2014

MAXIMAL ARCS, ABOVE AND BEYOND

Diego Domenzain-Gonzale
Michigan Technological University

MAXIMAL ARCS, ABOVE AND BEYOND

By
Diego Domenzain

A REPORT

Submitted in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

In Mathematical Sciences

MICHIGAN TECHNOLOGICAL UNIVERSITY
2014

This report has been approved in partial fulfillment of the requirements for the Degree of MASTER OF SCIENCE in Mathematical Sciences.

Department of Mathematical Sciences

Report Advisor: *Dr. Stefaan De Winter*

Committee Member: *Dr. Melissa Keranen*

Committee Member: *Dr. Laura Brown*

Department Chair: *Dr. Mark Gockenbach*

Dedication

To all the trees in the Keweenaw, who have seen me go through many changes.

Contents

List of Figures

Abstract

This report explores combinatorial structures in Finite Geometries by giving known constructions of maximal arcs; using maximal arcs to construct two-weight codes, partial geometries, strongly regular graphs and LDPC codes; a review on how to generalize maximal arcs to higher dimensions through Perp-Systems; and an effort in finding constructions of new Perp-Systems.

Chapter 1

Introduction

The structure of this report is as follows:

- Chapter 1 introduces projective geometries, maximal arcs, two weight sets, linear codes, partial geometries, strongly regular graphs and Low Density Parity Check Codes (LDPC codes); as well as some relationships among them.

- Chapter 2 explains how from a given maximal arc, other combinatorial structures arise. Two examples are given, and a third desirable example is outlined.

- Chapter 3 gives known constructions of maximal arcs, and outlines the known proof on why maximal arcs cannot exist in projective planes $\mathsf{PG}(2, \mathsf{q})$ with q odd.

- Chapter 4 introduces Perp-Systems as a generalization of maximal arcs in higher dimensions and explains how to build partial geometries from them.

  A solution to the desirable example of Chapter 2 is given, and the motivation for the last part of Chapter 6 is thus given.

- Chapter 5 summarises all given constructions.

- Chapter 6 gathers possible projects naturally arising from the previous chapters.

  The final part of this Chapter addresses a possible construction of perp-systems inspired in Mathon's construction of maximal arcs given in Chapter 3, attempting to generalize the desirable example of Chapter 2.

1.1 Projective Geometries

To build maximal arcs, we will first need to build Projective Geometries. To build Projective Geometries, we will first need to build a finite vector space. To build a finite vector space, we will first need to build a finite field. The next subsections will explain these constructions.

1.1.1 Finite fields

A field is a non-empty set F with two operations, addition and multiplication in which addition forms a group in F with an identity element 0_F, while multiplication forms a group in $F\backslash\{0_F\}$ with identity 1_F.

If a field F is finite, then it has size $q = p^h$ where p is a prime. Moreover, all fields with q elements are isomorphic, and we denote this "unique" field by $\mathbb{F}_q$. See [37].

We build $\mathbb{F}_p$ by taking the integers $\{0, 1, ..., p-1\}$ and defining addition and multiplication modulo p. To build a field with $q = p^h$ elements, we take an irreducible polynomial f over $\mathbb{F}_p$ of degree h where $f(\alpha) = 0$, and we consider the following quotient:

$$\begin{aligned} \mathbb{F}_p[X]/ < f > &\cong \{a_{h-1}\alpha^{h-1} + \cdots + a_1\alpha + a_0 : a_i \in \mathbb{F}_p\} \\ &\cong \{[a_{h-1}, ..., a_1, a_0] : a_i \in \mathbb{F}_p\} \\ &\cong \mathbb{F}_{p^h}. \end{aligned}$$

This quotient is a field because f is irreducible.

In general, for q a power of a prime we can build $\mathbb{F}_{q^h}$ by taking an irreducible polynomial f of degree h and considering its quotient over $\mathbb{F}_q[X]$:

$$\mathbb{F}_q[X]/ < f > \cong \mathbb{F}_{q^h}. \tag{1.1}$$

A *subfield* of a field F is a proper subset of F that is itself a field under the same operations as F. From the the isomorphisim 1.1 we see that the only subfields of $\mathbb{F}_{q^h}$ are $\mathbb{F}_{q^j}$ whenever j divides h.

The non-zero elements of the field $\mathbb{F}_{q^h}$ form a cyclic multiplicative group of order $q^h - 1$. We denote this group by $\mathbb{F}^*_{q^h}$ and we call a generator of $\mathbb{F}^*_{q^h}$ a *primitive element* of the field.

An *l-root of unity* is an element $a \in \mathbb{F}_{q^h}$ such that $a^l - 1 = 0$. Let g be a primitive element of $\mathbb{F}_{q^h}$ so $g^m = a$, then we have $a^l = 1$ if and only if $g^{ml} = 1$ and so $q^h - 1$ must divide ml. Let $d = x(q^h - 1) + yl$ be the greatest common divisor of $q^h - 1$ and l, then

$$a^{dm} = (a^{x(q^h-1)+yl})^m = (1^x 1^y)^m = 1 = a^{q^h-1}$$

and so $q^h - 1$ divides dm, which gives that $\frac{q^h-1}{d}$ divides m, and so a can be written as $g^{\frac{q^h-1}{d}m'}$. Conversely, any element in the group generated by $g^{\frac{q^h-1}{d}}$ is an l-root of unity. Hence, the number of l-roots of unity is d.

Having a way to know when a quadratic polynomial is irreducible in $\mathbb{F}_{2^h}$ will be important in the next chapters and we now collect some results. The *absolute trace* of an element x in $\mathbb{F}_{2^h}$ is given by

$$\mathrm{Tr}(x) = x + x^2 + \cdots + x^{2^{h-1}}.$$

We have $\mathrm{Tr}(x) \in \mathbb{F}_2$, $\mathrm{Tr}(x + y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ and $\mathrm{Tr}(x^2) = \mathrm{Tr}(x)$. The polynomial $f(X) = aX^2 + bX + c$ in $\mathbb{F}_{2^h}[X]$ with $b \neq 0$ is irreducible if and only if

$$\mathrm{Tr}\Big(\frac{ac}{b^2}\Big) = 1.$$

The interested reader can refer to [31] for details.

1.1.2 Vector Spaces and an Incidence Relation

Once we have a finite field $\mathbb{F}_q$ we can build a vector space $\mathbb{F}_q^n$ by taking the direct product of n copies of $\mathbb{F}_q$

$$\underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{n} = \mathbb{F}_q^n.$$

We denote the vector space $\mathbb{F}_q^n$ by $\mathsf{V}(\mathsf{n}, \mathsf{q})$.

To build our *projective geometry* we now consider the vector space $\mathsf{V}(\mathsf{n}, \mathsf{q})$ and define the points of this geometry as the one-dimensional subspaces of $\mathsf{V}(\mathsf{n}, \mathsf{q})$, the lines as the two-dimensional subspaces, and in general a $(k-1)$-dimensional subspace of our projective geometry as a k-dimensional subspace of $\mathsf{V}(\mathsf{n}, \mathsf{q})$.

The resulting projective geometry is denoted by $\mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q})$. Note that this construction also tells us that each $(k-1)$-dimensional subspace of $\mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q})$ is itself a $\mathsf{PG}(\mathsf{k}-\mathsf{1}, \mathsf{q})$. Moreover we have that in $\mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q})$, each *hyperplane*

$\mathsf{PG}(\mathsf{n}-2,\mathsf{q})$ meets in exactly one $\mathsf{PG}(\mathsf{n}-3,\mathsf{q})$ with another hyperplane.

For any two subspaces

$$\mathsf{PG}(\mathsf{k}_1,\mathsf{q}),\mathsf{PG}(\mathsf{k}_2,\mathsf{q}) \subset \mathsf{PG}(\mathsf{n}-1,\mathsf{q})$$

we say that $\mathsf{PG}(\mathsf{k}_1,\mathsf{q})$ is *incident* to $\mathsf{PG}(\mathsf{k}_2,\mathsf{q})$ if

$$\mathsf{PG}(\mathsf{k}_\mathsf{i},\mathsf{q}) \subseteq \mathsf{PG}(\mathsf{k}_\mathsf{j},\mathsf{q}).$$

We can count how many points there are in $\mathsf{PG}(\mathsf{n}-1,\mathsf{q})$ by counting how many vector lines there are in $\mathsf{V}(\mathsf{n},\mathsf{q})$.

To count vector lines in $\mathsf{V}(\mathsf{n},\mathsf{q})$, we first count how many vectors different from $\bar{0}$ there are in $\mathsf{V}(\mathsf{n},\mathsf{q})$, and then we reason that each vector line is counted as many times as there can be scalar multiples of a given vector, therefore there are

$$[n]_q := \frac{q^n-1}{q-1}$$

vector lines in $\mathsf{V}(\mathsf{n},\mathsf{q})$, and so $[n]_q$ many points in $\mathsf{PG}(\mathsf{n}-1,\mathsf{q})$.

In general we can count how many k-dimensional subspaces there are in $\mathsf{V}(\mathsf{n},\mathsf{q})$, which is the same as counting $(k-1)$-subspaces in $\mathsf{PG}(\mathsf{n}-1,\mathsf{q})$, by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{[n]_q!}{[k]_q![n-k]_q!}.$$

Given a subspace $\mathsf{U} \subset \mathsf{V}(\mathsf{n},\mathsf{q})$ with dimension k, we can count how many subspaces of $\mathsf{V}(\mathsf{n},\mathsf{q})$ with dimension $k+c$ contain U, by counting how many ways there are of choosing c different linearly independent vector lines in $\mathsf{V}(\mathsf{n},\mathsf{q})\backslash\mathsf{U}$. Let $\mathrm{I}(k,c)$ be the number of different subspaces with dimension $k+c$ containing a subspace of dimension k, we have

$$\mathrm{I}(k,c) \;=\; \begin{bmatrix} n-k \\ c \end{bmatrix}_q. \tag{1.2}$$

Note that this also gives us a way to count the number of projective geometries of dimension $k+c-1$ incident to those of dimension $k-1$ in $\mathsf{PG}(\mathsf{n}-1,\mathsf{q})$.

As an example Figure 1.1 shows $\mathsf{PG}(2,3)$. Since points in $\mathsf{PG}(2,3)$ come from 1-dimensional subspaces in $\mathsf{V}(3,3)$, each point could be labeled with $q-1=2$ different vectors, corresponding to the different scalar multiples a given vector in $\mathsf{V}(3,3)$. Out of the $q-1$ choices for labelling a given point in our projective geometry, we choose the vector in $\mathsf{V}(3,3)$ whose first non-zero entry is 1.

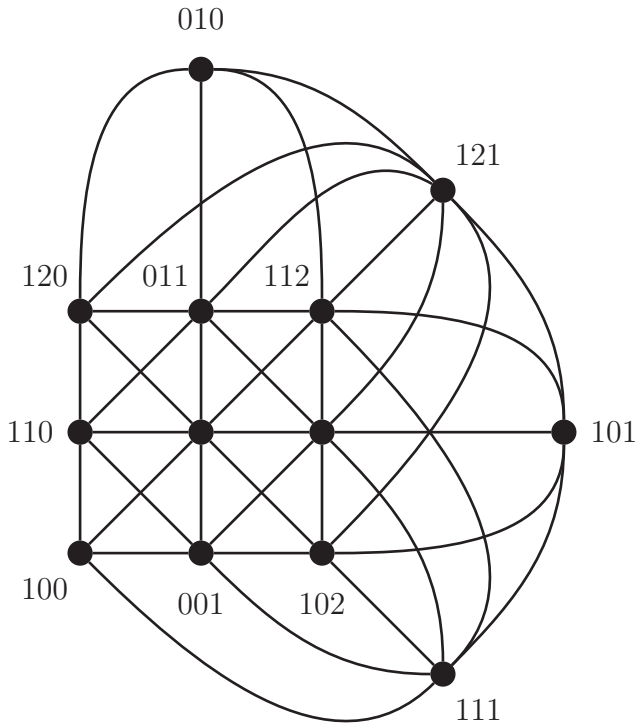

Figure 1.1: $\mathsf{PG}(2,3)$

1.1.3 Blowing up

We next describe how to "blow up" the vector space $\mathsf{V}(\mathsf{n},\mathsf{q}^\mathsf{h})$. In light of relation (1.1) we have that

$$\begin{aligned}\mathbb{F}_q[X]/<f> &\cong \{a_{h-1}\alpha^{h-1}+\cdots+a_1\alpha+a_0 : a_i\in\mathbb{F}_q\}\\ &\cong \{[a_{h-1},...,a_1,a_0] : a_i\in\mathbb{F}_q\}\\ &\cong \mathbb{F}_{q^h}\end{aligned}$$

and so we can think of $\mathbb{F}_{q^h}$ as the h-dimensional vector space $\mathbb{F}_q^h$.

This gives us that for any $\mathsf{v}\in\mathsf{V}(\mathsf{n},\mathsf{q}^\mathsf{h})$ we can think of each entry v_i of v as a vector $v\in\mathbb{F}_q^h$.

By replacing each entry v_i with its expression as v, we get the vector space $\mathsf{V}(\mathsf{h}\cdot\mathsf{n},\mathsf{q})$. We call this construction a *blow up* of $\mathsf{V}(\mathsf{n},\mathsf{q}^\mathsf{h})$. We summarise:

$$\mathsf{V}(\mathsf{n},\mathsf{q}^\mathsf{h}) \overset{\text{blow up}}{\longrightarrow} \mathsf{V}(\mathsf{h}\cdot\mathsf{n},\mathsf{q}) \tag{1.3}$$

Since each projective geometry was built by taking an incidence relation on a vector space, the blow up over $\mathsf{V}(\mathsf{n}, \mathsf{q}^\mathsf{h})$ also gives us a blow up for $\mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q}^\mathsf{h})$:

$$\mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q}^\mathsf{h}) \overset{\text{blow up}}{\longrightarrow} \mathsf{PG}(\mathsf{h}\cdot\mathsf{n}-\mathsf{1}, \mathsf{q}) \tag{1.4}$$

Note that the blow up (1.3) is a one to one onto assignment, while the blow up (1.4) is one to $q^h - 1$.

Specifically, a point $\mathsf{p} \in \mathsf{PG}(\mathsf{n}-\mathsf{1}, \mathsf{q}^\mathsf{h})$ coming from the one dimensional subspace $p \subset \mathsf{V}(\mathsf{n}, \mathsf{q}^\mathsf{h})$, gets assigned to $q^h - 1$ points in $\mathsf{PG}(\mathsf{h}\cdot\mathsf{n}-\mathsf{1}, \mathsf{q})$, which correspond to the image of $p\backslash\{\overline{0}\} \subset \mathsf{V}(\mathsf{n}, \mathsf{q}^\mathsf{h})$ under the blow up (1.3).

Let's look at an example. Let $\mathbb{F}_3 = \{-1, 0, 1\}$ and $f \in \mathbb{F}_3[X]$ with $f(x) = x^2 + 1 = 0$. We have

$$\begin{aligned}
\mathbb{F}_3[X]/ < f > &\cong \{a_1 x + a_0 : a_i \in \mathbb{F}_3\} \\
&\cong \{0, 1, -1, x+1, -x, 1-x, -x-1, x, x-1\} \\
&\cong \{[a_1, a_0] : a_i \in \mathbb{F}_3\} \\
&\cong \mathbb{F}_{3^2}.
\end{aligned}$$

We will build the blow up

$$\mathsf{V}(\mathsf{3}, \mathsf{3}^\mathsf{2}) = \mathsf{V}(\mathsf{3}, \mathsf{9}) \overset{\text{blow up}}{\longrightarrow} \mathsf{V}(\mathsf{6}, \mathsf{3}) = \mathsf{V}(\mathsf{2}\cdot\mathsf{3}, \mathsf{3})$$

by the following assignment

$$[\mathsf{v_1}, \mathsf{v_2}, \mathsf{v_3}] \rightarrow [a_{11}, a_{10}, a_{21}, a_{20}, a_{31}, a_{30}]$$

where

$$\mathsf{v_i} = [a_{i1}, a_{i0}] \in \mathbb{F}_{3^2}, \quad a_{ij} \in \mathbb{F}_3$$

This induces the blow up

$$\mathsf{PG}(\mathsf{2}, \mathsf{9}) \overset{\text{blow up}}{\longrightarrow} \mathsf{PG}(\mathsf{5}, \mathsf{3})$$

where, for example the point $[0, 0, 1] \in \mathsf{PG}(\mathsf{2}, \mathsf{9})$ gets assigned to the $3^2 - 1$ points

$$[0, 0, 0, 0, a_1, a_0], \quad [a_1, a_0] \neq [0, 0]$$

1.1.4 Polarities

A *duality* [5, 6] on a projective space $\mathsf{PG}(\mathsf{n},\mathsf{q})$ is a map from $\mathsf{PG}(\mathsf{n},\mathsf{q})$ to itself such that it reverses inclusion and preserves incidence, where points are mapped to hyperplanes, lines are mapped to subspaces of one dimension less than a hyperplane, and so on. A *polarity* ρ is a duality such that ρ^2 is the identity [5, 6].

Let π be a subspace of $\mathsf{PG}(\mathsf{n},\mathsf{q})$ of dimension r. We call π^ρ the image of π under ρ. Note that since ρ is a duality, the dimension of π^ρ is $n-r-1$.

Figure 1.2 gives an example of a polarity ρ on $\mathsf{PG}(2,2)$. The image L^ρ of a line L is denoted by a pair of points that determine L, and the image p^ρ of a point p is denoted by p written closely to the line p^ρ.

1.2 Maximal Arcs

We next describe an important structure within the projective plane $\mathsf{PG}(2,\mathsf{q})$, and leave the constructions of such objects for Section 3. Maximal arcs were first introduced in [2].

A maximal arc is a non-empty proper subset $\mathcal{K}$ of points in $\mathsf{PG}(2,\mathsf{q})$, such that every line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points.

We can count the size k of $\mathcal{K}$ by fixing a point $\mathsf{p} \in \mathcal{K}$. Since p is already in $\mathcal{K}$, every line containing p must meet $\mathcal{K}$ in $d-1$ more points. Since there are $q+1$ lines through p we have

$$\begin{aligned} k = |\mathcal{K}| &= (d-1)(q+1)+1 \\ &= qd - q + d. \end{aligned}$$

What conditions must d satisfy in terms of q?

First observe that if $d = q+1$ then $k = q^2+q+1$ and so $\mathcal{K}$ consists of all the points in $\mathsf{PG}(2,\mathsf{q})$.

