors. Unfortunately, this decoding method can require large amounts of computational resources. As a result, a great deal of effort has been expended to identify faster and simpler decoding schemes which give similar results.

Majority-logic decoding was one of the first efficient decoding schemes to be discovered. The decoding method is easy to implement in hardware, allowing for excellent decoding speed. The idea of majority-logic decoding was first described by Reed [Ree53], in terms of the binary Reed-Muller codes. This was extended by Massey [Mas62], who described a multiple-step decoding procedure which applied to all geometric codes. Smith [Smi67] studied the properties of finite geometry codes and the use of majority-logic decoding with them in great detail, as well as developing a generalized decoding algorithm. This decoding method often guarantees the same level of error-correction as nearest-neighbor decoding, and in some cases, it can correct even more errors than is guaranteed by the minimum distance [Mas62]. The geometric codes are among the best majority-logic decodable codes, and have been used in deep-space communication and telecommunications.

Similarly, the sum-product algorithm is a fast and efficient algorithm which may be implemented in a simple manner. The algorithm makes use of a sparse parity-check matrix – hence codes which satisfy this are given the name *low-density parity-check codes*, or LDPC codes. LDPC codes and the sum-product decoding algorithm were first described in 1963 by Gallager [Gal63], and rediscovered by MacKay and Neal [MN95] in 1995. Since that time, the study of these codes has expanded rapidly. The sum-product algorithm is probabilistic and does not guarantee perfect decoding. However, it does produce excellent practical decoding performance: Many of the codes with the best-known real-world performance are LDPC codes. The geometric codes are classical examples of LDPC codes which admit sum-product decoding, giving excellent results.

The fact that the geometric codes are closely linked to finite geometry designs provides many of their best decoding properties. We will examine the relation between majority-logic decoding and the modified finite geometry designs in Chapter 3, by showing that the block codes of these designs have strong performance under multi-step majority logic decoding. We will demonstrate that the strength of the geometric codes under sum-product decoding extends to a quantum setting in Chapter 5.

1.3 Summary and contributions

Designs and error-correcting codes are two fundamental structures in the study of combinatorics. Finite geometry designs provide some of the most interesting and highly structured examples in both of these fields. This dissertation uses finite geometry designs as a basis for studying a variety of combinatorial objects.

In Chapter 2, we will use affine geometry designs to construct an infinite family of counterexamples to Hamada's conjecture. This provides the first known infinite family of counterexamples in the affine case, and also provides tools which will be used in several other chapters.

Chapter 3 examines the performance of the block codes of these modified geometric designs under majority-logic decoding. The error-correcting performance of these codes is close or equal to the performance of the finite geometry codes on which they are based. The finite geometry codes are some of the best-known codes in this regard, demonstrating a close link between the modified codes and the finite geometry codes.

In Chapter 4, we use relatives of finite geometry designs to construct infinite families of quantum stabilizer error-correcting codes. These codes provide new examples of quantum codes for a wide variety of parameters.

Chapter 5 develops a general theory for constructing a different, more flexible category of quantum error-correcting codes. This chapter demonstrates how Steiner designs – and in particular, certain finite geometry designs – can solve a difficult quantum problem. This gives the first general construction in which the parameters of the resulting codes are fully understood, rather than being partly determined by random choices.

Finally, Chapter 6 summarizes the work in this dissertation, and gives directions for future research.

In each chapter, the structure of finite geometry designs is the basis upon which our results are built.

Chapter 2

Affine geometry designs, polarities, and Hamada's conjecture

In this chapter[*] we examine the history surrounding Hamada's conjecture. We then use affine geometry designs to construct an infinite family of counterexamples to Hamada's conjecture. This provides the first known infinite family of counterexamples in the affine case. The constructions and designs developed here will be used in several other chapters.

2.1 Ranks of incidence matrices and Hamada's conjecture

One of the earliest and most fundamental results in design theory is known as Fisher's inequality: a 2-design with v points and b blocks of size k (where $0 < k < v$) must have $v \leq b$. As a result, the $b \times v$ incidence matrix of any 2-design has at least as many rows as columns. Thus, this simple statement immediately implies that the rank of the incidence matrix is at most v, no matter what field the rank is taken over.

From this point, the study of the ranks of incidence matrices becomes much more complicated. Motivated by the study of the geometric codes and their majority-logic decoding algorithms, a great deal of effort has gone into determining the p-ranks of incidence matrices of geometric designs over various fields.

[*] Sections 2.2 and beyond are reprinted from Journal of Combinatorial Theory, Series A, Volume 18, D. Clark, D. Jungnickel, and V. D. Tonchev: *Affine geometry designs, polarities, and Hamada's conjecture*, 231–239 [CJT11], Copyright 2011, with permission from Elsevier. See permission letter in Appendix C. The article is presented here with an expanded historical review, along with minor editorial changes.

In this section, we will examine historical results concerning the p-ranks of finite geometry designs. This leads naturally to Hamada's conjecture, a key conjecture which motivates the major results of this chapter.

2.1.1 Ranks of Finite Geometry Designs

By Fisher's inequality, any 2-design D satisfies rank $D \leq v$ over any field. In particular, over any field of characteristic 0 (most commonly, $\mathbb{C}$), $\operatorname{rank} D = v$. It is natural to ask about the ranks of incidence matrices when taken over fields of finite characteristic.

Historically, it is most common to study the p-rank of finite geometry designs, where p is the characteristic of the field over which the design was constructed. In the case of pseudo-geometric designs which have the same parameters as a finite geometry design, the rank is taken over the same field $\mathbb{F}_p$ as the geometric design.

To justify this focus on the p-rank, we will examine a result of Hamada. The following result shows that, effectively, the only numbers p over which the p-rank of a design is interesting are those such that $p \mid r - \lambda$. More specifically, we have this result:

Theorem 1 (Hamada [Ham68]). *Let D be a 2-(v,k,λ) design with replication number r. Let p be a prime. Then:*

1. *If $p \nmid r(r-\lambda)$, then* $\mathrm{rank}_\mathrm{p} D = v$.
2. *If $p \mid r$ but $p \nmid r-\lambda$, then* $\mathrm{rank}_\mathrm{p} D \in \{v, v-1\}$.

Only when $p \mid r-\lambda$ may the p-rank be less than $v-1$.

In particular, for a finite geometry design constructed over $\mathbb{F}_q$ where $q = p^e$, we have $p \mid r - \lambda$. It is possible that other primes may divide $r - \lambda$. However, the work of Mortimer [Mor80] and Frumkin and Yakir [FY90] shows that such primes will not produce interesting codes. In fact, such codes are typically trivial, consisting of the entire vector space, or else consist of all of the even-weight words in the vector space. Thus, we will focus on the p-rank of $PG_t(m, p^e)$ and $AG_t(m, p^e)$.

The ranks of the finite geometry designs have been studied since the 1950's, due to interest in the dimensions of these majority-logic decodable codes. The p-rank of a geometric projective plane of order q was first given by Graham and MacWilliams [GM66] (1966) and independently by Weldon [Wel67] (1967):

Theorem 2 (Graham and MacWilliams [GM66], Weldon [Wel67])**.** *For the geometric projective plane,*

$$\operatorname{rank}_{\mathrm{p}} PG_1(2, p^e) = \binom{p+1}{2}^e + 1.$$

Note that projective planes can be viewed as hyperplane designs: lines are hyperplanes in a 2-dimensional projective geometry. This result was generalized by Smith [Smi67] in his 1967 dissertation, and later in a 1969 paper [Smi69] which thoroughly introduced the codes and dimensions obtained from finite geometries:

Theorem 3 (Smith [Smi67], [Smi69])**.** *For the classical projective geometry design of points and hyperplanes,*

$$\operatorname{rank}_{\mathrm{p}} PG_{m-1}(m, p^e) = \binom{p+m-1}{m}^e + 1.$$

This result was found independently, using different methods, by Goethals and Delsarte [GD68] in 1968, and MacWilliams and Mann [MM68] (also in 1968, with extensive use of character theory) and conjectured by Rudolph [Rud67] in 1967.

MacWilliams and Mann also provided this result for a design closely related to affine geometries:

Theorem 4 (MacWilliams and Mann [MM68])**.** *For the incidence structure D of points other than the origin and hyperplanes not containing the origin in an affine geometry,*

$$\operatorname{rank}_{\mathrm{p}} D = \binom{m+p-1}{m}^e - 1.$$

The grandfather of rank formulas was found by Hamada in 1968 [Ham68] using an extension of the methods of Smith [Smi67]. Hamada also found a slightly simplified version of this formula in 1973 [Ham73], which we present below.

Theorem 5 (Hamada [Ham68, Ham73])**.** *The p-rank of $PG_t(m, p^e)$ is exactly:*

$$\sum_{(s_0, s_1, \ldots, s_e)} \prod_{j=0}^{e-1} \sum_{i=0}^{L(s_{j+1}, s_j)} (-1)^i \binom{m+1}{i} \binom{m + s_{j+1}p - s_j - ip}{m}$$

where the sum is taken over all ordered sets $(s_0, s_1, \ldots, s_e)$ *such that* $s_0 = s_e$, $s_j \in \mathbb{Z}$ *such that* $t+1 \leq s_j \leq m+1$ *and* $0 \leq s_{j+1}p - s_j \leq (m+1)(p-1)$, *and where*

$$L(s_{j+1}, s_j) = \left\lfloor \frac{s_{j+1}p - s_j}{p} \right\rfloor.$$

Hamada also provided several formulas for variations on $AG_t(m,q)$ (such as the incidence matrix of points and t-flats not through the origin), as well as the following useful relation for the full affine case:

Theorem 6 (Hamada [Ham68])**.** *The affine geometry design* $AG_t(m,q)$ *satisfies:*

$$\mathrm{rank_p} AG_t(m,q) = \mathrm{rank_p} PG_t(m,q) - \mathrm{rank_p} PG_t(m-1,q)$$

These summation formulas give the ranks of all projective and affine geometry designs. However, these formulas require the calculation of many parameters, and are difficult to work with. Thus, much effort has been expended in finding simpler formulas for specific cases.

Hamada provided several simplifications, including a result identical to Smith (Theorem 3). Hamada also proved these results (which also follow from Theorem 3):

Corollary 1 (Hamada [Ham68])**.**

$$\mathrm{rank_p} AG_{m-1}(m, p^e) = \binom{m+p-1}{m}^e.$$

Corollary 2 (Hamada [Ham68])**.**

$$\mathrm{rank_p} AG_t(m,2) = \sum_{s=0}^{m-t} \binom{m}{s}.$$

In 1979, Sachar found a formula for the p-rank of *all* projective planes of prime order, which includes the geometric plane $PG_1(2,p)$:

Theorem 7 (Sachar [Sac79])**.** *Let* P *be a* 2-$(p^2+p+1, p+1, 1)$ *design over* $\mathbb{F}_p$, *where* p *is a prime. Then* $\mathrm{rank_p} P = (p^2+p+2)/2$.

Notice also that this result is an equality, not an inequality: *all* projective planes (geometric or not) have the same rank. This relates to the "Hamada-Sachar conjecture," (Conjecture

4, to be discussed in Subsection 2.1.2) which conjectures that geometric projective planes are the unique designs with minimum rank, among all projective planes of the same order. The truth of the Hamada-Sachar conjecture together with this theorem would therefore show that the only projective planes of prime order are geometric. This result extends an earlier result of Assmus, Mattson, and Guza [AMG74] (1974), who produced the same rank formula for projective planes of order n, where $n \equiv 2 \pmod 4$ (including, at the time, a putative plane of order 10).

In some cases, the ranks of designs over a prime order field prove easier to find than those over a prime-power field. We present several results in this vein:

Theorem 8 (Key and Mackenzie [KM91], 1991)**.** *For an affine geometry design whose blocks have half the dimension of the vector space, over a prime field,*

$$\mathrm{rank_p} AG_t(2t,p) = \sum_{i=0}^{t-1} (-1)^i \binom{2t}{i} \binom{t+(t-i)p}{2t}.$$

Theorem 9 (Hirschfeld and Shaw [HS94], 1994)**.** *For a projective geometry design over a prime field,*

$$\mathrm{rank_p} PG_t(m,p) = \frac{p^m+1}{p-1} - \sum_{i=0}^{t-1} (-1)^i \binom{(t-i)(p-1)-1}{i} \binom{t+(t-i)p}{m-i}.$$

The special case of this formula for $t=1$ was also found by Ceccherini and Hirschfeld [CH92] in 1992. All of these are summarized in a survey by Assmus and Key [AK99].

Finally, a simplified formula has also been extracted for lines in affine geometry designs over a prime field:

Theorem 10 (Assmus and Key [AK99])**.** *For the affine geometry design of points and lines over a prime field,*

$$\mathrm{rank_p} AG_1(m,p) = p^m - \binom{m+p-2}{m}.$$

In the case that $p=3$, $AG_1(m,3)$ is a Steiner triple system. Thus, a simplified version of this result was used in [DHV78].

Finally, in 1999, Calkin, Key, and de Resmini [CKdR99] proved that the p-rank of any projective geometry design (and hence affine geometry designs as well) is a polynomial function in the dimension of the geometry:

Theorem 11 (Calkin, Key, and de Resmini [CKdR99])**.** *The p-rank of $PG_t(m,q)$ is given by*

$$\mathrm{rank_p}\, PG_t(m,q) = \frac{q^{m+1}-1}{q-1} - h(m)$$

where, for any fixed value of t, $h(m)$ is a polynomial in m of degree $(q-1)t$.

A number of additional results on p-ranks are given in various proofs of special cases of Hamada's conjecture, which will be covered in the next subsection.

2.1.2 Hamada's conjecture

Hamada's extensive work on the ranks of projective and affine geometric designs resulted in several papers [Ham68, Ham73] which brought together several special results and established the basic formulas for ranks of these designs. Near the end of Part 1 of [Ham73], Hamada presents several tables of pseudo-geometric designs, together with their p-ranks, where p is the characteristic of the field used in constructing the corresponding finite geometry design. The only designs of minimum rank in these tables are the geometric designs. Hamada made the following comment: "This suggests that the p-rank of the BIB design $PG(t,q)$: μ or $EG(t,q)$: μ might be, in general, minimum in BIB designs with the same parameters." This conjecture is usually restated in the following manner:

Conjecture 1 (Hamada [Ham68, Ham73], strong version)**.** *Let G be a geometric design over $\mathbb{F}_q$ ($q = p^e$ a prime power), and let D be any design with the same parameters as G. Then* $\mathrm{rank_p}\, D \geq \mathrm{rank_p}\, G$ *with equality if and only if D is isomorphic to G.*

Hamada's conjecture is important for several reasons. First, Hamada's conjecture suggests that the codes whose parity check matrices are given by the incidence matrices of finite geometry designs have maximum dimension among all codes obtained from designs with the same parameters. This indicates that these duals are the best possible choices for majority-logic decoding, among all codes with the same parameters. In addition, Hamada's conjecture indicates that the p-rank may be a simple and useful invariant which distinguishes the finite geometry designs from pseudo-geometric designs. The p-rank of an incidence matrix may be calculated in polynomial time, and is considerably easier than the question of design isomorphism, which is known to be as hard as the notoriously difficult question of graph isomorphism. Finally, the truth of Hamada's conjecture would immediately solve the famous and long-open question of whether there exist non-geometric projective planes of prime order.

We will separate Hamada's conjecture into a "strong" and a "weak" version. The strong version is as stated above. The weak version drops the requirement of uniqueness:

Conjecture 2 (Hamada [Ham68, Ham73], weak version)**.** *The p-rank of a finite geometry design is the minimum p-rank among all designs with the same parameters.*

The strong version of Hamada's conjecture is known to be false in general, as there exist pseudo-designs with the same parameters and p-ranks as finite geometry designs, but which are not themselves geometric. However, no counterexamples have been found to the weak version. That is, there are no known pseudo-geometric designs with a *lower* p-rank than the corresponding finite geometry designs. In fact, the truth of the weak version is completely unknown, except in a few cases in which the strong version has also been proved. In this review, references to Hamada's conjecture will always mean the strong version unless otherwise specified.

Because of the properties of the relatively small number of known counterexamples, a restricted version of Hamada's conjecture was made by Assmus:

Conjecture 3 (Assmus, cf [Ton99])**.** *The strong form of Hamada's conjecture is true for the designs of points and hyperplanes in a projective or affine geometry.*

However this too has been shown to be false in general, as will be shown later. Finally, another version of the conjecture was made independently by Sachar [Sac79]:

Conjecture 4 (Hamada-Sachar [Sac79])**.** *The strong form of Hamada's conjecture is true for $PG_1(2,q)$.*

Note that $PG_1(2,q)$ is a projective plane, and so this conjecture may be restated as: the p-rank of any projective plane of order q is at least $\mathrm{rank_p}\, PG_1(2,q)$, with equality if and only if the plane is desarguesian. This is considered to be a particularly important conjecture (see, for example, [AK66]). Together with Sachar's result on the p-rank of projective plans of prime order (Theorem 7), the conjecture's truth would imply that the only projective planes of prime order are the classical geometric planes.

2.1.3 Proved cases

This section will survey the cases in which Hamada's conjecture is known to be true. Hamada's extensive original papers [Ham68, Ham73] on the topic of the ranks of incidence matrices of designs did not prove the conjecture in any cases. However, they did provide a large amount of computational evidence supporting the conjecture. The first proof of a particular case came from Hamada and Ohmori [HO75] in 1975, who proved the strong version of the conjecture for the binary hyperplane designs:

Theorem 12 (Hamada, Ohmori [HO75])**.** *The strong form of Hamada's conjecture is true for $PG_{m-1}(m,2)$ and $AG_{m-1}(m,2)$. In particular:*

1. *For any design D with the same parameters as $PG_{m-1}(m,2)$, $\text{rank}_2(D) \geq m+2$ with equality if and only if D is isomorphic to $PG_{m-1}(m,2)$.*
2. *For any design D with the same parameters as $AG_{m-1}(m,2)$, $\text{rank}_2(D) \geq m+1$ with equality if and only if D is isomorphic to $AG_{m-1}(m,2)$.*

The approach used by Hamada and Ohmori was, partly, to identify a unique subcode contained within the block code of the complement of any pseudo-geometric design of minimum rank. This approach was extended by Tonchev [Ton99], a result which will be discussed later in this section.

The next progress appeared in 1978, when Doyen, Hubaut, and Vandensavel [DHV78] proved the conjecture for certain Steiner designs which are equivalent to geometric designs:

Theorem 13 (Doyen, Hubaut, Vandensavel [DHV78])**.** *The strong form of Hamada's conjecture is true for $PG_1(m-1,2)$ and $AG_1(m,3)$. In particular:*

1. *For any design D with the same parameters as $PG_1(m-1,2)$, $\text{rank}_2(D) \geq 2^m - m - 1$ with equality if and only if D is isomorphic to $PG_1(m-1,2)$.*
2. *For any design D with the same parameters as $AG_1(m,3)$, $\text{rank}_3(D) \geq 3^m - 1 - m$ with equality if and only if D is isomorphic to $AG_1(m,3)$.*

The authors phrase these results in terms of Steiner triple systems. In particular, the paper gives results for $STS(2^m-1)$ and $STS(3^m)$, which have parameters of $PG_1(m,2)$ and $AG_1(m,3)$, respectively.

The authors obtain their results by identifying substructures (called projective or affine "hyperplanes") in pseudo-geometric designs, which are isomorphic to smaller projective spaces. By showing that only the finite geometry designs contain the *largest* possible structure of projective hyperplanes, the uniqueness is established.

Two years later, in 1980, Teirlinck proved Hamada's conjecture for the case of planes in a binary affine design. This theorem summarizes his result, based on the presentation of Dehon [Deh80] in terms of finite geometries:

Theorem 14 (Teirlinck [Tei80])**.** *The strong form of Hamada's conjecture is true for the design $AG_2(m,2)$. In particular, for any design D with the same parameters as $AG_2(m,2)$,* $\operatorname{rank}_2(D) \geq 2^m - 1 - m$ *with equality if and only if D is isomorphic to $AG_2(m,2)$.*

Teirlinck's results extend the method used in [DHV78] (see also [Deh80]), by finding the "projective dimension" of a substructure contained in each quadruple system. However, Teirlinck's results are not stated in the language of geometric designs and ranks, nor does he mention Hamada's conjecture. Note that $AG_2(m,2)$ is a 3-$(2^m,4,1)$ design, also known as a Steiner quadruple system and denoted $SQS(2^m)$.

There have also been several partial proofs of Hamada's conjecture. That is, there are proofs that certain geometric designs are the unique designs with minimum p-rank among a more restricted set of designs.

A paper of Tonchev and Lam [LT96], [LT00] (1996) provides support for Hamada's conjecture. The authors completely classify *affine resolvable* 2-$(27,9,4)$ designs, these being the parameters of $AG_2(3,3)$, and find that only the classical design has minimum rank. An affine resolvable design is a resolvable design which possesses a unique resolution, in which each pair of non-parallel blocks intersect in a constant number of points. This does not completely finish this case, however, as a design with such parameters need not be affine resolvable.

A paper of Sarami and Tonchev [ST08] (2008) also provides support, by showing that the only cyclic quasi-symmetric design with the same parameters and block intersection numbers as $PG_3(5,2)$ is the finite geometry design. Again, although these are the properties of the geometric design, they need not be the properties of other designs with the same parameters.

Azzam, Clark, and Tonchev [ACT09] (2008) searched for cyclic codes and extensions with the same parameters and weight distributions as the codes of certain finite geometry designs, whose extended codes are self-orthogonal (as are the Reed-Muller codes in these cases). The results of their search did not produce any new codes besides the known Reed-Muller codes. Thus the authors provide evidence supporting Hamada's conjecture in the following cases: $PG_4(6,2)$, $PG_3(6,2)$, $PG_5(7,2)$, $AG_5(7,2)$, $AG_4(7,2)$, and $AG_6(8,2)$.

More recently, a new category of Hamada-type results has appeared under modified conditions. These results are based on a generalization of the concept of the "dimension" of a design, first proposed by Tonchev in 1999 [Ton99]. In fact, the results cited below are the first characterizations of the geometric designs which are fully based in coding theory. The first generalized definition of "dimension" is given below:

Definition 3 (Tonchev [Ton99])**.** *The* dimension *of a t-(v,k,λ) design D over $\mathbb{F}_q$, denoted dim(D), is the minimum dimension among all linear codes of length v over $\mathbb{F}_q$ whose code words of weight k support the blocks of D.*

This definition is based on the idea that words in a code may *support* the blocks of a design without being *equal* to the incidence vectors of those blocks. Instead, the words which support the design may have any nonzero elements from $\mathbb{F}_q$ in their nonzero positions. Hamada's conjecture extends naturally to this definition. Using this definition, Tonchev proved that the following Hamada-type results:

Theorem 15 (Tonchev [Ton99])**.** *The strong form of Hamada's conjecture (with dimension as in Definition 3) is true for the complementary design of $PG_{m-1}(m,q)$ and for the complementary design of $AG_{m-1}(m,q)$. In particular:*

1. *For any design D with the same parameters as the complement of $PG_{m-1}(m,q)$, dim$(D) \geq m+1$ with equality if and only if D is isomorphic to the complementary design of $PG_{m-1}(m,q)$.*
2. *For any design D with the same parameters as the complement of $AG_{m-1}(m,q)$, dim$(D) \geq m+1$ with equality if and only if D is isomorphic to the complementary design of $AG_{m-1}(m,q)$.*

Here the complementary design is the design whose blocks are the complements of the blocks in the original design.

A similar result in the spirit of Hamada's conjecture was also proved by Tonchev in 2003 [Ton03] using the generalied dimension as in Definition 3. This result covers "complete" designs, that is, designs whose blocks consist of all k-subsets of their points. These designs have parameters k-$(n,k,1)$.

Theorem 16 (Tonchev [Ton03])**.** *The dimension (as in Definition 3) over $\mathbb{F}_q$ of a complete design is at least $n-k+1$, with equality if and only if a $[n,n-k+1,k]_q$ code exists.*

Such a code is called a *Maximum Distance Separable* (or *MDS*) code, and its existence is closely related to the existence of certain substructures in projective geometries.

The concept of generalized dimension was further generalized and extended by Jungnickel and Tonchev in a series of two papers [JTa, JTb]. We will require a few preliminary concepts. The *trace code* of a code C over $\mathbb{F}_{q^t}$ is a code over $\mathbb{F}_q$ obtained from C by applying the trace map from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ coordinate-wise: $Tr(x) = x + x^2 + \cdots + x^{q^{t-1}}$. Similarly, an $\mathbb{F}_{q^t}$-incidence matrix is an incidence matrix in which the nonzero coordinates have been replaced by nonzero elements of $\mathbb{F}_{q^t}$. Note that there are many possible $\mathbb{F}_{q^t}$-incidence matrices for the same design.

Definition 4 (Jungnickel and Tonchev [JTa, JTb]). *Let D be the complement of a finite simple incidence structure, and let $E = \mathbb{F}_{q^t}$ be an extension field of $\mathbb{F}_q$. Let M be an incidence matrix for D. Then the* q-dimension *of D is the smallest dimension of any $\mathbb{F}_q$-linear code which arises as the trace code of M, where E runs over all finite extensions of $\mathbb{F}_q$, and M runs over all E-incidence matrices of D.*

As with the original definition, the code spanned by an E-incidence matrix may contain words which *support* the blocks of a design without being *equal* to the incidence vectors of the blocks. Jungnickel and Tonchev used this concept of q-dimension to produce Hamada-type results for the complements of projective geometry designs:

Theorem 17 (Jungnickel, Tonchev [JTa]). *Let D be a design with the parameters of the complement of $PG_t(m,q)$ or $AG_t(m,q)$. Then the q-dimension of D is at least $m+1$, with equality if D is the complement of a geometric design.*

The authors also give a result which proves the equivalent of the strong version of Hamada's conjecture for certain designs, under the q-dimension:

Theorem 18 (Jungnickel, Tonchev [JTa]). *Let D be a design with the parameters of the complement of $PG_t(m,q)$ (for $1 \leq t \leq m-1$) or $AG_t(m,q)$ (for $t = 1$ or $(m-2)/2 \leq t \leq m-1$). If the q-dimension of D is $m+1$, then D is the complement of the corresponding geometric design.*

These results generalize the work of Tonchev [Ton99], which applied specifically to complements of hyperplane designs, and which in turn generalized the results of Hamada and Ohmori [HO75]. However, these results are special cases of a much more general result which applies to more general structures [JTb]. Thus, it seems that the idea of q-dimension is a very promising development, and will hopefully produce further Hamada-type characterizations in the future.

To summarize, the strong form of Hamada's conjecture is known to be true for the following geometric designs: $PG_{m-1}(m,2)$ and $AG_{m-1}(m,2)$, $PG_1(m,2)$ and $AG_1(m,3)$, $AG_2(m,2)$, and finally, a modified form of the conjecture is true for the complementary designs of

$PG_t(m,q)$ (for $1 \leq t \leq m-1$) and $AG_t(m,q)$ (for $t = 1$ or $(m-2)/2 \leq t \leq m-1$), using the modified definition of “dimension” as in [JTb]. As a special case, we note that Hamada’s conjecture is true for all designs obtained from $PG(m-1,2)$ or $AG(m,2)$ for $m \leq 4$.

2.1.4 Counterexamples

The strong form of Hamada’s conjecture has been shown to be false in general. As of this writing, all known counterexamples provide examples of pseudo-geometric designs with the *same* p-rank as geometric designs, but which are not isomorphic to the geometric designs. However, there are no known pseudo-geometric designs which have a *lower* rank than the geometric designs. Thus the strong version of Hamada’s conjecture is false, but the weak version remains unknown.

The first counterexample to Hamada’s conjecture appeared in a paper of Goethals and Delsarte [GD68] from 1968, and was published before Hamada made his conjecture. The paper describes a class of majority-logic decodable codes. The dual of one such code is a $[31,16]$ binary code which supports a design with the same parameters and 2-rank as $PG_2(4,2)$, but which is not isomorphic. This result was generalized by Tonchev [Ton86] in 1986:

Theorem 19 (Tonchev [Ton86])**.** *There exist exactly five nonisomorphic quasi-symmetric designs with the parameters of $PG_2(4,2)$. The extensions of these designs are nonisomorphic and have the parameters of $AG_3(5,2)$. All of these designs have 2-rank 16, the same as the respective finite geometric designs.*

This result is a consequence of the classification of extremal doubly-even $[32,16]$ binary codes. *Extremal* codes are those with the largest possible minimum distance, and *doubly-even codes* contain only codewords whose weights are multiples of 4. The minimum weight words of these codes may support a pseudo-geometric design. The 2-ranks of all such designs obtained from these extremal doubly-even codes are equal (because the codes have the same dimension), but designs obtained from nonisomorphic codes are themselves nonisomorphic. This classification also implies a classification of self-orthogonal 3-$(32,8,7)$ designs, where *self-orthogonal* indicates that the intersection of any two blocks is even.

For many years, the designs from [Ton86] were the only known counterexamples. The next examples were produced by Harada, Lam, and Tonchev [HLT05] in 2005:

Theorem 20 (Harada, Lam, Tonchev [HLT05])**.** *There exist at least two designs with the same parameters and 2-rank as $AG_2(3,4)$, which are not geometric.*

This result follows from a computer search enumerating all symmetric $(4,4)$-nets. A *symmetric net* is a symmetric 1-design with additional structural properties. The words of weight 16 in the block code of some symmetric $(4,4)$-nets support 2-$(64,16,5)$ designs. These are the parameters of $AG_2(3,4)$. Among the nets which the authors discovered were three nets with 2-rank 16. The codes generated by these nets support three non-isomorphic 2-$(64,16,5)$ designs with 2-rank 16, only one of which is isomorphic to $AG_2(3,4)$.

These designs are also the first and (currently) only counterexamples to the Assmus conjecture. In addition, these were, at the time, the only known counterexamples not constructed over the binary field, and remain the only counterexamples over a field of non-prime order.

The counterexamples found by Harada, Lam, and Tonchev have been found in other contexts. In 2008, Mavron, McDonough, and Tonchev [MMT08] found one of the counterexamples using *line spreads* in $PG(5,2)$. A *line* in a design is the intersection of all blocks containing a given pair of points. A *line spread* is a set of lines which partition the points of the design. A construction due to Rahilly [Rah91] produces affine resolvable 2-designs from certain symmetric 2-designs whose duals contain a line spread. Using this technique on spreads in the dual of $PG(5,2)$, one of the counterexamples of [HLT05] was found. In 2009, Mateva and Topalova [MT09b] completely enumerated the spreads in $PG(5,2)$, confirming that the single counterexample found by Mavron, McDonough, and Tonchev is the only counterexample to be found by this construction in $PG(5,2)$. Also in 2009, Mateva and Topalova [MT09a] constructed 2-$(63,31,15)$ designs invariant under the group D_{10} and created designs with the parameters of $AG_2(3,4)$ using Rahilly's construction. They found all three known designs of minimum rank (the geometric design and two special designs), but no others.

In 2008, Clark and Tonchev [CT09] identified the two counterexamples from [HLT05] as designs supported by the minimum-weight codewords of the Reed-Muller code $R(2,6)$. The paper also proves that this technique may be extendable to larger Reed-Muller codes.

The most important recent results concerning Hamada's conjecture come from two papers, in which Jungnickel and Tonchev [JT09], and later Clark, Jungnickel, and Tonchev [CJT11], discovered two infinite classes of counterexamples to the conjecture.

Theorem 21 (Jungnickel, Tonchev [JT09])**.** *For any prime p and $t \geq 2$, there exists a design with the same p-rank and parameters as $PG_t(2t,p)$ which is not isomorphic to $PG_t(2t,p)$.*

Theorem 22 (Clark, Jungnickel, Tonchev [CJT11])**.** *For any $t \geq 1$, there exists a design with the same 2-rank and parameters as $AG_{t+1}(2t+1,2)$ which is not isomorphic to $AG_{t+1}(2t+1,2)$.*

The paper of Jungnickel and Tonchev [JT09] constructs counterexamples by modifying the blocks of $PG_t(2t,p)$, where p is a prime. All blocks which intersect a fixed hyperplane of the geometry, but which are not contained in it, are modified by permuting the parts contained in the hyperplane. By using a polarity of the projective geometry induced on the hyperplane for this permutation, the modified design retains the same p-rank. This construction produces exactly one of the nongeometric 2-$(31,7,7)$ designs from [Ton86]. Munemasa and Tonchev [MT] recently showed that the block graph of these *polarity designs* is a distance-regular graph which is isomorphic to the twisted Grassmann graph of van Dam and Koolen [vDK05].

