University of New Brunswick
Saint John

Faculty of Science, Applied Science, and Engineering

Math 4200: Honours Project

The upper bound of general Maximum Distance Separable codes

Svenja Huntemann

Supervisor: Dr. Tim Alderson

May 28, 2012
Contents

1 Introduction 1
   1.1 Motivation ................................................. 1
   1.2 Definitions ............................................... 3
      1.2.1 MDS codes ........................................... 3
      1.2.2 Latin Squares, Orthogonal Arrays, and Transversal Designs 4
      1.2.3 BIBD and Steiner Triple Systems ......................... 5
      1.2.4 Finite Geometry ...................................... 6
   1.3 Constructs equivalent to MDS codes ......................... 7
   1.4 Properties of MDS codes .................................. 9
   1.5 Short History ............................................. 11
      1.5.1 Singleton bound and MDS codes ......................... 11
      1.5.2 Latin Squares ....................................... 12
      1.5.3 Orthogonal arrays ................................... 13
      1.5.4 Steiner Triple Systems and BIBD ....................... 13
      1.5.5 Bruck nets .......................................... 13

2 Upper bounds on MDS codes 14
   2.1 Extending MDS codes .................................... 14
   2.2 General upper bounds on MDS codes ....................... 15

3 Upper bounds on linear MDS codes 18
   3.1 Main Conjecture for linear MDS .......................... 18
   3.2 The known results ...................................... 18

4 2-dimensional case 21
   4.1 General .................................................. 21
   4.2 Bruck’s completion theorem ............................... 22
   4.3 Prime power conjecture .................................. 22
   4.4 Range of $M(2, q)$ for $q \leq 100$ .................... 23

5 General MDS codes 24
   5.1 Main Conjecture for general MDS ......................... 24
   5.2 $k = 3$ ................................................. 24
   5.3 $k = 4$ ................................................. 25
List of Tables

2.1 General upper bounds on the length of MDS codes . . . . . . . . 17
4.1 Range of $M(2,q)$ for $q \leq 100$ . . . . . . . . . . . . . . . 23
5.1 Upper bounds for $q \leq 100$ . . . . . . . . . . . . . . . 30
Acknowledgements

Many thanks go to my supervisor Dr. Tim L. Alderson for his encouragements, ideas, and explanations.

I also have to thank the Faculty of Science, Applied Science, and Engineering and the Department of Mathematical Sciences for granting me permission to finish my degree at the Saint John campus.

Thanks go to my family as well for supporting me all the way while writing this thesis.
Abstract

A maximum distance separable (MDS) code has $q^k$ codewords of length $n$ over an alphabet of size $q$ and meets the singleton bound for block codes, therefore the minimum (Hamming) distance of the code is given by $d = n - k + 1$.

The main research problem is finding the maximum possible length $n$ if the alphabet size $q$ and the dimension $k$ are fixed.

For linear MDS codes, we give a summary of the current state of the research. For the general, not necessarily linear, case an extensive list of the known upper bounds is given, and we investigate using the partition weight enumerator as a technique to improve the upper bounds.
Chapter 1

Introduction

For any citations given, the objective was to choose the paper or book that first published the result, both for theorems and in the history section.

1.1 Motivation

A \( q \)-ary code \( C \) of length \( n \) and minimum distance \( d \) is a collection of \( n \)-tuples (codewords) over an alphabet of size \( q \) such that any two codewords have at most \( n - d \) common coordinates, and some pair of codewords does in fact have \( n - d \) common coordinates. That is to say, the minimum Hamming distance of the code is \( d \). When \( C \) is comprised \( q^k \) codewords, for some integer \( k \), we say \( C \) has dimension \( k \).

The main coding theory problem [16, Section 18.9] is to maximize the number of codewords when the minimum distance, the alphabet size, and the length of a code are fixed. As the number of codewords increases in a code, the number of messages that can be transmitted increases. Since this is bounded by the Singleton bound, and Maximum Distance Separable (MDS) codes meet this bound by their definition, MDS codes are a solution to the main coding theory problem. This is why they are also sometimes called optimal codes.

Another important goal in coding theory is to maximize the minimum distance \( d \) for given alphabet size and number of codewords. This increases the number of errors that can be detected or corrected, thus making the transmission more reliable. In MDS codes, when the dimension \( k \) and the alphabet size \( q \) are fixed (thus the number of codewords), the minimum distance \( d \) is proportional to the length \( n \) of the code. Therefore, it is important to know what the maximum length for an MDS code is when \( k \) and \( q \) are given. This value is denoted by \( M(k, q) \) and chapters 2-5 concern results on this upper bound.

A third goal in coding theory is to minimize the length of the code as this decreases the time (and cost) needed for transmission. This is contradictory to maximizing the minimum distance for MDS codes (as just stated, the distance and length are proportional when the size of the code is given). But in
cases where the transmission cost and time are not an issue, the reliability of the transmission is important though, one wants to use the longest MDS code possible, thus the search for $M(k, q)$.

Simeon Ball [5] recently proved the main conjecture for linear MDS codes is true for all cases where $q$ is prime. The main conjecture states that the upper bound on linear MDS codes is $M(k, q) = q + 1$ if $k \leq q$, except for $M(k, q) = q + 2$ if $k = 3$ or $q - 1$ and $q$ is even. The value of $M(k, q)$ is now known for the majority of cases when the MDS code is linear. On the other hand, the general case is almost completely open as very little is known. The main goal of this paper is to summarize/survey all results on MDS codes (not necessarily linear) related to the main conjecture; to show where more work is needed; and also to introduce a new method for proving an upper bound on $M(k, q)$ using the partition weight enumerator and balanced incomplete block designs.

Since MDS codes meet the singleton bound, they also have the highest possible minimum distance (therefore Maximum Distance separable) for given alphabet size $q$ and length $n$. They therefore have the highest error-detection, error-correction, and erasure-correction capability. This is very important in industry and it thus legitimizes further research on MDS codes.

Reed-Solomon (RS) codes, a specific form of linear MDS codes, are used frequently in situations where bursts of errors occur, or a combination of random and bursts of errors. They are “the main codes used in industry” and their “applications are everywhere” [10]. For example, most CDs use cross-interleaved Reed-Solomon coding (CIRC) [73, Ch. 4] for error correction. RS codes are also used for DVDs and Blu-Ray discs, bar codes, digital TV, xDSL, digital video broadcasting, and deep-space and satellite communication [73, 34]. One of the first big uses of RS codes was during the Voyager mission to improve the quality of pictures sent from Uranus and Neptune [73, Ch. 3].

Sudan and Guruswami [29] constructed an efficient algorithm in 1999 that increases the error-correctability of RS codes beyond the error correction bound ($e = \lfloor \frac{d-1}{2} \rfloor$). See also [65]. This makes RS codes even more valuable for the industry, and more research has been done into constructing even better decoding algorithms.

MDS codes, not necessarily linear, can also be used to construct $(S, T)$ threshold sharing schemes. In 2003 Pieprzyk and Zhang [45] constructed these using linear MDS codes. The scheme, as described by Bruen and Forcinito for general MDS codes in [10], uses the property that any $k$ entries will uniquely determine a code word, while $k - 1$ or less do not. In this setting, longer codewords allow for a greater number of participants in the “shared secret”. MDS codes and the main conjecture are thus also of interest to people working in cryptography or security.
1.2 Definitions

1.2.1 MDS codes

Definition 1.1. A $q$-ary (block) code $C$ of length $n$ is a collection of $n$-tuples, called codewords, with elements from a set $A$ of size $q$, called the alphabet, thus $C \subseteq A^n$. Usually the size of the code is a power of $q$, i.e. $|C| = q^k$, where $k$ is called the dimension of the code.

A code is linear if its codewords form a $k$-dimensional subspace of the vector space $F_q^n$ where $F_q$ is the alphabet.

Definition 1.2. The Hamming distance $d(x, y)$ between two codewords $x$ and $y$ is the number of coordinates in which they differ. The minimum Hamming distance of a code $C$ is $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$.

During transmission of data, errors might be introduced into the message. This can be overcome by adding redundancy. Using this redundancy, we can either detect if an error has occurred and then request re-transmission (if possible), or in the ideal case we might even be able to correct the error and receive the original message. This is called error detection and error correction.

Proposition 1.1. A code $C$ with minimum distance $d$ can detect up to $d - 1$ errors and can correct up to $\lfloor \frac{d-1}{2} \rfloor$ errors.

For a short proof see for example [16].