If $d \leq q$ then there is at least one point $\mathsf{p} \in \mathsf{PG}(2,\mathsf{q})$ that is not in $\mathcal{K}$. If p were to have all the $q+1$ lines incident to it meeting $\mathcal{K}$, then each line would contain d points of $\mathcal{K}$ and we would have

$$k \geq d(q+1) = qd + d$$

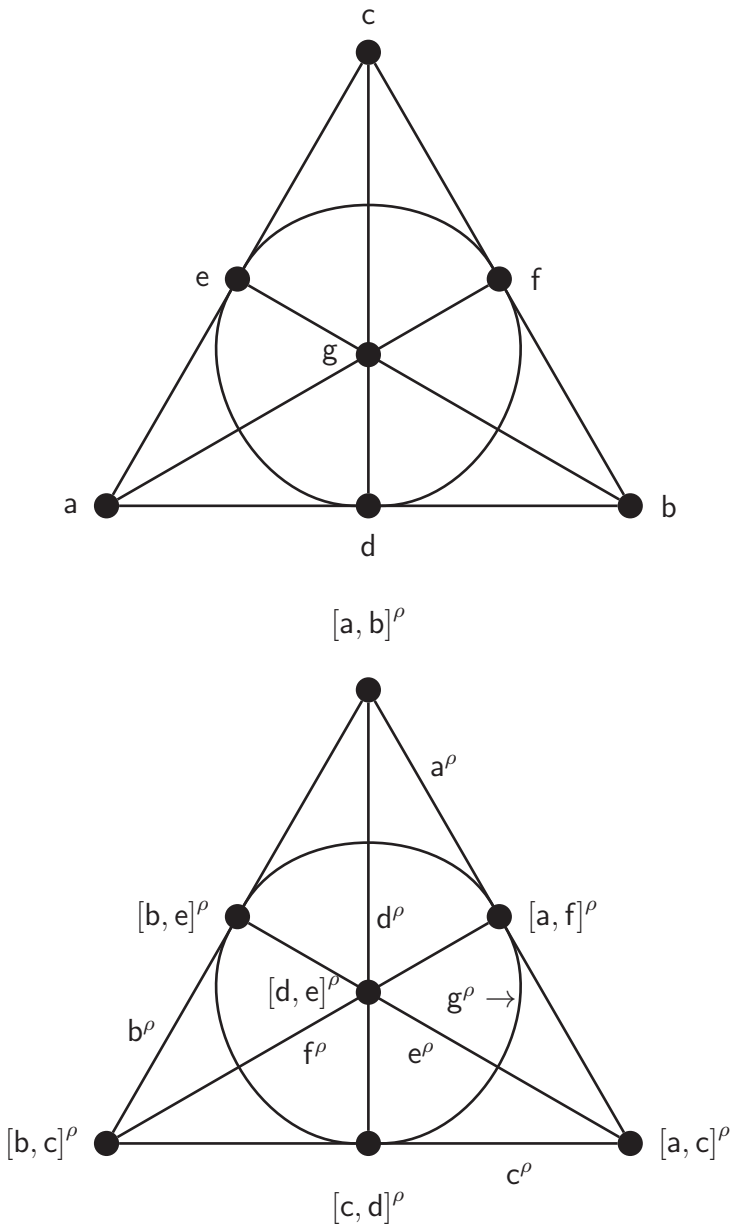

Figure 1.2: $\mathsf{PG}(2,2)$ and the image of a polarity ρ.

which is a contradiction. So there is at least one line $\mathsf{L} \subset \mathsf{PG}(2,\mathsf{q})$ that doesn't contain any point of $\mathcal{K}$.

For a given point $\mathsf{p} \in \mathsf{L}$ there are another q lines incident to it. Let this set

of q lines be

$$\{\mathsf{L}_1, ..., \mathsf{L}_\mathsf{q}\}.$$

We have that $\mathcal{K}$ is contained in this set, and each L_i contains exactly 0 or d points of $\mathcal{K}$. Let m be the the number of L_i's that contain d points of $\mathcal{K}$, then we have

$$\begin{aligned} dm &= qd - q + d \\ \Rightarrow \quad m &= q - \frac{q}{d} + 1 \end{aligned}$$

and so d must divide q. Note that if $d = q$ then $k = q^2$ and $\mathcal{K}$ is the set of all points in $\mathsf{PG}(2, \mathsf{q})\backslash\mathsf{L}$. We say that $\mathcal{K}$ is non trivial if $1 < d < q$, and we will only consider these arcs. Figure 1.3 summarises this count.

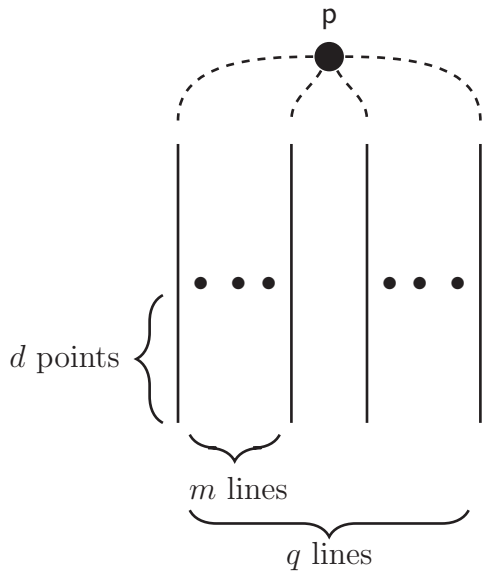

Figure 1.3: A maximal non trivial arc satisfies $1 < d < q$ and $d|q$.

1.2.1 Two weight sets

We can generalize the definition of maximal arcs in $\mathsf{PG}(2, \mathsf{q})$ to that of a *two weight set* in $\mathsf{PG}(\mathsf{k}-1, \mathsf{q})$. Some authors [9] use the term *projective set* instead of two weight set.

A *two weight set* is a non-empty proper subset $\mathcal{O}$ of n points in $\mathsf{PG}(\mathsf{k}-1, \mathsf{q})$, such that any hyperplane $\mathsf{PG}(\mathsf{k}-2, \mathsf{q}) \subset \mathsf{PG}(\mathsf{k}-1, \mathsf{q})$ contains either h_1 or h_2 points of $\mathcal{O}$.

1.3 Codes

A *linear code* is a k-dimensional subspace of $\mathsf{V}(\mathsf{n},\mathsf{q})$ [38]. We denote it by C. Vectors in C are called *codewords*. Codes are used for aiding transmition of information over a noisy channel, enabling the use of an "alphabet" made of just codewords to send messages. In order to have many words in the alphabet, the dimension k (also refered to as *rank* of the code) should be large with respect to n.

Since C is a k-dimensional subspace embedded in $\mathsf{V}(\mathsf{n},\mathsf{q})$, we can think of a $k \times n$ matrix G that "encodes" the vector $\mathsf{v} \in \mathsf{V}(\mathsf{k},\mathsf{q})$ by left multiplication. We call G a *generator* matrix of C and n its length.

Let $\mathsf{y}_i \in \mathsf{V}(\mathsf{k},\mathsf{q})$ be the columns of G for $1 \leq i \leq n$, then for every $\mathsf{v} \in \mathsf{V}(\mathsf{k},\mathsf{q})$, a codeword $\mathsf{c} \in \mathsf{C}$ is of the form

$$\mathsf{c} = \mathsf{v} \cdot G = (v \cdot \mathsf{y}_1, ..., v \cdot \mathsf{y}_n).$$

Given a way to encode a vector $\mathsf{v} \in \mathsf{V}(\mathsf{k},\mathsf{q})$, we now give a way to check if a vector $\mathsf{y} \in \mathsf{V}(\mathsf{n},\mathsf{q})$ is an encoded vector or not. Let $G^{\perp}$ be a matrix such that

$$G^{\perp} \cdot G^t = 0$$

that is, the row space of $G^{\perp}$ is orthogonal to the row space of G. We then have that $G^{\perp} \cdot \mathsf{y} = 0$ if and only if y is a codeword. Such a matrix $G^{\perp}$ is called the *parity check matrix* of C.

Let d be such that any $d-1$ columns of $G^{\perp}$ are linearly independent and some d columns are linearly dependent, then d is called the *minimum distance* of C. The minimum distance determines how different a transmitted message can be with respect to a codeword in order to correct it.

For now, we will only consider codes for which the vectors $\{\mathsf{y}_i\}_1^n$ are linearly independent, and thus we can think of the code C as being determined by a set of points $\{\hat{\mathsf{y}}_i\}_1^n$ in $\mathsf{PG}(\mathsf{k}-1,\mathsf{q})$, where $\hat{\mathsf{y}}_i$ is the 1-dimensional subspace spanned by y_i.

1.3.1 Two weight codes

The *weight* of a vector $\mathsf{c} \in \mathsf{C}$ is the number of non-zero entries of c [38][9]. We have that the minimum weight of C is the minimum distance of the code. We say that a code C is a *two weight code* if all its codewords have either one of two weights.

Two weight codes are two weight sets

Given a two weight code we can build a two weight set, and given a two weight set we can build a two weight code [9]. We describe these constructions.

Let C be a code of dimension k over $\mathsf{V}(\mathsf{n},\mathsf{q})$ with generator matrix G,

$$G = [\mathsf{y}_1|\cdots|\mathsf{y}_\mathsf{n}].$$

For a given $(k-1)$-dimensional subspace $\mathsf{U} \subset \mathsf{V}(\mathsf{k},\mathsf{q})$, we can take a vector $\mathsf{u}^\perp \in \mathsf{V}(\mathsf{k},\mathsf{q})$ such that for every $\mathsf{u} \in \mathsf{U}$ we have

$$\mathsf{u}^\perp \cdot \mathsf{u} = \mathsf{0}.$$

If C is a two weight code, then the weight of the codeword $\mathsf{u}^\perp \cdot G$ is either w_1 or w_2, so

$$|\mathsf{U} \cap \{\mathsf{y}_\mathsf{i}\}_1^\mathsf{n}| = \begin{cases} w_1 \\ w_2 \end{cases}$$

This gives that in $\mathsf{PG}(\mathsf{k}-1,\mathsf{q})$ the hyperplane $\hat{\mathsf{U}}$ coming from U has either $\mathsf{n}-w_1$ or $\mathsf{n}-w_2$ points from the set $\{\hat{\mathsf{y}}_i\}_1^n$, so $\{\hat{\mathsf{y}}_i\}_1^n$ is a two weight set in $\mathsf{PG}(\mathsf{k}-1,\mathsf{q})$.

If $\{\hat{\mathsf{y}}_i\}_1^n$ is a two weight set, then reasoning in reverse gives that C is a two weight code.

1.4 Strongly regular graphs

A *graph* is an ordered set (V, E) of vertices (V) and two-element subsets of V called edges (E), in which two distinct vertices are said to be *adjacent* to each other if they lie on the same edge, and where two distinct vertices define at most one edge. Vertices that are adjacent to each other are also referred to as *neighbours*.

We call the *degree* of a vertex the number of vertices adjacent to it. We say that a graph is *k-regular* if all vertices have the same degree k.

A *strongly regular graph* is a k-regular graph in which

- any two adjacent vertices have exactly λ common neighbours;
- any two non-adjacent vertices have exactly μ common neighbours.

A strongly regular graph on v vertices is denoted $\mathrm{srg}(v, k, \lambda, \mu)$.

We can count how many vertices it has in terms of the parameters k, λ and μ by setting three levels on our graph.

The first level consists of just one vertex a. The second level has all the k neighbours of a. The third level has all the remaining vertices of our graph. A vertex b in the second level shares λ neighbours with a, and so it has $k - \lambda - 1$ neighbours in the third level. Each of these neighbours in the third level has μ neighbours with a, so in total the third level has

$$\frac{k(k-\lambda-1)}{\mu}$$

vertices, and so

$$v = 1 + k + \frac{k(k-\lambda-1)}{\mu}.$$

Figure 1.4 summarises this count.

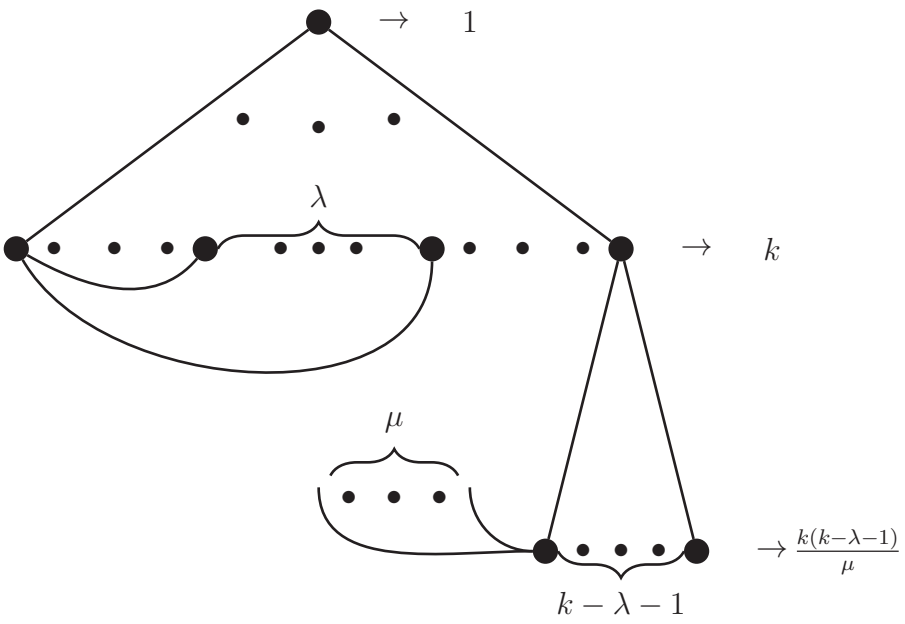

Figure 1.4: A $\mathrm{srg}(v, k, \lambda, \mu)$ has $v = 1 + k + \frac{k(k-\lambda-1)}{\mu}$ points.

Given a strongly regular graph we define its *adjacency matrix* A, where rows

and columns are indexed by its vertices:

$$A_{ij} = \begin{cases} 1 & \text{if vertices } i \text{ and } j \text{ are adjacent} \\ 0 & \text{if vertices } i \text{ and } j \text{ are not adjacent} \end{cases}$$

We can calculate one eigenvalue of A by noting that because each vertex is adjacent to k other vertices, the all one vector $\hat{1}$ is an eigenvector with eigenvalue k and multiplicity 1.

To calculate the remaining $v-1$ eigenvalues we first observe that A is symmetric and thus all other eigenvectors are orthogonal to $\hat{1}$. The second step is to use A^2. The matrix A^2 has the following entries

$$A^2_{ij} = \begin{cases} k & \text{if vertices } i \text{ and } j \text{ are equal} \\ \lambda & \text{if vertices } i \text{ and } j \text{ are adjacent} \\ \mu & \text{if vertices } i \text{ and } j \text{ are not adjacent} \end{cases}$$

and so we can write A^2 as

$$A^2 = kI + \lambda A + \mu(J - I - A).$$

This tells us that an eigenvector orthogonal to $\hat{1}$ has an eigenvalue that is a solution of

$$x^2 = k + \lambda x + \mu(-1 - x).$$

Let f and g be the two remaining eigenvalues with multiplicities f_m and g_m respectively. Using the fact that the sum of the diagonal entries of A is zero and it is also the sum of its eigenvalues, we get

$$\begin{aligned} 1 + f_m + g_m &= v \\ k + f \cdot f_m + g \cdot g_m &= 0 \end{aligned}$$

By solving for f, g, f_m, g_m explicitly we have

$$f, g = \frac{1}{2}\left[(\lambda - \mu) \pm \sqrt{(\lambda - \mu)^2 + 4(k - \mu)}\right] \tag{1.5}$$

$$f_m, g_m = \frac{1}{2}\left[(v-1) \mp \frac{2k + (v-1)(\lambda - \mu)}{\sqrt{(\lambda - \mu)^2 + 4(k - \mu)}}\right]. \tag{1.6}$$

1.5 Partial geometries

A *partial geometry* with parameters s, t and α is an incidence structure on a finite set $\mathcal{P}$ of points and a finite set $\mathcal{L}$ of lines in which the following properties hold

- two points are incident with at most one line;
- there are $s + 1$ points on a line;
- there are $t + 1$ lines incident to one point;
- a point not on a given line is collinear to α points on that line.

We denote this incidence structure by $\mathrm{pg}(s, t, \alpha)$.

We can count the number of points of a $\mathrm{pg}(s, t, \alpha)$ just in terms of its parameters. To do this, we fix a line L and count all the points not on that line. Each point on L has t more lines incident to it, and each of these lines has s more points, so for each point on L we have st points not on L. For each point p not on L, there are α points on L that are incident to p, so counting all the points not on L we get

$$\frac{(s+1)st}{\alpha}$$

points, and so adding the points on L we get

$$v = \frac{(s+1)st}{\alpha} + s + 1.$$

Figure 1.5 summarises this count.

Note that there is an implicit duality in the definition of partial geometry, so counting the number l of lines we have

$$l = \frac{(t+1)st}{\alpha} + t + 1.$$

We give an example of a partial geometry with parameters $\mathrm{pg}(2, 2, 2)$ in Figure [1.6]. According to their parameters, partial geometries are broken down into four non-disjoint classes [10]:

- The partial geometries with $\alpha = 1$. These partial geometries are called *generalised quadrangles*.
- The partial geometries with a $\alpha = s + 1$; dually $\alpha = t + 1$.

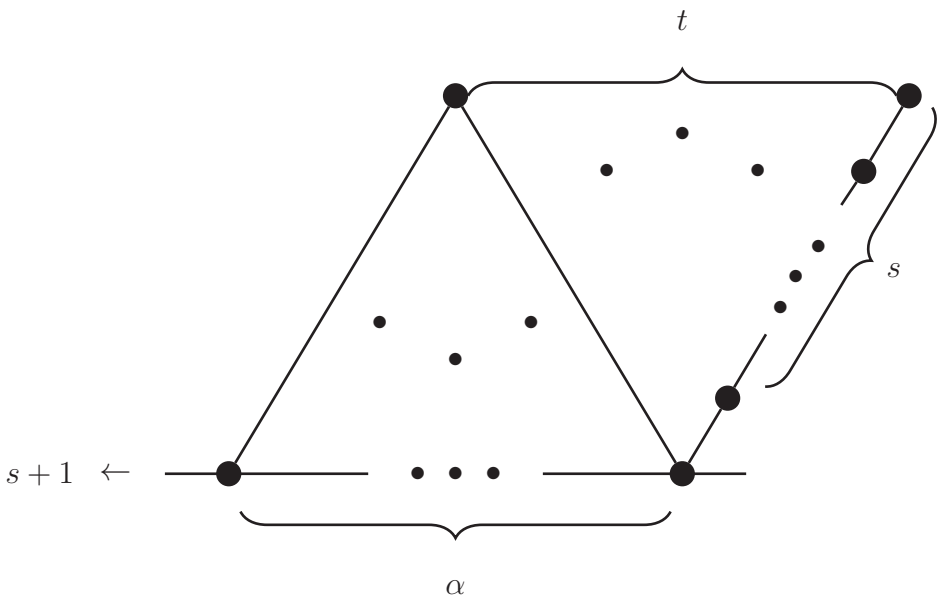

Figure 1.5: A $\mathrm{pg}(s,t,\lambda)$ has $v = \frac{(s+1)st}{\alpha} + s + 1$ points.

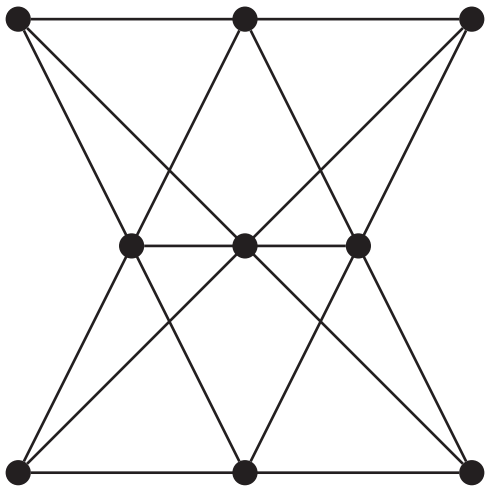

Figure 1.6: $\mathsf{pg}(2,2,2)$

- The partial geometries with $\alpha = t$; dually with $\alpha = s$.
- The partial geometries with $1 < \alpha < \min\{s,t\}$. These partial geometries are called *proper*.