The results of Clark, Jungnickel, and Tonchev [CJT11] extend these methods to the affine setting in the binary case. These results are contained in the remainder of this chapter.

In summary, counterexamples exist only for the strong form of Hamada's conjecture. Several sporadic counterexamples are known, some of which have been generalized into infinite classes. The parameters of counterexamples are those of the designs $PG_2(4,2)$, $AG_3(5,2)$, $AG_2(3,4)$, plus infinite classes with the parameters of $PG_t(2t,p)$ for p prime, and $AG_{t+1}(2t+1,2)$.

The remainder of this chapter consists of the original paper by Clark, Jungnickel, and Tonchev [CJT11] which provides the first infinite class of counterexamples to the affine case of Hamada's conjecture.

2.2 Introduction

Let X be a set of v *points*, and B be a collection of k-subsets of X called *blocks*. Then $D=(X,B)$ is a t-(v,k,λ) *design* or *block design* if every t-subset of X is contained in exactly λ blocks. Two designs $D_1=(X_1,B_1)$ and $D_2=(X_2,B_2)$ are *isomorphic* if there is a bijection from X_1 to X_2 which maps B_1 to B_2. The *automorphism group* of D is the subgroup of $\mathrm{Sym}(X)$ whose action on X preserves B.

If v is divisible by k, a *parallel class* of D is a set of v/k blocks which partition X. If B can be partitioned into disjoint parallel classes, then D is said to be *resolvable*, and any particular partition is called a *resolution*.

The *incidence matrix* of D is a $v \times b$ matrix $A=(a_{ij})$ where $a_{ij}=1$ if point i of X is contained in block j of B, and 0 otherwise. The rows of A^T are the incidence vectors of the blocks of D. The span of the rows of this matrix is a linear error-correcting code called the *block code* of D.

Classical examples of designs are obtained from finite geometries. We construct these geometries using the n-dimensional vector space V over a finite field $GF(q)$. The $(n-1)$-dimensional *projective geometry* $PG(n-1,q)$ over $GF(q)$ has as points the 1-dimensional subspaces of V. Its lines are the 2-dimensional subspaces of V, and in general the d-dimensional projective subspaces are the $(d+1)$-dimensional subspaces of V. Taking the d-dimensional projective subspaces of $PG(n-1,q)$ as blocks, we obtain a design denoted by $PG_d(n-1,q)$ with parameters

$$v = \frac{q^n-1}{q-1},\ k = \frac{q^{d+1}-1}{q-1},\ \lambda = \begin{bmatrix} n-2 \\ d-1 \end{bmatrix}_q,$$

where $\begin{bmatrix} n-2 \\ d-1 \end{bmatrix}_q$ is the Gaussian coefficient given by

$$\begin{bmatrix} n-2 \\ d-1 \end{bmatrix}_q = \frac{(q^{n-2}-1)(q^{n-3}-1)\cdots(q^{n-d}-1)}{(q^{d-1}-1)(q^{d-2}-1)\cdots(q-1)}.$$

Similarly, the n-dimensional *affine geometry* $AG(n,q)$ over $GF(q)$ has as points the vectors of V. Its lines are the 1-dimensional subspaces of V and their cosets, and in general the d-dimensional affine subspaces are the d-dimensional subspaces of V and their cosets. Taking the d-dimensional affine subspaces of $AG(n,q)$ as blocks, one obtains a design denoted by $AG_d(n,q)$ with parameters

$$v = q^n,\ k = q^d,\ \lambda = \begin{bmatrix} n-1 \\ d-1 \end{bmatrix}_q.$$

This design is resolvable: the set of all cosets of a vector subspace forms a natural parallel class.

For further terminology and results on designs, see [BJL99].

Let q be a prime power and $\Pi = PG_d(2d,q)$, $d \geq 2$. Let $H \simeq PG(2d-1,q)$ be a hyperplane in $PG(2d,q)$, and let α be a polarity [Hir98] of H. A block B of Π is either contained in H or intersects H in a $(d-1)$-subspace. It was proved by Jungnickel and Tonchev in [JT09] that replacing each $(d-1)$-subspace $B \cap H$ by $\alpha(B \cap H)$ yields a design $\alpha(\Pi)$ having the same parameters and block intersection numbers as $PG_d(2d,q)$. In addition, if q is prime, $\alpha(\Pi)$ has the same q-rank as $PG_d(2d,q)$, thus providing a counterexample to the "only if" part of Hamada's conjecture [Ham68], which states that a design with the parameters of $PG_d(n,q)$ or $AG_d(n,q)$ is geometric if and only if it has minimum q-rank among all designs with the given parameters.

It was proved recently by Munemasa and Tonchev [MT] that the block graph of the design obtained from $PG_d(2d,q)$ via the construction of Jungnickel and Tonchev [JT09], where two blocks are adjacent if they share $(q^d-1)/(q-1)$ points, is a distance-regular graph isomorphic to the twisted Grassmann graph discovered by van Dam and Koolen [vDK05].

In this paper, we show that the construction from [JT09] can be extended to yield an infinite family of non-geometric designs with the same parameters, intersection numbers, and 2-rank as the affine geometry design $\mathscr{A}$=$AG_{d+1}(2d+1,2)$ having as blocks the $(d+1)$-dimensional subspaces of the binary affine space $AG(2d+1,2)$, for any $d \geq 2$. This provides the first known infinite family of counterexamples to the “only-if”-part of Hamada's conjecture in the affine case. This work was motivated by the smallest example ($d=2$), which corresponds to one of the four non-geometric self-orthogonal 3-$(32,8,7)$ designs [Ton86] of 2-rank 16.

Let $\mathscr{A} = AG_{d+1}(2d+1,2)$. Then $\mathscr{A}$ is a 3-(v,k,λ_3) design with parameters

$$v = 2^{2d+1},\ k = 2^{d+1},\ \lambda_3 = \frac{(2^{2d-1}-1)\dots(2^{d+1}-1)}{(2^{d-1}-1)\cdots(2-1)} = \begin{bmatrix} 2d-1 \\ d-1 \end{bmatrix}_2. \tag{2.1}$$

The number of blocks containing a pair of points of $\mathscr{A}$ is given by

$$\lambda_2 = \frac{2^{2d+1}-2}{2^{d+1}-2}\lambda_3 = \begin{bmatrix} 2d \\ d \end{bmatrix}_2,$$

while the number of blocks containing a single point of $\mathscr{A}$ is equal to

$$\lambda_1 = \frac{2^{2d+1}-1}{2^{d+1}-1}\lambda_2 = \begin{bmatrix} 2d+1 \\ d+1 \end{bmatrix}_2.$$

Let X denote the point set of $\mathscr{A}$, and let $\bar{0} \in X$ be the point of $AG(2d+1,2)$ that corresponds to the zero vector in $GF(2)^{2d+1}$. The collection of blocks of $\mathscr{A}$ which contain $\bar{0}$ induces on $X \setminus \{\bar{0}\}$ a 2-$(2^{2d+1}-1, 2^{d+1}-1, [{2d-1 \atop d-1}]_2)$ design D_0 isomorphic to $PG_d(2d,2)$.

Let $H \subset X$ be a set of 2^{2d} points such that $\bar{0} \in H$, and H is a $2d$-subspace of $AG(2d+1,2)$. Then H is a hyperplane of $\mathscr{A}$. Note that H is a linear subspace of $\mathscr{A}$. A block B which intersects H in a d-dimensional affine subspace will be called a *cross* block. Note that $|B \cap H| = |B \setminus H| = 2^d$. We will write $B = B_{out} \cup B_{in}$, where $B_{out} = B \setminus H$ and $B_{in} = B \cap H$. We refer to B_{out} as the *outer* part of B, and B_{in} as the *inner* part. Note that $B_{out} \cap B_{in} = \emptyset$.

All blocks of $\mathscr{A}$ have 2^d translates (or cosets) in the group of translations of $\mathscr{A}$. For a cross block B, these translates may be written as $\{B+h_i | h_i \in H\}$. That is, the group of translations of H is enough to produce all translates of B within $\mathscr{A}$. Note that for any cross block B, any translate also intersects H in exactly 2^d points.

In addition, for any cross block $B = B_{out} \cup B_{in}$ of $\mathscr{A}$, B_{out} is a translate of B_{in} by an element of $X \setminus H$. As a result, the set $\{B' \setminus H | B' \cap H = B_{in}\}$ consists of a partition of $X \setminus H$ into translates. Similarly, $\{B' \cap H | B' \setminus H = B_{out}\}$ partitions H into translates.

With this in mind, we present the following construction, which extends the construction of [JT09] to certain binary affine geometries.

Construction 2. With H as above, let α be a permutation of the affine d-subspaces through $\bar{0}$, of the affine space $AG(2d,2)$ induced on H.

Using α, we make the following alterations to the blocks of $\mathscr{A}$:

- If B is a block such that $B \subset H$ or $B \cap H = \emptyset$, we leave B unchanged.
- If $|B \cap H| = 2^d$ and $\bar{0} \in B$, we replace the inner part B_{in} of B by $\alpha(B_{in}) = \alpha(B \cap H)$.
- If $|B \cap H| = 2^d$ and $\bar{0} \notin B$, there is a block B_1 such that $\bar{0} \in B_1$, $|B_1 \cap H| = 2^d$, and $B \cap H$ is a translate (or coset) of $B_1 \cap H$ in the group of translations of H, by considering H as a $2d$-dimensional vector space. Let $\{h_1 = \bar{0}, h_2, \ldots, h_{2^d}\}$ be 2^d distinct elements of H such that:
    - Each coset of B_1 is represented exactly once in the set $\{B_1 + h_i | i = 1, \ldots, 2^d\}$, and
    - Each coset of $\alpha(B_1 \cap H)$ is represented exactly once in the set $\{\alpha(B_1 \cap H) + h_i | i = 1, \ldots, 2^d\}$.

  Such a set of h_i exists by Hall's matching theorem [Die05], see Lemma 1 below.

  Let $B_2, B_3, \ldots, B_{2^d}$ be all other blocks such that $B_i \cap H = B_1 \cap H$. Note that the outer part of B_i is a translate of the outer part of B_1 by an element $h \in H$, and that $\bar{0} \in B_i$ for each $1 \leq i \leq 2^d$. In particular, each coset of B_i may be represented as $B_i + h_j$ for some $1 \leq j \leq 2^d$. We replace the part of B_i equal to $B_i \cap H$ with $\alpha(B_i \cap H)$, for $1 \leq i \leq 2^d$. For the coset of B_i equal to $B_i + h_i$, we replace the part equal to $(B_i + h_i) \cap H$ with $\alpha(B_i \cap H) + h_i$.

Notice that this construction effectively permutes the inner parts of all cross blocks, including those which are translates. The construction guarantees that the multiset of inner portions of cross blocks is preserved.

For a cross block $B = B_{out} \cup B_{in}$, we will write $\alpha(B) = B_{out} \cup \alpha(B_{in})$ to represent the "distorted" block produced by the construction. Note that writing the block this way makes sense, because the construction does not touch the outer parts of cross blocks.

The following technical lemma is necessary to show the correctness of the construction. It will also provide the basis for a related construction over any finite field. Note that our original definition of a cross block extends naturally to q-ary affine geometries: any block which intersects a hyperplane H in a d-dimensional affine space is still a *cross block*.

Lemma 1. *Let $\mathscr{A} = AG_{d+1}(2d+1, q)$ and H be a hyperplane of $\mathscr{A}$ through $\bar{0}$, and let α be a permutation of the affine d-subspaces of H which contain $\bar{0}$.*

Let B_1 be a cross block of $\mathscr{A}$ through $\bar{0}$. Then there exists a set $\{h_1 = \bar{0}, h_2, \ldots, h_{q^d}\}$ of distinct elements of H such that:

- *Each coset of B_1 is represented exactly once in the set*

  $$\{B_1 + h_i \mid i = 1, \ldots, q^d\},$$

  and

- *Each coset of $\alpha(B_1 \cap H)$ is represented exactly once in the set*

  $$\{\alpha(B_1 \cap H) + h_i \mid i = 1, \ldots, q^d\}.$$

Proof. First, as mentioned above, it is possible to find all translates of B_1, and all translates of $\alpha(B_1 \cap H)$ respectively using only elements of H. This holds for affine geometry designs over any finite field.

Let $G = (V_1 \cup V_2, E)$ be a bipartite multigraph with V_1 being the q^d translates of B_1 shifted by elements of H, and V_2 being the q^d translates of $\alpha(B_1 \cap H)$ by elements in H. We place an edge $\{x, y\}$ if there exists an $h \in H$ such that $x = B_1 + h$ and $y = \alpha(B_1 \cap H) + h$. Finding a set of h_i as described is equivalent to finding a perfect matching in G.

For each coset of B_1 or of $\alpha(B_1 \cap H)$, there are q^d values of h which produce the same coset. For any $X \subseteq V_1$, there are $q^d \cdot |X|$ vectors h which produce some coset in X. Similarly, for the cosets in $N(X)$, there are $q^d \cdot |N(X)|$ vectors which produce some coset in $N(X)$, where $N(X)$ represents the set of neighbors of X in V_2. As each vector corresponds to a distinct edge, we have $q^d|X| = q^d|N(X)|$, and so $|X| = |N(X)|$. Thus by Hall's matching theorem [Die05], a perfect matching exists in G.

Specializing with $q = 2$, we obtain the result necessary for Construction 2. □

Theorem 23. *The collection of blocks $\alpha(\mathscr{A})$ obtained from $\mathscr{A}$ via Construction 2 is a resolvable 3-design with the same parameters as $\mathscr{A}$=$AG_{d+1}(2d+1,2)$.*

Proof. All blocks in $\alpha(\mathscr{A})$ have size 2^{d+1}, because α only permutes d-subspaces within H.

The resulting structure is resolvable by construction. Consider a parallel class P of blocks in $\mathscr{A}$. If any block of P is contained entirely in H, then 2^{d-1} blocks of P are entirely contained in H, and the rest are disjoint from H. These blocks are untouched by the construction, and so remain a parallel class. On the other hand, if any block of P intersects H in 2^d points, then all blocks of P do so. In this case, recall that P consists of all cosets of the block $B \in P$ containing $\bar{0}$. The construction distorts B and its cosets in such a way that the distorted versions of the blocks of P remain pairwise disjoint, and thus form a parallel class. Thus $\alpha(\mathscr{A})$ is resolvable.

We must check that Construction 2 does not change distinct blocks into the same block. Suppose B, B' are blocks of $\mathscr{A}$ both containing $\bar{0}$. It is clear from the construction that if $B \neq B'$, then $\alpha(B) \neq \alpha(B')$. Now we must consider cosets. Suppose B, B' are cross blocks containing $\bar{0}$. Write $B = B_{out} \cup B_{in}$ and $B' = B'_{out} \cup B'_{in}$. Then $\alpha(B) = B_{out} \cup \alpha(B_{in})$ and $\alpha(B') = B'_{out} \cup \alpha(B'_{in})$. Suppose $\alpha(B) + h = \alpha(B') + h'$ for some $h, h' \in H$. Then $B_{out} \cup \alpha(B_{in}) = (B'_{out} \cup \alpha(B'_{in})) + (h + h')$, and in particular $\alpha(B_{in}) = \alpha(B'_{in}) + (h + h')$. But both $\alpha(B_{in})$ and $\alpha(B'_{in})$ are vector subspaces, so $h + h' \in \alpha(B'_{in})$, and thus $\alpha(B_{in}) = \alpha(B'_{in})$. Thus B and B' have the same inner parts, and so h and h' were chosen as specified in the construction. If $h = h'$, then $B_{out} = B'_{out}$ and so $B = B'$. If $h \neq h'$, then $\alpha(B_{in}) + h \neq \alpha(B'_{in}) + h'$ by construction, and so $\alpha(B_{in}) \neq \alpha(B'_{in}) + (h + h')$, contradicting our previous argument. Thus $B + h \neq B + h'$. In either case, we see that this construction produces distinct blocks from the blocks of $\mathscr{A}$. Note that if h, h' were not chosen as in the construction, it would be possible to transform two distinct blocks into the same block.

Finally, we show that $\alpha(\mathscr{A})$ is a 3-design with the same value of λ_3. Consider a triple $T = \{x, y, z\}$ of distinct points of $AG(2d+1, 2)$. We consider several cases:

- The number of blocks which contain T and which are unchanged by the construction does not change.
- If $T \subset H$, then any block $B = B_{out} \cup B_{in}$ containing T has $T \subset B_{in}$. Because α permutes the inner parts of cross blocks, the number of cross blocks containing T is unchanged.

- Similarly, if $T \subset X \setminus H$, then the number of cross blocks containing T is unchanged.
- Suppose $\{x,y\} \subseteq H$ and $z \in X \setminus H$. Consider any d-dimensional vector subspace S of H containing $\{x,y\}$ and $\bar{0}$. Then among all cross blocks meeting H in S, exactly one contains z (because the outer parts of these blocks are translates which partition $X \setminus H$). There is a one-to-one correspondence between cross blocks of $\mathscr{A}$ containing S, and cross blocks of $\alpha(\mathscr{A})$ containing S. In $\alpha(\mathscr{A})$, the outer parts of each such block still partition $X \setminus H$. Thus the number of cross blocks containing both $\bar{0}$ and T is fixed.

  To account for cosets, suppose R is a d-dimensional vector subspace of H containing $\bar{0}$. Then $\{x,y\}$ is contained in a coset $R+h$ for some $h \in H$ if and only if $\{x+h, y+h\}$ is contained in R, so the argument remains the same for cosets.
- Similarly, suppose that $x \in H$ but $\{y,z\} \subseteq X \setminus H$. Let $B = B_{out} \cup B_{in}$ be a cross block of $\mathscr{A}$ containing $\bar{0}$ such that $\{y,z\} \subset B_{out}$. Let C be the set of cross blocks of $\mathscr{A}$ whose outer parts are equal to B_{out}. Then the inner parts of the blocks in C are translates of B_{in} which partition H. Thus exactly one such inner part contains x. The construction replaces the inner part of each block of C with a distinct coset of $\alpha(B_{in})$, and these cosets partition H. Thus exactly one of these distorted blocks contains $\{x,y,z\}$.

  To account for cosets, note that a cross block's outer part contains $\{y,z\}$ if and only if there is a translate of the block, through $\bar{0}$, whose outer part contains $\{y+h, z+h\}$.

Thus the number of blocks containing T is unchanged, and so $\alpha(\mathscr{A})$ is a 3-design with index λ_3. □

We defined α to be a permutation of affine d-spaces through $\bar{0}$. Because we are working with binary geometries, each point of $\mathscr{A}$ may be identified with a unique point of the projective geometry $PG(2d,q)$ induced on X. Each projective $(d-1)$-space in the copy of $PG(2d,2)$ induced on H may be uniquely extended to an affine d-space through $\bar{0}$ by simply adding $\bar{0}$ to the space. Note that if α is a polarity of the projective space $PG(2d-1,2)$ induced on H, then it permutes projective $(d-1)$-spaces. Thus we may view α as a permutation of the affine d-spaces through $\bar{0}$ of H. In this case, we can obtain more detailed information about the properties of $\alpha(\mathscr{A})$.

Theorem 24. *If α is a polarity of the projective space $PG(2d-1,2)$ induced on H, then the design $\alpha(\mathscr{A})$ has the same intersection numbers as $\mathscr{A}$.*

Proof. Any two blocks of $\mathscr{A}$ are either disjoint or share 2^i points for some integer $1 \leq i \leq d$.

Let $B = B_{out} \cup B_{in}$ and $B' = B'_{out} \cup B'_{in}$ be cross blocks of $\mathscr{A}$, both containing $\bar{0}$. Construction 2 as applied to any block through $\bar{0}$ is equivalent to the construction of [JT09], and thus the intersection numbers of these blocks are unchanged. In particular, $|\alpha(B) \cap \alpha(B')| = |B \cap B'|$, and if $B \cap B' \neq \emptyset$, then $|\alpha(B_{in}) \cap \alpha(B'_{in})| = |B_{in} \cap B'_{in}| = 2^i$ for some $0 \leq i \leq d$.

Now we consider cosets. For $h \in H$, $|\alpha(B_{in}) \cap (\alpha(B'_{in}) + h)|$ is either 0, or exactly $|\alpha(B_{in}) \cap \alpha(B'_{in})|$. The cosets of $\alpha(B_{in}) \cap \alpha(B'_{in})$ shifted by elements of $\alpha(B_{in})$ partition $\alpha(B_{in})$, whereas the cosets of $\alpha(B_{in}) \cap \alpha(B'_{in})$ by any other elements of H are disjoint from $\alpha(B_{in})$.

For the outer parts, note that $X \setminus H$ is (the only) coset of H in X. Thus all of our previous arguments for inner parts apply to the outer parts as well. In particular, B_{out} and B'_{out} may be written as $S + k$ and $S' + k$ for some d-dimensional vector subspaces S, S' of H, and $k \in X \setminus H$. Thus,

$$|B_{out} \cap (B'_{out} + k)| = |(S + k) \cap (S' + k + h)| = |S \cap (S' + h)|,$$

and by the previous argument, these intersections have the same sizes as the intersections of inner parts. Consequently, $|B_{out} \cap (B'_{out} + h)|$ is either 0 or $|B_{out} \cap B'_{out}|$, where $|B_{out} \cap B'_{out}| = 2^i$ for some $0 \leq i \leq d$.

Thus, $|B \cap (B' + h)|$ is either 0, $|B_{in} \cap B'_{in}|$, $|B_{out} \cap B'_{out}|$, or $|B \cap B'|$. In any case, B and $B' + h$ are either disjoint, or intersect in 2^i points for some $0 \leq i \leq d$. We can actually make a stronger statement: B_{out} is a coset of B_{in} for any cross block of $\mathscr{A}$, and so $|B_{in} \cap B'_{in}| = |B_{out} \cap B'_{out}|$. Thus $|B \cap (B' + h)|$ has only three possible values: 0, $|B \cap B'|$, or $|B \cap B'|/2$.

Assume that $|B_{out} \cap B'_{out}| = 1$ or $|\alpha(B_{in}) \cap \alpha(B'_{in})| = 1$. In the design $\mathscr{A}$, we have $|B_{out} \cap B'_{out}| = 1$ if and only if $|B_{in} \cap B'_{in}| = 1$, because intersection numbers in $\mathscr{A}$ are even. Then $B_{in} \cap B'_{in} = \{\bar{0}\}$, and so $(B_{in} \setminus \{\bar{0}\}) \cap (B'_{in} \setminus \{\bar{0}\}) = \emptyset$. Since α is incidence-preserving, we have $|\alpha(B_{in}) \cap \alpha(B'_{in})| = 1$ as well. In addition, note that if $|B_{out} \cap B'_{out}| = 1$, then $|B_{out} \cap (B'_{out} + h)| = 1$ for all $h \in H$, and similarly for $|B_{in} \cap (B'_{in} + h)|$. Thus $|B_{out} \cap (B'_{out} + h)| = 1$ if and only if $|\alpha(B_{in}) \cap (\alpha(B'_{in}) + h)| = 1$, and so $|B \cap (B' + h)| = 2$.

Therefore, the set of intersection numbers of cross blocks and their cosets is the same as the set of intersection numbers of $\mathscr{A}$.

Finally, we consider a non-cross block B. The intersection of B with other non-cross blocks is obviously unchanged. The intersection of B with a cross block B' occurs entirely in either H or $X \setminus H$, thus it is either 0 or 2^i, for some $0 \leq i \leq d$. Note however that by their dimensions, no block of size 2^{d+1} contained entirely in H or entirely in $X \setminus H$ can intersect a space of size 2^d in only 1 point.

Thus, the block intersection numbers of $\alpha(\mathscr{A})$ are a subset of the block intersection numbers of $\mathscr{A}$. Blocks contained entirely in H do have all intersection numbers including 0 and

2^i for each $1 \leq i \leq d$. Consequently, the set of intersection numbers of blocks in $\mathscr{A}$ and $\alpha(\mathscr{A})$ are identical. $\square$

Theorem 25. *If α is a polarity of the projective space $PG(2d-1,2)$ induced on $H \setminus \{\bar{0}\}$, then the design $\alpha(\mathscr{A})$ has the same 2-rank as $\mathscr{A}$, but is not isomorphic to $\mathscr{A}$.*

Proof. Note that the block code of $\mathscr{A}$ is the Reed-Muller code $R(d,2d+1)$ which has dimension 2^{2d} and is self-dual [AK92]. Thus the 2-rank of $\mathscr{A}$ is 2^{2d}.

From the intersection numbers, the block code $\mathscr{C}$ of $\alpha(\mathscr{A})$ is self-orthogonal. Thus we have $\dim \mathscr{C} \leq 2^{2d}$, and so the 2-rank of $\alpha(\mathscr{A})$ is at most 2^{2d}. On the other hand, Construction 2 transforms the design D_0 of $\mathscr{A}$ into a design $\alpha(D_0)$ with the same parameters, but not isomorphic to $PG_d(2d,2)$, and having 2-rank equal to 2^{2d} [JT09]. Hence, the 2-rank of $\alpha(\mathscr{A})$ is equal to 2^{2d}, and the design $\alpha(\mathscr{A})$ is not isomorphic to $\mathscr{A}$. $\square$

The designs produced by Construction 2 provide an infinite family of examples of geometric designs, $AG_{d+1}(2d+1,2)$, $d \geq 2$, which are not characterized as the unique designs with the given parameters and 2-rank. Thus, if Hamada's conjecture about the minimum 2-rank of $AG_{d+1}(2d+1,2)$ is true, it follows that for each $d \geq 2$ there is at least one other design, namely $\alpha(\mathscr{A})$, having the same parameters and the same (minimum) 2-rank. This is the first known infinite family in the affine case.

Example 1. The smallest example of this construction corresponds to the design $\mathscr{A} = AG_3(5,2)$ whose blocks are the 3-dimensional vector subspaces of a 5-dimensional binary vector space, and their cosets. The design $\mathscr{A}$ is a 3-$(32,8,7)$ design with 620 blocks. We apply Construction 2 using the hyperplane $H = \langle 00001, 00010, 00100, 01000 \rangle$ and the orthogonal polarity α of $PG(4,2)$. The 2-rank of both $\mathscr{A}$ and $\alpha(\mathscr{A})$ is 16.

The automorphism group of $\mathscr{A}$ is $A\Gamma L(5,2)$ of order $2^{15} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$. It is 3-transitive on points and transitive on blocks (See for example [BJL99].) The automorphism group of $\alpha(\mathscr{A})$ has order $2^{15} \cdot 3^2 \cdot 5 \cdot 7$. It is point-transitive but not block-transitive.

To examine the block orbits of $\alpha(\mathscr{A})$, we view the points of $\mathscr{A}$ as elements of $F = GF(2^5)$. Thus 01000 represents w^2, where w is a primitive element of F. We identify each point with the exponent i of its representation w^i, thus $3 = 00100$, $4 = 00010$, …, $31 = 10000$, and $0 = 00000$. In this notation, the automorphism group of $\alpha(\mathscr{A})$ is generated by the following eleven permutations found by computer with Magma:

$(0,16,28,25,13,23,24,29,30,17,19,26)(1,14,9,18,3,27,21,5,2,10,20,31)(4,22,6,8,7,15)(11,12)$
$(5,25)(8,10)(11,16)(14,31)(15,18)(17,23)(22,29)(26,27)$
$(1,21,2,24)(3,28,7,20)(4,30,6,12)(5,27,14,17)(8,22)(9,13)(10,26,15,31)(11,25,29,23)$
$(2,12,7)(3,21,30)(4,6,9)(5,18,14,23,29,26)(8,17,31,11,25,27)(10,16)(15,22)(19,20,28)$
$(5,27)(8,18)(10,15)(11,29)(14,17)(16,22)(23,31)(25,26)$
$(4,9)(7,24)(8,14)(11,26)(13,28)(17,18)(21,30)(25,29)$
$(4,28)(5,15,22,23)(7,30)(8,26,14,11)(9,13)(10,16,31,27)(17,29,18,25)(21,24)$
$(4,21)(5,25,22,29)(7,13)(8,31,14,10)(9,30)(11,16,26,27)(15,17,23,18)(24,28)$
$(5,8)(10,25)(11,23)(14,22)(15,26)(16,17)(18,27)(29,31)$
$(3,30)(4,6)(5,17)(7,12)(8,18)(10,15)(11,29)(14,27)(16,22)(20,28)(23,25)(26,31)$
$(5,23)(8,11)(10,16)(14,26)(15,22)(17,25)(18,29)(27,31)$

The blocks of $\alpha(\mathscr{A})$ have two orbits under the action of this group, with orbit representatives:

$$\begin{array}{ll} \{0,1,2,3,6,12,19,20\} & \text{(orbit of size 60)} \\ \{0,1,2,5,8,14,19,22\} & \text{(orbit of size 560)} \end{array}$$

2.3 Polarity designs from $AG_{d+1}(2d+1,q)$ for $q>2$

We can modify Construction 2 for the case when $q>2$. However, these modified designs do not typically have the same p-rank, nor the same intersection numbers, as the corresponding geometric design.

Let $\mathscr{A}=AG_{d+1}(2d+1,q)$ for a prime power $q=p^s$. As before, let H be a hyperplane of $\mathscr{A}$ containing $\bar{0}$. For $q>2$, $|H|<|X\setminus H|$, and so the outer and inner parts of any cross block will have different sizes. Thus, many of the special considerations in Construction 2 are unnecessary. The terminology from the binary case extends in natural ways. In particular, a block B is still either contained in H, or intersects H in q^d points. In the latter case, we still refer to B as a cross block.

The construction simplifies as follows:

Construction 3. Let α be a permutation of the affine d-spaces through $\bar{0}$ of the affine $2d$-space induced on H. Using α, we make the following alterations to the blocks of $\mathscr{A}$:

- If B is a block such that $B\subset H$ or $B\cap H=\emptyset$, we leave B unchanged.
- If $|B\cap H|=q^d$ and $\bar{0}\in B$, we replace the part of B equal to $B\cap H$ by $\alpha(B\cap H)$.
- If $|B\cap H|=q^d$ and $\bar{0}\notin B$, there is a block B_1 such that $\bar{0}\in B_1$, $|B_1\cap H|=q^d$, and $B\cap H$ is a translate (or coset) of $B_1\cap H$ in the group of translations of H, by

considering H as a $2d$-dimensional vector space. Let $\{h_1 = \bar{0}, h_2, \dots, h_{q^d}\}$ be q^d distinct elements of H such that:

- Each coset of B_1 is represented exactly once in the set $\{B_1 + h_i | i = 1, \dots, q^d\}$, and
- Each coset of $\alpha(B_1 \cap H)$ is represented exactly once in the set $\{\alpha(B_1 \cap H) + h_i | i = 1, \dots, q^d\}$.

By Lemma 1, such a set of h_i exists. We replace the part of B_1 equal to $B_1 \cap H$ with $\alpha(B_1 \cap H)$. For the coset of B_1 equal to $B_1 + h_i$, we replace the part equal to $(B_1 + h_i) \cap H$ with $\alpha(B_1 \cap H) + h_i$.

In particular, note that we no longer treat all blocks with the same inner part together. The outer parts of these blocks are not necessarily affine translates for $q > 2$.

Theorem 26. *The collection of blocks $\alpha(\mathscr{A})$ obtained from $\mathscr{A}$ via Construction 3 is a resolvable 2-design with the same parameters as $\mathscr{A}$=$AG_{d+1}(2d+1, q)$.*

Proof. First note that, as in Construction 2, this construction preserves parallel classes, and so $\alpha(\mathscr{A})$ is resolvable.

We need to check that λ is unchanged. Let $P = \{x, y\}$ be a distinct pair of points in X.

- The number of blocks which contain P and are unchanged by the construction does not change.
- If $P \subset H$, then any block $B = B_{out} \cup B_{in}$ containing P has $P \subset B_{in}$. Because α permutes the inner parts of cross blocks, the number of cross blocks containing P is unchanged.
- Similarly, if $P \subset X \setminus H$, then the number of cross blocks containing P is unchanged.
- Suppose $x \in H$, $y \in X \setminus H$. Let B be a cross block containing x. Note that $\{B' \setminus H | B' \cap H = B \cap H\}$ partitions $X \setminus H$, and so exactly one such block contains $\{x, y\}$. Construction 3 preserves this property, and so the number of blocks with inner part $B \cap H$ containing $\{x, y\}$ is unchanged. Finally, for any block B, $\{x, y\} \subseteq B + h$ if and only if $\{x - h, y - h\} \subseteq B$, and so the counting does not change for cosets.