Definition 1.3. Let $C$ be a code and $c \in C$. The support of $c$ (denoted $\text{supp}(c)$) is defined as
\[ \text{supp}(c) = \{ n_i \mid c_{n_i} \neq 0 \} \]
(i.e. $\text{supp}(c)$ is the collection of coordinate positions in which $c$ has non-zero entries).

Definition 1.4. The weight $\text{wt}(c)$ of a codeword $c$ is defined by $\text{wt}(c) = |\text{supp}(c)|$. If the zero codeword is included in the code, we have $\text{wt}(c) = d(c, 0)$.

Theorem 1.2. The number of codewords for a code $C$ over an alphabet of size $q$, length $n$, and minimum (Hamming) distance $d$ is bounded by
\[ |C| \leq q^{n-d+1} \]
This is known as the singleton bound.

For a short proof see [16]. The singleton bound is sometimes also called the MDS bound (see [16] Thm. 18.20) or even the Joshi bound (see [21] section 10.1).

Definition 1.5. A code for which the singleton bound holds with equality is known as Maximum Distance Separable (MDS) code. Thus an MDS code has $q^k$ codewords of length $n$ over an alphabet of size $q$ with minimum Hamming
distance \( d = n - k + 1 \). This is equivalent to the statement that all codewords agree in at most \( k - 1 \) coordinates.

A linear MDS code is an MDS code with the alphabet being \( \mathbb{F}_q \), where \( q \) is a prime power, and the codewords form a \( k \)-dimensional subspace of the vector space \( \mathbb{F}_q^n \).

An MDS code is denoted by \( (n, k, n - k + 1)_q \) herein, and a linear MDS code is denoted by \([n, k, n - k + 1]_q\).

**Definition 1.6.** The dual code \( C^\perp \) of an \( [n, k, d]_q \)-code \( C \) is defined by

\[
C^\perp = \{ x \in \mathbb{F}_q^n \mid x \cdot c = 0 \ \forall c \in C \}
\]

Therefore \( C^\perp \) is the collection of vectors in \( \mathbb{F}_q^n \) which are orthogonal (with respect to the usual dot product) to the codewords in \( C \).

**Definition 1.7.** A generator matrix \( G \) of a linear code \( C \) is a \( k \times n \) matrix whose rows are a basis for \( C \). A parity check matrix \( H \) is a generator matrix of the dual code \( C^\perp \). \( H \) has dimensions \( (n - k) \times n \). The two matrices are related through \( GH^T = 0 \) and \( HG^T = 0 \).

**Definition 1.8.** Two MDS codes are called equivalent if one can be constructed from the other by a series of

1. symbol permutations: fix a coordinate position and apply a permutation over the alphabet to all the elements of that position
2. positional permutations: choose two coordinate positions and exchange their entries in every codeword

It follows that an arbitrary MDS code \( C \) is equivalent to an MDS code \( C' \) containing the all zero codeword by converting any codeword \( c \in C \) to the zero codeword. Hence we may assume without loss of generality that \( C \) contains the zero codeword. In the sequel we shall make great use of this observation.

**Proposition 1.3.** If \( C \) is an \( (n, k, d)_q \) MDS code, then \( C \) is equivalent to an \( (n, k, d)_q \) MDS code \( C' \) containing the zero codeword.

**Definition 1.9.** The weight enumerator \( E(w) \) for a code \( C \) counts the codewords of a given weight \( w \). That is

\[
E(w) = |\{ c \in C : \text{wt}(c) = w \}|
\]

### 1.2.2 Latin Squares, Orthogonal Arrays, and Transversal Designs

**Definition 1.10.** A latin square of order \( n \) is a \( n \times n \) array with entries from the set \( \{1, \ldots, n\} \) such that each element appears exactly once in each row and exactly once in each column. Two latin squares are orthogonal if, when one is superimposed on the other, each ordered pair appears exactly once. A collection of latin squares is called a set of mutually orthogonal latin squares (MOLS) if they are pairwise orthogonal.
**Definition 1.11.** A latin rectangle is a $n \times k$ array ($k < n$) with entries from the set $\{1, \ldots, n\}$ such that each element appears exactly once in each of the $k$ columns and at most once in each of the $n$ rows.

Two latin rectangles are orthogonal if, when one is superimposed on the other, each ordered pair appears at most once. A set of latin rectangles is called mutually orthogonal if they are pairwise orthogonal.

The definition for a latin hypercube varies in the literature depending on the use. The following definition is chosen for the equivalence with MDS codes.

**Definition 1.12.** An $r$-dimensional latin hypercube of order $n$ is an $n \times n \times \ldots \times n$ array with entries from the set $\{1, \ldots, n\}$ such that if $r - 1$ coordinates are fixed each of the $n$ symbols appears exactly once in the remaining coordinates.

A set of $s$ hypercubes is called mutually $t$-wise orthogonal if when any $t \leq s$ hypercubes are superimposed each $t$-tuple appears exactly $n^{r-t}$ times.

Therefore, a 2-dimensional hypercube is a latin square. A 3-dimensional hypercube is a cube such that each row-plane, column-plane and layer is a latin square [61]. A latin hypercube with this definition is also called a permutation cube [39, Section 3.1].

**Definition 1.13.** An orthogonal array $\text{OA}[N, k, s, t]$ is a $k \times N$ array with entries from an alphabet of size $s$ such that each $t \times N$ subarray contains each $t$-tuple exactly $\lambda$ times as a column. $t$ is the strength of the array, $N = \lambda s^t$ is the size, $\lambda$ is the index, $k$ the number of constraints, and $s$ the number of levels.

**Definition 1.14.** A transversal design $\text{TD}_\lambda(k, n)$ of group size $n$, block size $k$, and index $\lambda$ is a design with

1. $kn$ elements divided into $k$ groups of size $n$
2. blocks of size $k$ which are subsets of the $kn$ elements
3. each unordered pair of elements is part of exactly one group or exactly $\lambda$ blocks, but not both.

### 1.2.3 BIBD and Steiner Triple Systems

**Definition 1.15.** A $(v, b, r, k, \lambda)$ balanced incomplete block design (BIBD) is a collection of $b$ subsets of size $k$ of a finite set $S$ with $v$ elements where each element belongs to $r$ of the subsets, and each pair of elements belongs to $\lambda$ of the subsets. The elements are called treatments, the subsets of size $k$ are called blocks, $r$ is the replication number, and $\lambda$ the covalency. A BIBD is called symmetric if $v = b$.

A BIBD with $k = 3$ is called a triple system. If $k = 3$ and $\lambda = 1$, the design is called a Steiner Triple System (STS).

**Proposition 1.4.** 1. In a balanced incomplete block design $(v, b, r, k, \lambda)$ the following hold:
(a) \( bk = vr \)
(b) \( \lambda(v - 1) = r(k - 1) \)

2. A Steiner triple system exists if and only if \( v \equiv 1,3 \pmod{6} \).

Proof. For 1. see for example [65]. For the if direction of 2. see [35] or [57], the only if follows directly from the definition and the equalities in 1. \( \square \)

Note. To avoid confusion between the dimension of an MDS code and the block size of a BIBD, the block size is herein denoted by \( K \).

1.2.4 Finite Geometry

Definition 1.16. A (Bruck) net \( N \) of degree \( n \) and order \( q \) is an incidence structure of points and lines such that the following are met:

1. every line contains exactly \( q \) points;
2. there are \( n \) parallel classes of \( q \) lines each;
3. any two lines that are not parallel meet in exactly one point;
4. each point is on exactly one line of each parallel class.

The net then has \( q^2 \) points and \( qn \) lines.

Definition 1.17. A finite net \( N \) of degree \( n \), order \( q \), and dimension \( k \) is an incidence structure of points and lines such that the following are met:

1. every line contains exactly \( q^{k-1} \) points;
2. there are \( n \) parallel classes of \( q \) lines each;
3. every \( k \) lines belonging to pairwise distinct classes meet in exactly one point;
4. each point is on exactly one line of each parallel class.

The net then has \( q^k \) points and \( qn \) lines.

Thus a finite net of dimension 2 is a Bruck net.

Definition 1.18. An affine plane of order \( n \) is a finite incidence structure of points and lines satisfying the following axioms:

1. any two distinct points are incident with exactly one line;
2. given a line \( l \) and a point \( P \) not incident with the line, there is exactly one line through \( P \) that is parallel to \( l \) (has no points in common);
3. 3 points exists that are not all collinear.
There are exactly \( n \) points on each line, the order of the affine plane. The affine plane has exactly \( n^2 \) points, \( n^2 + n \) lines, and \( n + 1 \) lines through each point.