The *point graph* of a partial geometry is the graph whose vertices are the set of points of our partial geometry, and two vertices are adjacent if and only if they

are different and lie on the same line [25].

The *incidence matrix* N of a partial geometry $\mathrm{pg}(s,t,\alpha)$ is a $v \times l$ matrix where rows are indexed by its points, and columns are indexed by its lines:

$$N_{ij} = \begin{cases} 1 & \text{if the point } i \text{ is incident to the line } j \\ 0 & \text{if the point } i \text{ is not incident to the line } j \end{cases}$$

The rows have a constant sum of $t+1$ and the columns have a constant sum of $s+1$.

Partial geometries as strongly regular graphs

The point graph of a given partial geometry $\mathrm{pg}(s,t,\alpha)$ has the following properties.

- The number of vertices in the point graph is determined by the number of points on $\mathrm{pg}(s,t,\alpha)$
$$v = \frac{(s+1)st}{\alpha} + s + 1.$$

- Every point u in our partial geometry has $t+1$ lines incident to it and each line has s points different from u, so in the point graph the vertex corresponding to the point u must have
$$k = s(t+1)$$
neighbours.

- For any two points u, w on a line L in our partial geometry there are $s-1$ more points on that line. Moreover, u has t lines different from L incident to it. Each of these t lines is not incident to w, so w is incident with $\alpha - 1$ points different from u on each of the t lines.

  These arguments show that in the point graph of our partial geometry any two neighbouring vertices (corresponding to any two points on a given line) have
$$\lambda = s - 1 + t(\alpha - 1)$$
common neighbours.

- Any point u in our partial geometry has $t+1$ lines incident to it, and every point v not on any of those $t+1$ lines is incident to α points on each line.

So in the point graph of our partial geometry any two non-adjacent vertices (corresponding to any two points not on a line) have

$$\mu = \alpha(t+1)$$

common neighbours.

These properties show that the point graph of a partial geometry $\mathrm{pg}(s,t,\alpha)$ is a strongly regular graph with the following parameters

$$\mathrm{srg}\Big(\frac{(s+1)st}{\alpha} + s + 1, s(t+1), s - 1 + t(\alpha - 1), \alpha(t+1)\Big). \tag{1.7}$$

It is important to note that although the point graph of a partial geometry gives a way to build a strongly regular graph from a given partial geometry, the inverse process is not always true. That is, there are strongly regular graphs which satisfy the properties on s, t and α as in [1.7] that cannot arise from a partial geometry [25]. The next section will provide an example of this.

1.6 LDPC codes

Let C be a linear code whose parity check matrix $G^{\perp}$ has "much" more zero than nonzero entries, we then say that C is an LDPC code [28]. The author of this report is aware of the vagueness in "much" more zeros in this definition, nevertheless, as we will see later on the motivation of using LDPC codes is their iterative decoding process rather than the sparsity of their parity check matrix, even though these two concepts are tightly related.

Let $\mathsf{L}(\mathsf{C})$ be the graph whose vertices are indexed by rows (parity nodes) and columns (bit nodes) of $G^{\perp}$, and where the vertex corresponding to row i is adjacent to a vertex corresponding to a column j whenever the entry ij has a nonzero entry. Such a graph is called the *Tanner graph* of C. Since neither parity nodes nor bit nodes are adjacent to each other, $\mathsf{L}(\mathsf{C})$ is a *bipartite graph*.

Note that for a partial geometry, the Tanner Graph of its incidence matrix has girth at least 6 since any two points can only be in one line, and so the smallest polygon to be made in a partial geometry is a triangle, which in the Tanner graph corresponds to a cycle of length 6. The Tanner graph of the incidence matrix of a partial geometry is also referred to as its *Levi graph* or *Line graph*.

The motivation for building LDPC codes is the iterative procedure used to decode

them which acts as a Belief Propagation algorithm on $\mathsf{L}(\mathsf{C})$, and has shown to perform very close to the Shannon limit. LDPC codes are used in multimedia mobile broadcasting, digital video broadcasting, ethernet and wifi communications.

We now briefly explain how iterative decoding works [16]. Given a recieved message m, we will check wether m is a codeword or not. The entries of m are assigned to the corresponding bit nodes in the tanner graph in a way that the ith vertex has the ith coordinate of m. Each bit node b then sends a message b_m to their adjacent parity nodes regarding which value they belive is correct (correct in the sense of the value b_m being a coordinate of a codeword). Each parity node p then sends a message back to their adjacent bit nodes regarding which value p believes to be correct for each adjacent bit node. This message passing between bit nodes and parity nodes loops until a codeword is encountered or a threshold number of iterations is carried over. The messages sent are usually polynomials with as many variables as adjacent edges.

Given the nature of the decoding process, mainly the complexity in the message polynomials, it is desirable to use linear codes whose Tanner graph has long girth and as few edges as possible. These two objectives indicate that using the incidence matrix N of a partial geometry as the parity check matrix of the code, is a good idea since the incidence matrix is sparse, and the Tanner Graph has girth at least 6.

1.6.1 The incidence matrix of a partial geometry as an LDPC code

Let N be the incidence matrix of a partial geometry $\mathrm{pg}(s,t,\alpha)$ of size $v \times l$ where

$$v = \frac{(s+1)st}{\alpha} + s + 1 \qquad\qquad l = \frac{(t+1)st}{\alpha} + t + 1.$$

Define a linear code C over the field $\mathbb{F}_2$ whose parity check matrix is N, and generator matrix is $N^\perp$ such that

$$N \cdot (N^\perp)^t = 0.$$

The code C has length l. We will now give bounds on the minimum distance, rank of the code C and the girth of $\mathsf{L}(\mathsf{C})$ as given in [18]. We need some preliminary results first.

The point graph of this partial geometry is a strongly regular graph with parameters as in (1.7). The adjacency matrix A of this strongly regular graph and

the incidence matrix N are related by

$$A = NN^t - (t+1)I.$$

This can be seen by considering two rows v_i, v_j of N, where their dot product gives the number of lines where the vertices i and j are both collinear to.

This last equation tells us that if h is an eigenvalue of A with multiplicity h_m, then $h + (t+1)$ is an eigenvalue of NN^t with multiplicity h_m.

The eigenvalues of A given in (1.5), can be written in terms of the partial geometry by

$$s(t+1), \quad s-\alpha, \quad -(t+1)$$

with respective multiplicities

$$1, \quad \frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}, \quad \frac{s(s+1-\alpha)(st+\alpha)}{\alpha(s+t+1-\alpha)}$$

and so the eigenvalues of NN^t are

$$(s+1)(t+1), \quad s+t+1-\alpha, \quad 0$$

with the same multiplicities as those of A.

Moreover, a non-zero eigenvalue e of an eigenvector $\mathbf{e}$ of N^tN, is also an eigenvalue for a non-zero eigenvector of NN^t:

$$N^tN\mathbf{e} = e\mathbf{e} \Rightarrow NN^t \cdot N\mathbf{e} = eN\mathbf{e}.$$

We will be refering to the eigenvalues of NN^t and N^tN interchangeably.

1.6.2 Minimum distance of the code C

We proceed as in [18, 17]. Let c be a codeword of minimum weight d, that is it has d entries with the value 1 and the remaining entries with the value 0. Since N is the parity check matrix of C, the vector $N\mathsf{c} = \mathsf{x}$ is the zero vector over the field $\mathbb{F}_2$ and thus the number of entries it has in the real numbers is either 0 or an even number. Recall that N has constant row sum $t+1$ and constant column sum $s+1$. We have

$$||N\mathsf{c}||^2 = \sum_{i=1}^{t+1} \mathsf{x}_i^2 \geq 2\sum_{i=1}^{t+1} \mathsf{x}_i = 2d(s+1).$$

Let c_{p_i} be the projection of c onto the ith eigenspace of N^tN, and let the eigenspaces be indexed in ascending order with respect to its eigenvalues' absolute value in the real numbers.

The eigenvalue $(s+1)(t+1)$ of N^tN corresponds to the eigenvector $\hat{1}$, and so normalising the eigenspace we have

$$\begin{aligned} ||\mathsf{c}_{p_1}||^2 &= d^2/l \\ ||\mathsf{c}||^2 &= d. \end{aligned}$$

Writing $N\mathsf{c}$ as a linear combination of the eigenspaces of N^tN and noting that since N^tN is symmetric its eigenvectors are orthogonal to each other we have

$$\begin{aligned} ||N\mathsf{c}||^2 &= (s+1)(t+1)||\mathsf{c}_{p_1}||^2 + (s+t+1-\alpha)||\mathsf{c}_{p_2}||^2 \\ &= (s+1)(t+1)\cdot d^2/l + (s+t+1-\alpha)||\mathsf{c}_{p_2}||^2 \\ &= (s+1)(t+1)\cdot d^2/l + (s+t+1-\alpha)(||\mathsf{c}||^2 - ||\mathsf{c}_{p_1}||^2) \end{aligned}$$

hence we have

$$2d(s+1) \leq (s+1)(t+1)\cdot d^2/l + (s+t+1-\alpha)(d - d^2/l)$$

and so

$$d \geq \frac{(t+1)(s+1-t+\alpha)}{\alpha}. \tag{1.8}$$

This bound (1.8) for d can also be thought of as being deduced by considering how a minimum weight codeword acts on the bit nodes of $\mathsf{L}(\mathsf{C})$. We can come up with another bound for d by considering how a minimum weight codeword acts on the parity nodes of $\mathsf{L}(\mathsf{C})$.

We say that a bit node of $\mathsf{L}(\mathsf{C})$ is *active* if its associated value of a minimum weight codeword is non-zero. The edges incident on active bit nodes will be called *active* edges and the parity nodes incident with at least one active edge will be called *active* parity nodes.

Let p be a vector of length r with a one in each active parity node, and a zero otherwise. Let ω be the number of ones in p. We have that the ith entry of the vector $N^t\mathsf{p} = \mathsf{y}$ satisfies:

$$\mathsf{y}_i = \begin{cases} s+1 \text{ if } i \text{ is an active parity bit} \\ \#\text{ of adjacent active parity nodes otherwise} \end{cases}$$

We want a way to bound $||\mathsf{y}||^2$. For the active ith parity node from p, let $u_i(j)$ be the number of adjacent bit nodes whose weight is j in $\mathsf{y}, 1 \leq j \leq s+1$. Since there is an even number of active bits, we have

$$\sum_{j}^{s+1}(1/j)u_i(j)j^2 \geq 2(s+1)+(t+1)-2.$$

Since there are ω active parity nodes we have

$$||\mathsf{y}||^2 = \sum_{i}^{l}\mathsf{y}_i^2 \geq \omega \cdot (2(s+1)+(t+1)-2).$$

Similarly as for the previous (1.8) bound for d, we have that the eigenvalue $(s+1)(t+1)$ of NN^t has as eigenvector $(1,...,1)/\sqrt{v}$, and so

$$\begin{aligned} ||\mathsf{p}_{p_1}||^2 &= \omega^2/v \\ ||\mathsf{p}||^2 &= \omega. \end{aligned}$$

Converting to eigenspace representation

$$\begin{aligned} ||N^t\mathsf{p}||^2 &= (s+1)(t+1)||\mathsf{p}_{p_1}||^2 + (s+t+1-\alpha)||\mathsf{p}_{p_2}||^2 \\ &= (s+1)(t+1)\cdot\omega^2/v + (s+t+1-\alpha)||\mathsf{p}_{p_2}||^2 \\ &= (s+1)(t+1)\cdot\omega^2/v + (s+t+1-\alpha)(||\mathsf{p}||^2 - ||\mathsf{p}_{p_1}||^2) \end{aligned}$$

hence we have

$$\begin{aligned} (s+1)(t+1)\cdot\omega^2/v + (s+t+1-\alpha)(\omega-\omega^2/v) &\geq \omega(2(s+1)+(t+1)-2) \\ \Rightarrow \omega \geq \frac{v(2(s+1)+(t+1)-2-(s+t+1-\alpha))}{(s+1)(t+1)-(s+t+1-\alpha)}&. \end{aligned}$$

Now we note that $d(s+1) \geq 2\omega$ and $v(t+1) = l(s+1)$ to get

$$d \geq \frac{2(s+\alpha)}{\alpha}. \tag{1.9}$$

Taking inequalities (1.8,1.9) we have

$$d \geq \max\left\{\frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha}\right\}. \tag{1.10}$$

1.6.3 Rank of the code C

Since the code C was defined by giving a $v \times l$ parity check matrix N, we have that the rank r of the code is

$$r = l - \text{rank}_2(N)$$

where rank_2 is the rank over $\mathbb{F}_2$.

We can give an upper bound for $\text{rank}_2(N)$ by giving an upper bound for $\text{rank}(N)$

$$\text{rank}_2(N) \leq \text{rank}(N) \leq \text{rank}(NN^t).$$

Considering the multiplicity of the non-zero eigenvectors of NN^t, we have

$$r \geq l - \left(1 + \frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}\right). \tag{1.11}$$

1.6.4 6 cycles on $\mathsf{L}(\mathsf{C})$

We can count the number of six cycles in $\mathsf{L}(\mathsf{C})$ by counting the number of triangles in the partial geometry [18]. On a given line L we have $s+1$ points, and so $\binom{s+1}{2}$ different pairings of points. Take two points p, q on L. There are t lines different from L incident to p, and on each line there are $\alpha - 1$ points collinear to q. Hence there are

$$t(\alpha - 1)\binom{s+1}{2}$$

triangles containing two points of L. Since there are l lines in total and each triangle has three sides, we have

$$N_6 = \frac{lt(\alpha-1)}{3}\binom{s+1}{2}. \tag{1.12}$$

Chapter 2

Maximal arcs and above objects

As we have seen in the introductory chapter, a given partial geometry gives rise to a strongly regular graph. In this chapter we will build partial geometries from a given maximal arc.

For a given maximal arc we will describe two methods for building a partial geometry following [13, 22, 28], and in the end of the chapter we will give an example of these constructions.

2.1 Maximal Arcs give rise to partial geometries

Let $\mathcal{K}$ be a maximal arc in $\mathsf{PG}(2,\mathsf{q})$ in which each line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points, and so $|\mathcal{K}| = qd - q + d$.

2.1.1 Method 1

We define a geometry $\mathcal{G}$ with point set the points in $\mathsf{PG}(2,\mathsf{q})\backslash\mathcal{K}$. We let the lines of $\mathcal{G}$ be the lines of $\mathsf{PG}(2,\mathsf{q})$ that meet $\mathcal{K}$ in d points. We let the incidence be the one of $\mathsf{PG}(2,\mathsf{q})$.

Our geometry $\mathcal{G}$ has the following properties.

- Each line in $\mathcal{G}$ has $q - d + 1$ points.
- Recall figure 1.3 in which for a given point in $\mathsf{PG}(2,\mathsf{q})$ we get m lines of $\mathsf{PG}(2,\mathsf{q})$ that meet $\mathcal{K}$. This tells us that in $\mathcal{G}$ every point is incident to

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

  lines.

- Let $\mathsf{p} \in \mathsf{PG}(2,\mathsf{q})\backslash\mathcal{K}$ be a point, and $\mathsf{L} \subset \mathsf{PG}(2,\mathsf{q})$ a line meeting $\mathcal{K}$ but not containing p.

  We have that there are d lines incident to p meeting L in the d points where L meets $\mathcal{K}$. We also have that there can only be m lines incident to p meeting $\mathcal{K}$.

  This tells us that for any point p and line L in $\mathcal{G}$ such that $\mathsf{p} \notin \mathsf{L}$, there are
  $$m - d = q - \frac{q}{d} + 1 - d$$
  lines incident to p and meeting L.

These three properties give that $\mathcal{G}$ is a partial geometry with parameters
$$\mathrm{pg}(q-d, q-\frac{q}{d}, q-\frac{q}{d}+1-d).$$

2.1.2 Method 2

Let our projective plane $\mathsf{PG}(2,\mathsf{q})$ in which $\mathcal{K}$ is contained be called π. Consider π to be embedded in $\mathsf{PG}(3,\mathsf{q})$ and define $\mathcal{G}$ to be the geometry whose points are the points of $\mathsf{PG}(3,\mathsf{q})\backslash\pi$. Define the lines of $\mathcal{G}$ to be the lines of $\mathsf{PG}(3,\mathsf{q})\backslash\pi$ that meet $\mathcal{K}$ in a unique point. We let the incidence be the one of $\mathsf{PG}(3,\mathsf{q})$.

Our geometry $\mathcal{G}$ has the following properties.

- A line L of $\mathsf{PG}(3,\mathsf{q})\backslash\pi$ that meets π, meets π in just one point. In particular, if L meets $\mathcal{K}$ in a unique point it also meets π in just one point. We have that in $\mathcal{G}$ every line has q points.

- A point $\mathsf{p} \in \mathsf{PG}(3,\mathsf{q})\backslash\pi$ is joined to all points in $\mathcal{K}$, so every point in $\mathcal{G}$ is incident to $|\mathcal{K}| = qd - q + d$ lines.

- For a point p and a line L in $\mathsf{PG}(3,\mathsf{q})\backslash\pi$ such that $\mathsf{p} \notin \mathsf{L}$ and $\mathsf{L} \cap \mathcal{K} \neq \emptyset$, there is a plane $\pi_{\mathsf{p},\mathsf{L}} \cong \mathsf{PG}(2,\mathsf{q})$ contained in $\mathsf{PG}(3,\mathsf{q})$ such that p and L are contained in $\pi_{\mathsf{p},\mathsf{L}}$.

  The plane $\pi_{\mathsf{p},\mathsf{L}}$ meets π in exactly one line. This line has a common point with $\mathcal{K}$, the point meeting L, and hence has d common points with $\mathcal{K}$.

  We also have that in $\pi_{\mathsf{p},\mathsf{L}}$ any two points are joined by exactly one line, and any two lines intersect in exactly one point. In particular p meets the d

points of $\mathcal{K}$ in $\pi_{\mathsf{p},\mathsf{L}}$ in d distinct lines. These d distinct lines through p meet L in d distinct points. Out of these d distinct points in L, only one of them is in $\mathcal{K} \subset \pi$, namely $\mathsf{L} \cap \mathcal{K}$.

We have that p is collinear with L on $d-1$ points not in π.

These properties tell us that $\mathcal{G}$ is a partial geometry with parameters

$$\mathrm{pg}(q-1, qd-q+d-1, d-1).$$

2.2 Summary of constructions

We now give a brief summary of the constructions given so far.

- A two weight code can be built by taking the points of a maximal arc as the column vectors of a generator matrix for the code. Conversely, two weight sets can be built by taking the column vectors of a generator matrix of a two weight code as points in a projective plane.
- Maximal arcs give rise to partial geometries via **Method 1** (2.1.1) and **Method 2** (2.1.2).

  Let $\mathcal{K}$ be a maximal arc in $\mathsf{PG}(2,\mathsf{q})$ in which each line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points.