Thus we again have a design, although in this case we are only guaranteed a 2-design. □

Note that in this construction, we have specified that α permutes affine spaces. For $q > 2$, each point in our affine space is no longer identified with a unique point of a projective space, so we must make a small change in order to use a polarity of a projective space.

Let α be a polarity of the projective geometry $PG(2d-1,q)$ induced on H. Then α permutes the projective $(d-1)$-spaces in H. By viewing each point of $PG(2d-1,q)$ as a 1-dimensional vector subspace, we can interpret each projective $(d-1)$-space in H as an affine d-subspace containing $\bar{0}$. Thus α permutes the affine d-spaces of H containing $\bar{0}$, as required. Thus, it makes sense to speak of $\alpha(\mathscr{A})$. In this case, we can obtain more specific information about $\alpha(\mathscr{A})$.

Theorem 27. *If α is a polarity of the projective geometry $PG(2d-1,q)$ induced on H, then the intersection numbers of the blocks of $\alpha(\mathscr{A})$ are congruent to 0 (modulo q).*

Proof. Any two blocks of $\mathscr{A}$ are either disjoint or share q^i points for some integer $1 \leq i \leq d$.

Let $B = B_{out} \cup B_{in}$ and $B' = B'_{out} \cup B'_{in}$ be cross blocks of $\mathscr{A}$, both containing $\bar{0}$. Construction 3 as applied to any block through $\bar{0}$ is equivalent to the construction of [JT09], and thus the intersection numbers of these blocks are unchanged. In particular, $|\alpha(B) \cap \alpha(B')| = |B \cap B'|$, and $|\alpha(B_{in}) \cap \alpha(B'_{in})| = |B_{in} \cap B'_{in}|$.

However, it is possible for the intersection numbers of cosets of cross blocks to change. In particular, it is not necessarily true (as it was for the case $q = 2$) that if two blocks share the same inner portion, then their outer portions are affine translates. They may be simply disjoint.

As before, $|\alpha(B_{in}) \cap \alpha(B'_{in}) + h| \in \{0, |B_{in} \cap B'_{in}|\}$, because the inner parts are affine subspaces. Note that $|B_{in} \cap B'_{in}| = q^j$ for some $0 \leq j \leq d$. If $|B \cap B' + h| = q^i$ for some $1 \leq i \leq d$, then $|B_{out} \cap B'_{out} + h| = q^i - |B_{in} \cap B'_{in}|$. Thus either $|B_{out} \cap B'_{out} + h| = q^i$, or else $|B_{out} \cap B'_{out} + h| = q^i - q^j = q^j(q^{i-j} - 1)$. It is clear that if $j \neq 0$, $|\alpha(B) \cap \alpha(B') + h|$ is a multiple of q. If $j = 0$, then as in the binary case, $|B_{in} \cap B'_{in} + h| = 1$ for all $h \in H$. Thus, $|B_{out} \cap B'_{out} + h| = q^k - 1$ for some $1 \leq k \leq d$, and so these blocks still intersect in a multiple of q points.

Finally, we consider the intersection of a cross block B and a non-cross block B'. Then $B \cap B'$ is entirely contained in either H or $X \setminus H$. If it is contained in H, then $B \cap B'$ is an affine subspace. By their dimensions, B and B' cannot intersect in only 1 point, so the size is a power of q. If the intersection is contained entirely in $X \setminus H$, then the intersection is unchanged by the construction. □

Example 2. The smallest example of a non-binary design is based on $\mathscr{A} = AG_3(5,3)$, whose blocks may be viewed as the 3-dimensional vector subspaces of a 5-dimensional ternary vector space, and their cosets. The design $\mathscr{A}$ is a 2-$(243,27,130)$ design with 10890 blocks. It is point- and block-transitive, with automorphism group $A\Gamma L(5,3)$ of order $2^{10}\cdot 3^{15}\cdot 5\cdot 11^{2}\cdot 13$ (see for example [BJL99]). Its 3-rank is 96, and the block intersection numbers are $\{0,3,9\}$.

The distorted design $\alpha(\mathscr{A})$, constructed with the orthogonal polarity of $AG(4,3)$, has 82 point orbits, 1330 block orbits, and an automorphism group of order $2\cdot 3^{4}$. There are 128 block orbits of size 1, 40 block orbits of size 6, and all remaining 1170 block orbits have size 9. Its 3-rank is 112, and the block intersection numbers are $\{0,3,6,9\}$.

Acknowledgments. These acknowledgements refer to the paper [CJT11], of which this chapter is a reprint. Vladimir Tonchev wishes to thank the University of Augsburg, Germany, for the hospitality during his visit in 2008, when the present research was started. He is also grateful for the support provided by a grant of the Alexander von Humboldt Foundation.

Chapter 3

Multi-step majority logic decoding and the modified finite geometry designs

This chapter examines majority-logic decoding as applied to the codes whose parity check matrices are the incidence matrices of the polarity designs constructed in Chapter 2, and by Jungnickel and Tonchev [JT09]. The error-correcting performance of these codes is close or equal to the performance of the finite geometry codes on which they are based. The finite geometry codes are some of the best-known codes in this regard, demonstrating the highly geometric structure of the polarity designs.

3.1 Introduction

Majority logic decoding was one of the first efficient decoding algorithms discovered for linear error-correcting codes, and can be easily implemented in hardware. It was initially described by Reed [Ree53] for what are now called Reed-Muller codes. Massey [Mas62] gave a general description of the decoding scheme, and Goethals and Delsarte [GD68] generalized Reed's algorithm to make use of the structure of finite geometries. Detailed information about majority logic decoding algorithms and decoding circuits may be found in [PW72, Chapter 10].

The strength of majority logic decoding depends on the structure of the parity checks of a given code. We will focus on codes whose parity check matrices contain the incidence vectors of a design. A t-(v,k,λ) *design* (also *t-design* or *block design*) is a pair $(\mathscr{P},\mathscr{B})$ where $\mathscr{P}$ is a set of v *points*, and $\mathscr{B}$ is a set of k-subsets of $\mathscr{P}$ called *blocks* such that every t-subset of $\mathscr{P}$ appears in exactly λ blocks. We denote the number of blocks $|\mathscr{B}|$ by b, and the number of blocks containing a given point is a constant r depending only on the parameters. The *incidence matrix* of a design D is a $b \times v$ matrix whose (i,j) entry is 1 if the ith block contains point j, and 0 otherwise.

When used as a parity check matrix, the block-by-point incidence matrix of a design defines a code which supports majority logic decoding. Rudolph [Rud67] showed that if the dual of a linear code of length v contains words of weight k which support the blocks of a 2-(v,k,λ) design, then the code can be decoded using a "one-step" majority logic decoding scheme. Rudolph's decoding scheme is able to correct up to $\lfloor r/(2\lambda) \rfloor$ errors, where r is the number of blocks of the design containing a point. This may be improved to $\lfloor (r+\lambda-1)/(2\lambda) \rfloor$ in general. Rahman and Blake [RB75] showed that if the design is a t-design for $t>2$, then a stronger result holds.

It is well known that the codes whose parity check matrices are the block-by-point incidence matrices of projective and affine geometry designs are especially amenable to majority logic decoding. Goethals and Delsarte [GD68] described a multi-step majority logic decoding algorithm based on Reed's algorithm which takes advantage of the nested structure of the subspaces in finite geometries. Smith [Smi67] gave further modifications of this algorithm. In this paper, we will examine the codes whose parity check matrices are the incidence matrices of the modified designs constructed from $PG_d(m,q)$ and $AG_d(m,q)$ (see Chapter 2 and [JT09]). We will show that these parity check matrices retain a great deal of geometric structure, and that their corresponding codes admit multi-step majority logic decoding based on this structure. In particular, we will demonstrate that the polarity designs produce codes which compare favorably to their geometric counterparts. For polarity designs constructed over binary fields, these maintain the same error-correcting strength as the finite geometry codes on which they are based.

3.2 Majority logic decoding

Let C be a q-ary linear code of length n with dual $C^{\perp}$. Suppose that vector $c \in C$ is transmitted over a noisy channel. The received vector y may be written $y = c + e$ for some error vector $e \in \mathbb{F}_q^n$. Then for any $h \in C^{\perp}$, $y \cdot h = (c+e) \cdot h = e \cdot h$. Throughout, we will write the components of a vector (say, h) as $h = (h_1, h_2, \ldots, h_t, \ldots h_n)$.

Definition 5. *Let $h \in C^{\perp}$. Then $S_h = y \cdot h = \sum_{j=1}^{n} e_j h_j$ is called a* parity check equation *(or simply a* check*), and in particular S_h is called a* parity check sum *(or simply* check sum*).*

Definition 6. *Let $h \in C^{\perp}$. If $h_t = 1$, then the parity check sum S_h is said to* check *error component e_t.*

Definition 7. *Let $S = \{S_1, S_2, \dots, S_J\}$ be a set of parity check sums. Suppose that every S_i checks the error component e_t, and each other error component e_j is checked by at most one of the S_i. Then S is said to be* orthogonal on e_t.

A set of J parity check sums which are orthogonal on an error component e_t have the property that each error component other than e_t can affect at most one of the parity check sums. Thus, if at most $\lfloor J/2 \rfloor$ errors have occurred, then at most $\lfloor J/2 \rfloor$ of the parity check sums will *not* give the correct value of e_t. Then the value which the majority of the check sums takes will be the correct value of e_t. With this idea in hand, we can now describe the fundamental idea of majority logic decoding:

Proposition 1 (Single-step majority logic decoding, [Ree53, Mas62])**.** *Let $y = c + e$ be a received message vector. Suppose that, for each error component e_t, a set of at least J check sums can be found which are orthogonal on e_t. Then the correct value of e (and hence c) can be decoded if at most $\lfloor J/2 \rfloor$ errors have occurred.*

The results of Rudolph [Rud67] and Goethals and Delsarte [GD68] extend this "single step" majority logic decoding to situations in which the checks are not necessarily orthogonal. If each error component is checked by at most λ of the checks in a set of parity checks, then up to $\lfloor J/(2\lambda) \rfloor$ errors may be corrected. This result may be improved to $\lfloor (r + \lambda - 1)/(2\lambda) \rfloor$.

The single-step algorithm can be extended to "multi-step majority logic decoding", by decoding the value of a sum of error components, instead of single error components.

Definition 8. *Let $E = \{e_{i_1}, e_{i_2} \dots, e_{i_k}\}$ be a set of k error components for a received message, and let $S = \{S_1, S_2, \dots, S_J\}$ be a set of parity checks. Suppose that each S_i checks every $e_t \in E$, and each other error component $e_j \notin E$ is checked by at most one of the S_i. Then S is said to be* orthogonal on E.

Following this definition, suppose that E is a subset of error components. We use the notation S_E to denote the sum of the error components in E, that is,

$$S_E = \sum_{e_i \in E} e_i.$$

Using the majority logic decoding procedure described above, it is possible to correctly decode the value S_E. As before, if there are J checks orthogonal on E, then the value of S_E can be correctly decoded as long as at most $\lfloor J/2 \rfloor$ errors have occurred.

Once we have obtained an estimate for S_E, then S_E can act as a parity check sum which is orthogonal on any subset $E' \subset E$. If we can obtain J check sums orthogonal on E', then we can decode the value of the sum of the error components in E' using majority logic decoding. This process may be iterated until we eventually decode the values of each individual error component. This process is stated formally in the following proposition:

Proposition 2 (Multi-step majority logic decoding, [Rud67, GD68])**.** *Let y be a received message vector which was transmitted using a code C, with (unknown) error vector e. Let $E_0 = \{h_1, \dots, h_m\}$ be the set of all parity checks in $C^{\perp}$. Let $E_1, \dots, S_L$ be nonempty sets containing nonempty subsets of error components, and let $E_L = \{e_1, \dots, e_n\}$ consist of every individual error component. Suppose that for each set of error components $E \in E_j$, $1 \leq j \leq L$, there are at least J check sums in $E_0 \cup E_1 \cup \cdots \cup E_{j-1}$ which are orthogonal on E. Then the correct value of y can be decoded if at most $\lfloor J/2 \rfloor$ errors have occurred.*

This proposition encodes the concept of decoding subsets of error components one step at a time. This idea is also called *L-step majority logic decoding*, indicating that L individual steps of decoding are necessary before decoding the individual error components. The major problem in using multi-step majority logic decoding is to find the sets $E_1, \dots, E_{L-1}$ of parity check sums which possess the appropriate structure.

For example, suppose that $E \in E_1$ is a set of error components. Then it must be possible to decode the value of S_E using only parity check sums in E_0. That is, there must be a collection of parity check sums in E_0 which are orthogonal on E. After decoding each sum of error components in E_1, these values, together with the check sums obtained from E_0, are available to act as check sums for the sets in E_2. Because all individual error components are included in E_L, the correct value of each error component e_i will be eventually decoded if at most $\lfloor J/2 \rfloor$ errors have occurred. Note that this description encodes single-step majority logic decoding as well: we need only the checks in E_0, and the individual error coordinates in $E_L = E_1$.

The natural question for both single-step and multi-step majority logic decoding is: how large can J be made? In the following section, we will answer this question for a particular class of codes.

3.3 Decoding finite geometry codes

We will now review the application of multi-step majority logic decoding to certain codes derived from finite geometry designs. This approach was developed from Reed's original algorithm [Ree53] by Goethals and Delsarte [GD68]. Specifically, we will focus on codes whose duals are the p-ary block codes of $PG_d(m,q)$ and $AG_d(m,q)$, where $q = p^e$. Thus, the checks for these codes will have a geometric structure.

More specifically, let D denote either $AG_d(m,q)$ or $PG_d(m,q)$, where $q = p^e$. Let M be the block-by-point incidence matrix of D. Let C be the p-ary code with parity check matrix M. Then $C^\perp$ is the subfield subcode of a generalized Reed-Muller code or punctured generalized Reed-Muller code, respectively. See [AK92, Chapter 5] for a complete description. Note that we take these codes to be p-ary codes, even if q itself is not prime.

Let B be a subspace of a finite geometry. Then we will use c_B to denote the incidence vector of B. That is, c_B is a $(0,1)$ vector whose coordinates correspond to points of the finite geometry, with a 1 only in the coordinates corresponding to points contained in that block. Similarly, we use $C_p(D)$ to denote the p-ary block code of a design D. Note then that the block code of a design D is spanned by $\{c_B : B \text{ is a block of } D\}$.

Let $C^\perp$ be the block code of one of these geometric designs. The incidence vector of any d-space in the geometric design is contained in $C^\perp$, and so it is a parity check. Consider the set of all d-spaces of D which contain a given $(d-1)$-space K. All such d-spaces are disjoint, except for the points of K. Thus

$$\{c_B : B \text{ is a block of } D \text{ and } K \subseteq B\}$$

is a set of checks orthogonal on K, allowing us to decode the value of the sum S_K. If we find check sums $S_{K'}$ for every $(d-1)$-space K', then we can use these to form a set of new sums which are orthogonal on any $(d-2)$-space contained in K'. Repeating this, we can eventually decode each individual error component.

Lemma 2. *In both $PG_d(m,q)$ and $AG_d(m,q)$, the number of d-spaces containing a given $(d-1)$-space is*

$$\frac{q^{m-d+1}-1}{q-1}.$$

If $d' < d$, the number of d'-spaces containing a given $(d'-1)$-space is greater than or equal to $\frac{q^{m-d+1}-1}{q-1}$.

Lemma 2 guarantees that multi-step majority logic decoding may be applied to the block codes of finite geometry designs. Using the terminology of Proposition 2, we may choose E_i to contain each $(d-i+1)$-subspace of the finite geometry, for $i = 1, \ldots, d$. Lemma 2 states that there will always be at least $\frac{q^{m-d+1}-1}{q-1}$ parity check sums obtained from larger subspaces which are available to check the incidence vector of each subspace. Thus multi-step majority-logic decoding can decode up to

$$\lfloor J/2 \rfloor = \left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$$

errors. In the binary case $q = 2$, this method can correct exactly $2^{m-d} - 1$ errors.

3.4 Decoding the modified finite geometry codes

3.4.1 Modified projective geometry designs

The *modified projective geometry designs* are pseudo-geometric designs constructed by Jungnickel and Tonchev [JT09]. They are constructed from $D = PG_d(m,q)$ by permuting certain projective subspaces relative to a fixed hyperplane H of D. These designs share many properties with their parent designs. If q is prime and the permutation is a polarity of the projective geometry induced on H, then the modified designs are named *polarity designs*, and form the first infinite class of counterexamples to Hamada's conjecture [Ham68]. In this section, we will give a very detailed description of an implementation of multi-step majority logic decoding, which gives good results on the modified and polarity designs.

We first note that the work of Rudolph [Rud67] and Rahman and Black [RB75] allows single-step majority logic decoding to be applied to *any* code which contains the supports of designs among its words. The strength of this decoding depends only on the parameters of the design in question. Thus, using these single-step decoding methods, the block codes of the regular and modified geometric designs give equal decoding strength. Below, we will demonstrate how the structure of the modified designs allows us to produce similar results for multi-step majority logic decoding. The following results will apply to all modified designs. We will later specialize these results to the polarity designs.

Definition 9. *Let $D = PG_d(m,q)$, and let H be a hyperplane on the points of D. A block B of D which intersects H in a projective $(d-1)$-space is called a* cross block. *We write $B = B_{in} \cup B_{out}$, where $B_{in} = B \cap H$ and $B_{out} = B \setminus H$. We also refer to B_{in} and B_{out} as the* inner *and* outer *parts of the block, respectively.*

Let H a hyperplane of D, and let $\overline{H}$ be the complement of H. Let α be a permutation of the $(d-1)$-spaces in the copy of $PG(m-1,q)$ induced on H. The modified design $\widetilde{D}$ is constructed by replacing each cross block $B_{in} \cup B_{out}$ with $\alpha(B_{in}) \cup B_{out}$. We leave all other blocks intact.

For the following results, we extend the notation c_B to denote the incidence vector of B, where B is any block or geometric subspace in $\widetilde{D}$. Similarly, $C_p(D)$ will still denote the p-ary block code of the design D. Let $C^{\perp} = C_p(D)$, that is, the p-ary block code of D, and let $\widetilde{C}^{\perp} = C_p(\widetilde{D})$. Recall that the incidence matrix of the design is used as a parity check matrix, and so $C_p(D)$ and $C_p(\widetilde{D})$ are the dual codes of the codes being decoded.

Lemma 3. *The restriction of both D and $\widetilde{D}$ to H is a design isomorphic to $PG_{d-1}(m-1,q)$.*

The restriction of both D and $\widetilde{D}$ to $\overline{H}$ is a design isomorphic to $AG_d(m,q)$.

Proof. For the geometric designs, this is well known. For the modified designs, we note that $\overline{H}$ is unchanged, and subspaces contained in H are simply permuted. Thus the same result applies. □

Lemma 4. *Let K be a projective $(d-1)$-space whose points are contained entirely in H. Then there exists a complete set of $\frac{q^{m-d+1}-1}{q-1}$ words of $\widetilde{C}^{\perp}$ which are orthogonal on K.*

Proof. By Lemma 2, there exist $\frac{q^{m-d+1}-1}{q-1}$ blocks of D which contain K. Each of these blocks is either contained in H (in which case it is also a block of $\widetilde{D}$), or it is a cross block whose inner part is equal to K. If it is a cross block, then there exist q^{m-d} blocks of D with inner part equal to K. The outer parts of these blocks are disjoint and form a parallel class in the affine design $AG_d(m,q)$ induced on $\overline{H}$. There are q^{m-d} corresponding blocks in $\widetilde{D}$ whose inner part are K, and whose outer parts are also a parallel class in $\overline{H}$ (possibly different from the parallel class in D). Thus each block of D containing K corresponds uniquely to a block in $\widetilde{D}$ containing K, and these blocks are disjoint outside of K. So, the incidence vectors of these $\frac{q^{m-d+1}-1}{q-1}$ blocks are orthogonal on K. Note that every point of $\widetilde{D}$ is contained in one such block, and so this is a maximal set. □

Lemma 5. *Let K' be a projective $(d-i)$-space $(i \geq 1)$ whose points are contained entirely in H. Then there exist at least $\frac{q^{m-d+1}-1}{q-1}$ checks orthogonal on K'.*

Proof. If $i=1$, we are in the case of Lemma 4, using incidence vectors of blocks of $\widetilde{D}$ as checks. So, suppose $i \geq 2$. In this case, the checks orthogonal on the points of a $(d-i)$-space correspond to projective $(d-i+1)$-spaces contained entirely in H, found during a previous step of the decoding. Note that we no longer have any checks which "cross" H – all of our checks contain points only in H. Applying Lemma 2 to H, we have the result. □

The *support* of a word c in a linear code C is the set of positions in which c is nonzero. Note that it is possible for a codeword to support a subspace without being equal to its incidence vector.

Lemma 6. *The code $\widetilde{C}^{\perp}$ contains a set of words which support the design $AG_{d+1}(m,q)$.*

Proof. First note that any block K of $AG_{d+1}(m,q)$ is a union of q cosets of an affine d-space. Next, recall that the outer parts of any set of blocks of $\widetilde{D}$ which share identical inner parts are cosets of an affine d-space. Fix any block K of $AG_{d+1}(m,q)$ and let $\{B_1,\ldots,B_q\}$ be q blocks of $\widetilde{D}$ whose inner parts are identical, and whose outer parts are the appropriate cosets of an affine d-space necessary to form K. Then $c_{B_1}+\cdots+c_{B_q}$ contains 1's exactly in the coordinates of $\widetilde{C}^{\perp}$ corresponding to the points of K. Because their inner parts are identical, the sum of these q blocks will be zero on all points corresponding to H. Thus, the incidence vector of each block of $AG_{d+1}(m,q)$ is embedded in $\widetilde{C}^{\perp}$, with nonzero positions only in the q^m positions corresponding to $\overline{H}$. □

Note that although the restriction of $\widetilde{D}$ to $\overline{H}$ gives an affine geometry design isomorphic to $AG_d(m,q)$, the incidence vectors of these affine d-spaces are not contained in $\widetilde{C}^{\perp}$.

Lemma 7. *Let K be an affine d-space contained entirely in $\overline{H}$. Then there exists a set of $2\frac{q^{m-d}-1}{q-1}+1$ parity checks in $\widetilde{C}^{\perp}$ which are orthogonal on K.*

Proof. We will construct this set in several parts. First, we use the affine $(d+1)$-spaces found in Lemma 6. There are $\frac{q^{m-d}-1}{q-1}$ affine $(d+1)$-spaces which contain K, and the incidence vector of each is contained in $\widetilde{C}^{\perp}$. These give $\frac{q^{m-d}-1}{q-1}$ checks containing K, which partition $\overline{H}\setminus K$.

In addition, K is the outer part of a unique cross block B of $\widetilde{D}$. Thus we may use c_B as a check.

Finally, let K' denote the inner part of B, that is, $K'=B\cap H$. Note that K' is a projective $(d-1)$-space and $B=K'\cup K$. By construction $\widetilde{C}^{\perp}$ contains the incidence vectors of all projective d-spaces contained in H. Let B' be any projective d-space contained in H for which $K'\subseteq B'$. Then $c_B-c_{B'}$ is a vector contained in $\widetilde{C}^{\perp}$ which has several important features. First, $c_B-c_{B'}$ has a 1 at each point corresponding to K, and thus checks K. Second, $c_{B'}$ has a -1 at each point corresponding to B', except for the points of K' (which are all zeroes). Thus the vectors in

$$S=\{c_B-c_{B'} : B' \text{ is a projective } d\text{-space contained in } H\text{, and } K'\subseteq B'\}$$

all check K, and check each point in $H\setminus K'$ exactly once. Thus S is a set of $\frac{q^m-q^d}{q^{d+1}-q^d}=\frac{q^{m-d}-1}{q-1}$ checks orthogonal on K.

In total, we have

$$\frac{q^{m-d}-1}{q-1}+\frac{q^{m-d}-1}{q-1}+1=2\frac{q^{m-d}-1}{q-1}+1$$

checks orthogonal on K, and these checks cover every point of the design. □

Lemma 8. *Let K be an affine $(d-i)$-space $(i \geq 0)$ whose points are contained in $\overline{H}$. Then there exist at least $2\frac{q^{m-d}-1}{q-1}+1$ checks orthogonal on K.*

Proof. If $i=0$, we are in the case of Lemma 7. So, suppose $i \geq 1$. In this case, the checks orthogonal on an affine $(d-i)$-space contained in $\overline{H}$ correspond to affine $(d-i+1)$-spaces contained entirely in $\overline{H}$, found during a previous step of the decoding. In the copy of $AG_d(m,q)$ induced on $\overline{H}$, each $(d-i)$-space $(i \geq 1)$ is checked by $\frac{q^{m-d+i}-1}{q-1}$ of the $(d-i+1)$-spaces, and $\frac{q^{m-d+i}-1}{q-1} \geq 2\frac{q^{m-d}-1}{q-1}+1$ for all q, d, and $i \geq 1$. □

The preceding lemmas demonstrate how we can find parity checks orthogonal on any projective d-space in H, or any affine d-space in $\overline{H}$. Together, these allow us to find checks which are orthogonal on every error bit in a transmitted word. We will *separately* decode errors which occur in the coordinates corresponding to H, and those corresponding to $\overline{H}$.

Theorem 28. *The code $\widetilde{C}$ admits multi-step majority logic decoding. The code may be correctly decoded with this method if at most $\left\lfloor \frac{q^{m-d}-1}{q-1}+\frac{1}{2} \right\rfloor$ errors occur.*

Proof. Let y be a received word. The following rules will correctly decode y:

1. For each projective $(d-1)$-space K in H, use the $\frac{q^{m-d+1}-1}{q-1}$ words in $\widetilde{C}^{\perp}$ identified in Lemma 4 to decode the sum of the error components corresponding to K. Repeat this for $(d-2)$-spaces, using the parity check sums previously identified for $(d-1)$-spaces. There are at least $\frac{q^{m-d+1}-1}{q-1}$ such parity check sums orthogonal on each $(d-2)$-space, as guaranteed by Lemma 5. Repeat for $(d-i)$-spaces, $i=1,2,\ldots,d$, until 0-spaces (points) are decoded. Lemma 5 guarantees that at each step, at least $\frac{q^{m-d+1}-1}{q-1}$ parity check sums can be found which are orthogonal on each space. Thus multi-step majority logic decoding allows us to determine the value of each error coordinate e_j contained in H. This will succeed if at most $\left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors occurred among all points.

2. For each affine d-space K' contained in $\overline{H}$, use the $2\frac{q^{m-d}-1}{q-1}+1$ words identified in Lemma 7 to decode the sum of the error components corresponding to K'. Repeat this for affine $(d-1)$-spaces, using the parity check sums previously identified for d-spaces. There are at least $2\frac{q^{m-d}-1}{q-1}+1$ such parity check sums orthogonal on each affine $(d-1)$-space, as guaranteed by Lemma 8. Repeat for affine $(d-i)$-spaces, $i=1,2,\ldots,d$ in order until points are decoded. Lemma 8 guarantees that at each step, at least $2\frac{q^{m-d}-1}{q-1}+1$ parity check sums can be found which are orthogonal on

each space. Thus multi-step majority logic decoding allows us to determine the value of each error component e_j in $\overline{H}$. This will succeed if at most $\left\lfloor \frac{q^{m-d}-1}{q-1} + \frac{1}{2} \right\rfloor$ errors occurred among all points.

Thus all errors will be corrected if at most

$$\min\left\{ \left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor, \left\lfloor \frac{q^{m-d}-1}{q-1} + \frac{1}{2} \right\rfloor \right\} = \left\lfloor \frac{q^{m-d}-1}{q-1} + \frac{1}{2} \right\rfloor$$

errors occur among all components. □

Recall that the design $PG_d(m,q)$ can correct up to $\left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors using multi-step majority logic decoding. Thus, in general, the modified designs give codes which admit slightly weaker decoding than their geometric counterparts.

We also note that in general, the block codes of modified projective geometry designs have larger dimension than the block codes of the corresponding projective geometry designs. For the design obtained from $PG_d(2d,p)$ where p is a prime and α is a polarity, we know that the modified design (called the *polarity design*) has the same p-rank as the corresponding projective design. If $q = 2$, then Theorem 28 guarantees that we may correct up to $2^d - 1$ errors, which is exactly the same as the standard projective geometry design.

Theorem 29. *Let $D = PG_d(2d,2)$, and let $\widetilde{D}$ be the polarity design constructed from D. Then the codes whose parity check matrices are the incidence matrices of D and $\widetilde{D}$ have equal error-correcting strength under multi-step majority logic decoding.*

3.4.2 Modified affine geometry designs

The modified affine geometry designs were discovered by Clark, Jungnickel, and Tonchev [CJT11] as an extension of the methods used for projective geometry designs. Majority logic decoding may be applied to the modified designs constructed from $D = AG_d(m,q)$ with excellent results.

As before, let H be a hyperplane of D, and let $\overline{H}$ be the complement of H. We extend the terminology *cross block* naturally to D: any block which intersects H in a d-dimensional affine subspace is called a *cross block*. Let α be a permutation of the d-dimensional subspaces in the copy of $AG_d(m,q)$ induced on H. We create the modified design $\widetilde{D}$ from D in a manner similar to the modified projective designs. There are some subtleties of the application of this construction to cosets of subspaces; see [CJT11] for a full discussion. If we begin with $AG_{d+1}(2d+1,2)$ and α is a polarity of $PG(2d,2)$ extended naturally to the copy of $AG_d(2d,2)$ induced on H, then this design is called an *affine polarity design*. The affine polarity design constructed from $AG_{d+1}(2d+1,2)$ has the same 2-rank as $AG_{d+1}(2d+1,2)$, but is not isomorphic.

Let $\widetilde{C}$ be the code whose parity check matrix is the incidence matrix of $\widetilde{D}$. Thus $\widetilde{C}^{\perp}$ is the block code $C_p(\widetilde{D})$. This initial result shows that the block codes of the modified affine geometry designs possess as many words orthogonal on each block of the design as the unmodified affine geometry codes.

Lemma 9. *Let K be an affine $(d-1)$-space contained entirely in a coset of H (possibly equal to H itself). Then there exist a complete set of $\frac{q^{m-d+1}-1}{q-1}$ words of $\widetilde{C}^{\perp}$ which are orthogonal on K.*

Proof. Suppose that H' is a coset of H. Then there are $(q^{m-1}-q^{d-1})/(q^d-q^{d-1}) = \frac{q^{m-d}-1}{q-1}$ blocks of $\widetilde{D}$ contained in H' whose incidence vectors are orthogonal on K. Note that all blocks contained entirely in a coset of H are unchanged by the permutation construction. In addition, there are $\frac{q^{m-1}}{q^{d-1}} = q^{m-d}$ cross blocks with respect to H' whose inner part is equal to K, and whose outer parts form a parallel class in $\overline{H'}$. This is true for all cosets of H, as the permutation construction preserves parallel classes. This gives $\frac{q^{m-d}-1}{q-1} + q^{m-d} = \frac{q^{m-d+1}-1}{q-1}$ words orthogonal on K. □

Lemma 10. *Let K' be an affine $(d-i)$-space $(i \geq 0)$ contained in a coset H' of H. Then there exist at least $\frac{q^{m-d+1}-1}{q-1}$ checks orthogonal on K'.*

Proof. If $i=1$, we are in the case of Lemma 9. If $i \geq 2$, then use the $(d-i+1)$-spaces contained entirely in H'. Lemma 2 applied to H' gives a value which is at least $\frac{q^{m-d+1}-1}{q-1}$ in this case. □

The previous result guarantees that enough parity check sums may be found at each step of multi-step majority logic decoding to ensure correction of at least $\lfloor J/2 \rfloor = \left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors.