**Definition 1.19.** A **projective plane** of order \( n \) is a finite incidence structure of points and lines satisfying the following axioms:

1. any two distinct points are incident with exactly one line;
2. any two distinct lines are incident with exactly one point;
3. there exist four points of which no three are collinear.

There are exactly \( n + 1 \) points on each line. The finite projective plane has exactly \( n^2 + n + 1 \) points and \( n + 1 \) lines through each point.

**Definition 1.20.** A **projective space** is an incidence structure of points and lines satisfying the following:

1. any two distinct points are incident with exactly one line;
2. any line has at least three points;
3. given two lines \( l \) and \( m \) which intersect at \( P \) and the points \( Q \) and \( R \) on \( l \) and \( S \) and \( T \) on \( m \), the line passing through \( R \) and \( T \) intersects with the line through \( Q \) and \( S \).

A finite projective space is a projective space with finitely many points, and each line contains \( k + 1 \) points, where \( k \) is called the order of the projective space.

\( \text{PG}(N, q) \) denotes a projective space of dimension \( N \) over \( \mathbb{F}_q \), where \( q \) a prime power is the order.

**Definition 1.21.** A **\( n \)-arc** in \( \text{PG}(N, q) \) is a set of \( n \) points with at most \( N \) in any hyperplane of \( \text{PG}(N, q) \).

Normal Rational Curves in \( \text{PG}(N, q) \) \cite{32} and conics in \( \text{PG}(2, q) \) \cite{31}, are examples for \( (q + 1) \)-arcs.

### 1.3 Constructs equivalent to MDS codes

**Proposition 1.5.** The following are equivalent:

1. A \( (n, k, d)_q \) MDS code;
2. An orthogonal array with index \( \lambda = 1 \), strength \( k \), \( q \) levels, size \( q^k \), and \( n \) constraints;
3. \( (d - 1) \) mutually \( k \)-wise orthogonal \( k \)-dimensional latin hypercubes of order \( q \);
4. A finite net of degree $n$, order $q$, and dimension $k$.

Proof. One can construct hypercubes from MDS codes in the following way: Let $C$ be an $(n, k, d)\_q$ MDS code. If $C$ is not over the alphabet $A = \{1, \ldots, n\}$, construct an equivalent MDS code over this alphabet. Then for each $x = (a_1, \ldots, a_n) \in A^n$ there exists exactly one codeword $c \in C$ such that $c_i = a_i$, $1 \leq i \leq k$. Let $\Phi(x) = c$ be this unique codeword. For $j = 1, \ldots, d-1$ define the mutually orthogonal latin hypercubes $L_i = (l_{x})$ by $l_x = c_{k+i}$ where $c = \Phi(x)$. It is readily verified that the set $L_1, \ldots, L_{d-1}$ are mutually $k$-wise orthogonal $k$-dimensional latin hypercubes of order $q$.

MDS codes can be constructed from $(d-1)$ mutually $k$-wise orthogonal $k$-dimensional latin hypercubes of order $q$ in a similar way.

For equivalence between 1. and 4. and between 1. and 2. see [61]. □

Proposition 1.6. The following are equivalent:

1. A $(n,2,d)\_q$ MDS code;
2. A (Bruck) net of degree $n$ and order $q$;
3. $n-2$ MOLS of order $q$;
4. A transversal design with index one, block size $n$, and group size $q$.

Proof. Between 1. and 2. see [16]. Between 2. and 3. see [14]. Between 3. and 4. see [19]. □

Using this we also get:

Corollary 1.7. [14] An MDS code with $k = 2$ and $n = q + 1$ is equivalent to an affine plane of order $q$.

Proposition 1.8. The following are equivalent:

1. A linear $[n,k,d]_q$ MDS code;
2. A $n$-arc in $PG(k-1,q)$;
3. $n$ vectors in a $k$-dimensional vector space over $GF(q)$ such that any $k$ vectors of the $n$ form a basis.

Proof. The equivalence between 1. and 2. is given in [41]. For the equivalence between 1. and 3. see [42]. □

Because of all these equivalences any results on MDS codes might also be interesting for researchers working in different areas, for example finite geometries and statistics.
1.4 Properties of MDS codes

**Proposition 1.9.** The following are equivalent:

1. A linear code $C$ is an $[n, k, n - k + 1]_q$ MDS code.

2. Any $(n - k)$ columns of the parity check matrix of a linear code $C$ are independent.

3. The dual code of $C$ is an $[n, n - k, k + 1]_q$ MDS code.

4. Any $k$ columns of the generator matrix of a linear code $C$ are independent.

**Proof.** See [41, Theorems 10.1, 10.2, Corollary 10.3].

That the dual code of a linear MDS code is also an MDS code has been very useful in determining the upper bound on the length of linear MDS codes.

**Note.** Let $C$ be an $(n, k, d)_q$ MDS code. If one fixes $k$ coordinate positions and $k$ symbols from the alphabet, then there will be exactly one codeword with the $k$ symbols in the fixed positions. More generally we have:

**Theorem 1.10.** [61] Let $C$ be an $(n, k, d)_q$ MDS code. If one fixes $r \leq k$ coordinate positions $\{i_1, \ldots, i_r\}$ and $r$ symbols $\{\alpha_1, \ldots, \alpha_r\}$ from the alphabet, then there will be exactly $q^{k-r}$ codewords with $\alpha_1$ in position $i_1$, $\alpha_2$ in position $i_2$, and so forth up to $\alpha_r$ in position $i_r$.

**Proposition 1.11.** Let $C$ be an $(n, k, d)_q$ MDS code containing the zero codeword. Then $d = \min \{ wt(c) \mid c \in C \setminus \{0\} \}$.

**Proof.** Let $c \in C \setminus \{0\}$ be any codeword. If $wt(c) = w < d$, then $d(c, 0) = w$ is a contradiction to $d$ being the minimum distance of the code. Thus $wt(c) \geq d$ for all $c \in C \setminus \{0\}$.

Let $\alpha \neq 0$ be an element of the alphabet. By Theorem 1.10 there exists a codeword $c \in C$ such that $c_1 = \alpha$ and $c_2 = \ldots = c_k = 0$. For $j = k + 1, \ldots, n$, knowing $wt(c) \geq d$, we have $c_j \neq 0$. Thus $wt(c) = d$ for this codeword.

Using $wt(c) \geq d$ for all $c \in C \setminus \{0\}$ and at least one codeword exists for which equality holds, the result is proven.

**Note.** For linear MDS codes the proof for this theorem is easier, see for example [41, Theorem 1.1]

**Theorem 1.12.** [70] The weight distribution for MDS codes which contain the zero codeword is completely determined: $E(0) = 1$; for $0 < w < d$, $E(w) = 0$; and for $d \leq w$

$$E(w) = (q - 1) \binom{n}{w} \sum_{j=0}^{w-d} (-1)^j \binom{w-1}{j} q^{w-d-j}$$

(1.1)
Proof. Let \( C \) be an \((n, k, d)\)-MDS code. The only codeword with weight 0 is the all zero codeword, thus \( E(0) = 1 \). From Proposition 1.11 \( wt(c) \geq d \) for all \( c \in C \setminus \{0\} \), therefore \( E(w) = 0 \) if \( 0 < w < d \). The proof for \( d \leq w \) is as follows:

Fix \( w \) positions, say \( W = \{i_1, \ldots, i_w\} \), and let \( N \) be the number of codewords with support \( W \), i.e. \( N = |\{c \in C \mid supp(c) = W\}| \). Then for \( S \subseteq W \), let \( A_S = \{c \in C \mid c \neq 0, supp(c) \subseteq W \setminus S\} \). First, observe that if \( |S| \geq k - (n - w) = w - d + 1 \), then \( |A_S| = 0 \). Second, if \( |S| = t \leq w - d \), then by Theorem 1.10

\[
|A_S| = q^{k-(n-w+t)} - 1
= q^{w-d-t+1} - 1.
\]

For each \( i, 0 \leq i \leq w \), let \( A_i \) be the number of ordered pairs \((S, c)\) where \( S \subseteq W, |S| = w - i, c \in C, supp(c) \subseteq W \setminus S \). It follows by the principle of inclusion-exclusion that

\[
N = \sum_{j=0}^{w} (-1)^j A_j
= \sum_{j=0}^{w-d} (-1)^j A_j
= \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d-j+1} - 1).
\]

Therefore

\[
E(w) = \left(\begin{array}{c} n \\ w \end{array}\right) \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d-j+1} - 1),
\]

which can be rearranged to the original statement. \qed

The weight enumerator can also be generalized (see [25]). To do this, partition the coordinate set \( \{1, \ldots, n\} \) into \( s \) (pairwise disjoint) subsets \( T_1, \ldots, T_s \) such that \( |T_i| = n_i \) for \( i = 1, \ldots, s \). Define \( w_i = |supp(c) \cap T_i| \) for a fixed \( c \in C \).