  - **Method 1** (2.1.1) gives a partial geometry with parameters:

    $$\mathrm{pg}(q-d, q-\frac{q}{d}, q-\frac{q}{d}+1-d).$$

  - **Method 2** (2.1.2) gives a partial geometry with parameters:

    $$\mathrm{pg}(q-1, qd-q+d-1, d-1).$$

- The point graph of a partial geometry $\mathrm{pg}(s,t,\alpha)$ is a strongly regular graph with parameters:

  $$\mathrm{srg}\Big(\frac{(s+1)st}{\alpha}+s+1, s(t+1), s-1+t(\alpha-1), \alpha(t+1)\Big).$$

- The incidence matrix N of a partial geometry seen as a parity check matrix gives an LDPC code $\mathsf{C}_{\mathsf{LDPC}}$ over $\mathbb{F}_2$ with the following length n, minimum

distance d, rank r and number of minimum length cycles N_6 in its tanner graph:

$$n = l = \frac{(t+1)st}{\alpha} + t + 1$$
$$d \geq \max\left\{\frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha}\right\}$$
$$r \geq l - \left(1 + \frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}\right)$$
$$N_6 = \frac{lt(\alpha-1)}{3}\binom{s+1}{2}.$$

Its generator matrix is $N^{\perp}$ such that $N \cdot (N^{\perp})^t = 0$, and has only r rows different from the all zero vector.

- Given a projective geometry of dimension $\mathsf{n}-1$ over a finite field of order q^{h}, we can blow it up into a projective geometry of dimension $\mathsf{h}\cdot\mathsf{n}-1$ over a finite field of order q.

2.3 Examples

We will now build an example of a two weight code, a partial geometry and the arising strongly regular graph by both **Method 1** and **Method 2** using a maximal arc $\mathcal{K} \subset \mathsf{PG}(2,4)$.

We first build $\mathsf{PG}(2,4)$. To build $\mathbb{F}_4$ we take the irreducible polynomial $f = X^2 + X + 1$ over $\mathbb{F}_2$ and consider

$$\mathbb{F}_4 \cong \mathbb{F}_2[X]/ < f > .$$

Let $\alpha \in \mathbb{F}_4$ be such that $f(\alpha) = 0$, we have that

$$\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\} = \{0, 1, \alpha, \alpha^2\}$$

We can visualize $\mathsf{PG}(2,4)$ by Figures 2.1,2.2,2.3. The coloured points in these figures give a maximal arc $\mathcal{K}$ with $|\mathcal{K}| = 6$.

Given $\mathcal{K}$, we can now build the generator matrix G of a two weight code C by taking as columns the points of $\mathcal{K}$

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & \alpha & 1 & \alpha^2 \\ 1 & 1 & 1 & 1 & \alpha^2 & \alpha^2 \end{pmatrix}.$$

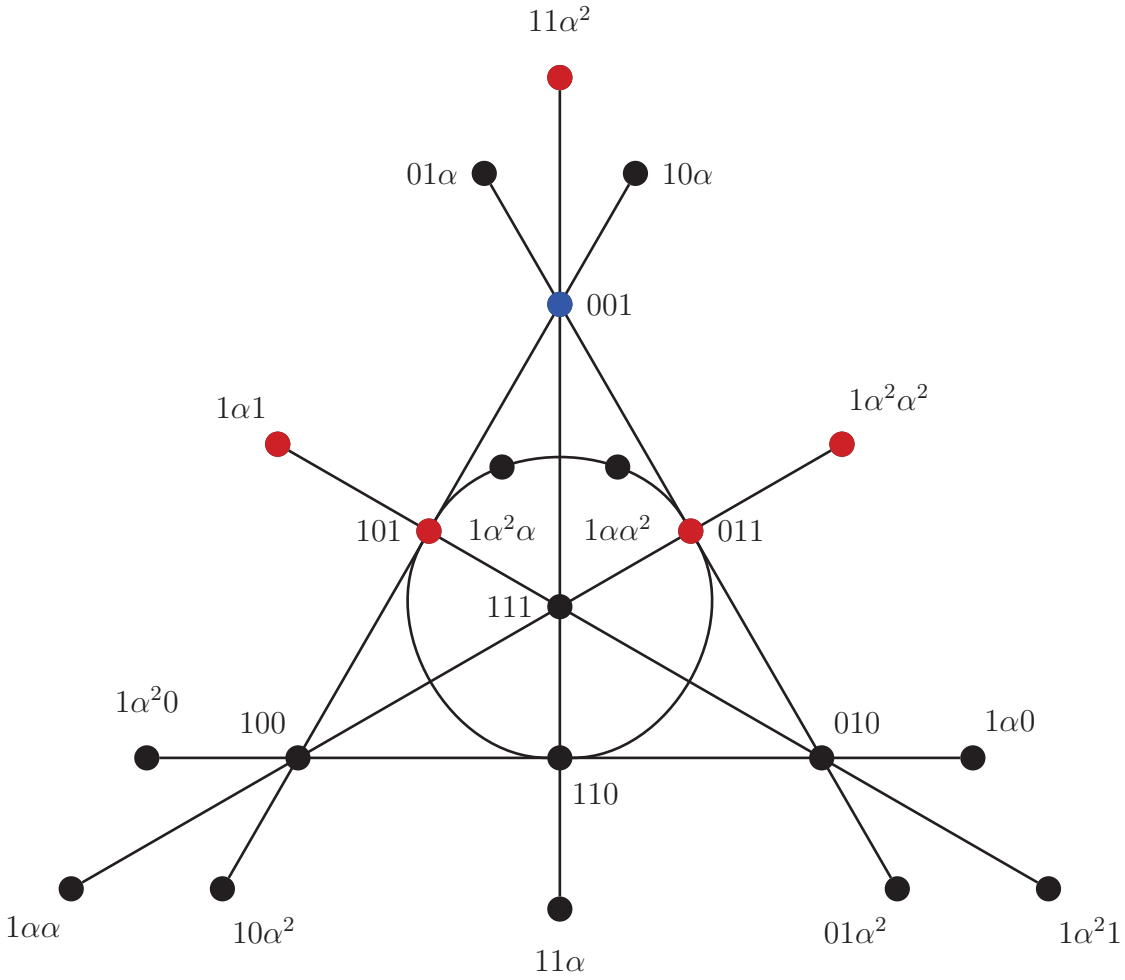

Figure 2.1: First part of $\mathsf{PG}(2,4)$

2.3.1 Example of Method 1

We now build the partial geometry as explained by **Method 1**. We have that this partial geometry has parameters

$$\mathrm{pg}(2,2,1)$$

and is represented in Figure 2.4. Note that we can also embed this partial geometry in $\mathsf{PG}(3,2)$ as shown in Figure 2.5. This partial geometry is also referred to in the literature as a "(2,2)-generalised quadrangle", and is unique up to isomorphisim [3, 14].

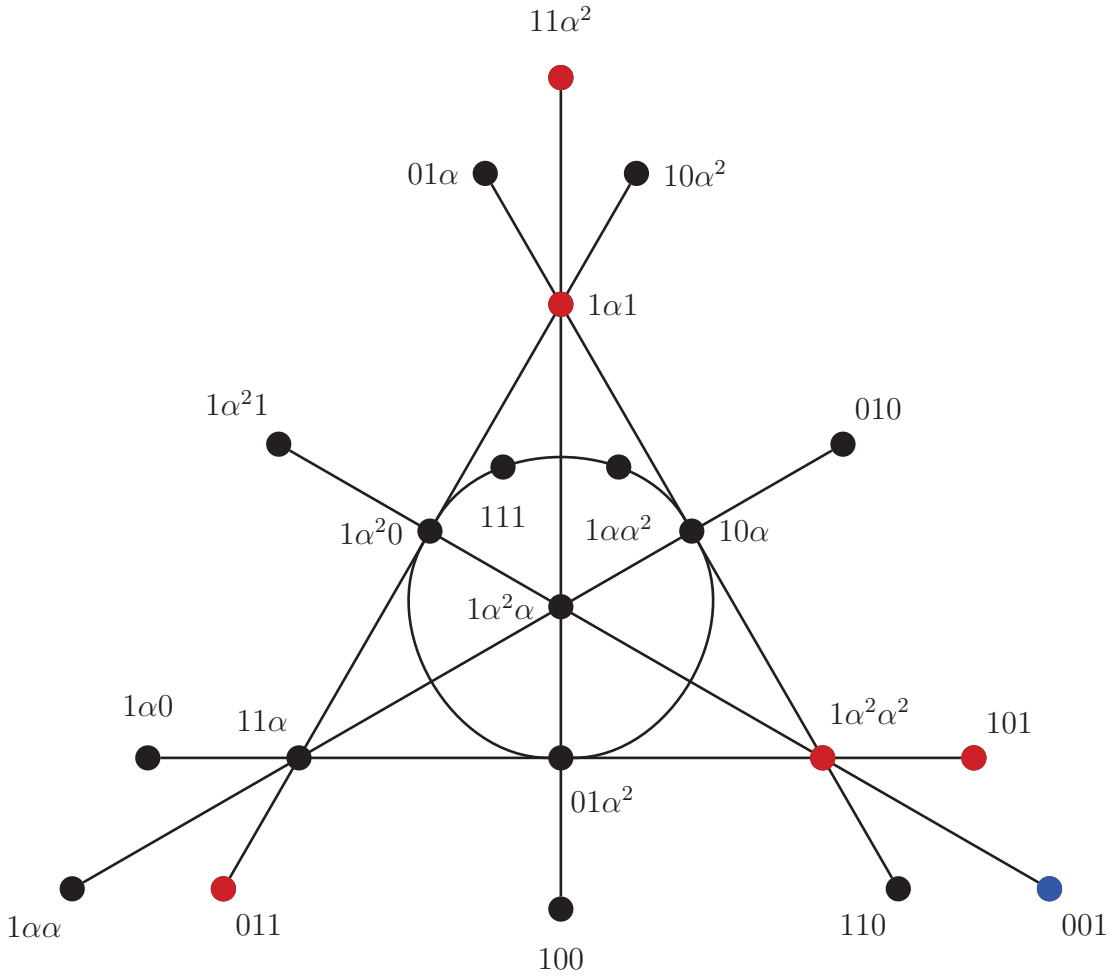

Figure 2.2: Second part of $\mathsf{PG}(2,4)$

The point graph of $\mathrm{pg}(2,2,1)$ is a strongly regular graph with parameters

$$\mathrm{srg}(15,6,1,3)$$

and is shown in Figure 2.6.

The LDPC code $\mathsf{C}_{\mathsf{LDPC}}$ whose parity check matrix is the incidence matrix N of the partial geometry (Figure 2.7) has a generator matrix $N^{\perp}$ as in figure 2.8.

This code has length $n = 15$, minimum distance $d = 6$, rank $r = 5$ and $N_6 = 0$ since the smallest polygon appearing in the partial geometry is a quadrangle.

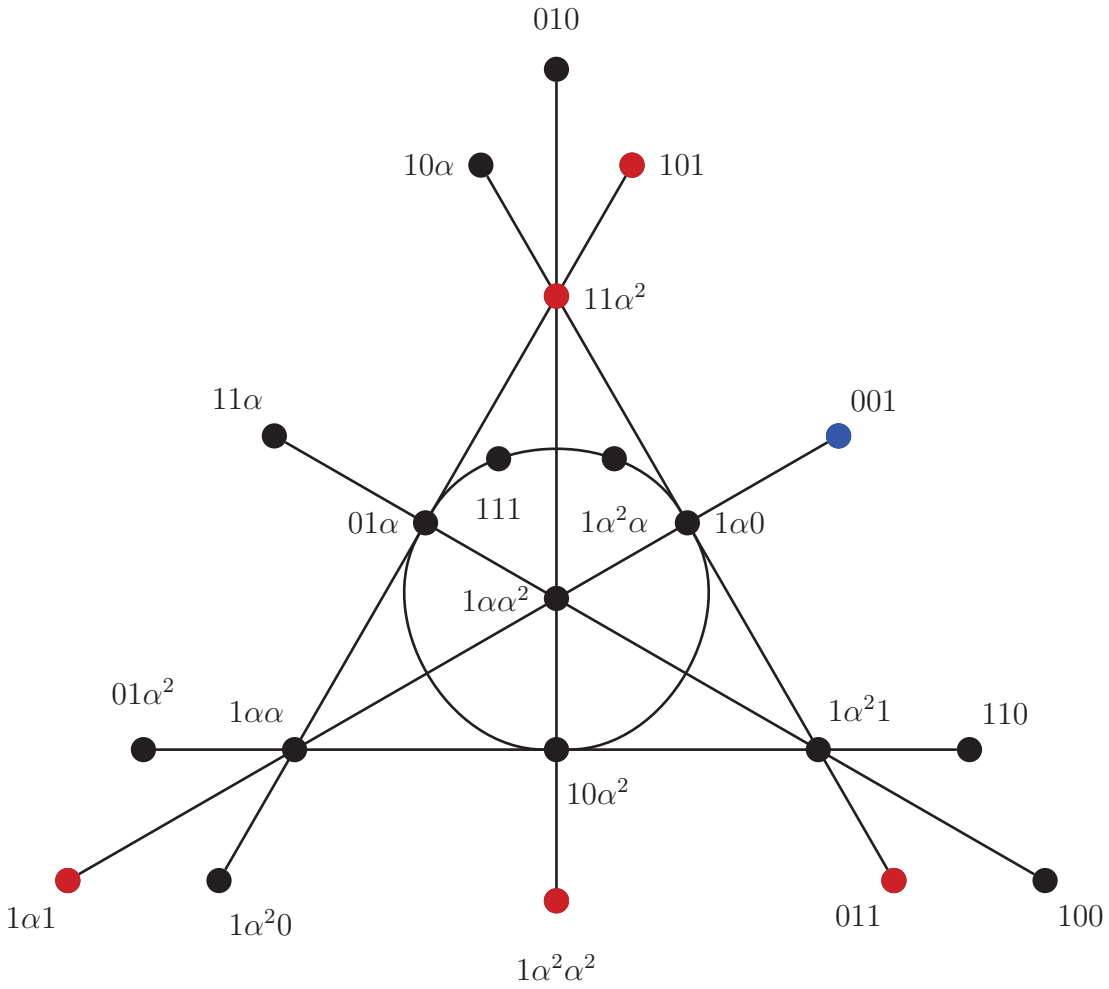

Figure 2.3: Third part of $\mathsf{PG}(2,4)$

2.3.2 Example of Method 2

We now build the partial geometry as explained by **Method 2**. We have that this partial geometry has parameters

$$\mathrm{pg}(3,5,1).$$

This partial geometry has 64 points and 96 lines. It is also referred to in the literature as a "(3,5)-generalised quadrangle", and up to isomorphism there is only one [3].

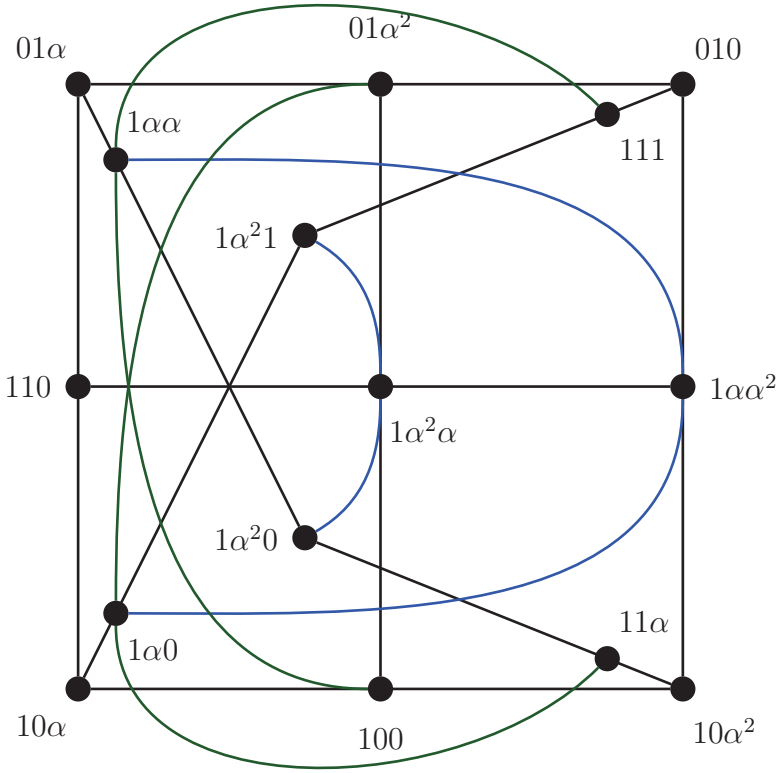

Figure 2.4: $\mathrm{pg}(2, 2, 1)$ embedded in $\mathsf{PG}(2, 4)$.

The point graph of $\mathrm{pg}(3, 5, 1)$ is a strongly regular graph with parameters

$$\mathrm{srg}(64, 18, 2, 6).$$

Haemers and Spence [15] gave 167 non-isomorphic strongly regular graphs that satisfy the previous parameters, out of which only one of them corresponds to the given $\mathrm{pg}(3, 5, 1)$. This provides an example of what was mentioned in Chapter 1 about strongly regular graphs and partial geometries, that is, not all strongly regular graphs satisfying the parameters of a partial geometry give rise to a partial geometry.

The LDPC code, whose parity check matrix is the incidence matrix N of size 64×96, has as length $n = 96$, minimum distance $d = 8$, rank $r = 50$ and $N_6 = 0$ since the smallest polygon appearing in the partial geometry is a quadrangle.

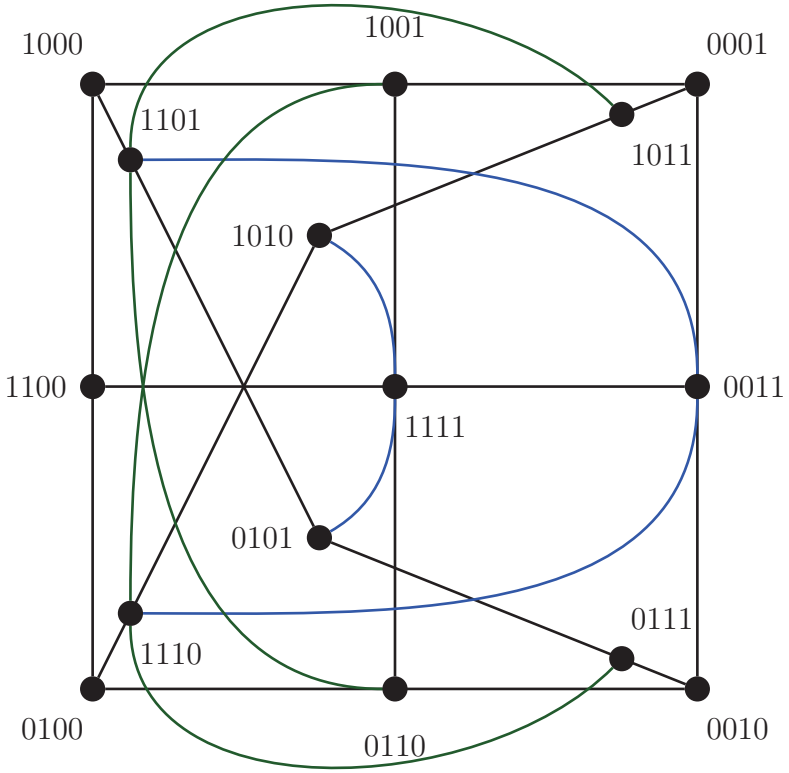

Figure 2.5: pg$(2, 2, 1)$ embedded in PG$(3, 2)$.