Theorem 30. *The code $\widetilde{C}$ admits majority logic decoding. The code may be correctly decoded if at most $\left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors occur.*

Proof. Let y be a received word. For each affine $(d-1)$-space K contained in a coset of H, use the $\frac{q^{m-d+1}-1}{q-1}$ words identified in Lemma 10 to decode the sum of the error components corresponding to K. Repeat this for $(d-2)$-spaces, using parity check sums found in the previous sum. Lemma 10 guarantees that at least $\frac{q^{m-d+1}-1}{q-1}$ checks may be found on each such $(d-2)$-space. Repeat this to decode $(d-i)$-spaces for each $i = 1, 2, \dots, d$ in order, with Lemma 10 guaranteeing at least the same number of checks orthogonal on each $(d-i)$-space. Thus multi-step majority logic decoding allows us to determine the value of each error coordinate e_j contained in each coset of H. This will succeed if at most $\left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors occurred among all points. □

As with projective geometry designs, recall that the design $AG_d(m,q)$ can correct up to $\left\lfloor \frac{q^{m-d+1}-1}{2(q-1)} \right\rfloor$ errors using multi-step majority logic decoding. Thus, in general, the modified affine geometry designs give codes which admit slightly weaker decoding than their geometric counterparts.

In general, the block codes of modified affine geometry designs have larger dimensions than the block codes of the affine geometry designs from which they are built. For the design obtained from $AG_{d+1}(2d+1,2)$ with α a polarity, we know that the modified design (also called the *affine polarity design*) has the same 2-rank as the corresponding projective design. In this case, Theorem 30 guarantees that we may correct up to $2^d - 1$ errors, which is exactly the same as the standard projective geometry design.

Theorem 31. *Let $D = AG_{d+1}(2d+1,2)$, and let $\widetilde{D}$ be the affine polarity design constructed from D. Then the codes whose parity check matrices are the incidence matrices of D and $\widetilde{D}$ have equal error-correcting strength under multi-step majority logic decoding.*

3.5 Minimum distances

In this section, we will prove that the codes formed from binary projective polarity designs and binary affine polarity designs have the same minimum distances as the original codes on which they are based. We will also characterize the minimum weight codewords.

Throughout this section, we let $D = PG_d(2d,2)$. Let H a hyperplane of $PG(2d,2)$, and let α be a polarity of the projective $(d-1)$-spaces in the copy of $PG_{d-1}(2d-1,2)$ which D induces on H. Let $\widetilde{D}$ be the polarity design created from D by using α. From [JT09], we know that $\widetilde{D}$ is a 2-design with the same parameters as D, and the same 2-rank, but which is not isomorphic to D. We also remark that the notation c_B is used to denote the incidence vector of any space B in an appropriate code.

Our proofs will make use of short exact sequences. This method is very similar to the method used in the proofs for the minimum distances of the block codes of $AG_d(m,2)$ and $PG_d(m,2)$ given in [AK92, Section 5, p. 148]. Recall that a short exact sequence is a sequence of mappings:

$$0 \xrightarrow{\phi_1} A \xrightarrow{\phi_2} B \xrightarrow{\phi_3} C \xrightarrow{\phi_4} 0$$

in which $\operatorname{im}\phi_i = \ker\phi_{i+1}$ for $i = 1,2,3$. In each case, "0" denotes the appropriate identity element. Thus ϕ_2 is necessarily an injection: $\operatorname{im}\phi_1 = 0$, and so we must have $\ker\phi_2 = \operatorname{im}\phi_1 = 0$ as well. Similarly, ϕ_3 must be a surjection. Typically, ϕ_1 and ϕ_4 are omitted, as they are completely determined. These short exact sequences turn out to be extremely helpful in identifying the minimum distances of geometric codes.

Lemma 11. *The design $\widetilde{D}$ gives rise to the following short exact sequence:*

$$0 \longrightarrow C_2(PG_d(2d-1,2)) \xrightarrow{\phi} C_2(\widetilde{D}) = \widetilde{C}^{\perp} \xrightarrow{\varphi} C_2(AG_d(2d,2)) \longrightarrow 0$$

We define the mappings as follows: For any d-space B in H, $\phi(c_B)$ is the incidence vector of B in $C_2(\widetilde{D})$, and ϕ is extended linearly. For any block $B' \in \widetilde{D}$, $\varphi(c_{B'})$ is the incidence vector of $B' \setminus H$ in $C_2(AG_d(2d,2))$, and φ is extended linearly.

Proof. First we show that ϕ is an injection from the copy of $C_2(PG_d(2d-1,2))$ induced on H, to $C_2(\widetilde{D}) = \widetilde{C}^{\perp}$. Each d-space in H is also a d-space of $\widetilde{D}$ (because it is untouched by the polarity construction). Thus any word $c \in C_2(H)$ corresponds to a sum of incidence vectors of d-spaces, and thus corresponds to a unique sum of incidence vectors of d-spaces in $\widetilde{C}^{\perp}$, and so ϕ is injective.

Next, we show that φ is a surjection. If B' is a cross block, then $\varphi(c_{B'}) = c_{B'_{out}}$ embedded in $\overline{H}$. Note that $c_{B'_{out}}$ is the incidence vector of an affine d-space. The incidence vector of each affine d-space in $AG_d(2d,2)$ can be obtained in this way. Note that if B is contained in H, then $\varphi(B) = 0$.

Finally, we show that $\operatorname{im}\phi = \ker\varphi$. Clearly the image of ϕ in $\widetilde{C}^{\perp}$ consists of the incidence vectors of all d-spaces contained in H. The kernel of φ contains the incidence vectors of all such d-spaces, and so $\operatorname{im}\phi \subseteq \ker\varphi$. We have $\dim\operatorname{im}\phi = \operatorname{rank}_2 PG_d(2d-1,2)$ and $\dim\ker\varphi = \operatorname{rank}_2 \widetilde{D} - \operatorname{rank}_2 AG_d(2d,2)$. We know from [JT09] that $\operatorname{rank}_2 \widetilde{D} = \operatorname{rank}_2 PG_d(2d,2)$ (because we used a polarity to modify the design). Hamada [Ham68] gives the result that $\operatorname{rank}_2 PG_d(2d,2) - \operatorname{rank}_2 AG_d(2d,2) = \operatorname{rank}_2 PG_d(2d-1,2)$. Thus $\dim\operatorname{im}\phi = \dim\ker\varphi$, and so $\operatorname{im}\phi = \ker\varphi$. □

Note that in Lemma 11, the fact that $\operatorname{rank}_2 \widetilde{D} = \operatorname{rank}_2 PG_d(2d,2)$ is essential to the argument. If $\operatorname{rank}_2 \widetilde{D}$ is larger than $\operatorname{rank}_2 PG_d(2d,2)$, then $\ker \varphi$ will be larger that $\operatorname{im} \phi$. As a result, the previous lemma can not be directly extended to apply to non-polarity modified designs.

Lemma 12. *The design $\widetilde{D}$ gives rise to the following short exact sequence:*

$$0 \longrightarrow C_2(AG_{d+1}(2d,2)) \xrightarrow{\psi} C_2(\widetilde{D}) = \widetilde{C}^{\perp} \xrightarrow{\omega} C_2(PG_{d-1}(2d-1,2)) \longrightarrow 0.$$

The mappings are defined as follows: for B an affine $(d+1)$-space in $AG_{d+1}(2d,2)$, $\psi(c_B)$ is the incidence vector of B in $\widetilde{C}^{\perp}$, and ψ is extended linearly. For $c \in \widetilde{C}^{\perp}$, $\omega(c)$ is the restriction of c to the points of H, and ω is extended linearly.

Proof. First we show that ψ is an injection. Let B, B' be two distinct blocks of $\widetilde{D}$ such that $B_{in} = B'_{in}$. Then B_{out} and B'_{out} are cosets of the same affine d-space, and so $c_B + c_{B'}$ is the incidence vector of an affine $(d+1)$-space (its support is contained entirely in $\overline{H}$). Every $(d+1)$-space can be obtained uniquely in this fashion. Thus $C_2(AG_{d+1}(2d,2))$ is contained in $\widetilde{C}^{\perp}$, and ϕ uniquely maps incidence vectors of affine $(d+1)$-spaces into $\widetilde{C}^{\perp}$.

Next, we show that ω is a surjection onto the binary block code of the copy of $PG_{d-1}(2d-1,2)$ induced on H. Let $c \in \widetilde{C}^{\perp}$. If c is the incidence vector of a cross block of $\widetilde{D}$, then $\omega(c) = c_{B_{in}}$. Every projective $(d-1)$-space may be obtained from some cross block, so ω is a surjection.

Finally, we show that $\operatorname{im} \psi = \ker \omega$. Note that $\operatorname{im} \psi$ contains all affine $(d+1)$-spaces, and that each such space A is in $\ker \omega$, so $\operatorname{im} \psi \subseteq \ker \omega$. From the fact that the block codes of binary affine and projective geometries are Reed-Muller and punctured Reed-Muller codes (respectively), we know their dimensions (see, for example, [AK92, Chapter 5]). In addition, $\dim \widetilde{C}^{\perp} = \dim PG_d(2d,2)$ by [CJT11]. The dimensions are equal: $\dim \operatorname{im} \psi = \dim \ker \omega$, and so $\operatorname{im} \psi = \ker \omega$. □

We define the support of a codeword c, denoted $\operatorname{supp} c$, as the points of $\widetilde{D}$ which correspond to nonzero coordinates in c.

Theorem 32. *The minimum distance of the block code $\widetilde{C}^{\perp}$ of $\widetilde{D}$ is exactly $2^{d+1} - 1$. Furthermore, the codewords of minimum weight are exactly the incidence vectors of the blocks of $\widetilde{D}$.*

Proof. First note that $\widetilde{C}^{\perp}$ contains the incidence vectors of all projective d-spaces in $\widetilde{D}$, and so the minimum distance is at most $2^{d+1} - 1$. Also, the minimum distances of the block codes of two related designs are already known: for $PG_d(2d-1,2)$, the minimum distance is $2^{d+1}-1$, and for $AG_d(2d,2)$, the minimum distance is 2^d [AK92].

Let $c \in \widetilde{C}^{\perp}$ be a minimum weight codeword. If $\operatorname{supp} c \subseteq H$, then c is zero on the points of $\overline{H}$. Thus $c \in \ker(\varphi)$ as defined in Lemma 11, and so by the short exact sequence in Lemma 11, c is in $\operatorname{im}\phi$. Thus c is the incidence vector of a projective d-space contained in H. Thus $\operatorname{wt} c \geq 2^{d+1}-1$, and we are done. In a similar fashion, suppose $\operatorname{supp} c \subseteq \overline{H}$. Then using Lemma 12, $\operatorname{wt}(c) \geq 2^{d+1}$. However, we know that the minimum distance is at most $2^{d+1}-1$, and so this is irrelevant.

Thus we may assume that $\operatorname{supp} c$ has a non-empty intersection with both H and $\overline{H}$. In this case, the restriction of c to points of H, $c|_H$, satisfies $c|_H \in C_2(H) = C_2(PG_{d-1}(2d-1,2))$, and so $\operatorname{wt} c|_H \geq 2^d - 1$. Similarly, $c|_{\overline{H}} \in C_2(\overline{H}) = C_2(AG_d(2d,2))$, and so $\operatorname{wt} c|_{\overline{H}} \geq 2^d$. Thus $\operatorname{wt} c \geq 2^{d+1}-1$, as desired.

Finally, we show that c is the incidence vector of a block of $\widetilde{D}$. If $\operatorname{supp} c \subseteq H$, then as above, c is the incidence vector of a projective d-space which is a block of $\widetilde{D}$. So, assume that $\operatorname{supp} c$ has a non-empty intersection with both H and $\overline{H}$. Note that $c|_H$ must be the incidence vector of a projective $(d-1)$-space, because the only minimum-weight words of $PG_{d-1}(2d-1,2)$ are projective $(d-1)$-spaces. Thus we can find a block B of $\widetilde{D}$ such that c_B agrees with c on all points in H, and at least one point in $\overline{H}$. Then $\operatorname{wt}(c_B - c) < 2^{d+1}-1$, and so $c_B = c$. □

Corollary 3. *The minimum distance of the code $C_2(\widetilde{AG}_{d+1}(2d+1,2))$ is exactly 2^{d+1}. Furthermore, the codewords of minimum weight are exactly the incidence vectors of blocks of the modified affine geometry design.*

Proof. The block code of the affine polarity geometry design is equal to the block code of the projective polarity design, extended with a parity check bit. □

Chapter 4

Nonbinary quantum codes derived from finite geometries

In this chapter [*], we use relatives of finite geometry designs to construct quantum stabilizer error-correcting codes.

4.1 Introduction

The theory of binary quantum stabilizer codes based on classical additive codes over $\mathbb{F}_4$ was developed in a systematic way by Calderbank, Rains, Shor, and Sloane [CRSS98]. It was extended to nonbinary fields by Bierbrauer and Edel [BE00]. In [KKKS06], Ketkar, Klappenecker, Kumar, and Sarvepalli proposed a construction of nonbinary stabilizer quantum codes based on classical linear codes over $\mathbb{F}_q$ for arbitrary prime power q.

The topic of this paper are some classes of q-ary quantum stabilizer codes obtained from finite projective or affine geometries. We use classical finite geometry codes [AK92] to construct several new infinite families of q-ary quantum codes. The properties of the related finite geometry structures allow us to determine or bound all parameters of the resulting codes.

A fundamental link between linear codes and binary quantum stabilizer codes is given by

[*] Reprinted with minor editorial changes from Finite Fields and their Applications, *to appear*, D. Clark, D. Jungnickel, and V. D. Tonchev: *Nonbinary quantum codes derived from finite geometries* [CT], Copyright 2011, with permission from Elsevier. See permission letter in Appendix C.

the Calderbank-Shor-Steane (CSS) construction [CS96, Ste96b]. We will make use of the following results which follow from the q-ary version of the CSS construction:

Theorem 33 (Ketkar, et. al [KKKS06])**.** *Let C be a classical linear $[n,k,d]_q$ code. (i) If C contains its dual, $C^{\perp} \subseteq C$, then there exists a quantum $[[n,2k-n,d]]_q$ stabilizer code.*
(ii) If C is self-orthogonal, $C \subseteq C^{\perp}$, and $d^{\perp}$ is the minimum distance of $C^{\perp}$, then there exists a quantum $[[n,n-2k,d^{\perp}]]_q$ stabilizer code.

In this paper, we will use Theorem 33 to construct q-ary quantum codes from linear codes which are spanned by the incidence matrices of combinatorial designs. In particular, we will focus on designs arise from finite geometries.

We refer to [BJL99] for basic terminology and results concerning combinatorial designs. The *incidence matrix* of a design with b blocks and v points is a $b \times v$ matrix, with rows indexed by blocks and columns indexed by points. An entry is 1 if the corresponding point is contained in the corresponding block, and 0 otherwise. The q-ary *block code* of a design with incidence matrix M is the linear span of the rows of M over a finite field $\mathbb{F}_q$. We denote the q-ary block code of a design D by $C_q(D)$. The p-rank of a design D is defined as the rank of its incidence matrix M over $\mathbb{F}_p$, and will be denoted by $\mathrm{rank_p}\, D$. The dimension of the q-ary block code of a design is equal to its p-rank, for $q = p^c$.

Our constructions will make extensive use of complementary designs. The *complementary design* $\overline{D}$ of a given design D has as blocks the complements of the blocks of D.

If M is an incidence matrix of a design D then $J-M$ is the incidence matrix of the complementary design $\overline{D}$, where J is the all-one matrix of appropriate size. If D is a 2-(v,w,λ) design, then $\overline{D}$ is a 2-$(v,v-w,v-2r+\lambda)$ design, where $r = \lambda(v-1)/(w-1)$.

We will focus on designs derived from finite geometries. The points and t-subspaces of the m-dimensional projective geometry $PG(m,q)$ form a 2-(v,w,λ) design, denoted by $PG_t(m,q)$, with parameters

$$v = \frac{q^{m+1}-1}{q-1},\ w = \frac{q^{t+1}-1}{q-1},\ \lambda = \begin{bmatrix} m-1 \\ t-1 \end{bmatrix}_q,$$

where $\begin{bmatrix} m \\ i \end{bmatrix}_q$ is the Gaussian coefficient given by

$$\begin{bmatrix} m \\ i \end{bmatrix}_q = \frac{(q^m-1)(q^{m-1}-1)\cdots(q^{m-i+1}-1)}{(q^i-1)(q^{i-1}-1)\cdots(q-1)}.$$

The design $PG_t(m,q)$ has $b = \begin{bmatrix} m+1 \\ t+1 \end{bmatrix}_q$ blocks, and each point appears in $r = \begin{bmatrix} m \\ t \end{bmatrix}_q$ blocks.

Similarly, the points and t-subspaces of the m-dimensional affine geometry $AG(m,q)$ form a 2-(v,w,λ) design, denoted by $AG_t(m,q)$, with parameters

$$v = q^m,\ w = q^t,\ \lambda = \begin{bmatrix} m-1 \\ t-1 \end{bmatrix}_q.$$

The design $AG_t(m,q)$ has $b = q^{m-t} \left[\begin{smallmatrix} m \\ t \end{smallmatrix}\right]_q$ blocks, and each point appears in $r = \left[\begin{smallmatrix} m \\ t \end{smallmatrix}\right]_q$ blocks. In the special case $q = 2$, $AG_t(m,2)$ is also a 3-$(2^m, 2^t, \left[\begin{smallmatrix} m-2 \\ t-2 \end{smallmatrix}\right]_2)$ design.

Traditionally, the block code of a design $PG_t(m,q)$ or $AG_t(m,q)$, $q = p^c$, is considered over $\mathbb{F}_p$ [AK92].

The binary code spanned by the incidence matrix of $AG_t(m,2)$ is equivalent to a Reed-Muller code of order $m-t$ and length 2^m. If $q = p$ is a prime, then the p-ary code of $AG_t(m,p)$ is equivalent to a generalized Reed-Muller code, and the p-ary code of $PG_t(m,p)$ is equivalent to a non-primitive generalized Reed-Muller code. The q-ary quantum codes obtained from generalized Reed-Muller codes have been studied previously in [Ste99, SK05].

In this paper, we will focus on the case where q is not prime. In this case, the p-ary block codes of affine and projective geometries are subcodes of certain generalized Reed-Muller codes. However, the dimensions and minimum distances of these codes are not related to the generalized Reed-Muller codes in any simple manner. We will focus on p-ary quantum codes arising from the block codes of projective or affine geometries which were constructed over a finite field of an arbitrary prime power order $q = p^c$. To the best of our knowledge, these quantum codes have not been studied systematically before.

4.2 Quantum codes from projective geometry

We begin by studying the parameters of designs and codes obtained from projective geometries. To determine the dimension of a quantum code obtained from a projective geometry design, it is necessary to know the p-rank of the design. The p-ranks of the incidence matrices of finite geometry designs were computed by Hamada [Ham68].

Theorem 34 (Hamada [Ham68])**.** *The p-rank of $PG_t(m,p^c)$ is equal to*

$$R_P(m,t,p^c) = \sum_{(s_0,s_1,\dots,s_c)} \prod_{j=0}^{c-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{m+1}{i} \binom{m+s_{j+1}p-s_j-ip}{m}$$

where the sum is taken over all ordered sets $(s_0, s_1, \ldots, s_c)$ *such that* $s_0 = s_c$, $s_j \in \mathbb{Z}$ *such that* $t+1 \le s_j \le m+1$ *and* $0 \le s_{j+1}p - s_j \le (m+1)(p-1)$*, and*

$$L(s_{j+1}, s_j) = \left\lfloor \frac{s_{j+1}p - s_j}{p} \right\rfloor.$$

In general, the code spanned by the incidence matrix of $PG_t(m,q)$ is not self-orthogonal. However, a related code is often self-orthogonal. Since the intersection of projective subspaces is a subspace, the size of the intersection of two distinct blocks of $PG_t(m,q)$ is of the form $\frac{q^i-1}{q-1}$, $(0 \le i \le t)$, and there are pairs of disjoint blocks ($i = 0$) only if $t \le (m-1)/2$. Consequently, if $t > (m-1)/2$, the intersection of the complements of any two blocks of $PG_t(m,q)$ is of size divisible by q, and we have the following.

Lemma 13 (Hirschfeld and Shaw [HS94])**.** *If* $t > (m-1)/2$*, the code* $C_p(\overline{PG}_t(m,p^c))$ *is self-orthogonal.*

The following lemmas establish basic relations between complementary projective geometry codes and the original projective geometry codes. Throughout, let $C = C_p(PG_t(m,q))$ and $\overline{C} = C_p(\overline{PG}_t(m,q))$. The symbol $\mathbf{1}$ denotes the all-ones vector of appropriate length.

Lemma 14. *The codes* $C = C_p(PG_t(m,q))$ *and* $\overline{C} = C_p(\overline{PG}_t(m,q))$ *are related as follows:*

1. $C = \left\langle \overline{C} \cup \mathbf{1} \right\rangle$
2. $C^\perp = \overline{C}^\perp \cap \langle \mathbf{1} \rangle^\perp$
3. $\overline{C} = C \cap \langle \mathbf{1} \rangle^\perp$
4. $\overline{C}^\perp = \left\langle C^\perp \cup \mathbf{1} \right\rangle$

Proof. Parts 1 and 2 are due to Hirschfeld and Shaw [HS94]. For part 3, we use part 1, and the facts that $\overline{C} \subseteq \langle \mathbf{1} \rangle^\perp$ and $\mathbf{1} \notin \langle \mathbf{1} \rangle^\perp$ (because the length of the code is not a multiple of p). Part 4 follows from taking the dual of the codes in part 3. □

Lemma 15. $\dim(\overline{C}) = \dim(C) - 1$.

Proof. Follows from Lemma 14. □

According to Theorem 33 (ii), if a q-ary quantum stabilizer code is constructed from a self-orthogonal classical linear code C, then the minimum distance of the quantum code is determined by the minimum distance of $C^{\perp}$. The following theorem gives the exact value of the minimum distance of the duals of the complementary projective geometry codes, as well as characterizing their minimum-weight codewords.

Theorem 35. *Suppose $(m-1)/2 < t < m$, and $q = p^c$, where p is an odd prime or $q \neq 2$. Let $\overline{C}^{\perp} = C_p(\overline{PG}_t(m,q))^{\perp}$. Then the minimum distance d of $\overline{C}^{\perp}$ is exactly $d = \frac{q^{m-t+1}-1}{q-1}$. Furthermore, each word of minimum weight in $\overline{C}^{\perp}$ is a scalar multiple of the incidence vector of a projective $(m-t)$-space.*

Proof. We use the notation c_B to denote the incidence vector of a projective subspace B. Let T be a projective t-space, and let M be a projective $(m-t)$-space in $PG(m,q)$. Then $|\overline{T} \cap M| = \frac{q^{m-t+1}}{q-1} - |T \cap M|$, where $T \cap M$ is a projective subspace with projective dimension at most $m-t$. Thus $|\overline{T} \cap M| = \frac{q^{m-t+1}-q^{i+1}}{q-1} = q^{i+1}\frac{q^{m-t-i}-1}{q-1}$ for some $i \in \{0,1,\ldots,m-t\}$. Thus $|\overline{T} \cap M| \equiv 0 \pmod{q}$, and so $c_M \in \overline{C}^{\perp}$. Therefore the incidence vector of each $(m-t)$-space in $PG(m,q)$ is in $\overline{C}^{\perp}$, and so $d \leq \frac{q^{m-t+1}-1}{q-1}$.

Next, note that a vector c is in $\overline{C}^{\perp}$ if an only if $c \cdot (\mathbf{1} - c_T) = 0$ for each block T of $PG_t(m,q)$. Thus $(c \cdot \mathbf{1}) - (c \cdot c_T) = 0$, and so $c \cdot c_T$ is a constant for all T. We consider two cases:

First, suppose that $c \cdot c_T = 0$. Then $c \in C_p(PG_t(m,q))^{\perp}$. It is well known that the minimum distance of $C_p(PG_t(m,q))^{\perp}$ at least $(q+p)q^{m-t-1}$ (see, for example, [AK92, Theorem 5.7.9]). We compare the minimum possible weight of c to the desired minimum weight of $\overline{C}^{\perp}$:

$$(q+p)q^{m-t-1} - \frac{q^{m-t+1}-1}{q-1} = \frac{(q-1)(q+p)q^{m-t-1} - (q^{m-t+1}-1)}{q-1}.$$

Then the numerator is:

$$(q-1)(q+p)q^{m-t-1} - (q^{m-t+1}-1) = (p-1)q^{m-t} - pq^{m-t-1} - 1.$$

As long as $q \neq 2$, $(p-1)q^{m-t} - pq^{m-t-1} - 1 > 0$, and so the weight of c is strictly larger than our desired minimum distance. We note that in the case that p is an odd prime, the code is a generalized Reed-Muller code, and the bound $(q+p)q^{m-t-1}$ is then tight [AK92, CKdR99].

Next, suppose that $c \cdot c_T \neq 0$. This implies that the support of c intersects every t-space. Thus, the support of c is a blocking set for t-spaces in $PG(m,q)$. By [BB66], the smallest blocking sets for t-spaces are exactly projective $(m-t)$-spaces, and so c is at least as large as such a space.

Thus in either case, $\mathrm{wt}(c) \geq \frac{q^{m-t+1}-1}{q-1}$, and so the minimum distance of $\overline{C}^{\perp}$ is exactly $\frac{q^{m-t+1}-1}{q-1}$.

Finally, let c be a word of minimum weight. By the above argument and [BB66], the support of c is an $(m-t)$-space N in $PG(m,q)$. Suppose that the first nonzero coordinate of c is $\alpha \in \mathbb{F}_p$. Then $\alpha \cdot c_N - c$ is in $\overline{C}^{\perp}$ and has at most $\mathrm{wt}(c)-1$ nonzero coordinates, and so it must be exactly the zero vector. Thus c is a scalar multiple of the incidence vector of N. □

Note that in the statement of Theorem 35, we excluded the case $q = 2$. In this case, the codes are exactly the classical Reed-Muller codes, which have been thoroughly studied in both a classical and quantum setting.

We are now ready to give the parameters of the quantum codes based on $C_p(\overline{PG}_t(m,q))$.

Theorem 36. *Suppose that $t > (m-1)/2$, and $q = p^c$, where p is prime. Then the code $C_p(\overline{PG}_t(m,q))$ gives rise to a p-ary quantum stabilizer code with parameters*

$$\left[\left[\frac{q^{m+1}-1}{q-1}, \frac{q^{m+1}-1}{q-1} - 2(R_P(m,t,q)-1), \frac{q^{m-t+1}-1}{q-1}\right]\right]_p$$

where $R_P(m,t,q)$ is given by Theorem 34.

Proof. We use Theorem 33. The code length is the number of points in the projective geometry. The dimension follows from Hamada's formula (Theorem 34) and the dimension of complementary codes (Lemma 14). The minimum distance is given by Theorem 35. □

Corollary 4. *The code $C_p(\overline{PG}_{m-1}(m,p^c))$ gives rise to a p-ary quantum stabilizer code with parameters*

$$\left[\left[\frac{q^{m+1}-1}{q-1}, \frac{q^{m+1}-1}{q-1} - 2\binom{p+m-1}{m}^c, q+1\right]\right]_p.$$

Proof. The dimension is a simplification of Hamada's formula, due to Smith [Smi69]. The minimum distance is given by Theorem 35. □

Table 4.1
Sample parameters of p-ary quantum codes obtained from $\overline{PG}_t(m,p^c)$.

m	t	q	rank	Quantum code
4	3	4	25	$[[341,291,5]]_2$
5	3	4	301	$[[1365,763,21]]_2$
5	4	4	36	$[[1365,1293,5]]_2$
3	2	8	64	$[[585,457,9]]_2$
4	3	8	125	$[[4681,4431,9]]_2$
2	1	9	36	$[[91,19,10]]_3$
3	2	9	100	$[[820,620,10]]_3$
4	2	9	2760	$[[7381,1859,91]]_3$
4	3	9	225	$[[7381,6931,10]]_3$
3	2	25	1225	$[[16276,13826,26]]_5$
4	2	25	132851	$[[406901,141199,651]]_5$

Table 4.1 gives a few sample parameters of the quantum codes obtained from complementary projective design codes.

4.3 Quantum codes from affine geometry

Affine geometries are closely related to projective geometries. However, their natural parallelism changes some of the related codes in important ways. In particular, the complementary designs will not play an important role in this case.

The p-ranks of affine geometry designs, and hence the dimensions of their codes, are known in all cases. They can be expressed simply in terms of the ranks of projective geometries, given in Theorem 34.

Theorem 37 (Hamada [Ham68])**.** *The p-rank of $AG_t(m,q)$, $q=p^c$, is given by*

$$R_A(m,t,q) = R_P(m,t,q) - R_P(m-1,t,q).$$

Lemma 16. *The intersection numbers of $AG_t(m,q)$ are $\{0\} \cup \{q^i : \max\{0,2t-m\} \leq i \leq t-1\}$.*

We note that intersection size 1 occurs if and only if $2t-m \leq 0$, that is, if $t \leq m/2$. If $t > m/2$, all intersection sizes are multiples of q. This leads to the fundamental result necessary for creating quantum codes:

Lemma 17. *If $t > m/2$, then the code $C_p(AG_t(m,q))$ is self-orthogonal.*

The minimum distances of the dual affine geometry codes are known only in a few cases, and bounded in others. The current best known results are summarized in the following two theorems.

Theorem 38 (Calkin, Key, de Resmini [CKdR99])**.** *The minimum distance of the code $C_p(AG_t(m,2^c))^\perp$ is $(q+2)q^{m-t-1}$.*

Theorem 39 (K. L. Clark, Key [CK99])**.** *The minimum distance $d^\perp$ of $C_p(AG_t(m,q))^\perp$, where $q = p^c$ and p is odd, is bounded by*

$$\frac{4(q^m-1)}{3(q^t-1)} + \frac{2}{3} \le d^\perp \le 2q^{m-t}.$$

If $p \neq 3$ then

$$\frac{3(q^m-1)}{2(q^t-1)} + \frac{1}{2} \le d^\perp \le 2q^{m-t}.$$

If $c = 1$ (that is, q is prime), then the minimum distance is exactly

$$d = 2q^{m-t}.$$

Using these results, Theorem 33 (ii), and Lemma 17, we obtain the following result concerning quantum codes.

Theorem 40. *Suppose that $t > m/2$, and let q be a power of a prime p. Then the code $C_p(AG_t(m,q))$ gives rise to a p-ary quantum stabilizer code with parameters*

$$\left[\left[q^m, q^m - 2R_A(m,t,q), d^\perp\right]\right]_p,$$

where $d^\perp$ is bounded as in Theorems 38 and 39, and $R_A(m,t,q)$ is given by Theorem 37.

Table 2 lists a few sample parameters of quantum codes obtained from affine geometry designs.

Finally, we note that the code of an affine geometry design and the code of its complementary design are equivalent.

Lemma 18. *Let $C = C_p(AG_t(m,q))$ and $\overline{C} = C_p(\overline{AG}_t(m,q))$. Then $C = \overline{C}$.*

Table 4.2
Sample parameters of p-ary quantum codes obtained from $AG_t(m,q)$.

m	t	q	rank	Quantum parameters
4	3	4	25	$[[256,206,6]]_2$
5	3	4	276	$[[1024,472,24]]_2$
5	4	4	36	$[[1024,952,6]]_2$
3	2	8	64	$[[512,384,10]]_2$
4	3	8	125	$[[4096,3846,10]]_2$
3	2	9	100	$[[729,529,d^{\perp} \geq 13]]_3$
4	3	9	225	$[[6561,6111,d^{\perp} \geq 13]]_3$
3	2	25	1225	$[[15625,13175,d^{\perp} \geq 39]]_5$
4	2	25	131625	$[[390625,127375,d^{\perp} \geq 940]]_5$

Proof. Because of the natural parallelism, $\mathbf{1} \in C$, and thus $\overline{C} \subseteq C$. However, the codewords of $\overline{C}$ corresponding to a parallel class of blocks in $AG_t(m,q)$ sum to form $(q^{n-t}-1)\mathbf{1}$, and thus $\mathbf{1} \in \overline{C}$ as well. Thus $C \subseteq \overline{C}$, and $C = \overline{C}$. □

4.4 Acknowledgments

The authors of [CT] (from which this chapter is reprinted) would like to thank the referee for the constructive suggestions which lead to an improvement of our original proof of Theorem 35. This research was partially supported by NSA Grant H98230-10-1-0177.

Chapter 5

Entanglement-assisted quantum low-density parity-check codes

In this chapter[*], we give constructions for a new and more flexible category of quantum error-correcting codes. We demonstrate how Steiner designs – and in particular, certain finite geometry designs – optimize certain parameters for these designs. This gives the first general construction in which the parameters of the resulting codes are fully determined, rather than being partly determined by random choices.