El-Khamy and McEliece denoted this partition by \( T \), and defined the \( T \)-weight profile for any \( c \in C \) as \( W_T(c) = (w_1, \ldots, w_s) \).

Definition 1.22. The \textbf{partition weight enumerator} for a code \( C \) with partition \( T \) and associated weight profile \((w_1, \ldots, w_s)\) is given by:

\[
A^T(w_1, \ldots, w_s) = |\{c \in C : W_T(c) = (w_1, \ldots, w_s)\}|.
\]

Theorem 1.13. [25] [75] Let \( C \) be an \((n, k, d)_q\) MDS code with the all zero codeword and let \( T = \{T_1, \ldots, T_s\} \) be a partition with associated weight profile \((w_1, \ldots, w_s)\). Then the partition weight enumerator is given by

\[
A^T(w_1, \ldots, w_s) = E(w) \frac{n_1}{w_1} \frac{n_2}{w_2} \cdots \frac{n_s}{w_s} \quad (1.2)
\]

where \( w = \sum_{i=1}^s w_i \) and \( E(w) \) the weight enumerator as above.
CHAPTER 1. INTRODUCTION

The following is an alternative proof to the one given by El-Khamy and McEliece.

**Proof.** Fix \( w \) support positions and as in the proof of Theorem 1.12 there are \( \sum_{j=0}^{w-d} \binom{w}{j}(-1)^j(q^{w-d+1-j}-1) \) codewords with exactly those support positions. There are \( \binom{n_1}{w_1}\binom{n_2}{w_2}\ldots\binom{n_s}{w_s} \) ways to fix the \( w \) support positions satisfying the partition and weight profile, such that

\[
A^T(w_1,\ldots,w_s) = \binom{n_1}{w_1}\binom{n_2}{w_2}\ldots\binom{n_s}{w_s} \sum_{j=0}^{w-d} (-1)^j \binom{w}{j} (q^{w-d+1-j}-1)
\]

and by using equation 1.1 we get the statement. \( \square \)

The following results are important properties of MDS codes when proving upper bounds on the length.

**Theorem 1.14.** [61] If a \((n,k,d)\) MDS code exists, then a \((n-1,k,d-1)\) MDS code exists.

**Theorem 1.15.** [42] If a \((n,k,d)\) MDS code exists, then a \((n-1,k-1,d)\) MDS code exists.

**Proposition 1.16.** [61] Let \( x \) and \( y \) be two codewords of an \((q+k-1,k,d)\) MDS code. If \( d(x,y) \leq q+1 \) then \( d(x,y) = q \).

### 1.5 Short History

The following will give a short history of the important concepts and the constructs equivalent to MDS codes. The influence of these concepts becomes more clear as one looks at the immense work in each of these areas.

#### 1.5.1 Singleton bound and MDS codes

MacWilliams and Sloane called MDS codes “one of the most fascinating chapters in all of coding theory” in their reputable book “The Theory of Error-Correcting Codes” [41].

Shannon [59] started the area of information theory with his paper in 1948. Hamming [30] coined the term coding theory in 1950 and in the same paper also introduced many of the important concepts.

The singleton bound was first proven for the binary case by Komamiya [38] in 1954, and then again by Joshi [33] in 1958. Dénes and Keedwell [21] remarked that the proof by Joshi also holds in the general \( q \)-ary case.

The first few results on MDS codes are by Bush [18] in 1952 through orthogonal arrays, and by Silverman [61] in 1960.

Reed-Solomon codes were introduced in 1960 by Reed and Solomon [54], having roots in a construction of Bush [18] in 1952. For a more complete history of Reed-Solomon codes and their applications see [73].
Singleton [62] was the first to call this special type of code an MDS code (1964). Golomb and Posner [28] constructed MDS codes in the same journal issue using Latin squares and hypercubes.

Maneri and Silverman [42] (based on Silverman’s work from 1960) published results both on general and linear MDS codes in 1966.

According to [71], MacWilliams and Sloane [41] (1977) were first to state the main conjecture for linear MDS codes, answering at least partially Segre’s [58] question about the maximal length of arcs (and therefore linear MDS codes) from 1955.

The weight enumerator for linear MDS codes has been known for a long time (see MacWilliams and Sloane [41, p. 330]), for nonlinear MDS codes it has been proven to be the same by Tolhuizen [70] in 1994. The partition weight enumerator has been introduced by El-Khamy and McEliece in 2005 [25] for linear MDS codes, Yang and Zhang [75] remarked that the proof also holds for non-linear MDS codes.

1.5.2 Latin Squares

Latin squares have been known since ca. 1200 AD [1, 20]. Euler seems to be one of the first to do research on MOLS, especially on the 36 officer problem (starting 1776). The 36 officer problem tries to arrange 36 officers of 6 different ranks and 6 different units in a square such that each row and each column contains one officer of each rank and one of each unit, and each combination of rank and unit appears exactly once. This problem is equivalent to trying to find two orthogonal latin squares of order 6. Euler called two orthogonal latin squares that have been superimposed a Graeco-Latin Square (because he used Latin and Greek letters to differentiate the two latin squares). Since he could not find a Graeco-Latin Square of order 10 in addition to side length 2 and 6, he (wrongly) conjectured in 1782 [26] that Graeco-Latin Squares do not exist for side lengths of the form $4t+2$.

As stated in [39], Moore [45] first showed in 1896 how to construct $n-1$ MOLS of order $n$ when $n$ is a prime power. Shortly after, in 1900-1901, Tarry proved that two orthogonal latin squares of order 6 do not exist by constructing all latin squares of this order. This work was published in [67] and [68]. Fisher and Yates [27] published a shorter proof of this in 1934.

In 1938, Bose [9] showed that an affine plane is equivalent to $n-1$ MOLS of order $n$ and that if $n$ is a prime power then $n-1$ MOLS of order $n$ exist.

Bose and Shrikhande [11] (1959) were the first to give a counterexample to Euler’s conjecture, and Bose, Parker, and Shrikhande [12] disproved the conjecture for all side lengths larger than 6 in 1959-1960.

1.5.3 Orthogonal arrays

Plackett and Burman [50] introduced orthogonal arrays of strength 2 in 1946. Plackett (1946) [49] and Rao (1946) [51] generalized this to orthogonal arrays of any strength.

The first major results were published by Rao in 1947 [52] and 1949 [53].

Many of the results on MDS codes are found in Bush’s 1952 [18] work on orthogonal arrays of index unity ($\lambda = 1$). Some further work on orthogonal arrays of strength 2 and 3 are in Bose and Bush’s paper from 1952 [10].

1.5.4 Steiner Triple Systems and BIBD

Woolhouse [74] was the first to pose the question eventually known as the “Kirkman’s schoolgirl problem” in 1844. The problem, which is equivalent to the construction of a Steiner Triple System with $v = 15$, $r = 7$, and $b = 35$, is [19]:

Fifteen young ladies in a school walk out three abreast for seven days in succession: it is required to arrange them daily, so that no two walk twice abreast.

Kirkman [36] made the problem popular in 1850, but he had already worked on the general problem of the existence of Steiner Triple Systems in 1847 [35] and gave necessary and sufficient conditions for this. Steiner independently worked on the same problem in 1853 [63], and interestingly, the sufficient conditions for the existence are sometimes attributed to Reiss [57] who only published these in 1859. For more information, see also [19] I.4.5 and I.6.3.

Yates [77] introduced Balanced Incomplete Block Designs through symmetric BIBDs in 1936. The main purpose of his work was the use of BIBDs for statistical design and he gave several examples for this.

1.5.5 Bruck nets

Baer [4] introduced the term ‘net’ in 1939. He states in his paper that the following articles also contain work on this area, nets are just termed slightly differently since the mathematicians published in German: in 1929 by Reidemeister [55] and by Thomsen [60], in 1930 in a book by Reidemeister [56], in 1932 by Kneser [37], in 1935 by Moufang [46], in 1937 by Bol [8], and in 1938 in a book by Blaschke and Bol [7]. All of these works are on nets of degree 3.