2.3.3 A desirable example

Now that we have considered the case of a maximal arc in PG$(2, 4)$, we consider what would result for the case of a maximal arc in PG$(2, 9)$. As we will see in Chapter 3, such a maximal cannot exist. Nevertheless, this case is interesting because the hypothetical partial geometry arising from such a maximal arc can be constructed using the methods of Chapter 4.

A hypothetical maximal arc $\mathcal{K}$ in PG$(2, 9)$ should meet each line in 0 or 3 points, hence

$$|\mathcal{K}| = 21$$

This maximal arc would give a partial geometry via **Method 2** with parameters

$$\text{pg}(8, 20, 2),$$

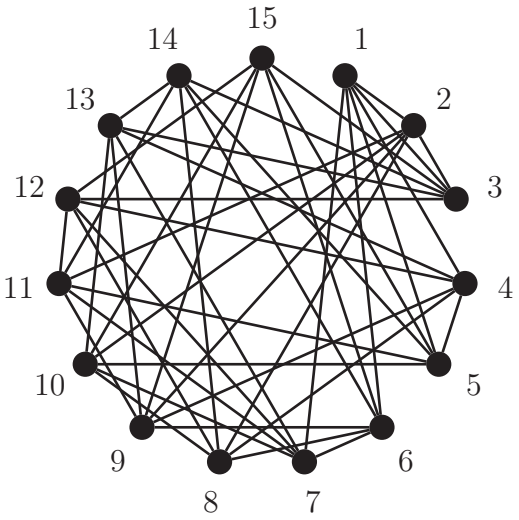

Figure 2.6: srg$(15, 6, 1, 3)$

```
1 . . . 1 . 1 . . . . . . . .
. 1 . 1 . . . . 1 . . . . . .
. 1 . . 1 . . . . . 1 . . . .
. . . . . 1 . . . 1 . 1 . . .
. . . 1 . 1 1 . . . . . . . .
1 . . . . . . . 1 . . . 1 . .
1 . . . . . . . . 1 . . . 1 .
. . . . . . . 1 1 . . 1 . . .
. . 1 . 1 . . . . . . 1 . . .
. 1 . . . . . . . 1 . . . . 1
. . 1 . . . . . . . . . 1 . 1
. . . . . . . 1 . . 1 . . 1 .
. . . . . . 1 1 . . . . . . 1
. . . . . 1 . . . . 1 . 1 . .
. . 1 1 . . . . . . . . . 1 .
```

Figure 2.7: Incidence matrix N of the partial geometry pg$(2, 2, 1)$ and parity check matrix for the code $\mathsf{C}_{\mathsf{LDPC}}$.

which gives a strongly regular graph with parameters

$$\text{srg}(729, 168, 141, 42).$$

The associated LDPC code would have length $n = 1701$, $d \geq 10$, $r \geq 1140$ and $T_6 = 408240$.

```
1 . . . . 1 1 . . 1 . . 1 . 1
. 1 . . . . . 1 1 . 1 . 1 . 1
. . 1 . . . . 1 . 1 . 1 . 1 1
. . . 1 . 1 . 1 1 1 . . 1 1 1
. . . . 1 1 1 1 . . 1 1 . . .
```

Figure 2.8: Generator matrix $N^{\perp}$ for the code $\mathsf{C}_{\mathsf{LDPC}}$.

The method used to build a partial geometry $\mathrm{pg}(8, 20, 2)$ developed in Chapter 4 is a generalisation of **Method 2** into higher dimensions, namely, instead of considering a set of points $\mathcal{K} \subset \mathsf{PG}(2, 3^2)$, a set of lines $\mathcal{L} \subset \mathsf{PG}(5, 3)$ is considered.

The geometries $\mathsf{PG}(5, 3)$ and $\mathsf{PG}(2, 3^2)$ are related via the blow up construction, in which points of $\mathsf{PG}(2, 3^2)$ correspond to lines of $\mathsf{PG}(5, 3)$. This raises the question as to what happens in $\mathsf{PG}(5, 3)$ allowing $\mathcal{L}$ to exist that does not happen in $\mathsf{PG}(2, 3^2)$ allowing $\mathcal{K}$ to exist, and is the central question driving this report.

2.4 Notes on the constructions of LDPC codes

How were the LDPC codes constructed? First I went into the open source web repository `http://www.maths.gla.ac.uk/~es/srgraphs.php` where I found the adjacency matrices A for the strongly regular graphs

$$\mathrm{srg}(15, 6, 1, 3) \qquad \text{and} \qquad \mathrm{srg}(64, 18, 2, 6).$$

I then used the software Mathematica [32] and ran the command

```
G = AdjacencyGraph[A]
clique_list = FindClique[G, Infinity, All]
```

to find all the cliques for each graph. Each clique had as many vertices as points on a line of the associated partial geometry ($\mathrm{pg}(2, 2, 1)$ and $\mathrm{pg}(3, 5, 1)$ respectively). Since the associated partial geometries are unique, it was shown that these strongly regular graphs were indeed the associated graphs to the partial geometries.

I then used Sage [33] to find the incidence matrix N for the partial geometries using the cliques found above:

```
sage: from sage.combinat.designs.block_design import BlockDesign
sage: P = IncidenceStructure(range(v), <list of cliques>)
sage: N = P.incidence_matrix()
sage: print N.str()
```

I then used Magma [34] and found out the code parameters using the incidence matrices N:

```
K := FiniteField(2);
Cperp := LinearCode< K, 1 | N >;
Nperp := ParityCheckMatrix(Cperp);
C := LinearCode(Nperp);
C;
```

The output of Magma gives the code parameters.

Chapter 3

Existence of Maximal Arcs in $\mathsf{PG}(2, \mathsf{q})$

We give two examples of constructions on how to build maximal arcs in projective planes $\mathsf{PG}(2, \mathsf{q})$ when q is even due to Denniston and Mathon [26, 27, 22, 13]. Next we give the first steps in constructing the known proof of why maximal arcs cannot exist when q is odd [7].

There are two more known constructions of maximal arcs given by Thas [30, 29], which will be omitted in this report since in the case of a projective plane $\mathsf{PG}(2, \mathsf{q})$ (see Chapter 6 for an axiomatic definition of a projective plane) they are equivalent to those of Mathon. These constructions due to Thas can be found in [30, 29, 13, 22].

Recall from Section 1 that a maximal arc $\mathcal{K}$ is a set of points in $\mathsf{PG}(2, \mathsf{q})$ where any line meets $\mathcal{K}$ in d or 0 points. The size of $\mathcal{K}$ is $qd - q + d$.

3.1 When q is odd

We proceed as in [7]. Given a projective plane $\mathsf{PG}(2, \mathsf{q})$ and a line L in it, we can consider the point set of $\mathsf{PG}(2, \mathsf{q}) \backslash \mathsf{L}$ with the induced incidence relation from $\mathsf{PG}(2, \mathsf{q})$. This new incidence structure has q^2 points, $q^2 + q$ lines, and is called the *affine plane* of order q denoted by $\mathsf{AG}(2, \mathsf{q})$.

Note that while in $\mathsf{PG}(2, \mathsf{q})$ any line meets every other line in exactly one point, in $\mathsf{AG}(2, \mathsf{q})$ there are lines that do not meet in any point, such lines are called *parallel*. Parallel lines correspond to lines that meet in a point $\mathsf{p} \in \mathsf{L} \subset \mathsf{PG}(2, \mathsf{q})$, so there are $q + 1$ different *parallel classes*.

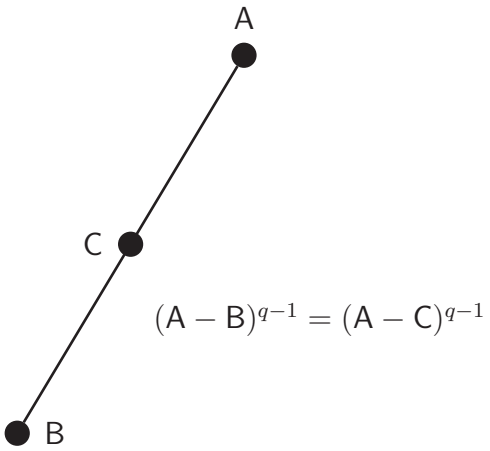

Figure 3.1: Direction of a line containing points A,B and C in $\mathbb{F}_{q^2}$

There is a natural isomorphism between $\mathsf{AG}(2,\mathsf{q})$ and $\mathsf{V}(2,\mathsf{q})$. In this setting, each parallel class is determined by the "direction" of its lines. We can also assign the points of $\mathsf{V}(2,\mathsf{q})$ with the elements of $\mathbb{F}_{q^2}$ by relation 1.1.

Given two points $[\mathsf{a},\mathsf{b}]$ and $[\mathsf{c},\mathsf{d}]$ in $\mathsf{V}(2,\mathsf{q})$, the direction of the line joining them in $\mathbb{F}_{q^2}$ is given by $(\mathsf{a}-\mathsf{c})\alpha+(\mathsf{b}-\mathsf{d})$. Any other point $[\mathsf{e},\mathsf{f}]$ on the same line as the points $[\mathsf{a},\mathsf{b}],[\mathsf{c},\mathsf{d}]$ must satisfy

$$(\mathsf{a}-\mathsf{c})\alpha+(\mathsf{b}-\mathsf{d})=\beta\cdot((\mathsf{a}-\mathsf{e})\alpha+(\mathsf{b}-\mathsf{f}))$$

with $\beta\in\mathbb{F}_q$.

Since for any $\beta\in\mathbb{F}_q$ we have $\beta^{q-1}=1$, any three points $[\mathsf{a},\mathsf{b}],[\mathsf{c},\mathsf{d}],[\mathsf{e},\mathsf{f}]\in\mathsf{V}(2,\mathsf{q})$ on the same line corresponding to $\mathsf{A},\mathsf{B},\mathsf{C}\in\mathbb{F}_{q^2}$ respectively, must satisfy

$$(\mathsf{A}-\mathsf{B})^{q-1}=(\mathsf{A}-\mathsf{C})^{q-1}.$$

There are q^2-1 possible non-zero differences $\mathsf{A}-\mathsf{B}$ in $\mathbb{F}_{q^2}$, and so

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

possible directions in $\mathbb{F}_{q^2}$. Each direction $(\mathsf{A}-\mathsf{B})^{q-1}$ satisfies

$$((\mathsf{A}-\mathsf{B})^{q-1})^{q+1}=(\mathsf{A}-\mathsf{B})^{q^2-1}=1$$

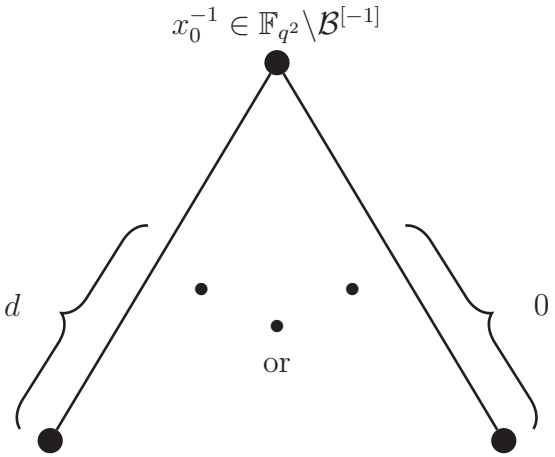

Figure 3.2: The case $x_0^{-1} \in \mathbb{F}_{q^2} \backslash \mathcal{B}^{[-1]}$.

and so each direction corresponds to a different $(q+1)$-root of unity in $\mathbb{F}_{q^2}$.

Given a maximal arc in $\mathsf{PG}(2,\mathsf{q})$, there is always a line whose points are not in the maximal arc. Let $\mathcal{B}$ be a maximal arc of $\mathsf{PG}(2,\mathsf{q})$ seen as elements of $\mathbb{F}_{q^2}$, and suppose that $0 \notin \mathcal{B}$. Let $\mathcal{B}^{[-1]}$ denote the set $\{b^{-1} | b \in \mathcal{B}\}$ and define the polynomials B, F as

$$B(x) = \prod_{b \in \mathcal{B}} (1 - bx) \qquad F(t,x) = \prod_{b \in \mathcal{B}} (1 - (1-bx)^{q-1} t)$$
$$= \prod_{b \in \mathcal{B}} (1 - (x^{-1} - b)^{q-1} x^{q-1} t).$$

Consider a non-zero element x_0 in $\mathbb{F}_{q^2} \backslash \mathcal{B}^{[-1]}$. The point x_0^{-1} is not in the arc, so every line incident to it has either d or 0 elements of $\mathcal{B}$. Thus, every direction $(x_0^{-1} - b)^{q-1}$ with $b \in \mathcal{B}$ occurs exactly d times each, so in $F(t, x_0)$ every factor occurs d times and $F(t, x_0)$ is a dth-power. If $x_0 = 0$ it is also a dth-power.

Consider now an element x_0 in $\mathcal{B}^{[-1]}$. Since x_0^{-1} is in $\mathcal{B}$, every line passing through x_0^{-1} contains $d-1$ elements of $\mathcal{B}$. Since there are $q+1$ lines through x_0^{-1}, the directions $(x_0^{-1} - b)^{q-1}$ with $b \in \mathcal{B}$ consist of every $(q+1)$-root of unity, each repeated $d-1$ times together with 0. Call D_i the direction corresponding to the

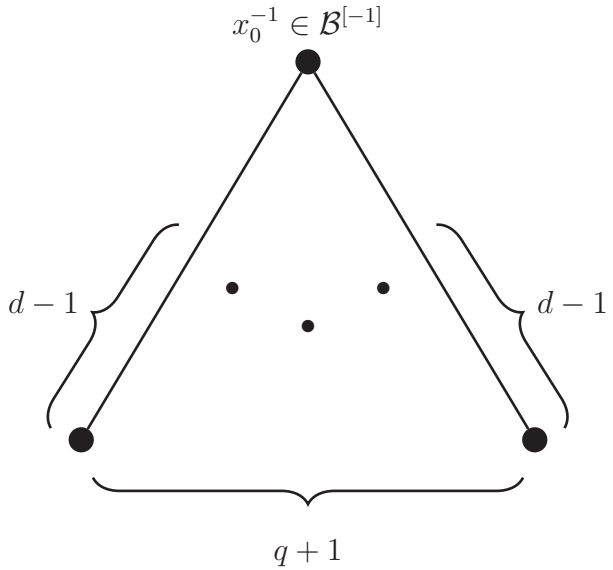

Figure 3.3: The case $x_0 \in \mathcal{B}^{[-1]}$.

ith line through x_0^{-1}, we have

$$\begin{aligned} F(t,x_0) &= \prod_{b\in\mathcal{B}}(1-(x_0^{-1}-b)^{q-1}x_0^{q-1}t) \\ &= (1-\mathsf{D}_1 x_0^{q-1}t)^{d-1}\cdots(1-\mathsf{D}_{q+1}x_0^{q-1}t)^{d-1} \\ &= \big((1-\mathsf{D}_1 x_0^{q-1}t)\cdots(1-\mathsf{D}_{q+1}x_0^{q-1}t)\big)^{d-1} \\ &= (1-x_0^{q^2-1}t^{q+1})^{d-1} \\ &= (1-t^{q+1})^{d-1} \end{aligned}$$

We have that $F(t,x_0)$ is $d-1$ power.

Summarising, we have that $F(t,x_0)$ is either a d or a $d-1$ power. This conlcudes the first steps on the known proof of why maximal arcs cannot exist if q is odd given in [7]. As seen in [7], with the use of algebraic techniques outside the scope of this report, it is shown that in order for the polynomials F and B to be well defined, q must be even and thus a power of 2. Setting the geometrical properties of a maximal arc in $\mathsf{PG}(2,\mathsf{q})$ as algebraic polynomials over $\mathbb{F}_{q^2}$ this way gives an interesting idea on how to approach the pointset of $\mathsf{PG}(2,\mathsf{q})$ that could be used in future work.

3.2 When q is even

Let our projective plane be $\mathsf{PG}(2, 2^{\mathsf{h}})$, where a point has coordinates $[x, y, z]$.

3.2.1 Denniston construction

We proceed as in [26]. Let $f(\omega) = \omega^2 + b\omega + 1$ be an irreducible polynomial over $\mathbb{F}_{2^h}$. Let F_λ be a conic in our projective plane defined as

$$F_\lambda : \quad x^2 + bxy + y^2 + \lambda z^2 = 0 \quad \lambda \in \mathbb{F}_{2^h}$$

We will construct a maximal arc $\mathcal{K}$ by taking the points of various conics F_λ where λ will range in an additive subgroup of $\mathbb{F}_{2^h}$.

For now, fix $\lambda \in \mathbb{F}_{2^h}^*$ and suppose $x = 1$. We have that since f is irreducible, F_λ has the form

$$\underbrace{1 + by + y^2}_{\text{never zero}} + \lambda z^2 = 0$$

and so each $y \in \mathbb{F}_{2^h}$ determines a unique z. Thus F_λ has 2^h points in $\mathsf{PG}(2, 2^{\mathsf{h}})$ with $x = 1$. If $x = 0$ then F_λ has the form

$$y^2 + \lambda z^2 = 0$$

and so without loss of generality we can take $y = 1$ and thus z is uniquely determined by λ. We have that F_λ has one point in $\mathsf{PG}(2, 2^{\mathsf{h}})$ with $x = 0$, and in total F_λ has $2^h + 1$ points for a fixed value of $\lambda \in \mathbb{F}_{2^h}^*$.

If $\lambda = 0$ then F_λ has the form

$$x^2 + bxy + y^2 = 0.$$

If x or y are equal to 1, then $f(y) = 0$ or respectively $f(x) = 0$ which is a contradiction with f being irreducible. We also have that $x = 0$ if and only if $y = 0$, and so we have that F_0 is only the point $[0, 0, 1]$.

We define F_∞ as the line whose points are of the form $[1, y, 0]$ together with $[0, 1, 0]$, and so by taking all the conics F_λ with $\lambda \in \mathbb{F}_{2^h} \cup \{\infty\}$ we have

$$\left| \bigcup F_\lambda \right| = 2^{2h} + 2^h + 1$$

and so $\bigcup F_\lambda$ is a partition of points in $\mathsf{PG}(2, 2^{\mathsf{h}})$.

The lines in $\mathsf{PG}(2,\mathsf{q})$ meet a given non-degenerate conic F_λ in $0, 1$ or 2 points. We say a line is *tangent* to a conic if it only meets the conic in one point.

The tangent lines to all the conics F_λ with $\lambda \in \mathbb{F}_{2^h}^* \cup \{\infty\}$ have a unique common point. Such a point is called the *nucleus* of the conics. We have

$$\frac{\partial F_\lambda}{\partial x} = by \qquad \frac{\partial F_\lambda}{\partial y} = bx \qquad \frac{\partial F_\lambda}{\partial z} = 0.$$

Let $[A, B, C]$ be a point of F_λ, we have that the tangent line through $[A, B, C]$ is

$$(x - A) \cdot bB + (y - B) \cdot bA = 0.$$

The point $[x, y, z] = [0, 0, 1] = F_0$ satisfies this condition for all $\lambda \in \mathbb{F}_{2^h}^* \cup \{\infty\}$ and is so the nucleus of such conics F_λ. Note that F_0 is incident to $q+1$ tangent lines to the conics F_λ, and so all the lines incident to F_0 meet every conic in just one point.