Quantum codes make use of *qubits*, which are analogous to bits in the classical setting. A qubit is a unit of quantum information which may be transmitted or stored, and is susceptible to accumulating errors. We also note that in this chapter, both orientations of incidence matrices of designs are used extensively. We clearly denote which orientation is in use. The default orientation (that is, the orientation to be assumed for a matrix M) is point-by-block. A matrix denoted M^T is a block-by-point incidence matrix.

5.1 Introduction

In this chapter, we develop a general combinatorial method for constructing quantum low-density parity-check (LDPC) codes under the entanglement-assisted stabilizer formalism established by Brun, Devetak, and Hsieh [BDH06a]. Our results include many new ex-

[*] Reprinted with minor editorial changes from Physical Review A, Volume 82, Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev: *Entanglement-assisted quantum low-density parity-check codes* [FCV$^+$10], Copyright 2010 by APS. See permission information in Appendix C.

plicit constructions for entanglement-assisted quantum error-correcting codes for a wide range of parameters. We also prove a variety of new results for classical error-correcting codes, which directly apply to the quantum setting. Most of the quantum codes designed in this chapter achieve high error correction performance and high rates while requiring prescribed amounts of entanglement. These codes can be efficiently decoded by message-passing algorithms such as the sum-product algorithm (for details of iterative probabilistic decoding, see [Mac03]).

The existence of quantum error-correcting codes was one of the most important discoveries in quantum information science [Sho95, Ste96a]. Unfortunately, most of the known quantum error-correcting codes lack practical decoding algorithms.

In this chapter, we focus on the use of LDPC codes in a quantum setting. Classical LDPC codes [Gal63] can be efficiently decoded while achieving information rates close to the classical Shannon limit [LMSS01, RU01, RSU01]. This extends to the quantum setting: the pioneering works of Hagiwara and Imai [HI07] and MacKay, Mitchison, and McFadden [MMM04] presented quantum LDPC codes which surpassed, in simulations, all previously known quantum error-correcting codes. Their quantum codes have nearly as low decoding complexity as their classical counterparts.

However, most of the previous results concerning quantum LDPC codes and related efficiently decodable codes have relied on the stabilizer formalism, which severely restricts the classical codes which can be used. The difficulty in developing constructions for non-stabilizer codes was also a substantial obstacle.

Our results will use the newly developed theory of entanglement-assisted quantum error-correcting codes (EAQECCs) [Bow02, BDH06a, BDH06b, DBH09]. The entanglement-assisted stabilizer formalism allows the use of arbitrary classical binary or quaternary linear codes for quantum data transmission and error correction by using shared entanglement [HDB07, WB08]. Previous work related to entanglement-assisted quantum LDPC codes is due to Hsieh, Brun, and Devetak [HBD09] and Hsieh, Yen, and Hsu [HYH11].

The major difficulty in using classical LDPC codes in the entanglement-assisted quantum setting is that very little is known about methods for designing EAQECCs requiring desirable amounts of entanglement. While entanglement-assisted quantum LDPC codes can achieve both notable error correction performance and low decoding complexity, the resulting quantum codes might require too much entanglement to be usable; in general entanglement is a valuable resource [WB08]. In some situations, one might wish to effectively take advantage of high performance codes requiring a larger amount of entanglement [BDH06b, BDH06a]. To the best of the authors' knowledge, no general methods have been developed which allow the code designer flexibility in choice of parameters and required amounts of entanglement.

Our primary focus in this chapter is to show that it is possible to create infinite classes of EAQECCs which consume prescribed amounts of entanglement and achieve good error correction performance while allowing efficient decoding. Our methods are flexible and address various situations, including the extreme case when an EAQECC requires only one preexisting entanglement bit.

The entanglement-assisted quantum LDPC codes which we construct include quantum analogues of the well-known finite geometry LDPC codes originally proposed by Kou, Lin, and Fossorier [KLF01] (see also [TXK$^+$04, TXLAG05]), and LDPC codes from balanced incomplete block designs that achieve the upper bound on the rate for a classical regular LDPC code with girth six proposed independently by several authors. (see [Joh10] and references therein). Some classes of our codes outperform previously proposed quantum LDPC codes having the best known error correction performance [HI07, MMM04, HBD09, HYH11].

Our primary tools come from combinatorial design theory, which plays an important role in classical coding theory [Ton98] and also gave several classes of stabilizer codes in quantum coding theory [Aly08, Djo08, Djo10, Ton08, Ton09]. The use of combinatorial design theory allows us to exactly determine or give tighter bounds on the parameters of the finite geometry LDPC codes in both quantum and classical settings. Comprehensive lists of the parameters of these codes are given in Tables 5.14 and 5.15 in Appendix 5.B.

In Section 5.2, we outline our framework for designing entanglement-assisted quantum LDPC codes by using combinatorial design theory. Section 5.3 gives explicit constructions for entanglement-assisted quantum LDPC codes based on finite geometries and related combinatorial structures. New results concerning the well-known classical finite geometry LDPC codes are also given in this section. Section 5.4 presents simulation results of our entanglement-assisted quantum LDPC codes and discusses their performance over the depolarizing channel. Section 5.5 contains concluding remarks and discusses some related problems that can be treated with the techniques developed in this chapter.

5.2 Combinatorial entanglement-assisted quantum LDPC codes

In this section we give a general construction method for entanglement-assisted quantum LDPC codes based on combinatorial designs. We do not describe the theory of classical LDPC codes in detail here, instead referring the reader to [Mac03, Joh10] and references therein. Relations between quantum error-correcting codes and LDPC codes are concisely yet thoroughly explained in [MMM04, HBD09]. Basic notions related to LDPC codes and their relations to combinatorial designs can be found in [AHK$^+$04]. For a detailed treatment of the entanglement-assisted stabilizer formalism, we refer the reader to [BDH06a, BDH06b, DBH09, HDB07].

In Subsection 5.2.1 we introduce necessary notions from coding theory and combinatorial design theory. A general method for designing entanglement-assisted quantum LDPC codes is presented in Subsection 5.2.2.

5.2.1 Preliminaries

An $[[n,k;c]]$ *entanglement-assisted quantum error-correcting code* (EAQECC) encodes k logical qubits into n physical qubits with the help of c copies of maximally entangled states. As in classical coding theory, n is the *length* of the EAQECC, and k the *dimension*. We say that the EAQECC requires c *ebits*. An $[[n,k;c]]$ EAQECC with *distance* d will be referred to as an $[[n,k,d;c]]$ code.

The *rate* of an $[[n,k;c]]$ EAQECC is defined to be $\frac{k}{n}$. The ratio $\frac{k-c}{n}$ is called the *net rate*. The latter figure describes the rate of an EAQECC when used as a catalytic quantum error-correcting codes to create c new bits of shared entanglement [BDH06a, BDH06b].

Throughout this chapter, matrix operations are performed over $\mathbb{F}_2$, the finite field of order two. The ranks of matrices are also calculated over $\mathbb{F}_2$.

We employ the well-known Calderbank-Shor-Steane (CSS) construction [CS96, Ste96a, BDH06a, HDB07]. Usually the CSS construction uses a minimal set of independent generators to construct an EAQECC. Hence, the construction is often described by using a classical binary linear code with a parity-check matrix of full rank. However, in actual decoding steps, sparse-graph codes may take advantage of redundant parity-check equations to improve error correction performance. Because the extended syndrome can be obtained in polynomial time without additional quantum interactions, we use the following formulation of the CSS construction for EAQECCs.

Theorem 41 (Hsieh, Brun, and Devetak [HBD09])**.** *If there exists a classical binary* $[n,k,d]$ *code with parity-check matrix* H*, then there exists an* $[[n,2k-n+c,d;c]]$ EAQECC*, where* $c = \operatorname{rank} HH^T$.

Note that H may contain redundant rows which are related only to classical operations to infer the noise by a message-passing algorithm.

We apply Theorem 41 to classical sparse-graph codes. An LDPC code is typically defined as a binary linear code with parity-check matrix H in which every row and column is sparse. In this chapter we consider LDPC codes with parity-check matrices whose rows and columns contain only small numbers of ones so that simple message-passing algorithms can efficiently give good performance in decoding.

Proposition 3. *An* LDPC *code with parity-check matrix H with n columns and minimum distance d defines a classical binary $[n, n - \operatorname{rank} H, d]$ code, which yields an $[[n, n - 2\operatorname{rank} H + \operatorname{rank} HH^T, d; \operatorname{rank} HH^T]]$* EAQECC.

The *Tanner graph* of an $m \times n$ parity-check matrix H is the bipartite graph consisting of n bit vertices and m parity-check vertices, where an edge joins a bit vertex to a parity-check vertex if that bit is included in the corresponding parity-check equation. A *cycle* in a graph is a sequence of connected vertices which starts and ends at the same vertex in the graph and contains no other vertices more than once. The *girth* of a parity-check matrix is the length of a shortest cycle in the corresponding Tanner graph. Short cycles can severely reduce the performance of an otherwise well-designed LDPC code. In fact, one of the greatest obstacles to the development of a general theory of LDPC codes in the quantum setting is the difficulty of avoiding cycles of length four (See, for example, [MMM04, PC08, COT07, HI07]). In order to improve error correction performance, we generally only treat LDPC codes with girth at least six.

The *weight* of a row or column of a binary matrix is its Hamming weight, that is, the number of ones in it. An LDPC code is *regular* if its parity-check matrix H has constant row and column weights, and *irregular* otherwise. Regular LDPC codes are known to be able to achieve high error correction performance. Irregular LDPC codes allow the code designer to optimize characteristics of performance by a careful choice of row weights and column weights [LMSS01, RU01, RSU01].

We now define several combinatorial structures, which we will need in Subsection 5.2.2 and the subsequent sections. For additional facts and design theoretical results, the interested reader is referred to [BJL99].

An *incidence structure* is an ordered pair $(V, \mathscr{B})$ such that V is a finite set of *points*, and $\mathscr{B}$ is a family of subsets of V, called *blocks*. A *point-by-block incidence matrix* of an incidence structure $(V, \mathscr{B})$ is a binary $v \times b$ matrix $H = (h_{i,j})$ in which rows are indexed by points, columns are indexed by blocks, and $h_{i,j} = 1$ if the ith point is contained in the jth block, and $h_{i,j} = 0$ otherwise. A *block-by-point incidence matrix* of $(V, \mathscr{B})$ is the transposed point-by-block incidence matrix H^T.

Any LDPC code can be associated with an incidence structure by interpreting its parity-check matrix as an incidence matrix. The converse also holds as long as the considered incidence matrix is sparse.

This chapter will focus on incidence structures which have been extensively studied in combinatorics. This allows us to effectively exploit combinatorial design theory to develop a framework for designing entanglement-assisted quantum LDPC codes.

A 2-(v,μ,λ) *design* is an incidence structure $(V,\mathscr{B})$, where V is a set of cardinality v and $\mathscr{B}$ is a family of μ-subsets of V such that each pair of points is contained in exactly λ blocks. We will refer to the parameters v, μ, and λ as the *order*, *block size*, and *index* of a 2-design. Note that the block size of a 2-design is usually written as k in the combinatorial literature. To avoid any confusion with the dimension of a code, we use μ instead.

The number $b = |\mathscr{B}|$ of blocks in a 2-(v,μ,λ) design is determined by the design parameters:

$$b = |\mathscr{B}| = \frac{v(v-1)}{\mu(\mu-1)}\lambda. \tag{5.1}$$

A 2-design is called *symmetric* if $b = v$.

Every point of a 2-(v,μ,λ) design occurs in exactly r blocks, where

$$r = \frac{v-1}{\mu-1}\lambda. \tag{5.2}$$

The number r is called the *replication number* of the design. A point-by-block incidence matrix H of a 2-(v,μ,λ) design satisfies the equation

$$HH^T = (r-\lambda)I + \lambda J, \tag{5.3}$$

where I is the identity matrix and J is the $v \times v$ all-one matrix. Because r and b are integers, it follows that the following two conditions

$$\begin{aligned} \lambda(v-1) &\equiv 0 \pmod{\mu-1}, \\ \lambda v(v-1) &\equiv 0 \pmod{\mu(\mu-1)} \end{aligned} \tag{5.4}$$

are necessary conditions for the existence of a 2-(v,μ,λ) design.

If the block size μ and index λ are relatively small, an incidence matrix of a 2-(v,μ,λ) design is sparse. Hence, a point-by-block incidence matrix of a 2-(v,μ,λ) design can be viewed as a parity-check matrix H of a regular LDPC code with constant row weight r and constant column weight μ. Similarly, a block-by-point incidence matrix defines a code with constant row weight μ and constant column weight r. In this chapter, incidence matrices will generally be point-by-block unless it is specifically noted otherwise. In the cases when block-by-point matrices are desirable, the notation H^T will be used.

A substantial part of this chapter deals with one of the most fundamental incidence structures in combinatorial design theory. A *Steiner* 2*-design*, denoted by $S(2,\mu,v)$, is a 2-$(v,\mu,1)$ design. A *Steiner triple system* of order v, denoted by $\mathrm{STS}(v)$, is a Steiner 2-design with block size three. The $S(2,\mu,v)$s are *trivial* Steiner 2-designs if $v \leq \mu$. We generally do not consider trivial designs to be Steiner 2-designs unless they play an important role.

It is easy to see that both point-by-block and block-by-point incidence matrices of an $S(2,\mu,v)$ give regular LDPC codes with girth six (see, for example, [JW01]).

5.2.2 General combinatorial constructions

In this subsection we present a general framework for designing entanglement-assisted quantum LDPC codes based on combinatorial design theory. Specialized construction methods for desirable EAQECCs in this framework will be illustrated in Section 5.3.

The following propositions are derived from Theorem 41 by using incidence matrices as parity-check matrices of binary LDPC codes.

Proposition 4. *Let H be a point-by-block incidence matrix of an incidence structure $(V,\mathscr{B})$. Then there exists a* $[[|\mathscr{B}|, |\mathscr{B}| - 2\operatorname{rank}H + \operatorname{rank}HH^T; \operatorname{rank}HH^T]]$ EAQECC.

Proposition 5. *Let H^T be a block-by-point incidence matrix of an incidence structure $(V,\mathscr{B})$. Then there exists a* $[[|V|, |V| - 2\operatorname{rank}H + \operatorname{rank}H^TH; \operatorname{rank}H^TH]]$ EAQECC.

We employ the following two theorems.

Theorem 42 (Hillebrandt [Hil92]). *The rank of an incidence matrix H of an $S(2,\mu,v)$ satisfies the following inequalities:*

$$\left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{(v-1)(v-\mu)}{\mu}} \right\rceil \leq \operatorname{rank}H \leq v.$$

Theorem 43 (Hamada [Ham73]). *If H is an incidence matrix of an $S(2,\mu,v)$ with even* *replication number $r = \frac{v-1}{\mu-1}$ then*

$$\operatorname{rank} H = \begin{cases} v-1 & \textit{when} \quad \mu \textit{ is even,} \\ v \textit{ or } v-1 & \textit{when} \quad \mu \textit{ is odd.} \end{cases}$$

We now give three simple constructions by applying Propositions 4 and 5 to incidence matrices of Steiner 2-designs. These constructions will be specialized and modified to give desirable codes.

Theorem 44 (High-Rate 1-Ebit Code)**.** *Let H be a point-by-block incidence matrix of an $S(2,\mu,v)$. Suppose $r = \frac{v-1}{\mu-1}$ is odd. Then H has row weight r, column weight μ, girth 6, and the corresponding $[[n,k;c]]$ EAQECC satisfies the following conditions:*

$$n = \frac{v(v-1)}{\mu(\mu-1)},$$

$$\frac{vr}{\mu} - 2v + 1 \le k \le \frac{vr}{\mu} - 2\left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{(v-1)(v-\mu)}{\mu}} \right\rceil + 1,$$

$$c = 1.$$

Proof. By Proposition 4 and Theorem 42, it suffices to prove that $\operatorname{rank} HH^T = 1$. Because r is odd, Equation (5.3) reduces to $HH^T = J$, which implies that the rank of HH^T is equal to one. □

Theorem 45 (High-Rate High-Consumption Code)**.** *Let H be a point-by-block incidence matrix of an $S(2,\mu,v)$. Suppose $r = \frac{v-1}{\mu-1}$ is even. Then H has row weight r, column weight μ, girth 6, and the corresponding $[[n,k;c]]$ EAQECC satisfies the following conditions:*

$$n = \frac{v(v-1)}{\mu(\mu-1)},$$

$$k = \begin{cases} \frac{vr}{\mu} - v + 1 & \textit{when} \quad \mu \textit{ is even,} \\ \frac{vr}{\mu} - v + 1 \textit{ or } \frac{vr}{\mu} - v - 1 & \textit{when} \quad \mu \textit{ is odd,} \end{cases}$$

$$c = v - 1.$$

Proof. By Proposition 4 and Theorem 43, it suffices to prove that $\operatorname{rank} HH^T = v-1$. Because r is even, Equation (5.3) reduces to

$$HH^T = \begin{bmatrix} 0 & 1 & & 1 \\ 1 & 0 & \cdots & 1 \\ & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{bmatrix},$$

that is, a matrix containing zeros on the diagonal and ones in the other entries. Because $r = \frac{v-1}{\mu-1}$ is even, v is odd. Hence, we have $\operatorname{rank} HH^T = v-1$ as desired. □

Theorem 46 (Low-Rate High-Redundancy Code)**.** *Let H^T be a block-by-point incidence matrix of an $S(2,\mu,v)$. Then H has row weight μ, column weight r, girth 6, and the corresponding* $[[n,k;c]]$ EAQECC *satisfies the following conditions:*

$$n = v,$$

$$k \leq v - 2\left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} + \frac{(v-1)(v-\mu)}{\mu}} \right\rceil + c,$$

$$c \geq 1.$$

Proof. Let H^T be a block-by-point incidence matrix of an $S(2,\mu,v)$. Because any nontrivial $S(2,\mu,v)$ contains a pair of blocks that share exactly one point, we have $\operatorname{rank} H^T H \geq 1$. Applying Proposition 5 to Theorem 42 completes the proof. □

It is worth mentioning that a weaker version of Theorem 44 was used in the context of integrated optics and photonic crystal technology [Djo10]. Also notable is that Theorems 44 and 45 can be easily extended to the case when preexisting entanglement is not available. For example, quantum LDPC codes that do not require entanglement can be obtained by applying the extra column method used in Construction U in [MMM04] and the CSS construction to $S(2,\mu,v)$s in the same manner as in Proposition 4. Aly's construction for quantum LDPC codes [Aly08] is a special case of this extended method. Djordjevic's construction for quantum LDPC codes [Djo08] can be obtained by applying the CSS construction to 2-designs of even index in the same way as in Proposition 4.

The existence of 2-designs is discussed in Appendix 5.A, which provides Steiner 2-designs necessary to obtain several infinite families of new entanglement-assisted quantum LDPC codes from Theorems 44, 45, and 46. Before applying our theorems to specific $S(2,\mu,v)$s, we explore general characteristics of our EAQECCs and further develop methods for designing desirable codes.

Theorem 44 yields entanglement-assisted quantum LDPC codes with very high net rates and various lengths while requiring only one ebit. Theorem 45 gives codes which have very high net rates and naturally take advantage of larger numbers of ebits when there is an adequate supply of entanglement. Because $\operatorname{rank} HH^T \leq \operatorname{rank} H$ holds for any parity-check matrix H, the required amounts of entanglement of high rate codes in Theorem 45 are expected to be relatively low when compared with randomly chosen codes of the same lengths. Theorem 46 generates entanglement-assisted quantum LDPC codes which can correct many quantum errors by taking advantage of the higher redundancy. The high error correction performance of these codes will be demonstrated in simulations in Section 5.4.

When a parity-check matrix H of an $S(2,\mu,v)$ is of full rank v, the corresponding classical LDPC code in Theorems 44 and 45 achieves an upper bound on the rate for an LDPC code with girth six.

Theorem 47 (MacKay and Davey [MD99])**.** *Let H be a $v \times n$ parity-check matrix of a classical regular* LDPC *code of length n, column weight μ, and girth* 6*. Let also* $\operatorname{rank} H = v$*. Then it holds that $n \leq \frac{v(v-1)}{\mu(\mu-1)}$, where equality holds if and only if H is an incidence matrix of an $S(2,\mu,v)$.*

It follows that EAQECCs based on Steiner 2-designs achieve the highest possible net rates for quantum LDPC codes with girth at least six constructed from full rank parity-check matrices with constant column weights through the CSS construction.

The rank of an incidence matrix of an $S(2,\mu,v)$ may not be full depending on the structure of the design. If one wishes a parity-check matrix to be regular and full rank at the same time, it is important to choose an $S(2,\mu,v)$ with a full rank incidence matrix. This can always be done for the case when $\mu = 3$ except for $v = 7$ [DHV78]. For a more detailed treatment of the ranks of $S(2,\mu,v)$s, we refer the reader to [Ham73, Ham68, AK92].

In general, the code minimum distance plays less of a role in the performance of sum-product decoding than maximum likelihood decoding [MMM04]. Therefore, we explore in detail the distance d of $[[n,k,d;c]]$ EAQECCs based on LDPC codes only when it is of great theoretical interest. Because codes derived from finite geometries are of great importance in coding theory, the distances of EAQECCs obtained from finite geometries will be investigated in detail in Section 5.3.

Here we briefly review the minimum distances of LDPC codes based on Steiner 2-designs. A pair of $S(2,\mu,v)$s which are not mutually isomorphic may give different minimum distances. The tightest known upper and lower bounds on the minimum distance of an LDPC code based on an $\mathrm{STS}(v)$ can be found in the very large scale integration (VLSI) literature as bounds on even-freeness.

Theorem 48 (Fujiwara and Colbourn [FC10]). *The minimum distance d of a classical binary linear code whose parity-check matrix forms an incidence matrix of a non-trivial* $\mathrm{STS}(v)$ *satisfies* $4 \leq d \leq 8$.

A carefully chosen triple system can have a good topological structure which gives good decoding performance. If conditions require larger minimum distances, the code designer may use either block-by-point incidence matrices, or $S(2,\mu,v)$s of larger block sizes. For known results on minimum distances, girths, and related characteristics of LDPC codes based on combinatorial designs, the reader is referred to [CF09, FC10, Joh04] and references therein.

In what follows, we describe general guidelines for designing entanglement-assisted quantum LDPC codes with desired parameters and properties by exploiting codes we have presented in this section.

We first consider an $[[n,k;c]]$ EAQECC requiring only a small amount of entanglement. The extreme case is when $c = 1$. The following theorem gives infinitely many such EAQECCs having extremely high rates and low decoding complexity.

Theorem 49. *Let v and μ be positive integers satisfying $v-1 \equiv 0 \pmod{\mu-1}$ and $v(v-1) \equiv 0 \pmod{\mu(\mu-1)}$. Suppose also that $\frac{v-1}{\mu-1}$ is odd. Then for all sufficiently large v and some k satisfying the condition of Theorem 44, there exists an* $[[\frac{v(v-1)}{\mu(\mu-1)},k;1]]$ EAQECC.

Proof. Use Wilson's Theorem [Wil72a, Wil72b, Wil75], which guarantees the existence of an $S(2,\mu,v)$ for all sufficiently large v, and apply Theorem 44. □

Similarly, applying Theorem 44 to known $S(2,\mu,v)$s with small v discussed in Appendix 5.A gives $[[n,k;1]]$ EAQECCs of shorter length n.

In general, the error floor of a well-designed LDPC code is not dominated by low-weight codewords. Nonetheless, it is desirable to carefully choose an $S(2,\mu,v)$ when applying our simple constructions so that the resulting code has a promising topological structure. While incidence matrices of $S(2,\mu,v)$s have long been investigated in various fields, it appears to be difficult to achieve the known upper bounds on the minimum distance of an LDPC code based on an incidence matrix of an $S(2,\mu,v)$. In fact, it is conjectured that the known upper bounds are generally not achievable even for the case $\mu = 3$ [CF09].

An STS is 4-*even-free* (or *anti-Pasch*) if its incidence matrix gives a classical LDPC code with minimum distance five or greater. A 4-even-free $\mathrm{STS}(v)$ exists for all $v \neq 7, 13$ satisfying the necessary conditions (5.4) [GGW00]. It is conjectured that an incidence matrix of a 4-even-free STS(v) gives the largest possible minimum distance [CF09].

Theorem 50. *There exists a* $[[\frac{v(v-1)}{6},k,d;1]]$ EAQECC *with* $k \geq \frac{v(v-1)}{6} - 2v + 1$ *and* $d \geq 5$ *for every* $v \equiv 3,7 \pmod{12}$ *except for* $v = 7$.

Proof. If $v \equiv 3,7 \pmod{12}$, then the replication number of an STS(v) is odd. Applying Theorem 44 to a 4-even-free STS(v) completes the proof. □

A block-by-point incidence matrix of a symmetric $S(2,\mu,v)$ can also be viewed as a point-by-block incidence matrix of a Steiner 2-design of the same parameters [CD07]. Hence, Theorems 44 and 46 can overlap when symmetric designs are employed. This special case gives the EAQECCs with $c = 1$ and good error correction performance originally presented in [HYH11]. For completeness, we give a simple proof by using the following two theorems.

Theorem 51. *For every integer* $t \geq 1$ *there exists a symmetric* $S(2,2^t+1,4^t+2^t+1)$ *whose incidence matrix* H *satisfies* $\operatorname{rank} H = 3^t + 1$.

Proof. Take as $S(2,2^t+1,4^t+2^t+1)$ the Desarguesian projective plane of order 2^t, whose incidence matrix has rank 3^t+1 [GM72]. □

Theorem 52 (Calkin, Key, and de Resmini [CKdR99])**.** *Let* H^T *be a block-by-point incidence matrix of a symmetric* $S(2,2^t+1,4^t+2^t+1)$ *being the Desarguesian projective plane* $PG(2,2^t)$*. Then* H^T *defines a classical binary linear* $[4^t+2^t+1,4^t+2^t-3^t,2^t+2]$ *code.*

Now as a corollary of Theorems 44 and 46 and the preceding two theorems, we obtain the following result.

Theorem 53. *For every integer* $t \geq 1$ *there exists a* $[[4^t+2^t+1,4^t+2^t-2\cdot 3^t,2^t+2;1]]$ EAQECC.

EAQECCs of this kind can be seen as quantum analogues of special Type I PG-LDPC codes, which have notable error correction performance in the classical setting [KLF01, TXK$^+$04, TXLAG05]. Because of the direct correspondence between entanglement assisted quantum codes and classical codes, these EAQECCs inherit excellent error correction performance while consuming only one initial ebit. We will further investigate entanglement-assisted quantum LDPC codes based on $S(2,\mu,v)$s with large minimum distances in Section 5.3.

Next we present general combinatorial methods for designing EAQECCs with relatively small c and better error correction performance. The main idea is that we discard some columns from an incidence matrix of an $S(2,\mu,v)$ and then apply Proposition 4 as we did in Theorem 44. Our methods encompass the rate control technique for classical LDPC codes proposed in [JW03] as a special case.

Let $(V,\mathscr{B})$ be an $S(2,\mu,v)$. Take two subsets $V' \subsetneq V$ and $\mathscr{B}' \subsetneq \mathscr{B}$. The pair $(V',\mathscr{B}')$ is called a *proper subdesign* of block size μ if it is an $S(2,\mu,|V'|)$. Because we do not consider other kinds of subdesigns, we simply call a proper subdesign $(V',\mathscr{B}')$ of block size μ a subdesign. A pair of subdesigns $(V',\mathscr{B}')$ and $(V'',\mathscr{B}'')$ of an $S(2,\mu,v)$ are *point-wise disjoint* if $V' \cap V'' = \emptyset$.

Theorem 54. *Let $(V,\mathscr{B})$ be an $S(2,\mu,v)$ with odd $r = \frac{v-1}{\mu-1}$. Assume that $(V,\mathscr{B})$ contains j point-wise mutually disjoint subdesigns $(V_i,\mathscr{B}_i)$, $1 \leq i \leq j$, such that $\bigcup_{i=1}^{j} V_i \subsetneq V$ and each $(V_i,\mathscr{B}_i)$ has odd replication number. Then there exists an $[[n,k;c]]$ EAQECC satisfying the following conditions:*

$$n = \frac{v(v-1)}{\mu(\mu-1)} - |\bigcup \mathscr{B}_i|,$$
$$c = j+1.$$

Proof. Take an arbitrary incidence matrix H of an $S(2,\mu,v)$ with odd r. Delete j point-wise mutually disjoint subdesigns $(V_i,\mathscr{B}_i)$ each of which has odd replication number. It is always possible to reorder the rows and columns of the resulting incidence matrix H' such that $H'H'^T$ has the form:

$$H'H'^T = \begin{bmatrix} J & J & & J \\ J & 0_1 & \cdots & J \\ & \vdots & \ddots & \vdots \\ J & J & \cdots & 0_j \end{bmatrix}$$

where 0_i is a $|V_i| \times |V_i|$ zero matrix and each J is an all-one matrix of appropriate size. It is easy to see that $\operatorname{rank} H'H'^T = j+1$. Applying Proposition 4 to H' completes the proof. □

Deleting subdesigns always shortens the length of the corresponding code. Discarding columns will not decrease the minimum distance or the girth. The rank of the parity-check matrix is unlikely to change. In this sense, we expect EAQECCs obtained through subdesign deletion to have better error correction performance than the original code. We will demonstrate this effect in simulations in Section 5.4.

In general, deleting a subdesign makes a parity-check matrix slightly irregular. If this irregularity is not desirable because of particular circumstances or conditions, it can be alleviated by discarding more point-wise disjoint subdesigns. In fact, if we delete subdesigns of the same order such that each point belongs to one deleted subdesign, we obtain a regular parity-check matrix again. The following construction demonstrates this.

Let $(V, \mathscr{B})$ be an $S(2, \mu, v)$ and $\mathscr{S}$ a set of Steiner 2-designs $(V_i, \mathscr{B}_i), 1 \leq i \leq |\mathscr{S}|$, where $V_1, \ldots, V_{|\mathscr{S}|}$ partition V, that is, $\bigcup V_i = V$ and $V_i \cap V_j = \emptyset$ for all $i \neq j$. Then $\mathscr{S}$ is called a *Steiner spread* in $(V, \mathscr{B})$ if each $(V_i, \mathscr{B}_i)$ forms a subdesign $S(2, \mu, |V_i|)$ of $(V, \mathscr{B})$.

Theorem 55. *Let $(V, \mathscr{B})$ be an $S(2, \mu, v)$ with odd replication number $r = \frac{v-1}{\mu-1}$. Assume that $(V, \mathscr{B})$ contains a Steiner spread $\mathscr{S}$, where each subdesign $(V_i, \mathscr{B}_i)$ has odd replication number. Then there exists an $[[n, k; c]]$* EAQECC *satisfying the following conditions:*

$$n = \frac{v(v-1)}{\mu(\mu-1)} - |\bigcup \mathscr{B}_i|,$$

$$c = \begin{cases} |\mathscr{S}| - 1 & \text{when} \quad |\mathscr{S}| \text{ is odd,} \\ |\mathscr{S}| & \text{when} \quad |\mathscr{S}| \text{ is even.} \end{cases}$$

Moreover, if $|V_i| = |V_{i'}| = w$ for all i and i', then the parity-check matrix of the corresponding LDPC *code is regular and has row weight $r - \frac{w-1}{\mu-1}$ and column weight μ.*

Proof. Let H be an incidence matrix of an $S(2, \mu, v)$ with odd r which contains a Steiner spread $\mathscr{S}$. Delete all members of the Steiner spread from $(V, \mathscr{B})$. By following the same argument as in the proof of Theorem 54, it is straightforward to see that $\operatorname{rank} HH^T = |\mathscr{S}| - 1$ when $|\mathscr{S}|$ is odd, and $|\mathscr{S}|$ otherwise. If $|V_i| = |V_{i'}| = w$ for all i and i', each subdesign has the same replication number $\frac{w-1}{\mu-1}$. Hence, the resulting code is regular. □

When there is an adequate supply of entanglement, it may be acceptable to exploit a relatively large amount of entanglement to improve error correction performance while keeping similar characteristics of high rate codes. Deleting an $S(2, \mu, w)$ with even replication number $\frac{w-1}{k-1}$ increases the required amount of entanglement to a slightly larger extent.