The major work on nets is by Bruck, published in 1951 [14] and 1963 [15]. Due to this they are named after him in subsequent work.

Silverman [61] seems to have introduced nets of higher dimensions in 1960.

A more complete history of Latin squares, orthogonal arrays, Steiner triple systems, Balanced incomplete block designs, and other designs is given in [20] I.2], wherein a short section on the beginnings of coding theory may also be found.
Chapter 2

General upper bounds on the length of MDS codes

One important research question is: If \( k \) and \( q \) are given, what is the maximum length \( n \) an MDS code can obtain? This maximum value is denoted by \( M(k, q) \).

This chapter concerns general upper bounds that hold for any MDS code, no matter if linear or not, with very few or no restrictions on the dimension \( k \) of the code.

2.1 Extending MDS codes

Definition 2.1. A code \( C' \) of length \( n + 1 \) is an extension of an MDS code \( C \) of length \( n \) if \( C \) can be constructed from \( C' \) by deleting a fixed coordinate. \( C \) is then called extendable.

Silverman [61] showed the following important theorem (as already stated in Section 1.4):

Theorem 2.1. [61] If an \((n, k, d)_q\)-MDS code exists, then an \((n - 1, k, d - 1)_q\)-MDS code exists.

The following corollary of this theorem is used repeatedly to prove upper bounds by proving the non-existence of a code.

Corollary 2.2. If no \((n + 1, k, d)_q\)-MDS code exists, then \( M(k, q) \leq n \).

Proof. If no \((n+1, k, d)_q\)-MDS code exists, then by Theorem 2.1 no \( k \)-dimensional MDS code of length \( n + 2 \) exists, and by repeated application no \( k \)-dimensional MDS code of length \( m \) exists if \( m \geq n + 1 \).

Alderson [2] proved the following theorem on the extendability of codes:

Theorem 2.3. [2] A \((q + k - 2, k, q - 1)_q\)-MDS code with \( k \geq 3 \) is extendable if and only if \( q \) is even.
It easily follows

**Corollary 2.4.** If \( q \) is even, \( k \geq 3 \) and no \((q + k - 1, k, q)_q\)-MDS code exists, then \( M(k, q) \leq q + k - 3 \).

### 2.2 General upper bounds on MDS codes

**Theorem 2.5.** [18] If \( k \geq 2 \), then \( M(k, q) \leq q + k - 1 \).

**Theorem 2.6.** [61] If \( k \geq q \), then \( M(k, q) \leq k + 1 \).

Bush [18] also showed this for linear codes a few years earlier.

The following has been shown in many different ways. To our knowledge, the alternative proof given here is new.

**Theorem 2.7.** If \( q \) is odd and \( k \geq 3 \), then \( M(k, q) \leq q + k - 2 \).

**Proof.** Let \( C \) be a \((q + k - 1, k, q)_q\)-MDS code with \( q \) odd. Assume without loss of generality that the zero codeword is contained in \( C \).

We choose to partition the code the following way with associated weight profile (\( T_3 = \emptyset \) is admissible):

\[
T_1 = \{1, 2\} \quad T_2 = \{3, \ldots, q + 2\} \quad T_3 = \{q + 3, \ldots, q + k - 1\}
\]

\[
w_1 = 2 \quad w_2 = q - 2 \quad w_3 = 0
\]

Let \( S \subseteq C \) be the collection of codewords satisfying this characteristic. From equation 1.2 we know

\[
|S| = A_T(2, q - 2, 0) = (q - 1)\binom{q}{q - 2} = (q - 1)\binom{q}{2} = \frac{q(q - 1)^2}{2}
\]

Let \( C_{a,b} = \{c \in S \mid c_1 = a, c_2 = b\} \) with \( a, b \neq 0 \). Then \( S = \bigcup C_{a,b} \). From the \((q - 1)^2\) choices for the pair \( a, b \), there will be one such that

\[
|C_{a,b}| \geq \left\lfloor \frac{q}{2} \right\rfloor
\]

Each codeword in \( C_{a,b} \) has exactly two zeroes in the positions of \( T_2 \). To achieve a minimum distance of \( q \) between any two codewords in \( C_{a,b} \), no two words have a zero entry in a common coordinate of \( T_2 \). It follows that

\[
|C_{a,b}| \leq \left\lfloor \frac{q}{2} \right\rfloor
\]

Therefore

\[
|C_{a,b}| = \left\lfloor \frac{q}{2} \right\rfloor
\]

which has to be an integer, thus \( q \) is even. This is a contradiction to the assumption that \( q \) is odd, therefore the code \( C \) does not exist, and \( M(k, q) \leq q + k - 2 \) if \( q \) is odd. \( \square \)
The following is a lower bound on the maximum length of any MDS code:

**Proposition 2.8.** \[61\] For any \( q, k \), \( M(k, q) \geq k + 1 \)

Together with Theorem 2.6, we then get the following well known corollary:

**Corollary 2.9.** \( M(k, q) = k + 1 \) if \( k \geq q \).

Silverman \[61\] showed the following, but it was first stated in this form in \[43\].

**Proposition 2.10.** \[61\] If there exist a prime \( p \) such that \( p < k \) and \( p \mid (q - 1) \), then \( M(k, q) \leq q + k - 2 \).

With \( p = 2 \), this also leads to Theorem 2.7.

The following is a collection of further known upper bounds on general MDS codes.

**Proposition 2.11.** \[43\] If \( k \geq 4, q > 2, q \equiv 1, 2, 4, 5 \) (mod 9), then \( M(k, q) \leq q + k - 2 \).

**Proposition 2.12.** \[17\] If \( k \geq 4, q > 6, q \not\equiv 0, 2 \) (mod 9), then \( M(k, q) \leq q + k - 2 \).

Combined with Proposition 2.11, this results in

**Corollary 2.13.** If \( k \geq 4, q > 6, 9 \nmid q \), then \( M(k, q) \leq q + k - 2 \).

**Proposition 2.14.** \[17\] If \( k \geq 3, q > 2, 4 \nmid q \), then \( M(k, q) \leq q + k - 2 \).

The previous two results, except for the case \( k = 3 \), are also subsumed in the following:

**Theorem 2.15.** \[17\] If \( k \geq 4, q > 2, 36 \nmid q \), then \( M(k, q) \leq q + k - 2 \).

**Corollary 2.16.** \[2\] If \( k \geq 4, q > 2, 36 \nmid q \), and \( q \) even, then \( M(k, q) \leq q + k - 3 \).

**Proposition 2.17.** If \( q \equiv 1, 2 \) (mod 4) and the square-free part of \( q \) is divisible by a prime of the form \( 4t + 3 \), then \( M(k, q) \leq q + k - 2 \).

**Proof.** See Bruen and Ryser \[13\] for \( k = 2 \), Maneri and Silverman \[42\] for \( k \geq 2 \). \( \square \)

**Corollary 2.18.** If \( q \equiv 1, 2 \) (mod 4) and the square-free part of \( q \) is divisible by a prime of the form \( 4t + 3 \), then \( M(k, q) \leq q + k - 3 \).

**Proof.** Maneri and Silverman \[42\] showed this result for \( q \equiv 1 \) (mod 4). If \( q \equiv 2 \) (mod 4), we can apply Corollary 2.4. \( \square \)

Summarizing these upper bounds we have Table 2.1.

The following result connects the number of mutually orthogonal latin rectangles with the upper bound for MDS codes.

**Proposition 2.19.** \[76\] Let \( L(n, k) \) be the maximum number of mutually orthogonal \( n \times k \) latin rectangles (or latin squares of order \( n \) if \( n = k \)). If \( C \) is an \( (n, k, d) \) MDS code with \( k < q \), then

\[
M(k, q) \leq L(q - 1, k) + k + 1
\]
Table 2.1: General upper bounds on the length of MDS codes

<table>
<thead>
<tr>
<th>Condition</th>
<th>$M(k, q)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>all $k, q$</td>
<td>$\geq k + 1$</td>
</tr>
<tr>
<td>$k \geq q$</td>
<td>$= k + 1$</td>
</tr>
<tr>
<td>$k \geq 2$</td>
<td>$\leq q + k - 1$</td>
</tr>
<tr>
<td>$p$ prime, $p &lt; k$, $p \mid (q - 1)$</td>
<td>$\leq q + k - 2$</td>
</tr>
<tr>
<td>$k \geq 4$, $q &gt; 2$, $36 \nmid q$; $q$ odd</td>
<td>$\leq q + k - 2$</td>
</tr>
<tr>
<td>$q$ even</td>
<td>$\leq q + k - 3$</td>
</tr>
<tr>
<td>$k \geq 3$, $q &gt; 2$, $4 \nmid q$</td>
<td>$\leq q + k - 2$</td>
</tr>
<tr>
<td>$q \equiv 1, 2 \pmod{4}$, square-free part of $q$ divisible by a prime of the form $4t + 3$</td>
<td>$\leq q + k - 3$</td>
</tr>
</tbody>
</table>
Chapter 3

Upper bounds on linear MDS codes

This chapter concerns the upper bound $M(k, q)$ on the length of a linear MDS code when its dimension $k$ and alphabet size $q$ are fixed. The main conjecture for this bound is stated and an up-to-date summary of the cases in which the conjecture is proven is given.