We now give a description on how the conics F_λ intersect the lines of $\mathsf{PG}(2, 2^{\mathsf{h}})$ by considering lines passing and not passing through the nucleus.

If L is a line passing through the nucleus F_0, then L can only have one point from a given conic F_λ, but since there are 2^h points left on L that are not the nucleus, L must meet all conics F_λ with $\lambda \in \mathbb{F}_{2^h} \cup \{\infty\}$ in exactly one point.

To build $\mathcal{K}$ we will pick the point set of d conics F_λ with $\lambda \in \mathbb{F}_{2^h}$, one of them being F_0. Hence, if L is a line passing through the nucleus we have $|\mathcal{K} \cap \mathsf{L}| = d$.

If L is a line not passing through the nucleus, then L meets the conic F_∞ in one point, and either meets a conic F_λ in 2 or 0 points.

To pick the other $d-1$ conics, we must answer how many conics intersect a given line L not passing through the nucleus. Let L and F_λ be given by the equations

$$\mathsf{L}: \quad cx + dy + z = 0 \quad \text{and} \quad F_\lambda: \quad x^2 + bxy + y^2 + \lambda z^2 = 0.$$

Since a point $[x, y, z]$ in $\mathsf{PG}(2,\mathsf{q})$ corresponds to a line in $\mathsf{V}(3,\mathsf{q})$, without loss of generality we can make $y = 1$ and substitute $z = cx + d$ from the equation for L in the equation for F_λ to see that $\mathsf{L} \cap F_\lambda = \emptyset$ if and only if the equation

$$x^2(1 + \lambda c^2) + bx + (1 + \lambda d^2) = 0$$

has no solution in $\mathbb{F}_{2^h}$. This quadratic equation in $\mathbb{F}_{2^h}$ has no solution if and only if

$$\mathrm{Tr}\left(\frac{(1 + \lambda c^2)(1 + \lambda d^2)}{b^2}\right) = \mathrm{Tr}\left(\frac{1 + \lambda(c^2 + d^2) + (\lambda cd)^2}{b^2}\right) = 1$$

where Tr denotes the absolute trace. Let λ_1 and λ_2 be such that $\mathsf{L} \cap F_{\lambda_i} = \emptyset$, then because Tr is additive and since f is irreducible $\mathrm{Tr}(\frac{1}{b}) = 1$, we have

$$\mathrm{Tr}\left(\frac{1 + (\lambda_1 + \lambda_2)(c^2 + d^2) + ((\lambda_1 + \lambda_2)cd)^2}{b^2}\right) = \mathrm{Tr}\left(\frac{1}{b^2}\right) = \mathrm{Tr}\left(\frac{1}{b}\right) = 1.$$

This means that the set $G_{\mathsf{L}} = \{\lambda \in \mathbb{F}_{2^h} \mid F_\lambda \cap \mathsf{L} = \emptyset\}$ is a group of index 2 in $(\mathbb{F}_{2^h}, +)$, and so we can partition $\mathbb{F}_{2^h}$ in G_{L} and its coset G'_{L}:

$$\begin{aligned} \lambda \in G_{\mathsf{L}} \quad &\Rightarrow \quad |F_\lambda \cap \mathsf{L}| = 0 \\ \lambda \in G'_{\mathsf{L}} \quad &\Rightarrow \quad |F_\lambda \cap \mathsf{L}| = 2. \end{aligned}$$

Hence, there are 2^{h-1} conics that meet L in 2 points, and 2^{h-1} conics that meet L in 0 points with $\lambda \in \mathbb{F}_{2^h}$.

To pick the remaining $d - 1$ conics F_λ that build $\mathcal{K}$, we take a subgroup $H \subset (\mathbb{F}_{2^h}, +)$ of order d and define $\mathcal{K}$ as the union of conics with $\lambda \in H$.

To verify that this set of conics forms a maximal arc, we must see that $|\mathsf{L} \cap \mathcal{K}|$ is 0 or d for a line not passing through the nucleus. We have two cases

$$H \subseteq G_{\mathsf{L}} \quad \text{or} \quad H \not\subseteq G_{\mathsf{L}}.$$

If $H \subseteq G_{\mathsf{L}}$, then $H \cap G'_{\mathsf{L}} = \emptyset$ and so $|\mathcal{K} \cap \mathsf{L}| = 0$. If $H \not\subseteq G_{\mathsf{L}}$, then $H \cap G'_{\mathsf{L}} \neq \emptyset$ and $HG'_{\mathsf{L}} = \mathbb{F}_{2^h}$, so

$$\mathbb{F}_{2^h}/G_{\mathsf{L}} = HG'_{\mathsf{L}}/G_{\mathsf{L}} \cong H/(H \cap G_{\mathsf{L}}).$$

Because the index of G_{L} in $\mathbb{F}_{2^h}$ is 2, the index of $H \cap G_{\mathsf{L}}$ in H is 2. Since each conic meets a line in 2 points, we have

$$|H \cap G_{\mathsf{L}}| = \frac{|H|}{2} \quad \Rightarrow \quad |\mathcal{K} \cap \mathsf{L}| = d.$$

We summarise the result. Given a projective plane $\mathsf{PG}(2, 2^{\mathsf{h}})$, we build a maximal arc $\mathcal{K}$ by taking the conics F_λ induced by an irreducible polynomial f, where λ ranges over an additive subgroup $H \subset (\mathbb{F}_{2^h}, +)$ of order $d = 2^m$.

As an example, consider $\mathsf{PG}(2, 4)$ and the maximal arc $\mathcal{K}$ introduced in Chapter 2 Figures [2.1,2.2,2.3], where the coloured points corresponding to $\mathcal{K}$ are the conics

$$x^2 + \alpha xy + y^2 + \lambda z^2 = 0, \;\; \lambda = 0, 1$$

where f is the irreducible polynomial

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

3.2.2 Mathon construction

We proceed and explain the construction given by Mathon in [27]. A way to interpret Denniston's construction of a maximal arc is to define an operation $\oplus$ on the set of all conics F_λ with λ in $\mathbb{F}_{2^h}$,

$$F_\lambda \oplus F_{\lambda'} := F_{\lambda+\lambda'}$$

and then consider all values for λ in which the operation $\oplus$ gives a *closed set* $\mathcal{C}$ of conics in the sense that if $F_\lambda, F_{\lambda'}$ are in $\mathcal{C}$, then $F_\lambda \oplus F_{\lambda'}$ is also in $\mathcal{C}$.

In Denniston's construction such a set $\mathcal{C}$ is characterised by taking all conics F_λ with λ in an additive subgroup of $\mathbb{F}_{2^h}$. In Mathon's construction, the idea of defining an operation $\oplus$ on a set of conics is further exploited.

Let $f(\omega) = \eta\omega^2 + \omega + \mu$ be an irreducible polynomial over $\mathbb{F}_{2^h}$. Let $F_{\eta,\mu,\lambda}$ be a conic in our projective plane $\mathsf{PG}(2, 2^{\mathsf{h}})$ defined as

$$F_{\eta,\mu,\lambda}: \quad \eta x^2 + xy + \mu y^2 + \lambda z^2 = 0 \quad \lambda \in \mathbb{F}_{2^h}$$

Let $\mathcal{F}$ be the set of all such non-degenerate conics and define the operation $\oplus$ in $\mathcal{F}$ with $\lambda \neq \lambda'$ as

$$F_{\eta,\mu,\lambda} \oplus F_{\eta',\mu',\lambda'} = F_{\eta\oplus\eta',\mu\oplus\mu',\lambda\oplus\lambda'}$$

where

$$\eta \oplus \eta' = \frac{\eta\lambda + \eta'\lambda'}{\lambda + \lambda'}, \quad \mu \oplus \mu' = \frac{\mu\lambda + \mu'\lambda'}{\lambda + \lambda'}, \quad \lambda \oplus \lambda' = \lambda + \lambda'.$$

Note that this operation is commutative, associative and $(F \oplus F') \oplus (G \oplus F') = F \oplus G$ for different F, F', G.

When are any two conics $F_{\eta,\mu,\lambda}$ and $F_{\eta',\mu',\lambda'}$ with $\lambda \neq \lambda'$ and their composition $F_{\eta,\mu,\lambda} \oplus F_{\eta',\mu',\lambda'}$ mutually disjoint? Consider the collineation defined by

$$H = \begin{pmatrix} 1/a & 0 & 0 \\ 0 & a & 0 \\ b & c & 1 \end{pmatrix}$$

where

$$a = \sqrt{A}, \quad b = \sqrt{\frac{\eta/A + 1}{\lambda}}, \quad c = \sqrt{\frac{A(\mu + B)}{\lambda}}$$

and

$$A = \frac{\eta'\lambda + \eta\lambda'}{\lambda + \lambda'}, \quad B = \frac{\mu'\lambda + \mu\lambda'}{\lambda + \lambda'}, \quad C = \frac{(\eta\mu' + \mu\eta')\lambda\lambda' + (\eta\mu + \eta'\mu')\lambda^2}{\lambda^2 + \lambda'^2}.$$

The collineation H maps $F_{\eta,\mu,\lambda}, F_{\eta',\mu',\lambda'}$ and $F_{\eta,\mu,\lambda} \oplus F_{\eta',\mu',\lambda'}$ into $F_{1,AB,\lambda}, F_{1,AB,\lambda'}$ and $F_{1,AB,\lambda+\lambda'}$ respectively. These conics are nondegenerate and mutually disjoint if $\mathrm{Tr}(AB) = 1$, which implies $\mathrm{Tr}((\eta \oplus \eta')(\mu \oplus \mu')) = 1$.

Let $\mathcal{C}$ be a closed subset of n elements of $\mathcal{F}$ in the sense that if F and G are in $\mathcal{C}$, then $F \oplus G$ is in $\mathcal{C}$. Suppose that $F' = F_{\eta',\mu',\lambda'} \in \mathcal{F} \backslash \mathcal{C}$ and $\mathrm{Tr}((\eta \oplus \eta')(\mu \oplus \mu')) = 1$ for every $F_{\eta,\mu,\lambda} \in \mathcal{C}$, then since F' is disjoint to all conics in $\mathcal{C}$, the set

$$< \mathcal{C} \cup \{F'\} >= \{F, F', F \oplus F' | F \in \mathcal{C}\}$$

is a closed subset of $\mathcal{F}$ and has $2n + 1$ elements.

Given a non-degenerate conic F we can proceed recursively d times adding disjoint conics, arriving to a closed subset $\mathcal{C}$ with $2(2^{d-1} - 1) + 1 = 2^d - 1$ elements. Every conic in $\mathcal{C}$ shares the common nucleus $F_0 = [0, 0, 1]$.

To build a maximal arc $\mathcal{K}$ we will take the point set of a closed subset $\mathcal{C}$ with $2^d - 1$ elements and their nucleus F_0. We will see that $\mathcal{C}$ meets every line in 0 or 2^d points.

Since the polynomial f is irreducible, F_∞ (the line $z = 0$) does not share points with any conic. We can see this by substituting $z = 0$ in $F_{\eta,\mu,\lambda}$. We have

$$\begin{aligned} \eta x^2 + xy + \mu y^2 = 0 & \\ \text{if } x = 1 \Rightarrow \mu y^2 + y + \eta = 0 & \\ \text{if } y = 1 \Rightarrow \eta x^2 + x + \mu = 0. & \end{aligned}$$

The last two polynomials have a solution in y or x respectively only when $\mathrm{Tr}(\mu\eta) = 0$, but since f is irreducible we have $\mathrm{Tr}(\mu\eta) = 1$, and so F_∞ is external to $\mathcal{K}$.

We now divide in three disjoint classes all other lines:

- All the lines passing through F_0, that is the lines defined by the points $[0, 0, 1]$ and $[1, a, 0]$ with $a \in \mathbb{F}_{2^h}$, and the line defined by the points $[0, 0, 1]$ and $[0, 1, 0]$. See Figure [3.4].
- The remaining lines passing through $[1, 0, 0]$ that are not F_∞ and don't meet F_0, that is the lines defined by the points $[1, 0, 0]$ and $[0, 1, b]$ with $b \in \mathbb{F}_{2^h}, b \neq 0$. See Figure [3.5]. A typical point incident to these lines has the form $[0, 1, b] + [x, 0, 0] = [x, 1, b]$ with $x \in \mathbb{F}_{2^h}$.
- The lines defined by the points $[a, 1, 0]$ and $[b, 0, 1]$ with $a, b \in \mathbb{F}_{2^h}, b \neq 0$. See Figure [3.6]. A typical point incident to these lines has the form $[a, 1, 0] + [bx, 0, x] = [a + bx, 1, x]$ with $x \in \mathbb{F}_{2^h}$.

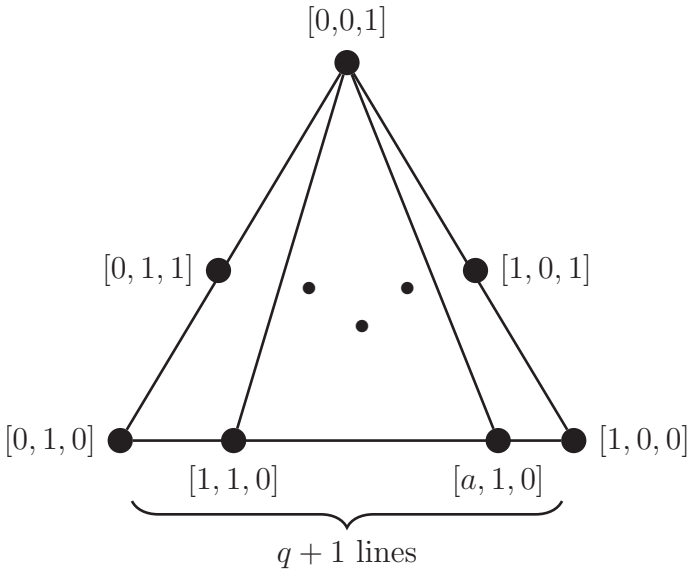

Figure 3.4: All the lines passing through F_0.

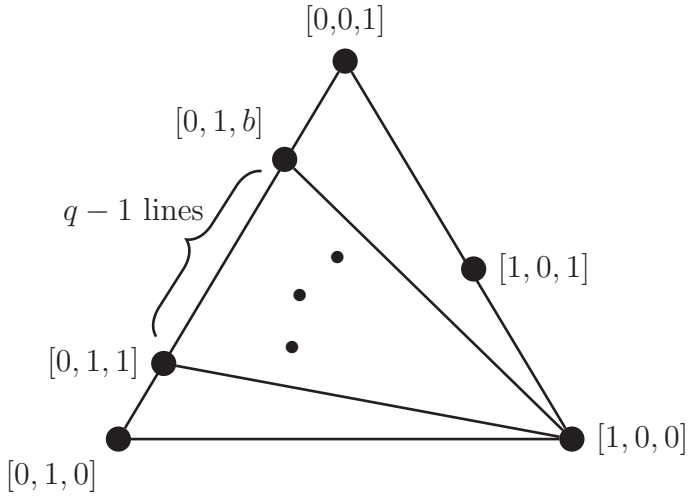

Figure 3.5: Lines joining the points $[1, 0, 0]$ and $[0, 1, b]$ with $b \in \mathbb{F}_{2^h}, b \neq 0$.

In how many points does $\mathcal{C}$ meet these classes of lines? For the first class, the nucleus $F_0 = [0, 0, 1]$ is in every line, so the first class of lines is tangent to every conic and thus meets $\mathcal{C}$ in 2^d points. The second and third class of lines do not meet a conic $F_{\eta,\mu,\lambda}$ if and only if the equations

$$\eta x^2 + x + \mu + \lambda b^2 = 0 \qquad \eta(a + bx)^2 + (a + bx) + \mu + \lambda x^2 = 0$$

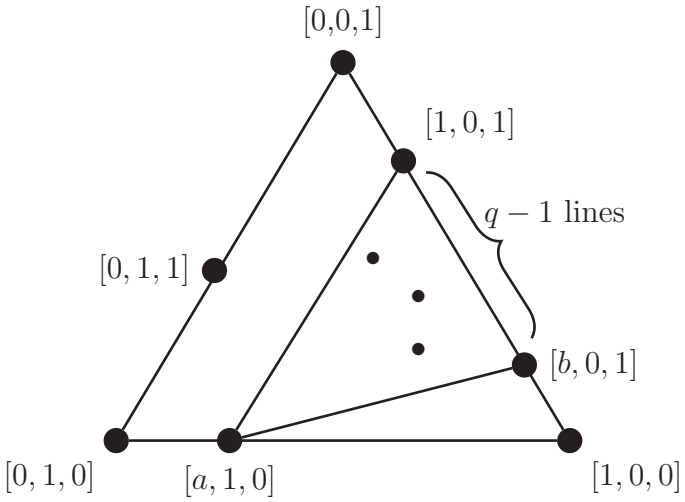

Figure 3.6: Lines joining the points $[a, 1, 0]$ and $[b, 0, 1]$ with $a, b \in \mathbb{F}_{2^h}, b \neq 0$. There are q choices for a, $q-1$ choices for b and so $q(q-1)$ lines in this class.

have no solution for $x \in \mathbb{F}_{2^h}$ respectively. In order for these equations to have no solution we must have

$$\begin{aligned}\mathrm{Tr}(\eta(\mu + \lambda b^2)) &= \mathrm{Tr}(\eta\mu + \eta\lambda b^2) \\ &= \mathrm{Tr}(\eta\mu) + \mathrm{Tr}(\eta\lambda b^2) \\ &= 1 + \mathrm{Tr}(\eta\lambda b^2) \\ &= 1 \\ &\Rightarrow \mathrm{Tr}(\eta\lambda b^2) = 0\end{aligned}$$

and

$$\begin{aligned}\mathrm{Tr}\Big(\frac{(\eta b^2 + \lambda)(\eta a^2 + a + \mu)}{b^2}\Big) &= \mathrm{Tr}(\eta^2 a^2 + \eta a + \eta\mu) + \mathrm{Tr}\Big(\frac{\eta a^2 + a + \mu}{b^2}\lambda\Big) \\ &= 2 \cdot \mathrm{Tr}(\eta a) + \mathrm{Tr}(\eta\mu) + \mathrm{Tr}\Big(\frac{\eta a^2 + a + \mu}{b^2}\lambda\Big) \\ &= 1 + \mathrm{Tr}\Big(\frac{\eta a^2 + a + \mu}{b^2}\lambda\Big) \\ &= 1 \\ &\Rightarrow \mathrm{Tr}\Big(\frac{\eta a^2 + a + \mu}{b^2}\lambda\Big) = 0\end{aligned}$$

respectively. To simplify notation [27], we call both of these conditions $\mathrm{Tr}(\eta, \mu, \lambda)$. We have

$$\mathrm{Tr}(\eta \oplus \eta', \mu \oplus \mu', \lambda \oplus \lambda') = \mathrm{Tr}(\eta, \mu, \lambda) + \mathrm{Tr}(\eta', \mu', \lambda')$$

and so if two conics $F, F' \in \mathcal{C}$ do not meet a given line, then $F \oplus F'$ does not meet the given line either. On the other hand, if a conic $F \in \mathcal{C}$ meets a given line (in just two points), then proceeding recursively we see that there are 2^{d-1} disjoint conics in $\mathcal{C}$ that meet the given line in just two points, hence the given line meets $\mathcal{K}$ in $2 \cdot 2^{d-1} = 2^d$ points.