Theorem 56. *Let $(V, \mathscr{B})$ be an $S(2, \mu, v)$ with odd replication number $r = \frac{v-1}{\mu-1}$. Assume that $(V, \mathscr{B})$ contains j point-wise mutually disjoint subdesigns $(V_i, \mathscr{B}_i)$, $1 \leq i \leq j$, such that $\bigcup_{i=1}^{j} V_i \subseteq V$ and each $(V_i, \mathscr{B}_i)$ has even replication number. Then there exists an $[[n, k; c]]$* EAQECC *satisfying the following conditions:*

$$n = \frac{v(v-1)}{\mu(\mu-1)} - |\bigcup \mathscr{B}_i|,$$

$$c = \sum_{i=1}^{j} (|V_i| - 1) + 1.$$

Moreover, if the subdesigns $(V_i, \mathscr{B}_i)$ for $1 \leq i \leq j$ form a Steiner spread with $|V_i| = |V_{i'}| = w$ for all i and i′, then the parity-check matrix of the corresponding LDPC *code is regular and has row weight $r - \frac{w-1}{\mu-1}$ and column weight μ.*

Proof. Take an arbitrary incidence matrix H of an $S(2,\mu,v)$ with odd r. Delete j point-wise mutually disjoint subdesigns $(V_i, \mathscr{B}_i)$ each of which has even replication number. If $\bigcup_{i=1}^{j} V_i \subsetneq V$, it is always possible to reorder the columns of the resulting incidence matrix H' such that $H'H'^T$ is of the form:

$$H'H'^T = \begin{bmatrix} J & J & & J \\ J & I_1 & \cdots & J \\ & \vdots & \ddots & \vdots \\ J & J & \cdots & I_j \end{bmatrix}$$

where I_i is the $|V_i| \times |V_i|$ identity matrix and each J is an all-one matrix of appropriate size. Because each I_i has V_i independent rows and each $|V_i|$ is odd, $\operatorname{rank} H'H'^T = \sum_{i=1}^{j} (|V_i| - 1) + 1$. Applying Proposition 4 to H' gives $c = \sum_{i=1}^{j} (|V_i| - 1) + 1$. If $\bigcup_{i=1}^{j} V_i = V$, we have identity matrices across the diagonal of $H'H'^T$. Hence, we have $c = \sum_{i=1}^{j} (|V_i| - 1) + 1$ again. If each V_i is of the same size, it is straightforward to see that the resulting code is regular. □

When irregularity in a parity-check matrix is acceptable or favorable, the code designer can combine the techniques of Theorems 54, 55, and 56. The required amount of entanglement is readily computed by the same argument as above.

In general, subdesign deletion changes the parameters of a code in a gradual manner. Hence, these techniques are also useful when one would like an EAQECC of specific length or dimension. While we only employed Theorem 44 in the above arguments, Theorem 45 can also be used in a straightforward manner to fine-tune the parameters of EAQECCs.

In order to exploit the subdesign deletion techniques, one needs Steiner 2-designs having subdesigns or preferably Steiner spreads of appropriate sizes. We conclude this section with a brief review of known general results and useful theorems for finding $S(2,\mu,v)$ with subdesigns and Steiner spreads. For a more thorough treatment, the reader is referred to [CD07, BJL99] and references therein.

The well-known Doyen-Wilson theorem [DW79] states that one can always find an STS(v)

containing an STS(w) as a subdesign as long as both v and w satisfy the necessary conditions for the existence of an STS and $v \geq 2w+1$. The following is a general asymptotic theorem on Steiner 2-designs having subdesigns.

Theorem 57 (Fujiwara [Fuj07])**.** *Let $\mu \geq 2$ be a positive integer and $w \equiv 1 \pmod{\mu(\mu-1)}$. Then there exist a constant number w_0 depending on μ, and a constant number v_0 depending on w and μ such that if $w > w_0$ and $v > v_0$ satisfies the conditions $v-1 \equiv 0 \pmod{\mu-1}$ and $v(v-1) \equiv 0 \pmod{\mu(\mu-1)}$, then there exists an $S(2,\mu,v)$ having an $S(2,\mu,w)$ as a subdesign.*

Theorem 57 states that one can always find an $S(2,\mu,v)$ having an $S(2,\mu,w)$ as a subdesign as long as v is a sufficiently large integer satisfying the necessary conditions (5.4) and w is a sufficiently large integer satisfying $w \equiv 1 \pmod{\mu(\mu-1)}$.

Steiner spreads are closely related to a special kind of combinatorial design. A *group divisible design* (GDD) with *index* one is a triple $(V,\mathscr{G},\mathscr{B})$, where

(i) V is a finite set of elements called *points*,

(ii) $\mathscr{G}$ is a family of subsets of V, called *groups*, which partition V,

(iii) $\mathscr{B}$ is a collection of subsets of V, called *blocks*, such that every pair of points from distinct groups occurs in exactly one block,

(iv) $|G \cap B| \leq 1$ for all $G \in \mathscr{G}$ and $B \in \mathscr{B}$.

If all groups are of the same size g, all blocks are of the same size μ, and $|\mathscr{G}| = t$, one refers to the design as a μ-GDD of *type* g^t.

Theorem 58. *The existence of an $S(2,\mu,g)$ and a μ-GDD $(V,\mathscr{G},\mathscr{B})$ of type g^t with index one implies the existence of an $S(2,\mu,gt)$ having a Steiner spread $\mathscr{S}$, where each member of $\mathscr{S}$ is an $S(2,\mu,g)$.*

Proof. Let $(V,\mathscr{G},\mathscr{B})$ be a μ-GDD of *type* g^t with index one and $(V',\mathscr{B}')$ an $S(2,\mu,g)$. For each $G \in \mathscr{G}$, we construct an $S(2,\mu,g)$, $(G,\mathscr{B}'_G)$, by mapping each point of $(V',\mathscr{B}')$ to an element of G by an arbitrary bijection $\pi_G : V' \rightarrow G$. Define $\mathscr{C} = \bigcup_{G\in\mathscr{G}} \mathscr{B}'_G$. It is straightforward to check that $(V,\mathscr{B}\cup\mathscr{C})$ is an $S(2,\mu,gt)$ having a Steiner spread whose members are all $S(2,\mu,g)$s. □

The above theorem is useful to obtain regular LDPC codes through Theorems 55 and 56 and similar subdesgin deletion techniques based on Theorem 45. One can also modify Theorem 58 for the case when a GDD has different group sizes by a similar argument. The existence of GDDs and their constructions have been extensively investigated in combinatorial design theory. For a comprehensive list of known existence results on GDDs, we refer the reader to [CD07].

5.3 Finite geometry codes

In this section, we demonstrate applications of our general designing methods by using combinatorial designs arising from finite geometries.

The classical LDPC codes obtained from finite geometries are known to have remarkable error correction abilities. By using these codes, we generate infinitely many new high performance entanglement-assisted quantum LDPC codes having numerous Steiner spreads of various sizes. The various Steiner spreads in each code allow the code designer to flexibly fine-tune the parameters and error correction performance.

This section is divided into three subsections. Subsection 5.3.1 studies entanglement-assisted quantum LDPC codes of girth six obtained from projective geometries. Codes based on affine geometries are investigated in Subsection 5.3.2. In Subsection 5.3.3 we investigate slightly modified affine geometry codes, called Euclidean geometry codes. Classical LDPC codes based on these three kinds of finite geometries are called *finite geometry LDPC codes* or simply *FG-LDPC codes*.

Many of the results presented in this section can also be seen as new results on classical finite geometry LDPC codes. In particular, properties of finite geometries have been independently studied in the combinatorial literature, and hence many of the “known" results are new results in the field of LDPC codes. For the convenience of the reader, we summarize our results on fundamental parameters of LDPC codes from finite geometries in Tables 5.14 and 5.15 in Appendix 5.B. Lengths, dimensions, and minimum distances of the FG-LDPC codes with girth six from projective geometry $PG(m,q)$, affine geometry $AG(m,q)$, and Euclidean geometry $EG(2,2^t)$ are all determined. Specifically for EAQECCs based on FG-LDPC codes, we also determine the required amounts of entanglement for most cases. For a few cases, we give upper bounds on the required amount of entanglement.

5.3.1 Projective geometry codes

We begin with EAQECCs obtained from finite projective geometries. The use of projective geometries for constructing EAQECCs first appeared in the work of Hsieh, Yen, and Hsu [HYH11]. This subsection illustrates how our combinatorial framework generalizes their method and determines fundamental parameters of quantum and classical LDPC codes obtained from $PG(m,q)$.

Points of the m-dimensional projective geometry $PG(m,q)$ over $\mathbb{F}_q$ are the 1-dimensional subspaces of $\mathbb{F}_q^{m+1}$. The i-dimensional projective subspaces of $PG(m,q)$ are the $(i+1)$-dimensional vector subspaces of $\mathbb{F}_q^{m+1}$. The points and lines of $PG(m,q)$ form an $S(2,q+1,\frac{q^{m+1}-1}{q-1})$, denoted by $PG_1(m,q)$, having $\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$ blocks and replication number $\frac{q^m-1}{q-1} = q^{m-1}+q^{m-2}+\cdots+q+1$.

One can obtain two types of EAQECCs from projective geometry designs: Type II (using a point-by-block incidence matrix) and Type I (using a block-by-point incidence matrix of the design). Applying Proposition 4 to an incidence matrix of $PG_1(m,q)$, we obtain a Type II EAQECC. This type of EAQECC belongs to the high rate entanglement-assisted quantum LDPC codes given in Theorems 44 and 45. If we apply Proposition 5 to a block-by-point incidence matrix, we obtain a Type I EAQECC. This kind of EAQECC belongs to the high redundancy entanglement-assisted quantum LDPC codes given in Theorem 46.

The rank of an incidence matrix determines the dimension of the corresponding FG-LDPC code, hence it is one of the key values in the quantum setting as well. Exact values for many sporadic examples have been computed in the fields of quantum and classical LDPC codes. The following two theorems give the exact rank for all projective geometry designs.

Theorem 59 (Hamada [Ham68]). *The rank of $PG_1(m,2^t)$ is given by*

$$\operatorname{rank} PG_1(m,2^t) = \varphi(m,2^t) = \sum_{(s_0,s_1,\ldots,s_t)} \prod_{j=0}^{t-1} \sum_{i=0}^{L(s_{j+1},s_j)} (-1)^i \binom{m+1}{i} \binom{m+2s_{j+1}-s_j-2i}{m}$$

where the sum is taken over all ordered sets $(s_0,s_1,\ldots,s_t)$ with $s_0=s_t$, $s_j\in\mathbb{Z}$ such that $0\le s_j\le m-1$, and $0\le 2s_{j+1}-s_j\le m+1$ for each $j=0,\ldots,t-1$, and

$$L(s_{j+1},s_j) = \left[\frac{2s_{j+1}-s_j}{2}\right].$$

We will use the notation $\varphi(m,2^t)$ for the rank of $PG_1(m,q)$ when q is even, that is, $q=2^t$. When q is odd, the rank of $PG_1(m,q)$ is given by a formula of Frumkin and Yakir [FY90].

Theorem 60 (Frumkin and Yakir [FY90])**.** *Let q be odd and H an incidence matrix of the design $PG_1(m,q)$ with $v=\frac{q^{m+1}-1}{q-1}$ points. Then* $\operatorname{rank} H = v-1 = \frac{q^{m+1}-q}{q-1}$.

Hence the exact dimensions of the corresponding FG-LDPC codes obtained from projective geometries can be calculated for all cases.

The rank of $PG_1(m,2^t)$ was conjectured by Hamada [Ham73] to be the lowest rank among all Steiner 2-designs of the same order and block size. This has been confirmed in a number of cases, although in general the conjecture is still open. Thus we expect that the designs $PG_1(m,2^t)$ should provide codes with the best possible dimensions among all non-isomorphic $S(2,2^t+1,\frac{2^{t(m+1)}-1}{2^t-1})$s.

We will now examine the codes obtained from $PG_1(m,q)$ in detail. This subsection is divided into two portions based on the orientation of the incidence matrix.

5.3.1.1 Point-by-block (Type II) Projective geometry codes

In this portion, we consider the EAQECCs corresponding to a point-by-block incidence matrix of $PG_1(m,q)$.

We first consider the case $q=2^t$ for some positive integer t. The following theorem gives an infinite family of entanglement-assisted quantum LDPC codes which consume only one initial ebit and have extremely large net rate.

Theorem 61. *For every pair of integers $t\geq 1$ and $m\geq 2$ there exists an entanglement-assisted quantum* LDPC *codes with girth six whose parameters $[[n,k,d;c]]$ are*

$$n=\frac{(2^{t(m+1)}-1)(2^{tm}-1)}{(2^{2t}-1)(2^t-1)},$$

$$k=\frac{(2^{t(m+1)}-1)(2^{tm}-1)}{(2^{2t}-1)(2^t-1)}-2\varphi(m,2^t)+1,$$

$$d=2^t+2, \textit{ and}$$

$$c=1.$$

To prove Theorem 61, we first prove a new result on the distance of EAQECCs obtained from an incidence matrix of $PG_1(m,2^t)$. We use a special set of lines. A *dual hyperoval* $\mathscr{H}$ is a set of $q+2$ lines of $PG_1(2,q)$, such that each point of $PG_1(2,q)$ lies on either zero or two lines of $\mathscr{H}$. Dual hyperovals exist if and only if q is even. An example is the set of projective lines with equations

$$\{X_0+\beta X_1+\beta^2 X_2=0:\beta\in\mathbb{F}_q\}\cup\{X_1=0\}\cup\{X_2=0\}.$$

Theorem 62. *Let H be an incidence matrix of $PG_1(m,2^t)$. The minimum distance of the classical binary linear code with parity-check matrix H is 2^t+2.*

Proof. First, we note that coordinates of the codewords correspond to lines of the geometry, and a codeword corresponds to a set S of lines in $PG_1(m,2^t)$ such that every point is contained in an even number of lines of S. Assume that c is a non-zero codeword, and let $\operatorname{supp}(c)$ denote the support of c, that is, the set of indices of the nonzero coordinates of c. Because $c\neq 0$, the support of c contains at least one line ℓ. Through each point of $PG(m,2^t)$, there pass an even number of lines from $\operatorname{supp}(c)$. In particular, each of the 2^t+1 points on ℓ lies on at least one other line of $\operatorname{supp}(c)$, and all these lines are different as they have different intersections with ℓ. Hence, there are at least $1+(2^t+1)$ lines in $\operatorname{supp}(c)$, that is, minimum distance d is at least 2^t+2. Let π be a plane in $PG(m,2^t)$ and S the set of the 2^t+2 lines of a dual hyperoval in π. Then S corresponds to a codeword of weight 2^t+2, hence $d=2^t+2$. □

Proof of Theorem 61. Let H be an incidence matrix of $PG_1(m,2^t)$. The rank of H is $\varphi(m,2^t)$ given by Theorem 59. The index of $PG_1(m,2^t)$ is one. The replication number is odd. By Equation (5.3) and Theorem 44, we have $\operatorname{rank} HH^T=1$. By Theorem 62, the minimum distance of the binary linear code with parity-check matrix H is 2^t+2. □

Next, we examine EAQECCs obtained from an incidence matrix of $PG_1(m,q)$ with q odd. This case also gives very high rate entanglement-assisted quantum LDPC codes.

Lemma 19. *Let H be an incidence matrix of $PG_1(2,q)$, q odd. Then the classical binary linear code defined by parity-check matrix H consists of only the zero vector and the all-one vector.*

Proof. This follows directly from Theorem 60. □

A *hyperbolic quadric* Q is a substructure $(\mathscr{P},\mathscr{L})$ of $PG_1(3,q)$ with $(q+1)^2$ points and $2(q+1)$ lines, such that each point of $\mathscr{P}$ lies on exactly two lines of $\mathscr{L}$ and every plane of

$PG(3,q)$ contains zero or two lines of $\mathscr{L}$. Hyperbolic quadrics exist for every odd prime power q.

Theorem 63. *Let H be an incidence matrix of $PG_1(m,q)$, $m \geq 3$, q odd. Then the minimum distance of the classical binary linear code with a parity-check matrix H is* $2(q+1)$.

Proof. Let Π be a 3-dimensional subspace of $PG(m,q)$ and $(\mathscr{P},\mathscr{L})$ a hyperbolic quadric in Π. The set of lines $\mathscr{L}$ determines a codeword of weight $2q+2$, because each point of $PG(m,q)$ is contained in zero or two lines of $\mathscr{L}$. Hence minimum distance d is at least $2q+2$.

We show that there are no codewords of weight smaller than $2q+2$. Assume that there exists a codeword c of weight smaller than $2q+2$, that is, $\operatorname{supp}(c)$ is a set of less than $2q+2$ lines of $PG(m,q)$, such that each point lies on an even number of lines of $\operatorname{supp}(c)$. We will show that for any 2-dimensional subspace π one has either $|\operatorname{supp}(c) \cap \pi| \leq 1$ or $|\operatorname{supp}(c) \cap \pi| \geq q+2$.

First, let $S = \operatorname{supp}(c) \cap \pi = \{\ell_1, \ldots, \ell_i\}$. For each $j \in \{1, \ldots, i\}$, each of the points on ℓ_j has to lie on at least one other line of $\operatorname{supp}(c)$, and at most $i-1$ of them can lie on a line of S. Hence, at least $q+1-(i-1)$ of them are lines in $\operatorname{supp}(c) \setminus S$ and because they all have different intersections with π, this yields $i(q-i+2)$ lines in $\operatorname{supp}(c) \setminus S$. Together with the i lines of S, we have

$$i(q-i+2)+i < 2q+2$$

and solving this quadratic inequality for i gives us that either $i > q+1$ or $i < 2$. Because i is an integer, hence $i \geq q+2$ or $i \leq 1$.

Now, let ℓ be any line of $\operatorname{supp}(c)$. Each point of ℓ must lie on at least one other line, hence there certainly exist planes π with $i \geq 2$, and we have $i \geq q+2$. Let π be such a plane. We will now show that all lines of $\operatorname{supp}(c)$ are contained in π. Assume the contrary, that there exists a line $\ell' \in \operatorname{supp}(c) \setminus S$. Through each of the points on $\ell' \setminus \pi$, we need at least one other line of $\operatorname{supp}(c)$ which is not contained in π. Because there are at least q points on $\ell' \setminus \pi$, one has

$$|\operatorname{supp}(c)| = |S| + |\operatorname{supp}(c) \setminus S| \geq (q+2)+(1+q) > 2q+2,$$

a contradiction. Hence, ℓ' does not exist and $\operatorname{supp}(c)$ is contained within a single plane π. However, π is a $PG_1(2,q)$ and by Lemma 19 we need $q^2+q+1 > 2q+2$ lines in this case, a contradiction. Hence, there are no codewords of weight less than $2q+2$. □

We now give another infinite family of Type II entanglement-assisted quantum LDPC codes.

Table 5.1
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $PG_1(m,q)$, q even.

m	q	n	k	d	c
3	2	35	14	4	1
4	2	155	104	4	1
5	2	651	538	4	1
6	2	2667	2428	4	1
3	4	357	236	6	1
4	4	5795	5204	6	1
2	8	73	18	10	1
3	8	4745	3944	10	1

Theorem 64. *Let q be an odd prime power. Then for every integer $m \geq 3$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = \frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)},$$

$$k = \frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - 2\frac{q^{m+1}-q}{q-1} + c,$$

$$d = 2q+2, \textit{ and}$$

$$c = \begin{cases} 1 & \textit{when} \quad m \textit{ is odd,} \\ \frac{q^{m+1}-q}{q-1} & \textit{when} \quad m \textit{ is even.} \end{cases}$$

Proof. This follows directly from Proposition 4 and Theorems 44, 60, and 63. □

Therefore in the case where m is odd, we have another infinite class of EAQECCs which consume only one ebit. If m is even, we obtain infinitely many high rate codes which consume reasonable numbers of ebit. Tables 5.1 and 5.2 give a sample of the parameters of the Type II codes obtained from $PG_1(m,q)$ with q even and q odd respectively.

In the reminder of this portion, we examine Steiner spreads of projective geometry designs. These substructures can be used in Theorems 54, 55, and 56 and their analogous techniques based on Theorem 45 to fine-turn the rates and distances of the EAQECCs.

An *s-spread* of $PG(m,q)$ is a set of s-dimensional projective subspaces which partition the

Table 5.2
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $PG_1(m,q)$, q odd.

m	q	n	k	d	c
3	3	130	53	8	1
3	5	806	497	12	1
3	7	2850	2053	16	1
4	3	1210	1090	8	120

points of the geometry. In other words, an s-spread consists of a set of $(s+1)$-dimensional vector subspaces of $\mathbb{F}_q^{m+1}$ which contain every nonzero vector exactly once. It is known that $PG(m,q)$ admits an s-spread if and only if $s+1$ divides $m+1$ (see [Seg64] and [Dem68, p. 29]).

Take $PG_1(m,q)$ and suppose $s \geq 2$ is chosen so that $s+1$ divides $m+1$. Then an s-spread of $PG(m,q)$ exists. Each s-dimensional subspace in the spread contains an isomorphic copy of $PG_1(s,q)$, and hence this forms a Steiner spread. Note that the blocks of $PG_1(s,q)$ have size $q+1$ and are also blocks of $PG_1(m,q)$. Therefore we have the following result.

Theorem 65. *Let s, $m \geq 1$ be positive integers such that $s+1$ divides $m+1$. Then $PG_1(m,q)$ contains $\frac{q^{m+1}-1}{q^{s+1}-1}$ disjoint copies of $PG_1(s,q)$ whose point sets partition the point of $PG_1(m,q)$.*

Thus, we can find a set of disjoint subdesigns which partition the points of $PG_1(m,q)$ whenever $m+1$ has a nontrivial factor. Naturally, we may further sub-divide each subdesign of dimension s into smaller subdesigns, based on the nontrivial factors of $s+1$. Hence, the $S(2,\mu,v)$s from $PG_1(m,q)$ are very flexible in that they have Steiner spreads of various sizes.

In general, the length, dimension, required ebits, and rate each change gradually as we delete subdesigns in a Steiner spread. The minimum distance and rank are either remain the same or improve slightly. Table 5.3 lists the example parameters of EAQECCs created by deleting subdesigns from $PG_1(5,2)$. The first and last rows correspond to regular LDPC codes.

5.3.1.2 Block-by-point (Type I) Projective geometry codes

Next we consider EAQECCs obtained via Theorem 46 by using the block-by-point incidence matrix of $PG_1(m,q)$. The codes obtained in this manner correspond to the classical Type I LDPC codes. As in the classical setting, Type I entanglement-assisted quantum regular LDPC codes can correct many quantum errors. Because an incidence matrix of $PG_1(m,q)$ for q odd is almost full rank, the corresponding Type I code is not of much interest. Hence, in this portion we always assume that $q = 2^t$ for some positive integer t.

Theorem 66. *For every pair of integers $t \geq 1$ and $m \geq 2$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = \frac{2^{t(m+1)}-1}{2^t-1},$$

$$k = \frac{2^{t(m+1)}-1}{2^t-1} - 2\varphi(m,2^t) + c,$$

$$d = (2^t+2)2^{t(m-2)}, \text{ and}$$

$$c \leq \varphi(m,2^t).$$

Proof. Let H^T be a block-by-point incidence matrix of $PG_1(m,2^t)$. Then $\operatorname{rank} H^T H \leq \operatorname{rank} H = \varphi(m,2^t)$, where $\varphi(m,2^t)$ is given by Theorem 59. By a result of Calkin, Key, and

Table 5.3
Summary of parameters of Type II codes obtained by deleting a Steiner spread of subdesigns isomorphic to $PG_1(2,2)$ from $PG_1(5,2)$. *Subs* denotes the number of subdesigns removed.

Subs	n	rank$H$	k	d	c	Rate
0	651	57	538	4	1	0.8264
1	644	57	532	4	2	0.8370
2	637	57	526	4	3	0.8477
3	630	57	520	4	4	0.8587
4	623	57	514	4	5	0.8700
5	616	57	508	4	6	0.8815
6	609	57	502	4	7	0.8933
7	602	57	496	4	8	0.9053
8	595	57	490	4	9	0.9176
9	588	57	482	4	8	0.9269

Table 5.4
Sample parameters of Type I $[[n,k,d;c]]$ EAQECCs obtained from
$PG_1(m,q)$, q even.

m	q	n	k	d	c
2	4	21	2	6	1
2	8	73	18	10	1
2	16	273	110	18	1
2	32	1057	570	34	1

de Resmini [CKdR99], the minimum distance of the binary linear code with parity-check matrix H^T is $(2^t+2)2^{t(m-2)}$. Applying Proposition 5 proves the assertion. □

Note that here the distance grows exponentially as the dimension of the geometry increases. When $m=2$, the EAQECCs are based on projective planes. As shown in Subsection 5.2.2, the EAQECC obtained from a Desarguesian projective plane of order 2^t consumes only one initial ebit. Basing on Hamada's conjecture, we expect that in general the EAQECCs given in Theorem 66 consume relatively small numbers of ebits.

It is not clear from the formula for $\varphi(m,2^t)$ whether the net rate of a Type I EAQECC based on $PG_1(m,2^t)$ is positive. In order to produce useful catalytic quantum codes, it is important to understand when the net rate is positive.

Proposition 6. *Let H be an incidence matrix of $PG_1(2,2^t)$. Then for all $t\geq 2$ the* EAQECC *obtained from H^T has a positive net rate.*

Proof. By Hamada's formula, we have $\operatorname{rank} H = 3^t+1$. The number of points in $PG_1(2,2^t)$ is $2^{2t}+2^t+1$. □

For $m\geq 3$, we note that as q increases, $\operatorname{rank} H$ grows at a slower rate than the code length. Thus we may expect that, for q large when compared to m, the net rate will eventually become positive. For example, one can check that the net rate of the Type I EAQECC obtained from $PG_1(3,2^t)$ is positive for $t\geq 7$. Table 5.4 gives sample parameters of the Type I codes obtained from $PG_1(m,2^t)$.

5.3.2 Affine geometry codes

In this subsection, we will study the EAQECCs obtained from affine geometry designs.

The affine geometry $AG(m,q)$ of dimension m over $\mathbb{F}_q$ is a finite geometry whose points are the vectors in $\mathbb{F}_q^m$. The i-dimensional affine subspaces (or *i-flats*) are the i-dimensional vector subspaces of $\mathbb{F}_q^m$ and their cosets. Thus $AG(m,q)$ has a natural parallelism.

The points and lines (that is, 1-flats) of an affine geometry form an $S(2,q,q^m)$, denoted by $AG_1(m,q)$. The design has $q^{m-1}\frac{q^m-1}{q-1}$ blocks and replication number $\frac{q^m-1}{q-1} = q^{m-1} + q^{m-2} + \cdots + q + 1$.

We note that in many papers concerning LDPC codes, the term “Euclidean geometry” and the notation $EG(m,q)$ are used for affine geometries. Most of the codes studied in relation to Euclidean geometries does not use the zero vector, and hence they do not generally correspond to $S(2,\mu,v)$s. Because the term “affine geometry" is standard in the recent research on finite geometry in mathematics, we use the notation $AG_1(m,q)$ when we take all points and lines to form an incidence matrix. The incidence structure obtained by discarding the zero vector and the lines containing the zero vector from $AG_1(m,q)$ will be denoted by $EG_1(m,q)$, which we will study in Subsection 5.3.3. Because many of the classical FG-LDPC codes obtained from affine geometries are based on $EG_1(m,q)$, they are generally not the same as the affine geometry codes presented in this section.

As with projective geometry designs, Propositions 4 and 5 give Type II and Type I affine geometry codes respectively. It is notable that the classical ingredients of these codes are quasi-cyclic LDPC codes similar to other FG-LDPC codes because the elementary abelian group acts transitively on the points of $AG_1(m,q)$ (see [BJL99, KLF01]). The rank of an affine geometry design $AG_1(m,2^t)$ is directly related to φ given in Theorem 59.

Theorem 67 (Hamada [Ham73])**.** *The rank of the affine geometry design $AG_1(m,2^t)$ is given by*

$$\operatorname{rank} AG_1(m,2^t) = \varphi(m,2^t) - \varphi(m-1,2^t).$$

If q is odd, the rank of $AG_1(m,q)$ over $\mathbb{F}_2$ is full.

Theorem 68 (Yakir [Yak93])**.** *Let H be an incidence matrix of the design $AG_1(m,q)$ with q odd. Then* $\operatorname{rank} H = q^m$.

Thus the dimensions of the corresponding FG-LDPC codes can be easily calculated.

As in the case of projective designs, Hamada conjectured that the rank of $AG_1(m, 2^t)$ is minimum among all Steiner 2-designs of the same order and block size. Thus, affine geometry designs with q even may be expected to give codes with the best possible dimensions among all non-isomorphic $S(2, 2^t, 2^{tm})$s.

We divide this subsection into two portions. In the first portion we examine high rate Type II entanglement-assisted quantum LDPC codes obtained from $AG_1(m, q)$. Then in the next portion we present Type I entanglement-assisted quantum LDPC codes based on $AG_1(m, q)$, which effectively exploit the redundancy to give excellent error correction performance.

5.3.2.1 Point-by-block (Type II) Affine geometry codes

The geometric structure of affine geometry has often been studied independently in various fields. The special substructure we need to give distances has been investigated in connection with the disk failure resilience ability of a class of redundant arrays of independent disks (RAID). Here we present a known result on RAID related to our codes in coding theoretic terminology.

Theorem 69 (Müller and Jimbo [MJ04]). *Let H be an incidence matrix of $AG_1(m, q)$. The minimum distance of the classical binary linear code having H as a parity-check matrix is $q + 1$ if q is even, and $2q$ otherwise.*

The following two theorems give infinite families of EAQECCs which consume only one initial ebit and have very large net rate.

Theorem 70. *For every pair of integers $t \geq 1$ and $m \geq 2$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n, k, d; c]]$ are*

$$n = 2^{t(m-1)} \frac{2^{tm} - 1}{2^t - 1},$$

$$k = 2^{t(m-1)} \frac{2^{tm} - 1}{2^t - 1} - 2(\varphi(m, 2^t) - \varphi(m - 1, 2^t)) + 1,$$

$$d = 2^t + 1, \text{ and}$$

$$c = 1.$$

Proof. Let H be an incidence matrix of $AG_1(m, 2^t)$. By Theorem 67, we have $\operatorname{rank} H = \varphi(m, 2^t) - \varphi(m - 1, 2^t)$. The index of the design $AG_1(m, 2^t)$ is one. Its replication number is always odd. Thus, by Theorem 44, we have $\operatorname{rank} HH^T = 1$. Applying Proposition 4 and Theorem 69 completes the proof. □

Theorem 71. *Let q be an odd prime power. Then for every integer $m \geq 2$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$\begin{aligned} n &= q^{m-1}\frac{q^m-1}{q-1}, \\ k &= q^{m-1}\frac{q^m-1}{q-1} - 2q^m + c, \\ d &= 2q, \text{ and} \\ c &= \begin{cases} 1 & \text{when} \quad m \text{ is odd,} \\ q^m - 1 & \text{when} \quad m \text{ is even.} \end{cases} \end{aligned}$$

Proof. Let H be an incidence matrix of $AG_1(m,q)$ with q odd. By Theorem 68, we have $\operatorname{rank} H = q^m$. The index of the design $AG_1(m,q)$ is one. Its replication number r is a sum of m terms, each being an odd number. Thus r is odd only when m is odd. By Theorem 44, we have $\operatorname{rank} HH^T = 1$ for m odd. If m is even, we have $\operatorname{rank} HH^T = q^m - 1$ from Theorem 45. Applying Proposition 4 and Theorem 69 proves the assertion. □

Theorem 71 gives an infinite family of high rate entanglement-assisted quantum LDPC codes which exploit reasonable amounts of entanglement as well. Tables 5.5 and 5.6 give a sample of the parameters of the Type II codes obtained from $AG_1(m,q)$ with q even and q odd respectively.

Next we show that affine geometry designs have numerous subdesigns and Steiner spreads, which make it possible to fine-tune the parameters and error correction performance of the corresponding EAQECCs.