3.1 Main Conjecture for linear MDS

The Main Conjecture on linear MDS codes, assuming $2 \leq k < q$, is the following:

Main Conjecture (Linear case).

\[ M(k, q) = \begin{cases} 
q + 2 & \text{if } q = 2^t \text{ and } (k = 3 \text{ or } k = q - 1), \\
q + 1 & \text{otherwise.} 
\end{cases} \] (3.1)

For $q \leq k$, $M(k, q) = k + 1$ as usual.

Since the dual code of a linear MDS code is also MDS, we know that all (non-)existence results regarding $[n, k, n-k+1]$-codes, also hold for their duals.

The lower bound for the maximum length of a linear MDS code is given by:

Proposition 3.1. \(38\) For any $k$ and $q$, $M(k, q) \geq q + 1$ for linear MDS codes.

Therefore, if it is shown that no code of length $q + 2$ or longer ($q + 3$ or longer in the case that $q$ is even and $k = 3, q - 1$) exists, the conjecture is true.

3.2 The known results

Hirschfeld and Storme \(32\) give an excellent summary of results known concerning the Main Conjecture in the linear case. Some of the main results are:
Proposition 3.2. [32] The Main Conjecture for linear MDS codes is true for

(i) any \( q \leq 27 \) a prime power;

(ii) any \( k \leq 5 \) or \( k \geq q - 3 \);

(iii) \( q \) is even and \( k = 6, 7 \).

Only recently, Ball [5] proved the Main Conjecture to be true for all cases where \( q \) is prime. This is included in the first of his following three results:

Theorem 3.3. [5]

1. If \( k \leq q \) and \( q = p^h \), where \( p \) is a prime, then \( M(k, q) \leq q + k + 1 - \min(k, p) \).

2. If \( q = p^h \), where \( p \) is a prime, and \( p < k < q \), then \( M(k, q) \leq q + k - p \).

3. If \( q = p^h \), where \( p \) is a prime, and \( 2 < q - p + 1 < k < q - 2 \), then \( M(k, q) \leq q + 1 \).

Together with DeBeule, Ball [6] improved this even more to include the following cases:

Theorem 3.4. [6]

1. If \( q = p^h \) where \( p \) is prime, \( h > 1 \), and \( k \leq 2p - 2 \), then \( M(k, q) \leq q + 1 \).

2. If \( q = p^h \) where \( p \) is prime, \( h > 1 \), and \( q - 2p + 4 \leq k \leq q \), then \( M(k, q) \leq q + 1 \).

Combining the results from Ball and DeBeule with the list from Hirschfeld and Storme, we get the following:

Theorem 3.5. The Main Conjecture for linear MDS codes is true for (always taking \( k < q \)):

1. \( q \) is a prime or \( q \leq 27 \);

2. \( k \leq 5 \) or \( k \geq q - 3 \);

3. \( k = 6, 7, q - 5, q - 4 \) except maybe \( q = 81 \) in each of the cases;

4. \( q = p^h \) where \( p \) is prime and \( k \leq p \);

5. \( q = p^h \) where \( p \) is prime and \( k = p + 1 < q \);

6. \( q = p^h \) where \( p \) is prime and \( 2 < q - p + 1 < k < q - 2 \);

7. \( q = 2^h, h > 2 \) and \( 5 \leq k < \sqrt{q}/2 + 15/4 \) or \( q - \sqrt{q}/2 - 7/4 < k \leq q - 4 \);

8. \( q = p^{2e}, e \geq 1, p \) odd and \( 3 \leq k < \sqrt{q}/4 + 55/16 \) or \( q - \sqrt{q}/4 - 23/16 < k \leq q - 2 \);
9. \( q = p^{2e+1}, e \geq 1, p \) odd and \( 3 \leq k < \sqrt{pq}/4 - 29p/16 + 4 \) or \( q - \sqrt{pq} + 29p/16 - 2 < k \leq q - 2 \);

10. \( q = p^h, p \leq 5 \) and \( 3 \leq k < \sqrt{q}/2 \) or \( q - \sqrt{q}/2 + 2 < k \leq q - 2 \);

11. \( q = p^h, p > 3 \) or \( p = 3 \) and \( h \) even, \( q \geq 23^2, q \neq 5^5, 3^6 \) and \( 3 \leq k < \sqrt{q}/2 + 2 \) or \( q - \sqrt{q}/2 < k \leq q - 2 \).
Chapter 4

MDS codes with $k = 2$, Bruck nets, and MOLS

This chapter concerns the upper bound $M(2,q)$ on the length of a 2-dimensional MDS code with the alphabet size $q$ fixed. Research on this bound has been extensive, especially due to the equivalence of 2-dimensional MDS codes with mutually orthogonal latin squares. A summary of the results will be given, as well as a list of the currently best known ranges of $M(2,q)$ for alphabet sizes up to 100.

Repeating from Section 1.3 we have

Proposition 4.1. The following are equivalent:
1. An $(n,2,d)_q$-MDS code;
2. A (Bruck) net of degree $n$ and order $q$;
3. $n-2$ MOLS of order $q$;
4. A transversal design with index one, block size $n$, and group size $q$.

Corollary 4.2. An MDS code with $k = 2$ and $n = q+1$ is equivalent to an affine plane of order $q$.

Since a finite projective plane of order $q$ can be constructed from an affine plane of order $q$, and conversely, (see for example [20]), the existence of an $(q+1,2,q)_q$ MDS code is also equivalent to the existence of a projective plane of order $q$.

4.1 General

Mullen [47] proposed that the quest of finding the maximum number of MOLS of a given order, and therefore $M(2,q)$, should be named the ‘next Fermat problem’. Indeed a lot of research has been done, but not a lot is known.
From Theorem 2.5 we know that \( M(2,q) \leq q + 1 \). Equality holds iff a complete set of MOLS of order \( q \) exists (this includes all the cases where \( q \) is a prime power) or equivalently iff an affine plane of order \( q \) exists [3].

**Theorem 4.3.** [60] If \( M(2,q) < q + 1 \) and \( q > 4 \), then \( M(2,q) \leq q - 2 \).

It is known that for \( q = 10 \) there are at most 6 MOLS of order 10, thus \( M(2,10) \leq 8 \) (see [47]).

Bose et al. [12] showed that there are at least 2 MOLS of order \( q \neq 2, 6 \). Thus if \( q \neq 2, 6 \), then \( M(2,q) \geq 4 \).

The currently highest lower bounds for orders \( q \leq 10,000 \) are given in the CRC handbook, second edition, [20] and updates are on the website of the book.

The following theorem comes from the construction of \( l \) MOLS of order \( s \) when \( l \) MOLS of order \( s \) and \( t \) are known.

**Proposition 4.4.** [40] \( M(2,s \cdot t) \geq \min\{M(2,s), M(2,t)\} \)

### 4.2 Bruck’s completion theorem

Bruck [15] gave a condition as to when a (Bruck) net is extendable to an affine plane, which was later improved by Metsch [44]. This is known as Bruck’s completion theorem and in coding theoretic terms is stated in the following form:

**Theorem 4.5.** Let \( q \equiv 1, 2 \pmod{4} \) where \( q \) is not the sum of two squares.

1. [15] Let \( t \) be the largest positive integer for which \( 0.5t^4 - t^3 + t^2 + 0.5t - 1 < q \). Then \( M(2,q) \leq q - t \).

2. [44] Let \( t \) be the largest positive integer for which \( 8t^3 + 18t^2 + 8t + 4 - 2\rho(t^2 - 1 - 1) + 9/2\rho(\rho - 1)(t - 1) < 3q \), where \( \rho \in \{0, 1, 2\} \) and \( \rho \equiv t + 1 \pmod{3} \). Then \( M(2,q) \leq q - t \).