Summarising, we have that any line of $\mathsf{PG}(2, 2^{\mathsf{h}})$ meets the point set $\mathcal{K}$ of a closed set of conics $\mathcal{C}$ in 0 or 2^d points, and so $\mathcal{K}$ is a maximal arc.

With respect to Denniston's construction, note that if the polynomial $f(\omega) = \omega^2 + b\omega + 1$ over $\mathbb{F}_{2^h}$ is irreducible, then the polynomial $f(\omega) = \frac{\omega^2}{b} + \omega + \frac{1}{b}$ is also irreducible, and so Denniston's construction reduces to Mathon's construction with $\mu = \eta = \frac{1}{b}$.

Chapter 4

Beyond maximal arcs

In this chapter, we will give a construction of a partial geometry with parameters $\mathrm{pg}(8, 20, 2)$. As mentioned in Chapter 2, this geometry is closely related via **Method 2** to what would be a maximal arc $\mathcal{K}$ of size 21 in $\mathsf{PG}(2, 9)$. From Chapter 3 however, we know such an arc $\mathcal{K} \subset \mathsf{PG}(2, 9)$ cannot exist.

It was also mentioned in Chapter 2, that $\mathsf{PG}(5, 3)$ is related to $\mathsf{PG}(2, 9)$ via a blow up, and that a set of 21 lines $\mathcal{L} \subset \mathsf{PG}(5, 3)$ would be considered to build a partial geometry $\mathrm{pg}(8, 20, 2)$.

In order to introduce $\mathcal{L}$ some new concepts are to be introduced. We proceed as in [10].

4.1 A generalisation of maximal arcs to higher dimensions

Let ρ be a polarity of $\mathsf{PG}(\mathsf{n}, \mathsf{q})$. Let $\mathcal{R}(r)$ be any set $\{\pi_1, ..., \pi_k\}$ $(k > 1)$ of mutual disjoint r-dimensional subspaces of $\mathsf{PG}(\mathsf{n}, \mathsf{q})$ such that no π_i^ρ meets an element of $\mathcal{R}(r)$. If $\mathcal{R}(r)$ is of maximal size, we say $\mathcal{R}(r)$ is a *perp-system*.

Note that in order for the subspaces π_i's to be disjoint in $\mathsf{PG}(\mathsf{n}, \mathsf{q})$, we must have $n \geq 2r + 1$.

How large can $|\mathcal{R}(r)|$ be?

We first count in two ways how many ordered pairs (p_i, π^ρ) there are where p_i is a point contained in π^ρ. Since each π^ρ is disjoint with each $\pi \in \mathcal{R}(r)$, we must

only consider points p_i contained in $\mathsf{PG}(\mathsf{n},\mathsf{q})\backslash\mathcal{R}(r)$. Let P be the number of p_i's, we have

$$\begin{aligned}\mathsf{P} &= [n+1]_q - |\mathcal{R}(r)| \cdot [r+1]_q \\ &= \frac{q^{n+1}-1}{q-1} - |\mathcal{R}(r)| \cdot \frac{q^{r+1}-1}{q-1}.\end{aligned}$$

Let t_i be the number of π^ρ's such that p_i is contained in π^ρ. Now observe that because π is of dimension r, then π^ρ is of dimension $n-r-1$ and so there are $[n-r]_q$ points contained in each π^ρ. These two arguments show that

$$\begin{aligned}\sum_i t_i &= |\mathcal{R}(r)| \cdot [n-r]_q \\ &= |\mathcal{R}(r)| \cdot \frac{q^{n-r}-1}{q-1}.\end{aligned}$$

We now count how many triples $(\mathsf{p}_i, \pi^\rho, \pi'^\rho)$ there are with p_i contained in $\pi^\rho \cap \pi'^\rho$ and $\pi \neq \pi'$. Counting the number of points in $\pi^\rho \cap \pi'^\rho$ corresponds to counting the number of hyperplanes containing both π and π'. The minimal subspace containing both π and π' is of dimension $2r+1$, and so using equation 1.2 we have that there are

$$\mathrm{I}(2r+2, n-2r-2) = [n-2r-1]_q$$

points in $\pi^\rho \cap \pi'^\rho$. Since there are $|\mathcal{R}(r)|(|\mathcal{R}(r)|-1)$ ways to choose $\pi^\rho \cap \pi'^\rho$ with $\pi \neq \pi'$, we have

$$\begin{aligned}\sum_i t_i(t_i-1) &= |\mathcal{R}(r)|(|\mathcal{R}(r)|-1) \cdot [n-2r-1]_q \\ &= |\mathcal{R}(r)|(|\mathcal{R}(r)|-1) \cdot \frac{q^{n-2r-1}-1}{q-1}.\end{aligned}$$

We now apply Cauchy-Schwartz inequality to get

$$\mathsf{P}\sum_i t_i^2 - \Big(\sum_i t_i\Big)^2 \geq 0.$$

After some calculations we arrive at

$$|\mathcal{R}(r)| \leq \frac{q^{(n-2r-1)/2}(q^{(n+1)/2}+1)}{q^{(n-2r-1)/2}+1}.$$

Hence $\mathcal{R}(r)$ is a perp-system if equality holds.

4.1.1 Perp-systems give rise to two weight codes

Recall from Chapter 1 that two weight codes are two weight sets, so we must check that any hyperplane of $\mathsf{PG}(\mathsf{n},\mathsf{q})$ has only two intersection sizes with the points of $\mathcal{R}(r)$. There are two kinds of hyperplanes in $\mathsf{PG}(\mathsf{n},\mathsf{q})$, those that under ρ are the image of a point in $\mathcal{R}(r)$, and those that are the image of a point in $\mathsf{PG}(\mathsf{n},\mathsf{q})\backslash\mathcal{R}(r)$.

Note that maximality of $|\mathcal{R}(r)|$ is obtained when all t_i's have the same value. We can calculate it by

$$\bar{t} = \frac{\sum_i t_i}{\mathsf{P}} = q^{(n-2r-1)/2}$$

and thus every point p_i not contained in $\mathcal{R}(r)$ is incident to $\bar{t}$ subspaces π^ρ. This means that the hyperplane p_i^ρ has $\bar{t}$ subspaces π of $\mathcal{R}(r)$. The hyperplane p_i^ρ intersects each of the remaining $|\mathcal{R}(r)| - \bar{t}$ subspaces π in

$$\dim(\mathsf{p}_i^\rho \cap \pi) = \dim(\mathsf{p}_i^\rho) + \dim(\pi) - \dim(\mathsf{p}_i^\rho \cup \pi).$$

Since π is not contained in p_i^ρ, their span has dimension n and so their intersection has projective dimension $r-1$. The hyperplane p_i^ρ thus meets $\mathcal{R}(r)$ in

$$h_1 = [r+1]_q \cdot \bar{t} + [r]_q \cdot (|\mathcal{R}(r)| - \bar{t})$$

points of $\mathcal{R}(r)$.

Since for any π we have $\pi^\rho \cap \mathcal{R}(r) \neq \emptyset$, we have that for a point a contained in a given π, the hyperplane a^ρ does not contain any subspace π and so meets $\mathcal{R}(r)$ only on the intersections $\mathsf{a}^\rho \cap \pi$. Similarly as above, we see that each of these intersections have projective dimension $r-1$, and so the hyperplane a^ρ meets $\mathcal{R}(r)$ in

$$h_2 = [r]_q \cdot |\mathcal{R}(r)|$$

points.

Figures 4.1 and 4.2 give a schematic diagram of the derivation for weights h_1 and h_2 respectively, where the subspaces π are represented by lines, hyperplanes are represented by rectangles, and π^ρ's are represented by ellipses.

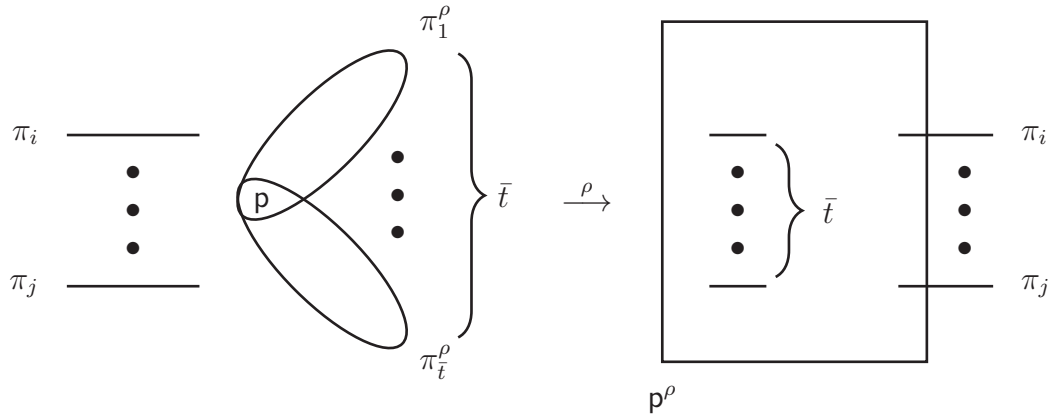

Figure 4.1: Diagram explaining the derivation of weight h_1.

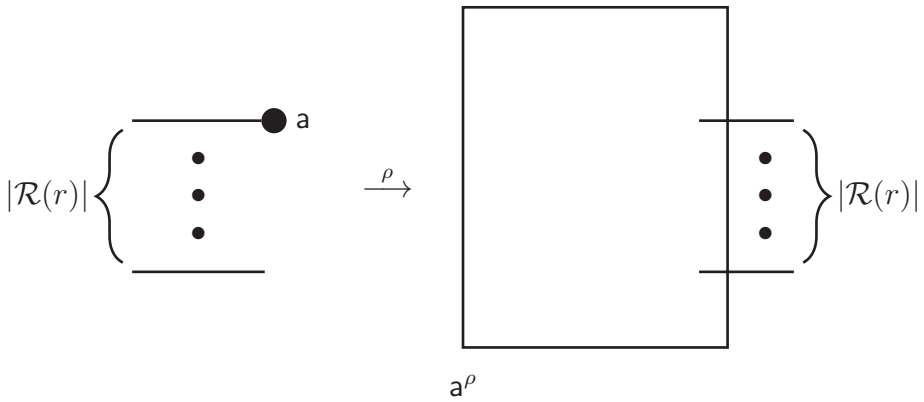

Figure 4.2: Diagram explaining the derivation of weight h_2.

4.2 Partial geometries from perp-systems

To build a partial geometry from a given perp-system $\mathcal{R}(r)$ in $\mathsf{PG}(\mathsf{n},\mathsf{q})$ we embed $\mathsf{PG}(\mathsf{n},\mathsf{q})$ in $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})$ and take as points the points of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})\backslash\mathsf{PG}(\mathsf{n},\mathsf{q})$, and as lines the $(r+1)$-dimensional subspaces of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})$ which contain an element of $\mathcal{R}(r)$ but are not contained in $\mathsf{PG}(\mathsf{n},\mathsf{q})$.

- A subspace L with dimension $r+1$ of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})\backslash\mathsf{PG}(\mathsf{n},\mathsf{q})$ that meets $\mathsf{PG}(\mathsf{n},\mathsf{q})$, meets $\mathsf{PG}(\mathsf{n},\mathsf{q})$ in only one subspace of dimension r. In particular, if L contains an element π of $\mathcal{R}(r)$ it only contains π. We have that L has

$$[r+1]_q - [r]_q = \frac{q^{r+2}-1}{q-1} - \frac{q^{r+1}-1}{q-1} = q^{r+1}$$

  points in $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})\backslash\mathsf{PG}(\mathsf{n},\mathsf{q})$.

- A point p of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})\backslash\mathsf{PG}(\mathsf{n},\mathsf{q})$ is incident to $|\mathcal{R}(r)|$ subspaces of dimension $r+1$ containing an element of $\mathcal{R}(r)$.

- Let L be a subspace with dimension $r+1$ of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})$ that meets $\mathsf{PG}(\mathsf{n},\mathsf{q})$ exactly in an element π of $\mathcal{R}(r)$, and let p be a point not in L nor $\mathsf{PG}(\mathsf{n},\mathsf{q})$.

  We will see that p is incident to a constant number α of subspaces with dimension $r+1$ of $\mathsf{PG}(\mathsf{n}+1,\mathsf{q})$ that meet L, and also meet $\mathsf{PG}(\mathsf{n},\mathsf{q})$ exactly in one element of $\mathcal{R}(r)$.

  As shown in [10] the path given by the authors to prove this, is to see that since $\mathcal{R}(r)$ gives a two-weight code, this two weight code yields a strongly regular graph [9], and that this graph gives a partial geometry [40]. In contrast to [10], the path taken in this report is a direct count to obtain α, and is not published in any paper at the time of writing this report.

  Let T be the subspace of dimension $r+2$ generated by the subspaces $\{\mathrm{L},\mathsf{p}\}$. We have

$$\begin{aligned}\dim(\mathsf{PG}(\mathsf{n},\mathsf{q})\cap\mathsf{T}) &= \dim(\mathsf{PG}(\mathsf{n},\mathsf{q})) + \dim(\mathsf{T}) - \dim(\mathsf{PG}(\mathsf{n},\mathsf{q})\cup\mathsf{T}) \\ &= n + (r+2) - (n+1) \\ &= r+1.\end{aligned}$$

  Let R be the $(r+1)$-dimensional subspace $\mathsf{PG}(\mathsf{n},\mathsf{q})\cap\mathsf{T}$. How does R intersect $\mathcal{R}(r)$? Let π' be an element of $\mathcal{R}(r)$ such that $\pi'\neq\pi$. We have

$$0 \leq \dim(\mathsf{R}\cap\pi') = (r+1) + r - \dim(\mathsf{R}\cup\pi')$$

so $\dim(\mathsf{R} \cup \pi') \leq 2r+1$. If $\dim(\mathsf{R} \cup \pi') \leq 2r$ then since $\pi \cap \pi' = \emptyset$ we have

$$-1 = \dim(\pi \cap \pi') = r + r - \dim(\pi \cup \pi') \quad \Rightarrow \quad \dim(\pi \cup \pi') = 2r+1$$

but $\pi \subset \mathsf{R} \subset \mathsf{R} \cup \pi'$ and so

$$2r+1 = \dim(\pi \cup \pi') \leq \dim(\mathsf{R} \cup \pi') \leq 2r$$

which is a contradiction. So $\dim(\mathsf{R} \cup \pi') = 2r+1$ and $\dim(\mathsf{R} \cap \pi') = 0$, so R meets $\mathcal{R}(r)$ only in points.

How many such points does $\mathsf{R} \cap \mathcal{R}(r)$ have? Recall that under ρ points are mapped to hyperplanes, and that every hyperplane has one of two possible weights h_1, h_2 with respect to $\mathcal{R}(r)$. We want to count the number of hyperplanes through R^ρ that are the image of a point in $\mathcal{R}(r)$ under ρ, and so must have weight h_2.

In order to do this, we count pairs (a, H) where a is a point in $\mathsf{H} \cap \mathcal{R}(r)$, and H is a hyperplane containing R^ρ. Counting the a's we have as many points as there are in $\mathcal{R}(r)$ times all the hyperplanes through the subspace generated by $\{\mathsf{R}^\rho, \mathsf{a}\}$. Counting the H's we have h_2 times the hyperplanes coming under ρ from the points of

$$\mathsf{R} \cap \mathcal{R}(r)$$

plus h_1 times the number of hyperplanes coming from the remaining points in R. Recalling that R contains only one subspace π we have:

$$\begin{aligned} |\mathcal{R}(r)| \cdot [r+1]_q \cdot [r+1]_q = \\ = h_2([r+1]_q + \alpha) + h_1([r+2]_q - ([r+1]_q + \alpha)) \end{aligned}$$

and so

$$\alpha = \frac{q^{r+1}-1}{\bar{t}+1}.$$

Since the choice of L and p was arbitrary, we conclude that α is indeed constant.

Thus we have that our partial geometry has parameters

$$\mathrm{pg}\Big(q^{r+1}-1, |\mathcal{R}(r)|-1, \alpha\Big)$$

The partial geometry arrived through this method is referred to in the literature as $\Gamma^*(\mathcal{R}(r))$.

4.3 21 lines in $\mathsf{PG}(5,3)$

We now have a way to construct a partial geometry with parameters $\mathrm{pg}(8,20,2)$ arising from a perp-system $\mathcal{L} = \mathcal{R}(1)$ consisting of 21 lines in $\mathsf{PG}(5,3)$. How to find such 21 lines is a difficult question. Mathon [10] found by computer search these lines, and a geometric construction was proposed by [11].