Theorem 72. *If $m \geq 3$, the points of $AG_1(m,q)$ can be partitioned into q disjoint subsets of size q^{m-1}, being the point sets of subdesigns isomorphic to $AG_1(m-1,q)$.*

Proof. Take a parallel class $\{H_1,\ldots,H_q\}$ of q hyperplanes of $AG(m,q)$. Let the point set of H_j be V_j. Clearly $\cup_{j=1}^{q} V_j = V$, and the set of all blocks of $AG_1(m,q)$ which are contained entirely in H_j form a subdesign isomorphic to $AG_1(m-1,q)$. □

Theorem 72 can be applied recursively to create additional disjoint subdesigns of smaller dimension, giving a variety of EAQECCs via Theorems 54, 55, and 56. Similar subdesign deletion techniques based on Theorem 45 further give infinitely many new high rate

Table 5.5
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $AG_1(m,q)$, q even.

m	q	n	k	d	c
3	2	28	15	3	1
4	2	120	91	3	1
5	2	496	435	3	1
6	2	2016	1891	3	1
2	4	20	3	5	1
3	4	336	235	5	1
4	4	5440	4971	5	1
2	8	72	19	9	1
3	8	4672	3927	9	1

Table 5.6
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $AG_1(m,q)$, q odd.

m	q	n	k	d	c
3	3	117	64	6	1
3	5	775	526	10	1
3	7	2793	2108	14	1
5	3	9801	9316	6	1
4	3	1080	998	6	80

EAQECCs. Table 5.7 lists the parameters of the EAQECCs created by spread deletion from $AG_1(3,4)$.

5.3.2.2 Block-by-point (Type I) Affine geometry codes

Next we consider EAQECCs obtained from a block-by-point incidence matrix of $AG_1(m,q)$. Because incidence matrices of $AG_1(m,q)$ with q odd are of full rank, here we always assume $q=2^t$ to obtain interesting codes. The entanglement-assisted quantum LDPC codes presented in this section effectively exploit redundancy. The excellent error correction performance will be demonstrated in simulations in Section 5.4.

Theorem 73 (Calkin, Key, and de Resmini [CKdR99]). *Let H be a block-by-point inci-*

Table 5.7
Summary of parameters of Type II codes obtained by deleting a Steiner spread of subdesigns isomorphic to $AG_1(2,4)$ from $AG_1(3,4)$. *Subs* denotes the number of subdesigns removed.

Subs	n	rank H	k	d	c	Rate
0	336	51	235	5	1	0.6994
1	316	51	216	5	2	0.7468
2	296	51	197	5	3	0.8007
3	276	51	178	5	4	0.8623
4	256	51	158	6	4	0.9297

dence matrix of $AG_1(m,2^t)$. Then the minimum distance of the classical binary linear code for which H is a parity-check matrix is $(2^t+2)2^{t(m-2)}$.

Theorem 74. *For every pair of integers $t \geq 1$ and $m \geq 3$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = 2^{tm},$$

$$k = 2^{tm} - 2(\varphi(m,2^t) - \varphi(m-1,2^t)) + c,$$

$$d = (2^t+2)2^{t(m-2)}, \text{ and}$$

$$c \leq \varphi(m,2^t) - \varphi(m-1,2^t).$$

Proof. Let H^T be a block-by-point incidence matrix of $AG_1(m,2^t)$. By Theorem 67, we have $\operatorname{rank} H^T H \leq \operatorname{rank} H = \varphi(m,2^t) - \varphi(m-1,2^t)$. By Theorem 73, the minimum distance of the binary linear code with a parity-check matrix H is $(2^t+2)2^{t(m-2)}$. The assertion follows from Proposition 5. □

It is worth mentioning that here the distance grows exponentially with linear increase of the geometry dimension m. Because the rank of $AG_1(m,2^t)$ is conjectured to be the smallest possible among all non-isomorphic $S(2,2^t,2^{tm})$s, we expect that the EAQECCs obtained from these affine geometry designs consume the smallest possible numbers of ebits attainable by this method with $S(2,2^t,2^{tm})$s.

When $m = 2$, we can easily determine the required amount of entanglement.

Theorem 75. *For every positive integer t there exists an entanglement-assisted quantum*

Table 5.8
Sample parameters of Type I $[[n,k,d;c]]$ EAQECCs obtained from $AG_1(m,q)$, q even.

m	q	n	k	d	c
2	8	64	18	10	8
2	16	256	110	18	16
2	32	1024	570	34	32
2	64	4096	2702	66	64

LDPC *code with girth six whose parameters* $[[n,k,d;c]]$ *are*

$$n = 4^t,$$

$$k = 4^t + 2^t - 2 \cdot 3^t,$$

$$d = 2^t + 2, \text{ and}$$

$$c = 2^t.$$

Proof. Let H^T be a block-by-point incidence matrix of $AG_1(2,2^t)$. We first prove that $\operatorname{rank} H^T H = 2^t$. Two lines of an affine plane are either parallel or intersect in exactly one point. There are $2^t + 1$ parallel classes of lines, each containing exactly 2^t lines, and each line contains 2^t points. Because 2^t is even, it is always possible to reorder the rows of H^T such that $H^T H$ is a block matrix of the following form:

$$H^T H = \begin{bmatrix} 0 & J & & J \\ J & 0 & \cdots & J \\ & \vdots & \ddots & \vdots \\ J & J & \cdots & 0 \end{bmatrix}$$

where J is the $2^t \times 2^t$ all-one matrix. Hence, we have $\operatorname{rank} H^T H = 2^t$. By Theorem 67, we have $\operatorname{rank} H = 3^t$. Applying Proposition 5 and Theorem 73 completes the proof. □

Table 5.8 gives sample parameters of the Type I EAQECCs obtained from $AG_1(m,2^t)$.

5.3.3 Euclidean geometry codes

In this final subsection concerning finite geometry EAQECCs, we will examine Euclidean geometry codes.

Given a prime power q and integer $m \geq 2$, we define an incidence structure $EG_1(m,q)$ having as points all points of $AG_1(m,q)$ except the zero vector, and having as blocks (or lines) all lines of $AG(m,q)$ except those lines containing the zero vector. The lines which are excluded from $AG_1(m,q)$ to form $EG_1(m,q)$ consist of all multiples of a single nonzero vector. Thus, $EG_1(m,q)$ has $q^m - 1$ points and $\left(q^{m-1}-1\right)\frac{q^m-1}{q-1}$ lines. Each line contains q points, and each point appears in $\frac{q^m-1}{q-1} - 1 = q^{m-1} + q^{m-2} + \cdots + q$ lines. Thus, $EG_1(m,q)$ yields regular LDPC codes. Each pair of points appears in *at most* one line. Hence, $EG_1(m,q)$ is a partial Steiner 2-design. Its Tanner graph does not contain 4-cycles.

Applying Proposition 5 to a line-by-point incidence matrix of $EG_1(m,q)$ gives a Type I EAQECC. If q is even, the distance is bounded from below by the BCH bound.

Theorem 76 (Kou, Lin, and Fossorier [KLF01])**.** *Let H be a line-by-point incidence matrix of $EG_1(m,2^t)$. Then the minimum distance d of the classical binary linear code having H as a parity-check matrix satisfies $d \geq \frac{2^{tm}-1}{2^t-1}$. Equality holds if $m = 2$.*

We use the following theorem to give the dimensions of FG-LDPC codes obtained from $EG_1(m,2^t)$ and their entanglement-assisted quantum counterparts.

Theorem 77 (Hamada [Ham73])**.** *The rank of the incidence structure $EG_1(m,2^t)$, $t > 1$, is given by*

$$\operatorname{rank} EG_1(m,2^t) = \varphi(m,2^t) - \varphi(m-1,2^t) - 1.$$

Theorem 78. *For every pair of integers $t \geq 1$ and $m \geq 2$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = 2^{tm} - 1,$$

$$k = 2^{tm} - 2(\varphi(m,2^t) - \varphi(m-1,2^t)) + 1 + c,$$

$$d \geq \frac{2^{tm}-1}{2^t-1}, \text{ and}$$

$$c \leq \varphi(m,2^t) - \varphi(m-1,2^t) - 1.$$

Proof. Let H^T be a line-by-point incidence matrix of $EG_1(m,2^t)$. By Theorem 77, we have

Table 5.9
Sample parameters of Type I $[[n,k,d;c]]$ EAQECCs obtained from $EG_1(2,q)$, q even.

m	q	n	k	d	c
2	8	63	19	9	8
2	16	255	111	17	16
2	32	1023	571	33	32

$\operatorname{rank} H^T H \leq \operatorname{rank} H = \varphi(m,2^t) - \varphi(m-1,2^t) - 1$. Applying Proposition 5 and Theorem 76 completes the proof. □

A simple observation gives exact values of all the parameters of the Type I codes based on $EG_1(2,2^t)$.

Theorem 79. *For every positive integer t there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = 4^t - 1,$$

$$k = 4^t + 2^t - 2\cdot 3^t + 1,$$

$$d = 2^t + 1, \text{ and}$$

$$c = 2^t.$$

Proof. Let H^T be a line-by-point incidence matrix of $EG_1(2,2^t)$. An incidence matrix of $EG_1(2,2^t)$ is obtained by removing one row and one column from each block from that of $AG_1(2,2^t)$. By following the argument in Theorem 75, it is straightforward to see that $\operatorname{rank} H^T H = 2^t$. By Theorem 77, we have $\operatorname{rank} H = \varphi(m,2^t) - \varphi(m-1,2^t) - 1 = 3^t - 1$. Theorem 76 and Proposition 5 prove the assertion. □

Table 5.9 gives a sample of the parameters of the Type I codes obtained from $EG_1(2,2^t)$.

As with $S(2,\mu,v)$s, the incidence structure $EG_1(m,q)$ can also generate a high rate LDPC code with girth six. Applying Proposition 4 to incidence matrices, we obtain Type II EAQECCs. Here we investigate their parameters.

Theorem 80. *The minimum distance of a Type II* EAQECC *based on $EG_1(m,q)$ is $q+1$ if q is even, and $2q$ if q is odd and $m > 2$.*

Proof. Consider any set of linearly dependent columns in an incidence matrix of $EG_1(m,q)$. The same columns appear in the corresponding incidence matrix of $AG_1(m,q)$, but with a single zero coordinate added. These columns are still dependent in $AG_1(m,q)$. Hence the minimum distance is upper bounded by Theorem 69. Thus we need only to show lower bounds.

We begin with q even. If $q = m = 2$, we can check by hand that the minimum distance is three. Henceforth assume that $q > 2$ or $m > 2$. Because the minimum distance of the code obtained from $AG_1(m,q)$ is $q+1$, there exists a set S of $q+1$ linearly dependent columns of an incidence matrix of $AG_1(m,q)$, corresponding to a set $\mathscr{D}$ of $q+1$ blocks of $AG_1(m,q)$. Let P be the multiset of points appearing in the blocks of $\mathscr{D}$. As each block of $\mathscr{D}$ has q points, $|P| = q(q+1)$. However, because the columns of S are dependent over $\mathbb{F}_2$, each point in P must appear with multiplicity two or more. Hence, the number of distinct points in P is at most $\frac{q(q+1)}{2} < q^m - 1$ except for $q = m = 2$. Therefore there is a nonzero point p of $AG(m,q)$ which does not appear in P. Let $\mathscr{D}' = \{B - p : B \in \mathscr{D}\}$, that is, we shift each block of $\mathscr{D}$ by p. Each new block corresponds to a coset of a linear space. Because $p \notin P$, no element of $\mathscr{D}'$ contains the zero vector, and so the elements of $\mathscr{D}'$ are lines of $EG_1(m,q)$. Thus $\mathscr{D}'$ is a linearly dependent set in $EG_1(m,q)$ of size $q+1$. Therefore in all cases, the minimum distance of Type II EAQECC based on $EG_1(m,q)$, q even, is $q+1$. A similar argument proves the case when q is odd and $m \neq 2$. □

Theorem 81. *For every pair of integers $t \geq 1$ and $m \geq 2$ there exists an entanglement-assisted quantum* LDPC *code with girth six whose parameters $[[n,k,d;c]]$ are*

$$n = (2^{t(m-1)} - 1)\frac{2^{tm} - 1}{2^t - 1},$$

$$k = (2^{t(m-1)} - 1)\frac{2^{tm} - 1}{2^t - 1} - 2\,\mathrm{rank}\,EG_1(m,2^t) + c,$$

$$d = 2^t + 1, \text{ and}$$

$$c = \frac{2^{tm} - 2^t}{2^t - 1},$$

where $\mathrm{rank}\,EG_1(m,2^t) = \varphi(m,2^t) - \varphi(m-1,2^t) - 1$.

Proof. Let H be an incidence matrix of $EG_1(m,2^t)$. Because H is obtained from an incidence matrix of $AG_1(m,2^t)$ by deleting the row representing the zero vector and the columns that represent the lines containing the zero vector, it is easy to see that the rows

Table 5.10
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $EG_1(m,q)$, q even.

m	q	n	k	d	c
3	2	21	15	3	6
4	2	105	91	3	14
5	2	465	434	3	30
6	2	1953	1891	3	62
3	4	315	235	5	20
4	4	5355	4971	5	84
2	8	63	19	9	8
3	8	4599	3927	9	72

and columns of HH^T can be reordered such that the matrix is of the form:

$$HH^T = \begin{bmatrix} 0 & J & & J \\ J & 0 & \cdots & J \\ & \vdots & \ddots & \vdots \\ J & J & \cdots & 0 \end{bmatrix}$$

where J is the $(2^t-1)\times(2^t-1)$ all-one matrix. Because $2^{tm}-1$ is odd, $\operatorname{rank} HH^T = \frac{2^{tm}-1}{2^t-1} - 1$. Applying Proposition 4 and Theorems 80 and 77 completes the proof. □

Tables 5.10 gives sample parameters for the Type II codes obtained from $EG_1(m,2^t)$.

For the case q odd, Hamada [Ham73] conjectured that an incidence matrix of $EG_1(m,q)$ is of full rank. As shown in Table 5.11, the conjecture is true for small m and q.

5.4 Performance

In this section, we present simulation results for EAQECC codes constructed in the previous sections. As in the related works [HBD09, HYH11], we performed simulations over the depolarizing channel. In this model, each error (X, Y, and Z) occurs independently in each qubit with equal probability f_m. For a given CSS type EAQECC, we performed each decoding in two separate decoding steps, each using the sum-product algorithm. The shared ebits, which do not pass through the noisy channel, are assumed to be error-free.

Table 5.11
Sample parameters of Type II $[[n,k,d;c]]$ EAQECCs obtained from $EG_1(m,q)$, q odd.

m	q	n	k	d	c
3	3	104	64	6	12
4	3	1040	960	6	80
5	3	9680	9316	6	120
3	5	744	526	10	30
3	7	2736	2108	14	56

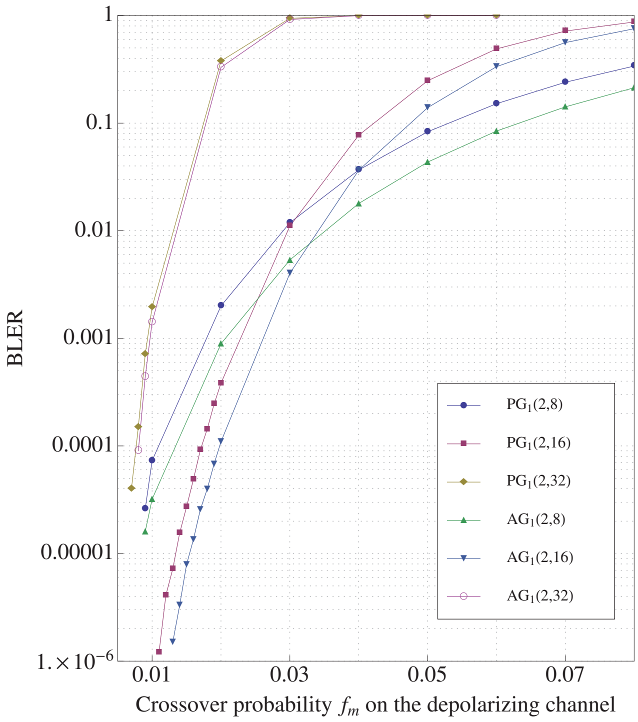


Figure 5.1: Performance of Type I EAQECCs

Our simulation results are reported in terms of the block error rate (BLER).

We first examine codes obtained from a block-by-point incidence matrix. Figure 5.1 shows the performance of several such codes based on projective and affine geometry designs. As shown in Section 5.3, these codes have very large distances for sparse-graph codes while avoiding short cycles. As expected, these codes perform excellently at relatively high f_m.

To illustrate how well these codes perform, we compare one of our Type I LDPC codes with previously known entanglement-assisted quantum LDPC codes with best BLERs.

Theorem 75 gives a new EAQECC with parameters $[[256,110,18;16]]$ obtained from the design $AG_1(2,16)$. The $[[255,111,17;16]]$ EAQECC in the work of Hsieh, Yen, and Hsu [HYH11] used $EG_1(2,16)$ outperformed all previously known quantum codes of similar rate in simulations over the depolarizing channel. Their code based on $PG_1(2,16)$, which also performed very well, has parameters $[[273,110,18;1]]$. Exactly the same EAQECCs as these two can be constructed using Theorems 79 and 53 in our framework without relying on computers to calculate their parameters.

These three EAQECCs based on finite geometries have similar geometrical structures, and they behave quite similarly in simulations. Performance of the $AG_1(2,16)$ and $PG_1(2,16)$ codes is directly compared in Figure 5.1. The BLER of the $EG_1(2,16)$ code, which is slightly worse than that of our $AG_1(2,16)$ code, is plotted in Figure 5.2 to compare the three with EAQECCs having different parameters. As shown in the figures, our new $[[256,110,18;16]]$ EAQECC obtained from $AG_1(2,16)$ shows a better BLER than the other two. The BLERs of $AG_1(2,16)$, $EG_1(2,16)$, and $PG_1(2,16)$ codes at $f_m = 0.02$ are 1.0×10^{-4}, 1.6×10^{-4}, and 3.8×10^{-4} respectively.

Entanglement-assisted quantum quasi-cyclic LDPC codes proposed by Hsieh, Brun, and Devetak in [HBD09] have also shown excellent BLERs. In simulations, their EAQECCs with parameters $[[128,58,6;18]]$, called EX1 and EX2, outperformed the previously known best quantum LDPC codes at a similar rate about 0.316. The net rate of EX1 and EX2 is $\frac{58-16}{128} \approx 0.312$. Our $[[256,110,18;16]]$ EAQECC obtained from $AG_1(2,16)$ has net rate $\frac{110-16}{256} \approx 0.367$, which is higher than that of EX1 and EX2. Their simulation results and our independent simulation results for EX1 and EX2 showed that their BLERs at $f_m = 0.02$ are higher than 1.1×10^{-2} while our $AG_1(2,16)$ code has BLER about 1.0×10^{-4} at the same f_m, which is better than EX1 and EX2 by two orders of magnitude. Our EAQECC also requires a smaller amount of entanglement than EX1 and EX2.

Our results here confirm the close linkage between EAQECCs and classical error-correcting codes: good performance in the classical setting translates directly into good performance from the corresponding quantum codes.

We next examine codes obtained from a point-by-block incidence matrix. These codes are capable of achieving extremely high rates even at moderate block lengths.

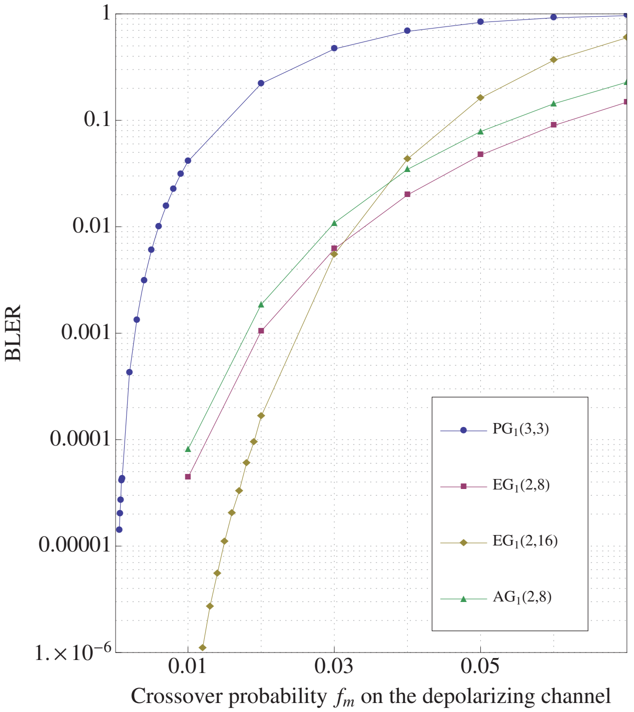


Figure 5.2: Performance of Type II EAQECCs

Figures 5.2 and 5.3 show the performance of several Type II codes based on finite geometries. The Type II code from $PG_1(3,3)$ is shown in both figures to serve as a point of reference between the two figures. Figure 5.4 gives the block error rates for several codes with high rates including $[[301,216,6;1]]$ and $[[1080,998,6;80]]$ codes from cyclic 5-sparse STSs of order 43 and 81 respectively. The incidence matrices of these two Steiner triple systems are constructed from the list of base blocks in [CMRv94]. Note that the cyclic automorphisms and sparse configurations immediately give the dimensions and distances of the EAQECCs obtained from the cyclic 5-sparse STSs (see [DHV78, Fuj07]). Table 5.12 lists the rates of selected finite geometry codes shown in figures.

As in the classical setting, our codes obtained from point-by-block incidence matrices have waterfall regions at low f_m and transmit at extremely high rates. This direct correlation in performance between the classical and quantum settings can also be seen when codes require only one ebit. It may be worth mentioning that changing geometries or choosing a non-geometric $S(2,\mu,v)$ can give slightly different BLER curves. It would be interesting to investigate theoretical methods for finding $S(2,\mu,v)$s with desirable performance curves in given situations.

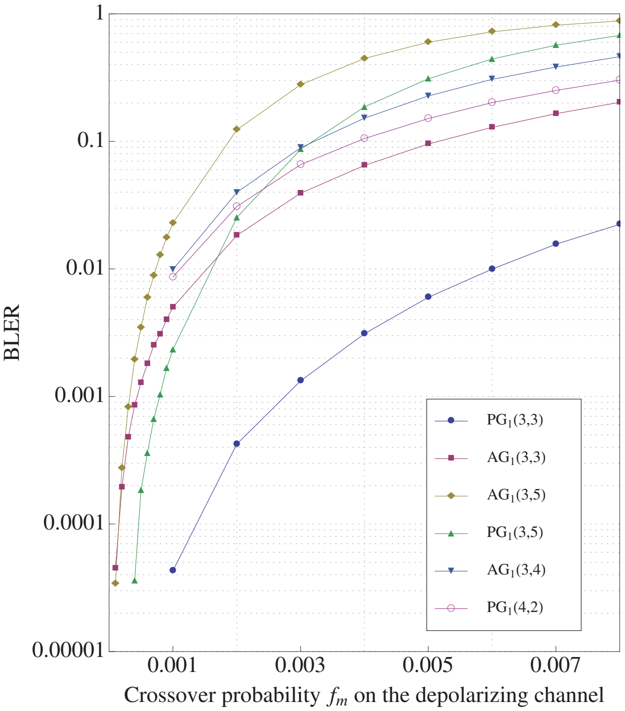


Figure 5.3: Performance of Type II EAQECCs

Finally, we compare EAQECCs obtained by removing subdesigns from the parent design. Here we test a subdesign deletion technique where each deletion step increases the required amount of entanglement to a slightly larger degree than the examples we gave in Section 5.3. Each code in Figure 5.5 is constructed from a Type II code based on $AG_1(3,3)$. Fundamental parameters of these codes are shown in Table 5.13. The original code is also shown for reference. The code labeled “one sub” has had a single subdesign isomorphic to $AG_1(2,3)$ removed. The code labeled “3 subs” has had a Steiner spread removed. This last code is a regular LDPC code. As can be seen from their BLERs, removing subdesigns has improved the error correction performance while increasing the rate and maintaining many of the essential properties.

Because removing subdesigns can increase the required amount of entanglement in a flexible manner, one can generate an EAQECC which effectively exploits preexisting entanglement. For example, a high net rate code consuming only one ebit can turn into a heavily entanglement-assisted code to achieve better error correction performance at the same f_m. As illustrated in Table 5.13, a $[[117,64,6;1]]$ code with a regular parity-check matrix becomes a $[[81,56,6;25]]$ code with a regular parity-check matrix through gradual steps.

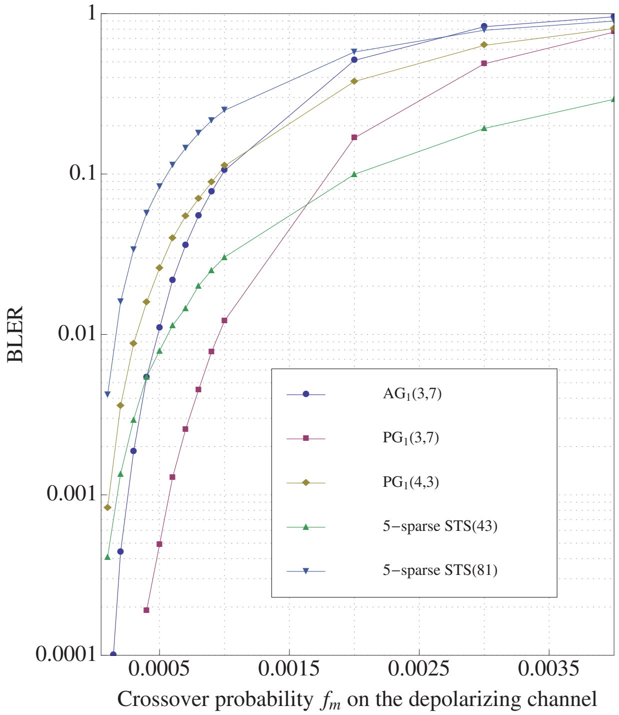


Figure 5.4: Performance of high-rate Type II EAQECCs

One can also fine-tune parameters and improve error correction performance while almost keeping the extremely low required amount of entanglement by applying Theorems 54 and 55. As shown in Section 5.3, all FG-LDPC codes found in [HYH11] can be constructed using our method. The subdesign deletion techniques further give infinitely many new codes by fine-tuning their parameters and error correction performance. In this sense, our method gives many kinds of new and known excellent EAQECCs in a single framework.

5.5 Conclusion

We have developed a general framework for constructing entanglement-assisted quantum LDPC codes using combinatorial design theory. Our constructions generate infinitely many new codes with various desirable properties such as high error correction performance, high rates, and requiring only one initial entanglement bit. Our methods are flexible and allow us to design EAQECCs with desirable properties while requiring prescribed amounts of entanglement. All quantum codes constructed in this chapter can be efficiently decoded through the sum-product algorithm.

Table 5.12
Rates of EAQECCs obtained from finite geometries.

Type	Geometry	m	q	Rate
II	PG	4	3	0.9008
II	PG	3	7	0.7203
II	PG	3	5	0.6166
II	PG	3	3	0.4076
II	AG	3	7	0.7547
II	AG	3	5	0.6787
II	AG	3	3	0.5470
II	AG	2	8	0.2638
II	EG	2	16	0.4352
II	EG	2	8	0.3015
I	PG	2	32	0.5392
I	PG	2	16	0.4029
I	PG	2	8	0.2465
I	AG	2	32	0.5566
I	AG	2	16	0.4296
I	AG	2	8	0.2812

Table 5.13
Summary of parameters of Type II EAQECCs obtained by deleting subdesigns from $AG_1(3,3)$. *Subs* denotes the number of subdesigns removed.

Subs	n	rank H	k	d	c	Rate
0	117	27	64	6	1	0.5470
1	105	27	60	6	9	0.5714
2	93	26	58	6	17	0.6236
3	81	25	56	6	25	0.6913

We have introduced many new families of entanglement-assisted quantum LDPC codes based on combinatorial designs as well as determined all fundamental parameters of the well-known families of LDPC codes based on finite geometries for most cases. Because the entanglement-assisted stabilizer formalism bridges classical and quantum codes in a direct manner, these results on entanglement-assisted quantum LDPC codes are useful both in quantum and classical coding theories.

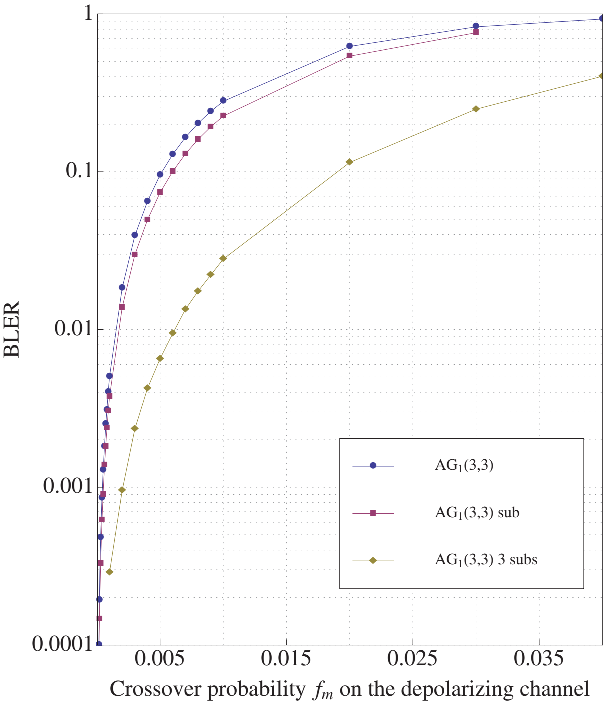


Figure 5.5: Performance of EAQECCs obtained by deleting subdesigns from $AG_1(3,3)$.

Our framework encompasses many previously proposed excellent quantum LDPC codes as well. In fact, our method can also be applied to quantum LDPC codes under the standard stabilizer formalism by employing the ideas found in [Aly08, Djo08].

We have focused on the fundamental classes of combinatorial designs. However, other classes of incidence structures may provide interesting results as well. For example, the entanglement-assisted quantum LDPC codes presented in [HBD09] can be seen as incidence structures generated from the so-called difference matrices and their generalizations (see [CD07] for the definition and basic facts about difference matrices). More general families of combinatorial designs can have nested structures or similar strong orthogonal relations between two incidence matrices. This kind of structure can give asymmetric quantum codes (see [IM07, SKR09]). Structures in finite geometry we did not employ may also give interesting quantum LDPC codes as well as classical LDPC codes. Because LDPC codes and sparse incidence structures are equivalent, we expect that our methods may be further generalized to encompass a wider range of both new and known quantum LDPC codes in future work.

Acknowledgments

The following acknowledgments refer to the paper [FCV$^+$10], from which this chapter is reprinted. Yuichiro Fujiwara acknowledges support from Japan Society for the Promotion of Science (JSPS) Grants-in-Aid for Scientific Research 20·5897. David Clark and Vladimir Tonchev acknowledge support by NSA Grant H98230-10-1-0177. A substantial part of the research was done while Yuichiro Fujiwara was visiting the Department of Mathematical Sciences of Michigan Technological University. He thanks the department for its hospitality. The authors would like to thank the anonymous referee for his valuable comments and suggestions.

5.A Appendix A: Existence of 2-designs

Here we discuss the existence of 2-designs to be applied to our constructions given in Subsection 5.2.2. The following is the well-known asymptotic existence theorem.

Theorem 82 (Wilson [Wil72a, Wil72b, Wil75])**.** *The necessary conditions for the existence of a* 2-(v,μ,λ) *design,* $\lambda(v-1) \equiv 0 \pmod{\mu-1}$ *and* $\lambda v(v-1) \equiv 0 \pmod{\mu(\mu-1)}$*, are also sufficient if* $v > v_{\mu,\lambda}$*, where* $v_{\mu,\lambda}$ *is a constant depending only on* μ *and* λ*.*

For $\mu \in \{3,4,5\}$, necessary and sufficient conditions for the existence of an $S(2,\mu,v)$ are known.

Theorem 83 (Kirkman [Kir47])**.** *There exists an* STS(v) *if and only if* $v \equiv 1,3 \pmod{6}$.

Theorem 84 (Hanani [Han61])**.** *There exists an* $S(2,4,v)$ *if and only if* $v \equiv 1,4 \pmod{12}$.

Theorem 85 (Hanani [Han72])**.** *There exists an* $S(2,5,v)$ *if and only if* $v \equiv 1,5 \pmod{20}$.

For $\mu \geq 6$, the necessary and sufficient conditions on v for the existence of an $S(2,\mu,v)$ are not known in general, although for small values of μ substantial results are known. For a comprehensive table of known Steiner 2-designs, see [CD07].

Theorems 82, 83, 84, and 85 were proved by constructive methods. Hence, these existence results allow us to construct infinitely many explicit examples of entanglement-assisted quantum LDPC codes. It is worth mentioning that many of the known proofs of these theorems employ the same construction technique we used in Theorem 58. In fact, most $S(2,\mu,v)$s in the original proofs of these existence theorems have either Steiner spreads or nontrivial subdesigns.