This means that for an infinite number of values of \( q \) no \((q + 1, 2,q)\) MDS code exists. The values of \( q \leq 100 \) for which this is true can be found in tables 4.1 and 5.1.

This is the only theorem known for an improved upper bound in the 2-dimensional case.

### 4.3 Prime power conjecture

It has been conjectured that a complete set of MOLS of order \( q \) exists if and only if \( q \) is a prime power (the only if direction is open). This would imply that \( M(2,q) < q + 1 \) for \( q \) not a prime power. Using Theorem 4.3 this bound can be even improved to \( M(2,q) \leq q - 2 \). From Bruck’s completion theorem we know that this is true for an infinite number of non-prime powers.
4.4 Range of $M(2, q)$ for $q \leq 100$

The best known ranges for $M(2, q)$ are given in Table 4.1 for $q \leq 100$ using results from [20]. If only one number is given, then equality holds. Note that for the trivial $(n, 2, d)_1$-MDS code there is no restriction on the length as there is only one codeword in the code.

Table 4.1: Range of $M(2, q)$ for $q \leq 100$

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>$\infty$</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>10</td>
<td>4–8</td>
</tr>
<tr>
<td>10</td>
<td>12</td>
<td>7–13</td>
<td>14</td>
<td>5–12</td>
<td>6–16</td>
<td>17</td>
<td>18</td>
<td>5–19</td>
<td>20</td>
<td>6–21</td>
</tr>
<tr>
<td>30</td>
<td>32</td>
<td>33</td>
<td>7–30</td>
<td>6–35</td>
<td>7–36</td>
<td>10–37</td>
<td>38</td>
<td>6–35</td>
<td>7–40</td>
<td>9–41</td>
</tr>
<tr>
<td>40</td>
<td>42</td>
<td>7–39</td>
<td>44</td>
<td>7–45</td>
<td>8–46</td>
<td>6–43</td>
<td>48</td>
<td>10–49</td>
<td>50</td>
<td>8–51</td>
</tr>
<tr>
<td>50</td>
<td>7–52</td>
<td>7–53</td>
<td>54</td>
<td>7–51</td>
<td>8–56</td>
<td>9–57</td>
<td>9–54</td>
<td>7–59</td>
<td>60</td>
<td>6–61</td>
</tr>
<tr>
<td>60</td>
<td>62</td>
<td>7–59</td>
<td>8–64</td>
<td>65</td>
<td>9–66</td>
<td>7–63</td>
<td>68</td>
<td>7–69</td>
<td>8–66</td>
<td>8–67</td>
</tr>
<tr>
<td>70</td>
<td>72</td>
<td>9–73</td>
<td>74</td>
<td>7–75</td>
<td>9–76</td>
<td>8–77</td>
<td>8–74</td>
<td>8–75</td>
<td>80</td>
<td>11–81</td>
</tr>
<tr>
<td>80</td>
<td>82</td>
<td>10–83</td>
<td>84</td>
<td>8–85</td>
<td>8–86</td>
<td>8–82</td>
<td>8–88</td>
<td>9–89</td>
<td>90</td>
<td>8–91</td>
</tr>
<tr>
<td>90</td>
<td>9–92</td>
<td>8–93</td>
<td>8–89</td>
<td>8–90</td>
<td>8–96</td>
<td>9–97</td>
<td>98</td>
<td>8–99</td>
<td>10–100</td>
<td>10–101</td>
</tr>
</tbody>
</table>
Chapter 5

General MDS codes

This chapter begins by stating the main conjecture for general, not necessarily linear, MDS codes. We will then take a look at known upper bounds related to the main conjecture for selected dimensions. Finally, a table of the currently best known upper bounds on general MDS codes with those dimensions and alphabet size up to 100 is given.

5.1 Main Conjecture for general MDS

To accommodate the cases where an MDS code is not linear, the main conjecture has to be slightly adjusted:

Main Conjecture (General case).

\[
M(k, q) \leq \begin{cases} 
q + 2 & \text{if } 4 \mid q \text{ and } k = 3 \text{ or } k = q - 1, \\
q + 1 & \text{otherwise.}
\end{cases}
\]

\[
M(k, q) = k + 1 \text{ if and only if } q \leq k \text{ or } q = 6
\]

This seems to be the first time that the Main Conjecture is being stated in this form.

In the following sections, the upper bounds on MDS codes given are either confirming the main conjecture or are very close.

5.2 \( k = 3 \)

From Theorem 2.5, we know that \( M(3, q) \leq q + 2 \). From the linear case, we know that equality holds for \( q = 2^e \). From Theorem 2.14, we also know that the bound is only possibly obtained if \( 4 \mid q \).

If \( q \) is odd, the bound cannot be met, thus giving \( M(3, q) \leq q + 1 \).

Alderson [2] showed the following case:
Proposition 5.1. [2] If \( q \equiv 2 \pmod{4} \), then \( M(3, q) \leq q \).

Proposition 5.2. \( M(3, 10) \leq 9 \)

Proof. From [47] and the equivalence of MOLS and MDS codes with \( k = 2 \) (see chapter 2 or 4), we know that no \((9, 2, 7)_{10}\) MDS code exists. Using Theorem 1.15 we get that no \((10, 3, 7)_{10}\) MDS code exists. \(\square\)

5.3 \( k = 4 \)

Proposition 5.3. If \( q \equiv 2 \pmod{4} \), then \( M(4, q) \leq q + 1 \).

Proof. From Proposition 5.1 we know that no \((q + 1, 3, q - 1)_q\) MDS code exists. Applying Theorem 1.15 to this we get that no \((q + 2, 4, q - 1)_q\) MDS code exists.

From Corollary 2.16 we know that if \( q \) is even and \( 36 \nmid q \), then \( M(4, q) \leq q + 1 \).

Also from Corollary 2.18 we know that if \( q \equiv 1 \pmod{4} \) and the square-free part is divisible by a prime of the form \( 4t + 3 \), then \( M(4, q) \leq q + 1 \). Equivalence is known to hold in the case that \( q \) is a prime power.

Similar to Proposition 5.2 we also know that \( M(4, 10) \leq 10 \).

5.4 \( k = q - 2 \)

The following result is due to Yang and Zang [75]. We provide an alternate proof.

Theorem 5.4. [75] If \( q \equiv 4 \pmod{6} \), then \( M(q - 2, q) \leq q + 1 \).

Proof. Assume that a \((q + 2, q - 2, 5)\) MDS code with \( q \equiv 4 \pmod{6} \) exists. Without loss of generality assume that the code contains the all zero codeword.

We choose to partition the code and associate a weight profile in the following way:

\[
T_1 = \{1, 2\} \quad T_2 = \{3, \ldots, q + 2\};
\]

\[
w_1 = 2 \quad w_2 = 3.
\]

Let \( S \subseteq C \) be the set of all codewords satisfying these criteria. From the partition weight enumerator (Equation 1.2) we know that

\[
|S| = A^T(2, 3) = (q - 1) \binom{q}{3} = \frac{q(q - 1)^2(q - 2)}{6}.
\]

Then there exist \( a, b \neq 0 \) from the alphabet, such that

\[
|C_{a,b}| \geq \left\lceil \frac{q(q - 2)}{6} \right\rceil,
\]

where \( C_{a,b} = \{c \in S \mid c_1 = a, c_2 = b\} \).
To achieve a minimum distance of \( d = 5 \), for any two codewords \( \alpha, \beta \in C_{a,b} \) we have that \( \text{supp}(\alpha) \cap T_2 \) and \( \text{supp}(\beta) \cap T_2 \) have at most one coordinate in common. Thus the set of \( \text{supp}(c) \cap T_2, c \in C_{a,b} \) forms a set of triples with no pair in common. Counting the number of triples, which is equal to \( |C_{a,b}| \) we get

\[
(|C_{a,b}|)(3) \leq (q) \left\lfloor \frac{q-1}{2} \right\rfloor .
\]

and from \( q \) being even, we then get

\[
\left\lfloor \frac{q(q-1)}{6} \right\rfloor \leq |C_{a,b}| \leq \frac{q(q-1)}{6}.
\]

This results in

\[
|C_{a,b}| = \frac{q(q-1)}{6}.
\]

Then, \( \frac{q(q-2)}{4} \) has to be an integer, thus \( q \equiv 0, 2 \pmod{6} \) which is a contradiction to \( q \equiv 4 \pmod{6} \). Therefore \( M(q-2, q) \leq q + 1 \) if \( q \equiv 4 \pmod{6} \).

\[\Box\]

5.5 \( k = q - 1 \)

Using the relationship with BIBDs we can establish an upper bound on the length of MDS codes of dimension \( q - 1 \). This upper bound is improved in the following two theorems, but the method of proof might be interesting.