The explicit lines of $\mathcal{L}$ (see [10]) represented by two points [...][...] in $\mathsf{PG}(5,3)$ are:

[010000][100000]	[101000][010010]	[201000][020010]
[100100][020001]	[200100][010001]	[111100][210021]
[121100][011021]	[112100][011011]	[122100][110011]
[210110][221001]	[220110][121001]	[101110][211101]
[221110][101201]	[102110][111201]	[212110][201101]
[210210][102201]	[220210][202101]	[101210][222201]
[111210][212001]	[102210][122101]	[122210][112001]

The set $\mathcal{L}$ has some interesting properties as noted by [10]. In particular, there are seven solids (by solid we mean a projective space of dimension 3) each containing three different lines from $\mathcal{L}$. These solids represented by four points in $\mathsf{PG}(5,3)$ are:

[100000][010000][000100][000001]	[100021][010010][001012][000102]
[100011][010020][001011][000102]	[100020][010011][001000][000102]
[102001][011000][000102][000012]	[101001][012000][000102][000010]
[100010][010021][001002][000102]	

Moreover, these seven solids meet in exactly one line:

$$[110001][000102].$$

To obtain explicit representations of these seven solids and their common line, a small script in GAP [35] and Fining [36] shown below was written.

```
LoadPackage("fining");
ps := ProjectiveSpace(5,3);
#
L1 := [[0,1,0,0,0,0],\
       [1,0,0,0,0,0]]\
      *Z(3)^0;
L2 := [[1,0,1,0,0,0],\
       [0,1,0,0,1,0]]\
      *Z(3)^0;
```

```
L3 := [[2,0,1,0,0,0],\
       [0,2,0,0,1,0]]\
      *Z(3)^0;
L4 := [[1,0,0,1,0,0],\
       [0,2,0,0,0,1]]\
      *Z(3)^0;
L5 := [[2,0,0,1,0,0],\
       [0,1,0,0,0,1]]\
      *Z(3)^0;
L6 := [[1,1,1,1,0,0],\
       [2,1,0,0,2,1]]\
      *Z(3)^0;
L7 := [[1,2,1,1,0,0],\
       [0,1,1,0,2,1]]\
      *Z(3)^0;
L8 := [[1,1,2,1,0,0],\
       [0,1,1,0,1,1]]\
      *Z(3)^0;
L9 := [[1,2,2,1,0,0],\
       [1,1,0,0,1,1]]\
      *Z(3)^0;
L10 := [[2,1,0,1,1,0],\
        [2,2,1,0,0,1]]\
      *Z(3)^0;
L11 := [[2,2,0,1,1,0],\
        [1,2,1,0,0,1]]\
      *Z(3)^0;
L12 := [[1,0,1,1,1,0],\
        [2,1,1,1,0,1]]\
      *Z(3)^0;
L13 := [[2,2,1,1,1,0],\
        [1,0,1,2,0,1]]\
      *Z(3)^0;
L14 := [[1,0,2,1,1,0],\
        [1,1,1,2,0,1]]\
      *Z(3)^0;
L15 := [[2,1,2,1,1,0],\
        [2,0,1,1,0,1]]\
      *Z(3)^0;
L16 := [[2,1,0,2,1,0],\
```

```
        [1,0,2,2,0,1]]\
      *Z(3)^0;
L17 := [[2,2,0,2,1,0],\
        [2,0,2,1,0,1]]\
      *Z(3)^0;
L18 := [[1,0,1,2,1,0],\
        [2,2,2,2,0,1]]\
      *Z(3)^0;
L19 := [[1,1,1,2,1,0],\
        [2,1,2,0,0,1]]\
      *Z(3)^0;
L20 := [[1,0,2,2,1,0],\
        [1,2,2,1,0,1]]\
      *Z(3)^0;
L21 := [[1,2,2,2,1,0],\
        [1,1,2,0,0,1]]\
      *Z(3)^0;
#
21_lines := [L1, L2, L3, L4, L5, L6, L7,\
     L8, L9, L10, L11, L12, L13, L14,\
     L15, L16, L17, L18, L19, L20, L21];
# assign lines to PG(5,3)
line := [];
for i in [1 .. Length(21_lines)] do
  line[i] := \
  VectorSpaceToElement( ps,21_lines[i] );
od;
#
line_list := function()
local line_listt;
line_listt := [];
  for i in [1 .. Length(21_lines)] do
    line_listt[i] := \
    VectorSpaceToElement( ps,21_lines[i] );
  od;
  return line_listt;
end;;
#
# "loop_1" returns a list of lines,
# all lines being in the solid made by
```

```
# line L and line j.
# if the solid made by lines L and j
# does not contain more of the 21 lines,
# the return list is empty.
loop_1 := function(L,j)
local new_line, intersec, solid, k,new_list;
      new_line := line_list();
      new_list := [];
      solid := Span(new_line[L],new_line[j]);
      k := Length(new_line);
    for i in [1..k] do
      intersec := Meet(solid, new_line[i]);
      if i = L then continue;
elif i = j then continue;
elif ProjectiveDimension(intersec) = 1 then
  Add(new_list, L);
  Add(new_list, j);
  Add(new_list, i);
#  update list!
      fi;
    od;
    return new_list;
end;;
#
# "loop_2" collects all non-empty lists
# from "loop_1" fixing line L and going
# through line j.
loop_2 := function(L)
local new_line,k,j, new_list;
new_line := line_list();
new_list := [];
k := Length(new_line);
    for j in [1..k] do
      if Length(loop_1(L,j))>0 then
Add(new_list, loop_1(L,j));
      fi;
#       Append(new_list,loop_1(L,j));
    od;
    return new_list;
end;;
```

```
#
# "loop_3" prints all lists of solids
# from "loop_2", going through L.
loop_3 := function()
local L;
  for L in [1..Length(line)] do
    Print(L, " ", loop_2(L),"\n","\n");
  od;
end;;
#
loop_3();
```

After the script is run, a list of all solids containing 3 of the 21 lines is produced. Given this list, a manual calculation was made to find 7 solids, holding the 21 lines in total. Such solids and their common line can explicitly be printed out by running:

```
7_solids := [ [ 1, 4 ], [ 2, 13 ], [ 3, 16 ],\
      [ 6, 8 ], [ 7, 11 ], [ 9, 12 ],\
      [ 10, 14 ] ];
solids := [];
for a in 7_solids do
  Add(solids, Span(line[a[1]],line[a[2]]));
od;
print_seven_S := function()
local i,j;
j := 1;
  for i in solids do
    Print("S",j,"\n");
    Display(i);
    j := j+1;
  od;
end;;
#
print_seven_S();
Display(Meet(solids[1],solids[2]));
```

In [11] the authors give a geometric construction specific for these 21 lines, but at the time of writing this report it is not yet clear how to generalize the construction for these 21 lines in $\mathsf{PG}(5,3)$ into higher dimensions or a projective space with a different underlying finite field.

Chapter 5

Conclusions

In this report maximal arcs were constructed as well as other combinatorial structures related to them. We now give a review.

5.1 Maximal arcs

As defined in 1, a maximal arc is a non-empty proper subset $\mathcal{K}$ of points in $\mathsf{PG}(2,\mathsf{q})$, such that every line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points. We have

$$\begin{aligned} k = |\mathcal{K}| &= (d-1)(q+1)+1 \\ &= qd - q + d \end{aligned}$$

Maximal arcs can only exist when q is even, as seen in Chapter 3.

Given an irreducible polynomial $f(\omega) = \eta\omega^2 + \omega + \mu$ over $\mathbb{F}_{2^h}$, one can construct a maximal arc $\mathcal{K}$ by considering the point set of a closed set of $2^g - 1$ conics of the form

$$F_{\eta,\mu,\lambda}: \quad \eta x^2 + xy + \mu y^2 + \lambda z^2 = 0 \quad \lambda \in \mathbb{F}_{2^h}$$

together with their nucleus F_0, in which every line meets $\mathcal{K}$ in 0 or $d = 2^g$ points.

5.2 Above maximal arcs

In Chapter 1 several combinatorial objects were defined, and in Chapters 1 and 2 their relationship with each other and with maximal arcs was established. We summarise.

Let $\mathcal{K}$ be a maximal arc in $\mathsf{PG}(2,\mathsf{q})$ in which each line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points, and so $|\mathcal{K}| = qd - q + d$. We have:

- A two weight code can be built by taking the points of a maximal arc as the column vectors of a generator matrix for the code. Conversely, maximal arcs can be built by taking the column vectors of a generator matrix of a two weight code as points in a projective plane.
- Maximal arcs give rise to partial geometries via **Method 1** (2.1.1) and **Method 2** (2.1.2).

  Let $\mathcal{K}$ be a maximal arc in $\mathsf{PG}(2,\mathsf{q})$ in which each line of $\mathsf{PG}(2,\mathsf{q})$ meets $\mathcal{K}$ in 0 or d points.

  - **Method 1** (2.1.1) gives a partial geometry with parameters:

    $$\mathrm{pg}(q-d, q-\frac{q}{d}, q-\frac{q}{d}+1-d).$$

  - **Method 2** (2.1.2) gives a partial geometry with parameters:

    $$\mathrm{pg}(q-1, qd-q+d-1, d-1).$$

- The point graph of a partial geometry $\mathrm{pg}(s,t,\alpha)$ is a strongly regular graph with parameters:

  $$\mathrm{srg}\Big(\frac{(s+1)st}{\alpha}+s+1, s(t+1), s-1+t(\alpha-1), \alpha(t+1)\Big).$$

- The incidence matrix N of a partial geometry seen as a parity check matrix gives an LDPC code $\mathsf{C_{LDPC}}$ over $\mathbb{F}_2$ with the following length n, minimum distance d, rank r and number of minimum length cycles N_6 in its tanner graph:

  $$\begin{aligned} n = l &= \frac{(t+1)st}{\alpha}+t+1 \\ d &\geq \max\left\{\frac{(t+1)(s+1-t+\alpha)}{\alpha}, \frac{2(s+\alpha)}{\alpha}\right\} \\ r &\geq l-\left(1+\frac{st(s+1)(t+1)}{\alpha(s+t+1-\alpha)}\right) \\ N_6 &= \frac{lt(\alpha-1)}{3}\binom{s+1}{2}. \end{aligned}$$

  Its generator matrix is $N^{\perp}$ such that $N\cdot(N^{\perp})^t = 0$, and has only r rows different from the all zero vector.

Examples of such constructions can be found in Chapter 2.

5.3 Beyond maximal arcs

A generalization of maximal arcs into higher dimensions is given in Chapter 4 by defining Perp-systems.

Given a perp-system $\mathcal{R}(r)$ in $\mathsf{PG}(\mathsf{n},\mathsf{q})$, we can build a partial geometry with parameters

$$\mathrm{pg}\Big(q^{r+1}-1, |\mathcal{R}(r)|-1, \alpha\Big)$$

where

$$|\mathcal{R}(r)| = \frac{\bar{t}(q^{(n+1)/2}+1)}{\bar{t}+1}$$
$$\alpha = \frac{q^{r+1}-1}{\bar{t}+1}$$
$$\bar{t} = q^{(n-2r-1)/2}.$$

An example of a perp-system $\mathcal{L} = \mathcal{R}(1)$ of 21 lines in $\mathsf{PG}(\mathsf{5},\mathsf{3})$, and its associated partial geometry with parameters

$$\mathrm{pg}(8, 20, 2)$$

was also given in Chapter 4, and in Chapter 2 the parameters of its associated strongly regular graph

$$\mathrm{srg}(729, 168, 141, 42)$$

and bounds for its associated LDPC code

$$n = 1701$$
$$d \geq 10$$
$$r \geq 1140$$
$$T_6 = 408240$$

were given.

Chapter 6

Future work

We now collect some interesting open topics related to the previous work.

6.1 Combinatorics and non-existance of maximal arcs

Projective planes were defined in Chapter 1 by having an underlying finite field as their coordinate system. One can also define a projective plane P in a purely combinatorial way by demanding three axioms [12]:

- Each two points are joined by exactly one line.
- Each two lines meet in exactly one point.
- There are at least two lines and each line contains at least three points.

An immediate consequence of these axioms is that each line contains a constant number $\mathcal{O}+1$ of points. We call $\mathcal{O}$ the *order* of the projective plane.

If Desargues' Theorem holds in an axiomatic projective plane P, then there must be an underlying finite field acting as a coordinate system for P; and if P has an underlying finite field acting as a coordinate system, then Desargues' Theorem holds. We refer to [4] for details.

There are finite projective planes P where Desargues' Theorem does not hold.

Given the hard algebraic nature of the proof why maximal arcs in projective planes $\mathsf{PG}(2,\mathsf{q})$ with q odd cannot exist, it would be desirable to extend it into a

more combinatorial reasoning. This might allow to prove non-existence of maximal arcs in projective planes that do not have an underlying finite field.

As seen in [39], by considering the internal structure of a possible projective plane of order 10, it was possible to determine the non-existance of such a plane. With this in mind, such a combinatorial proof would provide insight on the internal structure of projective planes, and so could possibly be used in determining whether or not projective planes can only exist when their order is the power of a prime.

6.2 Building impossible maximal arcs

Given Mathon's construction for maximal arcs given in Chapter 3, it would be of interest to find a similar construction for perp-systems, since perp-systems generalize maximal arcs into higher dimensions.

Moreover, because maximal arcs cannot exist in $\mathsf{PG}(2,\mathsf{q})$ with q odd [7], such a construction would be of particular interest when the perp-system is built in $\mathsf{PG}(\mathsf{n},\mathsf{q})$ with q odd and $n > 2$. In particular, we focus on q a power of 3.

We analyze the example of the 21 lines in $\mathsf{PG}(5,3)$ to arrive at a possible construction.

6.2.1 Analysis of the 21 lines

As mentioned in Chapter 2, a maximal arc in $\mathsf{PG}(2,9)$ would have 21 points. Following Mathon's construction, we could come up with the point set of a cubic polynomial F and its nucleus F_0 where F has 10 points [6].

The next step would be to find another cubic polynomial F' with 10 points and nucleus F_0 such that the point set of $\{F \cup F' \cup F_0\}$ would yield 21 points, and every line intersects in 0 or 3 points. We know this cannot be the case, so we try to fix it in $\mathsf{PG}(5,3)$.

Consider the blow up of $\mathsf{PG}(2,9)$ into $\mathsf{PG}(5,3)$. The image of the zeros of F and F_0 under the blow up yields 11 lines.

Also following Mathon's construction, the operation $\oplus$ acts as a movement of the conics fixing their nucleus, so it would be interesting to see if there is a way

to move the 11 lines fixing the image of F_0 to get 21 lines total in $\mathsf{PG}(5,3)$ that form a perp-system.

6.2.2 Recipe for what would be an impossible maximal arcs

We summarise the mentioned construction. Let $\mathsf{PG}(2,3^{\mathsf{h}})$ be our projective plane. We want to build a perp-system $\mathcal{R}(r)$ in $\mathsf{PG}(2\cdot\mathsf{h}-1,3)$ with

$$|\mathcal{R}(r)| = 3^{h+m} - 3^h + 3^m$$

where $r = 1$ and $m < h$.

- Consider a cubic polynomial F with $3^h + 1$ points in $\mathsf{PG}(2,\mathsf{q})$ and a nucleus F_0 (such polynomials exist [6]). Call $\mathcal{K}'$ the pointset of $F \cup F_0$.
- Blow up $\mathsf{PG}(2,3^{\mathsf{h}})$ into $\mathsf{PG}(2\cdot\mathsf{h}-1,3)$ and consider $\mathsf{B}(\mathcal{K}')$ the image of $\mathcal{K}'$ under the blow up consisting of 3^h+2 disjoint $(h-1)$-dimensional subspaces.
- Move $\mathsf{B}(\mathcal{K}')$ fixing F_0 in some "smart" way to get a total of:

  $$y(3^h+1)+1 = 3^{h+m} - 3^h + 3^m \tag{6.1}$$

  disjoint $(h-1)$-dimensional subspaces satisfying the conditions for a perp-system $\mathcal{R}(1)$ as in Chapter 4. From equation 6.1 we see that such a movement would have to have an order of at least $y = 3^m - 1$:

  $$(3^m-1)(3^h+1)+1 = 3^{h+m} - 3^h + 3^m.$$

Bibliography

[1] Simeon Ball, Zsuzsa Weiner. *An introduction to Finite Geometry*. 2011.

[2] A. Barlotti. *Sui k;n-Archi di un Piano Lineare Finito*. Boll. Un. Mat. Ital., 11:553-556, 1956.

[3] S.E. Payne, J.A. Thas. *Finite Generalized Quadrangles*. European Mathematical Society, 2009.

[4] Johannes Ueberberg. *Foundations of Incidence Geometry, Projective and Polar Spaces*. Springer, 2011.

[5] Burkhard Polster. *A geometrical picture book*. Universitext, Springer, 1998.

[6] J. W. P. Hirschfeld. *Projective Geometries over Finite Fields*. Oxford, 1998.

[7] Simeon Ball and Aart Blokhuis. *An easier proof of the maximal arcs conjecture*. Proc. Amer. Math. Soc. 126:3377-3380, 1998.

[8] Simeon Ball, Aart Blokhuis and Francesco Mazzocca. *Maximal Arcs in Desarguesian Planes of Odd Order do not Exist*. Combinatorica, 17(1):31-41, 1997.

[9] R. Calderbank and W. M. Kantor. *The geometry of two-weight codes*. Bulletin of the London Mathematical Society, 18(2):97-122, 1986.

[10] Frank De Clerck, Mario Delanote, Nicholas Hamilton and Rudolf Mathon. *Perp-systems and partial geometries*. Advances in Geometry, 2:1-12, 2002.

[11] John Bamberg and Frank De Clerck. *A geometric construction of Mathon's perp-system from four lines of PG(5,3).* Journal of Combinatorial Designs, 18(6):450-461, 2010.

[12] A. Klein, L. Storme. *Applications of finite geometry in coding theory and cryptography*. University of Ghent.

[13] Frank de Clerck. *Constructions and Characterizations of (Semi)partial Geometries*. University of Ghent, 1997.

[14] Markus Stroppel. *An affine proof of uniqueness for the smallest generalized quadrangles, including the determination of their automorphism groups*. Note di Matematica, 27(1):153-169, 2007.

[15] Willem H. Haemers and Edward Spence. *The Pseudo-Geometric Graphs for Generalised Quadrangles of Order (3,t)*.

[16] B.S. Ruffer, C.M. Kellett, P.M. Dower and S.R. Weller. *Belief propagation as a dynamical system: the linear case and open problems*. IET Control Theory and Applications, 4(7):1188, 2010.

[17] R. Michael Tanner. *Minimum distance bounds by graph analysis*. IEEE Trans. Inform. Theory, 47:808-821, 2001.

[18] Sarah J. Johnson and Steven R. Weller. *Codes for iterative decoding from partial geometries*. IEEE Trans. Commun, pages 236-243, 2004.

[19] Robert G. Gallager. *Low-Density Parity-Check Codes*. 1963.

[20] Peter J. Cameron. *Strongly regular graphs*. 2001.

[21] Elisabeth Kuijken. *A Study of Incidence Structures and Codes related to Regular Two-Graphs*. Universiteit Gent, May, 2003.

[22] Thomas Maes. *A geometric approach to Mathon maximal arcs*. Universiteit Gent, April, 2011.

[23] Beukje Temmermans. *Dualities and Collineations of Projective and Polar Spaces and of Related Geometries*. Universiteit Gent, January, 2010.

[24] Cristina Tonesi. *Distance-regular geometries and some group theoretical characterisations of (0,2)-geometries*. Universiteit Gent, March, 2005.

[25] Frank de Clerk. *Partial and semipartial geometries: an update*. Discrete Mathematics, 267(1-3):75-86, 2003.

[26] R.H.F. Denniston. *Some maximal arcs in finite projective planes*. Journal of Combinatorial Theory, 6(3):317-319, 1969.

[27] Rudolf Mathon. *New Maximal Arcs in Desarguesian Planes*. J. Comb. Theory, Ser. A, 97(2):353-368, 2002.

[28] Peter Vandendriessche. *LDPC codes arising from partial and semipartial geometries*. WCC 2011 - Workshop on coding and cryptography, pages 419-428, Paris, France, April, 2011.

[29] J.A. Thas. *Construction of Maximal Arcs and Dual Ovals in Translation Planes*. European Journal of Combinatorics, 1(2):189-192, 1980.

[30] J.A. Thas. *Construction of maximal arcs and partial geometries*. Geometriae Dedicata, 3(1):61-64, 1974.

[31] Klaus Pommerening. *Quadratic Equations in Finite Fields of Characteristic 2*. `http://www.staff.uni-mainz.de/pommeren/MathMisc/QuGlChar2.pdf`, 2000.

[32] Wolfram Research, Inc. *Mathematica*. Version 10.0, Champaign, IL. 2014.

[33] W. A. Stein et al., *Sage Mathematics Software (Version 10.9)*, The Sage Development Team, 2014, `http://www.sagemath.org`.

[34] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma algebra system. I. The user language*. J. Symbolic Comput., 24:235-265, 1997.

[35] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.7.5*; 2014, `http://www.gap-system.org`

[36] John Bamberg, Anton Betten, Philippe Cara, Jan De Beule, Michel Lavrauw, Max Neunhoeffer. *FinInG, Finite Incidence Geometry - a GAP package*. Version 1.0, September 2013. `http://cage.ugent.be/geometry/fining.php`

[37] David Dummit and Richard M Foote. *Abstract algebra*. John Wiley & sons. Hoboken, NJ. 2004.

[38] Gareth A. Jones and J.M. Jones. *Information and Coding Theory*, Springer-Verlag New York, Inc. Secaucus, NJ, USA. 2000.

[39] C. W. H. Lam, L. Thiel and S. Swiercz. *The Non-existence of Finite Projective Planes of Order 10*. 1989.

[40] W. Haemers. *A new partial geometry constructed from the HoÂ¤man-Singleton graph*. Finite geometries and designs (Proc. Conf., Chelwood Gate, 1980), 119-127. Cambridge Univ. Press, 1981.