Numerous other constructions for 2-designs also give explicit examples of $S(2,\mu,v)$s for a wide range of parameters. A detailed treatment of STS(v)s is available in [CR99]. Various constructions for $S(2,\mu,v)$s for many values of μ are also given in [Hal98].

5.B Appendix B: Parameters of quantum and classical FG-LDPC codes with girth six

Here we give tables of parameters of LDPC codes with girth six based on finite geometries. Table 5.14 gives parameters of entanglement-assisted quantum LDPC codes obtained from $PG_1(m,q)$, $AG_1(m,q)$, and $EG_1(m,q)$. Parameters of the corresponding classical FG-LDPC codes are listed in Table 5.15.

Table 5.14
Parameters of entanglement-assisted quantum LDPC codes from finite geometries.
All codes are $[[n,k,d;c]]$ EAQECCs obtained from $PG_1(m,q)$, $AG_1(m,q)$, or $EG_1(m,q)$. We omit EAQECCs which are created by subdesign deletion techniques or do not have dimension greater than one. $\varphi(m,2^t)$ is given by Theorem 59 in Subsection 5.3.1. $\rho(m,2^t)$ is defined as
$\rho(m,2^t) = \varphi(m,2^t) - \varphi(m-1,2^t)$.
Type refers to the traditional classification of FG-LDPC codes: Type I uses a line-by-point incidence matrix, while Type II uses the transposed (i.e., point-by-line) incidence matrix. For $EG(2,2^t)$, the codes obtained from either orientation of the incidence matrix are identical [KLF01].

Geometry	Type	m	q	n	k	d	c	girth
PG	II	any	2^t	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - 2\varphi(m,2^t)+1$	$q+2$	1	6
PG	II	odd	odd	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - 2\frac{q^{m+1}-q}{q-1}+1$	$2(q+1)$	1	6
PG	II	even	odd	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - \frac{q^{m+1}-q}{q-1}$	$2(q+1)$	$\frac{q^{m+1}-q}{q-1}$	6
PG	I	2	2^t	q^2+q+1	$q^2+q-2\cdot 3^t$	$q+2$	1	6
PG	I	any	2^t	$\frac{q^{m+1}-1}{q-1}$	$\frac{q^{m+1}-1}{q-1} - 2\varphi(m,2^t)+c$	$(q+2)q^{m-2}$	$\leq \varphi(m,2^t)$	6
AG	II	any	2^t	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - 2\rho(m,2^t)+1$	$q+1$	1	6
AG	II	odd	odd	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - 2q^m+1$	$2q$	1	6
AG	II	even	odd	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - q^m - 1$	$2q$	q^m-1	6
AG	I	2	2^t	q^2	$q^2+q-2\cdot 3^t$	$q+2$	q	6
AG	I	any	2^t	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - 2\rho(m,2^t)+c$	$(q+2)q^{m-2}$	$\leq \rho(m,2^t)$	6
EG	I, II	2	2^t	q^2-1	$q^2+q-2\cdot 3^t+1$	$q+1$	q	6
EG	II	any	2^t	$\frac{(q^{m-1}-1)(q^m-1)}{q-1}$	$\frac{(q^{m-1}-1)(q^m-1)}{q-1} - 2\rho(m,2^t)+2+c$	$q+1$	$\frac{q^m-q}{q-1}$	6

Table 5.15
Parameters of classical FG-LDPC codes.
We omit the cases when codes are created by subdesign deletion techniques or do not have enough dimension.
Type refers to the traditional classification of FG-LDPC codes: Type I uses a line-by-point incidence matrix, while Type II uses the transposed (i.e., point-by-line) incidence matrix. For $EG(2,2^t)$, the codes obtained from either orientation of the incidence matrix are identical [KLF01].

Geometry	Type	m	q	n	k	d	girth
PG	II	any	2^t	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - \varphi(m,2^t)$	$q+2$	6
PG	II	any	odd	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)}$	$\frac{(q^{m+1}-1)(q^m-1)}{(q^2-1)(q-1)} - \frac{q^{m+1}-q}{q-1}$	$2(q+1)$	6
PG	I	any	2^t	$\frac{q^{m+1}-1}{q-1}$	$\frac{q^{m+1}-1}{q-1} - \varphi(m,2^t)$	$(q+2)q^{m-2}$	6
AG	II	any	2^t	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - \varphi(m,2^t) + \varphi(m-1,2^t)$	$q+1$	6
AG	II	any	odd	$q^{m-1}\frac{q^m-1}{q-1}$	$q^{m-1}\frac{q^m-1}{q-1} - q^m$	$2q$	6
AG	I	any	2^t	q^m	$q^m - \varphi(m,2^t) + \varphi(m-1,2^t)$	$(q+2)q^{m-2}$	6
EG	I, II	2	2^t	q^2-1	q^2-3^t	$q+1$	6
EG	II	any	2^t	$(q^{m-1}-1)\frac{q^m-1}{q-1}$	$(q^{m-1}-1)\frac{q^m-1}{q-1} - \varphi(m,2^t) + \varphi(m-1,2^t) + 1$	$q+1$	6
EG	II	≥ 3	odd	$(q^{m-1}-1)\frac{q^m-1}{q-1}$	$\geq (q^{m-1}-1)\frac{q^m-1}{q-1} - q^m + 1$	$2q$	6

Chapter 6

Summary and future work

6.1 Summary

The central theme in this dissertation has been the power of finite geometry designs. These designs lie at the intersection of design theory and finite geometries, and are closely related to error-correcting codes. The highly structured nature of design and finite geometries allow us to create designs and codes with desirable properties.

Chapter 2 introduces an infinite family of counterexamples to Hamada's conjecture. This is the first infinite family of counterexamples in the affine case. These polarity designs share many properties with the corresponding finite geometry designs, including parameters and 2-ranks. The construction also allows us to create many non-geometric designs which maintain the same parameters (but not p-ranks) as the geometric designs.

Chapter 3 continues this thread, by demonstrating another way in which the projective and affine polarity designs retain a great deal of geometric structure. The polarity constructions from [JT09] and Chapter 2 produce designs which maintain the nested structure of the finite geometries from which they are obtained. We show that, as a result of this structure, the codes whose parity check matrices are the incidence matrices of polarity designs admit multi-step majority logic decoding. In the case of polarity designs constructed over the binary field, the codes obtained from these designs have error-correcting performance which is equal to the geometric codes. In addition, we showed that the minimum distance of the block codes of these designs is also equal to that of the codes obtained from finite geometries in the binary case. Thus, the polarity designs maintain a great deal of geometric structure. This structure exists even in the non-polarity modified designs.

Chapter 4 makes use of the structure of finite geometry designs in another way, this time in the context of quantum error-correcting codes. The properties of finite geometry designs allow us to construct quantum codes with known parameters. We not only show how to construct such codes from finite geometry designs and their relatives, but also determine the minimum distance of related classical codes.

Chapter 5 approaches the construction of quantum codes from a different direction. This chapter demonstrates that designs are the ideal structure from which to construct EAQECCs. This systematizes the construction of EAQECCs, by providing a framework for creating EAQECCs with known parameters and desirable structure. The properties of Steiner designs – especially those obtained from finite geometries – allow us to determine all parameters of the EAQECCs. These designs also impart a structure on the codes which admits an excellent decoding algorithm, as well as allowing for flexible parameters. This chapter includes not only new results on quantum codes, but also for the classical codes used to construct them.

Together, these chapters demonstrate how finite geometry designs may be used as a base on which to construct combinatorial objects which inherit their most desirable properties from the designs themselves.

6.2 Future work

The work presented in this dissertation opens many doors for further study. Several of these possibilities are enumerated below.

The affine polarity designs described in Chapter 2 provide, for the affine case, the first known infinite family of counterexamples to Hamada's conjecture. Together with the projective polarity designs of Jungnickel and Tonchev [JT09], these counterexamples open many questions concerning Hamada's conjecture.

- The main problem related to Hamada's conjecture is characterization. Hamada's conjecture is known to be true for a variety of parameters, but it is also known to be false for others. For many parameters, no results are known at all. Thus, the major question is: for which parameter sets are the finite geometry designs the unique designs of minimum p-rank? For which are there non-isomorphic designs with the same p-rank? Do there exist designs with a *lower* p-rank than the geometric designs? This answer to this final question is wholly unknown, other than those cases in which Hamada's conjecture has already been proven to be correct.

- To what extent can the polarity construction be extended? The polarity construction, as it currently stands, applies to designs constructed over prime fields (in the projective case) and the binary field (in the affine case). Are there counterexamples for general prime power q? The polarity constructions also limit the possible block dimensions: can these be expanded?
- Is there a construction which generalizes the other known counterexamples, which are not yet part of infinite families? What additional properties do these designs share with the finite geometry designs?

Chapter 3 addresses additional structural properties of the polarity designs, within the framework of a decoding algorithm for related codes.

- What other geometric properties do the polarity designs maintain? Are there equivalents of common finite geometric substructures (such as arcs, ovals, or generalized quadrangles) which may be found within these designs?
- Is it possible to determine the minimum distances of the block codes of the projective polarity designs other than in the binary case? Is it possible to determine the minimum distances for block codes obtained from non-polarity modified designs?

The quantum codes examined in Chapters 4 and 5 are constructed from finite geometries, and make use of key properties of the finite geometries.

- What other geometric structures have combinatorial properties which are desirable for quantum codes? For example, generalized quadrangles are a structure for which many properties are known, including rankHH^T for an incidence matrix H. What are the parameters and properties of the codes defined by these structures?
- There are many constructions which allow for the creation of quantum codes from classical codes. In these works, we explored two of these constructions. How do other constructions benefit from codes with strong combinatorial properties? In what ways do designs and finite geometries contribute to the construction of such codes?
- Is it possible to use the incidence matrices of the polarity designs to define quantum codes, whether q-ary or EAQECCs?

The process of discovering answers to these questions will address many fundamental questions of design and coding theory, while deepening our insight into the structure of finite geometries and their relatives.

References

[ACT09] A. Azzam, D. Clark, and V. D. Tonchev, *On extended cyclic codes, Reed-Muller codes, and related designs*, Journal of Combinatorics, Information & System Sciences **34** (2009), no. 1-4, 13–22.

[AHK$^+$04] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, *Construction of low-density parity-check codes based on balanced incomplete block designs*, IEEE Transactions on Information Theory **50** (2004), 1257–1268.

[AK66] E. F. Assmus and J. D. Key, *Designs and codes: an update*, Designs, Codes, and Cryptography **9** (1966), 7–27.

[AK92] ______, *Designs and their codes*, Cambridge Univ. Press, Cambridge, 1992.

[AK99] ______, *Polynomial codes and finite geometries*, The CRC Handbook of Coding Theory (W. C. Huffman and V. S. Pless, eds.), Elsevier Science, 1999.

[Aly08] S. A. Aly, *A class of quantum LDPC codes constructed from finite geometries*, Proc. IEEE GLOBECOM, 2008, pp. 1–5.

[AM69] E. F. Assmus Jr. and H. F. Mattson Jr., *New 5-designs*, Journal of Combinatorial Theory **6** (1969), 122–151.

[AMG74] E. F. Assmus, H. F. Mattson, and M. Guza, *Self-orthogonal Steiner systems and projective planes*, Mathematische Zeitschrift **138** (1974), 89–96.

[APS] *Copyright policies - Journals of the American Physics Society*, `http://publish.aps.org/copyrightFAQ.html`.

[BB66] R. C. Bose and R. C. Burton, *A characterization of flat spaces in a finite geometry and the uniqueness of the Hamming and the MacDonald codes*, Journal of Combinatorial Theory **1** (1966), 96–104.

[BDH06a] T. Brun, I. Devetak, and M. H. Hsieh, *Correcting quantum errors with entanglement*, Science **314** (2006), 436–439.

[BDH06b] T. A. Brun, I. Devetak, and M.-H. Hsieh, *Catalytic quantum error correction*, e-print, 2006.

[BE00] J. Bierbrauer and Y. Edel, *Quantum twisted codes*, Journal of Combinatorial Designs **8** (2000), 174–188.

[BJL99] T. Beth, D. Jungnickel, and H. Lenz, *Design theory*, 2 ed., Cambridge University Press, 1999.

[BLT96] A. Baartmans, I. Landjev, and V. D. Tonchev, *On the binary codes of Steiner triple systems*, Designs, Codes, and Cryptography **8** (1996), 29–43.

[Bow02] G. Bowen, *Entanglement required in achieving entanglement-assisted channel capacities*, Physical Review A **66** (2002), 052313.

[CD07] C. J. Colbourn and J. H. Dinitz (eds.), *Handbook of Combinatorial Designs*, Chapman & Hall/CRC, Boca Raton, FL, 2007.

[CF09] C. J. Colbourn and Y. Fujiwara, *Small stopping sets in Steiner triple systems*, Cryptography and Communications **1** (2009), 31–46.

[CH92] P. V. Ceccherini and J. W. P. Hirschfeld, *The dimension of projective geometry codes*, Discrete Mathematics **106/107** (1992), 117–126.

[CJT11] D. Clark, D. Jungnickel, and V. D. Tonchev, *Affine geometry designs, polarities, and Hamada's conjecture*, Journal of Combinatorial Theory, Series A **118** (2011), 231–239.

[CK99] K. L. Clark and J. D. Key, *Geometric codes over fields of odd prime power order*, Congressus Numerantium **137** (1999), 177–186.

[CKdR99] N. Calkin, J. D. Key, and M. de Resmini, *Minimum weight and dimension formulas for some geometric codes*, Designs, Codes, and Cryptography **17** (1999), 105–120.

[CMRv94] C. J. Colbourn, E. Mendelsohn, A. Rosa, and J. Širáň, *Anti-mitre Steiner triple systems*, Graphs and Combinatorics **10** (1994), 215–224.

[COT07] T. Camara, H. Ollivier, and J.-P. Tillich, *A class of quantum LDPC codes: Construction and performances under iterative decoding*, Proceedings of the IEEE International Symposium on Information Theory, 2007, pp. 811–815.

[CR99] C. J. Colbourn and A. Rosa, *Triple Systems*, Oxford Univ. Press, Oxford, 1999.

[CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, *Quantum error correction via codes over GF(4)*, IEEE Transactions on Information Theory **44** (1998), 1369–1387.

[CS96] A. R. Calderbank and P. W. Shor, *Good quantum error-correcting codes exist*, Physical Review A **54** (1996), 1098–1105.

[CT] D. Clark and V. D. Tonchev, *Nonbinary quantum codes derived from finite geometries*, Finite Fields and their Applications, to appear.

[CT09] ______, *Embedding symmetric nets in affine geometry and Reed-Muller codes*, Journal of Statistics and Applications **4** (2009), 479–488.

[DBH09] I. Devetak, T. A. Brun, and M.-H. Hsieh, *Entanglement-assisted quantum error-correcting codes*, New Trends in Mathematical Physics (Vladas Sidoravičius, ed.), Springer Netherlands, 2009, pp. 161–172.

[Deh80] M. Dehon, *Ranks of incidence matrices of t-designs* $S_\lambda(t,t+1,v)$, European Journal of Combinatorics **1** (1980), 97–100.

[Dem68] P. Dembowski, *Finite geometries*, Springer, 1968.

[DHV78] J. Doyen, X. Hubaut, and M. Vandensavel, *Ranks of incidence matrices of Steiner triple systems*, Mathematische Zeitschrift **163** (1978), 251–259.

[Die05] R. Diestel, *Graph theory*, electronic 3rd edition ed., Springer-Verlag, 2005.

[Djo08] I. B. Djordjevic, *Quantum LDPC codes from balanced incomplete block designs*, IEEE Communications Letters **12** (2008), 389–391.

[Djo10] ______, *Photonic entanglement-assisted quantum low-density parity-check encoders and decoders*, Optics Letters **35** (2010), 1464–1466.

[DW79] J. Doyen and R. M. Wilson, *Embeddings of Steiner triple systems*, Discrete Mathematics **5** (1979), 229–239.

[Els] *Ways to use journal articles published by Elsevier: a practical guide*, `http://libraryconnect.elsevier.com/lcp/0403/lcp0403.pdf`.

[FC10] Y. Fujiwara and C. J. Colbourn, *A combinatorial approach to X-tolerant compaction circuits*, IEEE Transactions on Information Theory **56** (2010), 3196–3206.

[FCV$^+$10] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev, *Entanglement-assisted quantum low-density parity-check codes*, Physical Review A **82** (2010), 1–19.

[Fuj07] Y. Fujiwara, *Halving Steiner* 2*-designs*, Discrete Mathematics **307** (2007), 1551–1558.

[FY90] A. Frumkin and A. Yakir, *Rank of inclusion matrices and modular representation theory*, Israel Journal of Mathematics **71** (1990), no. 3, 309–320.

[Gal63] R. G. Gallager, *Low density parity check codes*, MIT Press, Cambridge, MA, 1963.

[GD68] J-M. Goethals and P. Delsarte, *On a class of majority-logic decodable cyclic codes*, IEEE Transactions on Information Theory **14** (1968), 182–188.

[GGW00] M. J. Grannell, T. S. Griggs, and C. A. Whitehead, *The resolution of the anti-pasch conjecture*, Journal of Combinatorial Designs **8** (2000), 300–309.

[GM66] R. Graham and F. J. MacWilliams, *On the number of information symbols in difference-set cyclic codes*, Bell Systems Technical Journal **45** (1966), 1057–1080.

[GM72] A. D. Griffiths and V. C. Mavron, *On the construction of certain affine designs*, Journal of the London Mathematical Society **5** (1972), 105–113.

[Hal98] M. Hall, *Combinatorial Theory*, Wiley-Interscience, 1998.

[Ham68] N. Hamada, *The rank of the incidence matrix of points and d-flats in finite geometries*, Journal of Science of the Hiroshima University **32** (1968), 381–396.

[Ham73] ______, *On the p-rank of the incidence matrix of a balanced or partially balanced incomplete block design and its applications to error-correcting codes*, Hiroshima Math. J. **3** (1973), no. 1, 153–226.

[Han61] H. Hanani, *The existence and construction of balanced incomplete block designs*, The Annals of Mathematical Statistics **32** (1961), 361–386.

[Han72] ______, *On balanced incomplete block designs with blocks having five elements*, Journal of Combinatorial Theory, Series A **12** (1972), 184–201.

[HBD09] M.-H. Hsieh, T. A. Brun, and I. Devetak, *Entanglement-assisted quantum quasicyclic low-density parity-check codes*, Physical Review A **79** (2009), 032340.

[HDB07] M.-H. Hsieh, I. Devetak, and T. A. Brun, *General entanglement-assisted quantum error-correcting codes*, Physical Review A **76** (2007), 062313.

[HI07] M. Hagiwara and H. Imai, *Quantum quasi-cyclic LDPC codes*, Proceedings of the IEEE International Symposium on Information Theory, 2007, pp. 806–810.

[Hil92] G. Hillebrandt, *The p-rank of* $(0,1)$*-matrices*, Journal of Combinatorial Theory, Series A **60** (1992), 131–139.

[Hir98] J. W. P. Hirschfeld, *Projective geometries over finite fields*, 2 ed., Oxford University Press, 1998.

[HLT05] M. Harada, C. Lam, and V. D. Tonchev, *Symmetric $(4,4)$-nets and generalized Hadamard matrices over groups of order 4*, Designs, Codes, and Cryptography (2005), 71–87.

[HO75] N. Hamada and H. Ohmori, *On the BIB designs having minimum p-rank*, Journal of Combinatorial Theory, Series A **18** (1975), 131–140.

[HP03] W. C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003.

[HS94] J. W. P. Hirschfeld and R. Shaw, *Projective geometry codes over prime fields*, Finite Fields: Theory, Applications, and Algorithms (G. L. Mullen and P. J-S. Shiue, eds.), Contemporary Mathematics Series 168, American Mathematical Society, Providence, 1994, pp. 151–163.

[HYH11] M.-H. Hsieh, W. T. Yen, and L. Y. Hsu, *Performance of entanglement-assisted quantum LDPC codes constructed from finite geometries*, IEEE Transactions on Information Theory **57** (2011), no. 3, 1761–1769.

[IM07] L. Ioffe and M. Mézard, *Asymmetric quantum error-correcting codes*, Physical Review A **75** (2007), 032345.

[Joh04] S. Johnson, *Low-density parity-check codes from combinatorial designs*, Ph.D. thesis, The University of Newcastle, 2004.

[Joh10] ______, *Iterative error correction: Turbo, low-density parity-check and repeat-accumulate codes*, Cambridge University Press, 2010.

[JTa] D. Jungnickel and V. D. Tonchev, *A Hamada type characterization of the classical geometric designs*, Designs, Codes, and Cryptography, to appear.

[JTb] ______, *New invariants for incidence structures*, Designs, Codes, and Cryptography, to appear.

[JT09] ______, *Polarities, quasi-symmetric designs, and Hamada's conjecture*, Designs, Codes, and Cryptography **51** (2009), 131–140.

[JW01] S. J. Johnson and S. R. Weller, *Regular low-density parity-check codes from combinatorial designs*, In Proceedings of the IEEE Information Theory Workshop, 2001, pp. 90–92.

[JW03] ______, *Resolvable 2-designs for regular low-density parity-check codes*, IEEE Transactions on Communications **51** (2003), 1413–1419.

[Kir47] T. P. Kirkman, *On a problem in combinations*, The Cambridge and Dublin Mathematical Journal **2** (1847), 191–204.

[KKKS06] A. Ketkar, A. Klappenecker, S. Kumar, and P. K. Sarvepalli, *Nonbinary stabilizer codes over finite fields*, IEEE Transactions on Information Theory **52** (2006), 4892–4914.

[KLF01] Y. Kou, S. Lin, and M. P. C. Fossorier, *Low-density parity-check codes based on finite geometries: A rediscovery and new results*, IEEE Transactions on Information Theory **47** (2001), 2711–2736.

[KM91] J. D. Key and K. Mackenzie, *An upper bound for the p-rank of a translation plane*, Journal of Combinatorial Theory, Series A **56** (1991), 297–302.

[LMSS01] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, *Improved low-density parity-check codes using irregular graphs and belief propagation*, IEEE Transactions on Information Theory **47** (2001), 585–598.

[LT96] C. Lam and V. D. Tonchev, *Classification of affine resolvable 2-(27,9,4) designs*, Journal of Statistical Planning and Inference **56** (1996), 187–202.

[LT00] ______, *Classification of affine resolvable 2-(27,9,4) designs: Corrigendum*, Journal of Statistical Planning and Inference **86** (2000), 277–278.

[Mac03] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*, Cambridge University Press, Cambridge, 2003.

[Mas62] J. L. Massey, *Threshold decoding*, Ph.D. thesis, Massachusetts Institute of Technology, Cambridge, MA, 1962.

[MD99] D. J. C. MacKay and M. Davey, *Evaluation of Gallager codesfor short block length and high rate applications*, Proc. IMA Workshop Codes, Systems and Graphical Models, 1999, pp. 113–130.

[MJ04] M. Müller and M. Jimbo, *Erasure-resilient codes from affine spaces*, Discrete Applied Mathematics **143** (2004), 292–297.

[MM68] F. J. MacWilliams and H. B. Mann, *On the p-rank of the design matrix of a difference set*, Information and Control **12** (1968), 474–488.

[MMM04] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, *Sparse-graph codes for quantum error correction*, IEEE Transactions on Information Theory **50** (2004), 2315–2330.

[MMT08] V. C. Mavron, T. P. McDonough, and V. D. Tonchev, *On affine designs and Hadamard designs with line spreads*, Discrete Mathematics **308** (2008), 2742–2750.

[MN95] D. J. C. MacKay and R. M. Neal, *Good codes based on very sparse matrices*, Cryptography and Coding 5th IMA Conference (Berlin, Germany) (C. Boyd, ed.), Lecture Notes in Computer Science, no. 1025, Springer, 1995, pp. 100–111.

[Mor80] B. Mortimer, *The modular permutation representations of the known doubly transitive groups*, Proceedings of the London Mathematical Society, vol. 3, 1980, pp. 1–20.

[MT] A. Munemasa and V. D. Tonchev, *The twisted Grassman graph is the block graph of a design*, to appear in Innovations in Incidence Geometry, doi: arXiv:0906.4509v2.

[MT09a] Z. Mateva and S. Topalova, *Hadamard 2-(63,31,15) designs invariant under the dihedral group of order 10*, Discrete Mathematics **309** (2009), 1347–1356.

[MT09b] ______, *Line spreads of* $PG(5,2)$, Journal of Combinatorial Designs **17** (2009), 90–102.

[PC08] D. Poulin and Y.-J. Chung, *On the iterative decoding of sparse quantum codes*, Quantum Information and Computation **8** (2008), 986–1000.

[PW72] W. W. Peterson and E. J. Weldon, *Error-correcting codes*, 2 ed., MIT Press, Cambridge, MA, 1972.

[Rah91] A. Rahilly, *On the line structure of designs*, Discrete Mathematics **92** (1991), 291–303.

[RB75] M. Rahman and I. F. Blake, *Majority logic decoding using combinatorial designs*, IEEE Transactions on Information Theory **21** (1975), 585–587.

[Ree53] I. S. Reed, *A class of multiple-error-correcting codes and the decoding scheme*, Tech. Report 44, Lincoln Laboratory, MIT, 1953.

[RSU01] T. Richardson, M. A. Shokrollahi, and R. Urbanke, *Design of capacity-approaching irregular low-density parity check codes*, IEEE Transactions on Information Theory **47** (2001), 619–637.

[RU01] T. Richardson and R. Urbanke, *The capacity of low-density parity check codes under message-passing decoding*, IEEE Transactions on Information Theory **47** (2001), 599–618.

[Rud67] L. D. Rudolph, *A class of majority-logic decodable codes*, IEEE Transactions on Information Theory **13** (1967), 306–307.

[Sac79] H. Sachar, *The $\mathbb{F}_p$ span of the incidence matrix of a finite projective plane*, Geometriae Dedicata **8** (1979), 407–415.

[Seg64] B. Segre, *Teoria di Galois, proiettive e geometrie non Desarguesiane*, Annali di Matematica Pura ed Applicata (1964).

[Sho95] P. W. Shor, *Scheme for reducing decoherence in quantum computer memory*, Physical Review A **52** (1995), R2493–2496.

[SK05] P. K. Sarvepalli and A. Klappenecker, *Nonbinary quantum Reed-Muller codes*, Proceedings of the IEEE International Symposium on Information Theory (Adelaide, Australia), 2005, pp. 1023–1027.

[SKR09] P. K. Sarvepalli, A. Klappenecker, and M. Rotteler, *Asymmetric quantum LDPC codes*, Proceedings of the Royal Society A **465** (2009), 1645–1672.

[Smi67] K. J. C. Smith, *Majority decodable codes derived from finite geometries*, Ph.D. thesis, University of North Carolina, Chapel Hill, NC, 1967.

[Smi69] ______, *On the p-rank of the incidence matrix of points and hyperplanes in a finite projective geometry*, Journal of Combinatorial Theory **7** (1969), 122–129.

[ST08] C. Sarami and V. D. Tonchev, *Cyclic quasi-symmetric designs and self-orthogonal codes of length 63*, Journal of Statistical Planning and Inference **138** (2008), 80–85.

[Ste96a] A. M. Steane, *Error-correcting codes in quantum thoery*, Physical Review Letters **77** (1996), 793–797.

[Ste96b] ______, *Simple quantum error correcting codes*, Physical Review Letters **77** (1996), 793–797.

[Ste99] ______, *Quantum Reed-Muller codes*, IEEE Transactions on Information Theory **45** (1999), 1701–1703.

[Sti04] D. Stinson, *Combinatorial designs: Constructions and analysis*, Springer, New York, 2004.

[Tei80] L. Teirlinck, *On projective and affine hyperplanes*, Journal of Combinatorial Theory, Series A **28** (1980), 290–306.

[Ton86] V. D. Tonchev, *Quasi-symmetric 2-(31, 7, 7)-designs and a revision of Hamada's conjecture*, Journal of Combinatorial Theory, Series A **42** (1986), 104–110.

[Ton98] ———, *Codes and designs*, Handbook of Coding Theory (V. S. Pless and W. C. Huffman, eds.), North Holland, Amsterdam, 1998, pp. 1229–1267.

[Ton99] ———, *Linear perfect codes and a characterization of the classical designs*, Designs, Codes, and Cryptography **17** (1999), 121–128.

[Ton03] ———, *A note on MDS coeds, n-arcs, and complete designs*, Designs, Codes, and Cryptography **29** (2003), 247–250.

[Ton08] ———, *Quantum codes from caps*, Discrete Mathematics **308** (2008), 6368–6372.

[Ton09] ———, *Generalized weighing matrices and self-orthogonal codes*, Discrete Mathematics **309** (2009), 2697–2699.

[TW97] V. D. Tonchev and R. S. Weishaar, *Steiner triple systems of order 15 and their codes*, Journal of Statistical Planning and Inference **58** (1997), 207–216.

[TXK^{+}04] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, *On algebraic construction of Gallager and circulant low-density parity-check codes*, IEEE Transactions on Information Theory **50** (2004), 1269–1279.

[TXLAG05] H. Tang, J. Xu, S. Lin, and K. Abdel-Ghaffar, *Codes on finite geometries*, IEEE Transactions on Information Theory **51** (2005), 572–596.

[vDK05] E. R. van Dam and J. H. Koolen, *A new family of distance-regular graphs with unbounded diameter*, Inventiones Mathematicae **162** (2005), 189–193.

[WB08] M. M. Wilde and T. A. Brun, *Optimal entanglement formulas for entanglement-assisted quantum coding*, Physical Review A **77** (2008), 064302.

[Wel67] E. J. Weldon, *Euclidean geometry cyclic codes*, Tech. report, Defense Technical Information Center, University of Hawaii, Honolulu, HI, 1967.

[Wil72a] R. M. Wilson, *An existence theorem for pairwise balanced designs, I: composition theorems and morphisms*, Journal of Algebraic Combinatorics **13** (1972), 220–245.

[Wil72b] ———, *An existence theorem for pairwise balanced designs, II: the structure of PBD-closed sets and the existence conjecture*, Journal of Combinatorial Theory, Series A **13** (1972), 246–273.

[Wil75] ———, *An existence theorem for pairwise balanced designs, III: proof of the existence conjecture*, Journal of Combinatorial Theory, Series A **18** (1975), 71–79.

[Yak93] A. Yakir, *Inclusion matrix of k vs. l affine subspaces and a permutation module of the general affine group*, Journal of Combinatorial Theory, Series A **63** (1993), 301–317.

Appendix C

Copyright documentation

Several chapters in this dissertation are re-prints of previously published papers. This appendix includes documentation provided by each publisher, giving the author permission to reprint these papers.

Permission for the following papers is given below:

- *Affine geometry designs, polarities, and Hamada's conjecture* (Chapter 2)
- *Nonbinary quantum codes derived from finite geometries* (Chapter 4)

Each of these was printed in an Elsevier journal. The excerpt on the following page is taken from the Elsevier's information packet, "Ways to use journal articles published by Elsevier: a practical guide" [Els]. Note the final bullet point.

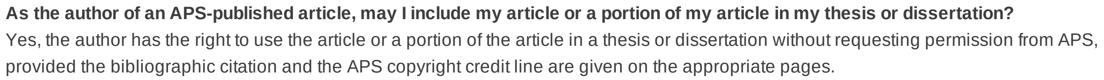
General use of articles

Authors publishing in Elsevier journals retain wide rights to continue to use their works to support scientific advancement, teaching and scholarly communication.

An author can, without asking permission, do the following after publication of the author's article in an Elsevier-published journal:

- Make copies (print or electronic) of the author's article for personal use or the author's own classroom teaching.
- Make copies of the article and distribute them (including via email) to known research colleagues for their personal use but not for commercial purposes as described in this pamphlet.
- Present the article at a meeting or conference and distribute copies of the article to attendees.
- Allow the author's employer to use the article in full or in part for other intracompany use (e.g., training).
- Retain patent and trademark rights and rights to any process or procedure described in the article.
- Include the article in full or in part in a thesis or dissertation.

Permission for “Entanglement-assisted quantum low-density parity-check codes” (Chapter 5) is given below. This excerpt is taken from the American Physics Society’s “Copyright FAQ” [APS]. The APS is the publisher of Physical Review A, in which this article was published.



As the author of an APS-published article, may I include my article or a portion of my article in my thesis or dissertation?
Yes, the author has the right to use the article or a portion of the article in a thesis or dissertation without requesting permission from APS, provided the bibliographic citation and the APS copyright credit line are given on the appropriate pages.