**Proposition 5.5.** If \( q \) is odd or \( q \equiv 1 \pmod{3} \), then \( M(q-1, q) \leq q + 3 \).

**Proof.** Assume that a \( (q + 4, q - 1, 6) \)-MDS code \( C \) exists. Assume without loss of generality that the zero codeword is in the code.

We choose to partition the code and associate a weight profile the following way:

\[
T_1 = \{1, 2\} \quad T_2 = \{3, \ldots, q + 4\}
\]

\[
w_1 = 2 \quad w_2 = 4
\]

Let \( S \subseteq C \) be the collection of codewords satisfying this partition and weight profile. From the weight enumerator (equation 1.2) we know that

\[
|S| = A^T_2(2, 4) = (q - 1) \binom{q + 2}{4} = \frac{(q + 2)(q + 1)(q)(q - 1)}{24}
\]

Then there exist \( a, b \neq 0 \) from the alphabet such that

\[
|C_{a,b}| \geq \frac{(q + 2)(q + 1)q}{24}
\]

where \( C_{a,b} = \{ c \in S \mid c_1 = a, c_2 = b \} \).

To achieve a minimum distance of 6 between all the codewords in \( C_{a,b} \), a BIBD with \( v = q + 1 \) treatments, block length \( K = 4 \), and covalency \( \lambda = \lfloor q/2 \rfloor \)
must exist.

**Case 1:** Let $q$ be odd, therefore $\lambda = (q - 1)/2$. We then have

$$r = \frac{(q - 1)(q + 1)}{6}$$

and the number of blocks, which is the maximum number of codewords in $C_{a,b}$, is

$$b = \frac{(q + 2)(q + 1)(q - 1)}{24}.$$ 

But this is a contradiction to $|C_{a,b}| \geq \frac{(q+2)(q+1)q}{24}$. Therefore $C$ does not exist and if $q$ is odd, $M(q - 1, q) \leq q + 3$.

**Case 2:** Let $q$ be even and $q \equiv 1 \pmod{3}$, then $\lambda = q/2$. We therefore have

$$r = \frac{q(q + 1)}{6}$$

and the number of blocks, which is the maximum number of codewords in $C_{a,b}$, is

$$b = \frac{(q + 2)(q + 1)q}{24}.$$ 

The number of codewords in $C_{a,b}$ is therefore equal to the number of blocks. For the BIBD to exist, $r$ needs to be an integer, and therefore $q \equiv 0, 2 \pmod{3}$, which is contradictory to the assumption that $q \equiv 1 \pmod{3}$. Therefore $C$ does not exist and if $q \equiv 1 \pmod{3}$, then $M(q - 1, q) \leq q + 3$. 

**Theorem 5.6.** If $q \equiv 1 \pmod{3}$, then $M(q - 1, q) \leq q + 2$.

**Proof.** Assume that a code $C$ with parameters $k = q - 1, n = q + 3, d = 5$ with $q \equiv 1 \pmod{3}$ exists. Assume without loss of generality that the zero codeword is contained in $C$.

We choose to partition the code and associate a weight profile the following way:

$$T_1 = \{1, 2\} \quad T_2 = \{3, \ldots, q + 3\},$$

$$w_1 = 2 \quad w_2 = 3.$$ 

Let $S \subseteq C$ be the collection of codewords satisfying this characteristic. From the weight enumerator we know that

$$|S| = A^T(2, 3) = (q - 1) \binom{q + 1}{3} = \frac{(q + 1)(q)(q - 1)^2}{6}.$$ 

Then there exist $a, b \neq 0$ from the alphabet such that

$$|C_{a,b}| \geq \left\lceil \frac{(q + 1)q}{6} \right\rceil,$$
where \( C_{a,b} = \{ c \in S \mid c_1 = a, c_2 = b \} \). To achieve a minimum distance of 5 between all codewords, a Steiner Triple System with \( q+1 \) treatments must exist. The number of blocks, which is the maximum number of codewords possible, is \((q + 1)q/6\). We therefore have

\[
|C_{1,1}| = \frac{(q + 1)q}{6}.
\]

This has to be an integer, thus \( q \equiv 0, 2 \pmod{3} \), which is a contradiction to the assumption that \( q \equiv 1 \pmod{3} \), thus the code \( C \) does not exist, and \( M(q-1,q) \leq q+2 \).

**Corollary 5.7.** [75] If \( q \equiv 4 \pmod{6} \), then \( M(q-1,q) \leq q+2 \).

A proof of the following reportedly appears in [72]. We provide a proof.

**Theorem 5.8.** If \( q \) is odd, then \( M(q-1,q) \leq q+1 \).

**Proof.** Assume that a code \( C \) with the parameters \( k = q-1, n = q+2, d = 4 \), and \( q \) odd exists. Assume without loss of generality that the zero codeword is included.

We choose to partition the code and associate a weight profile the following way:

\[
T_1 = \{1, 2\} \quad T_2 = \{3, \ldots, q+2\},
\]

\[
w_1 = 2 \quad w_2 = 2.
\]

Let \( S \subseteq C \) be the set of codewords satisfying these conditions. Then from the partition weight enumerator (equation 1.2) we know that

\[
|S| = A_T(2,2) = (q-1)\binom{q}{2} = \frac{q(q-1)^2}{2}.
\]

Then there exist \( a, b \) from the alphabet such that

\[
|C_{a,b}| \geq q/2,
\]

where \( C_{a,b} = \{ c \in S \mid c_1 = a, c_2 = b \} \).

Since \( w_2 = 2 \), there are two non-zero entries in the trailing \( q \) coordinates. For \( d = 4 \) to be true, given any two codewords \( \alpha, \beta \in C_{a,b} \) the following holds: \((\text{supp}(\alpha) \cap T_2) \cap (\text{supp}(\beta) \cap T_2) = \emptyset\). Thus there are at most \( q/2 \) codewords.

We get that \( |C_{a,b}| = q/2 \). Therefore \( q \) is even, which is a contradiction to the assumption that \( q \) is odd. Thus the code \( C \) does not exist, which implies \( M(q-1,q) \leq q+1 \).

Equality in the last two theorems as usual is known to hold if \( q \) is a prime power.
5.6 $q \leq 6$

Maneri and Silverman [42] showed the following:

Proposition 5.9. [42]

1. For $q \leq 5$, $M(k,q) = \max\{q+1, k+1\}$, except for $M(3,4) = 6$.
2. If $q = 6$, then $M(k,q) = k+1$.

5.7 $q \leq 100$

The currently best known upper bounds on $M(k,q)$ for $q$ up to 100 and for $k \in \{2, 3, 4, 5, 6, 7, q-2, q-1\}$ are given in Table 5.1. If equality holds, the values are given in italics. Values in bold are less than $q+1$ when $k < q$. Blanks mean that the best known upper bound does not satisfy the main conjecture, i.e. it is greater than $q + 1$ (or greater than $q + 2$ for $k = 3, q-1$). For the values of $M(2, q)$ see also Table 4.1.

References for each entry, given by the superscripts, are the following:

1 Corollary 2.9
2 Theorem 2.5
3 Theorem 2.7
4 $k = 3$ and $4 \parallel q$ (see Section 5.2)
5 Proposition 5.1
6 Proposition 5.9
7 $k = 4$, $q$ even and $36 \nmid q$ (see Section 5.3)
8 Theorem 5.4
9 Theorem 5.8
10 Theorem 5.6
11 Theorem 4.5 values are taken from [19].
12 Using $M(k-1,q)$ and Theorem 1.15 similar to Proposition 5.2
13 Maneri and Silverman [42]
14 $M(2,10) \leq 8$ (see Section 4.1)

Equivalence is generally from the existence of a linear code.
Table 5.1: Upper bounds for $q \leq 100$ and $k \in \{2, \ldots, 7, q-2, q-1\}$

<table>
<thead>
<tr>
<th>$q$</th>
<th>$k=2$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>$q-1$</th>
<th>$q-2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>$3^2$</td>
<td>$4^1$</td>
<td>$5^1$</td>
<td>$6^1$</td>
<td>$7^1$</td>
<td>$8^1$</td>
<td>$\infty$</td>
<td>DNE</td>
</tr>
<tr>
<td>3</td>
<td>$4^2$</td>
<td>$4^1$</td>
<td>$5^1$</td>
<td>$6^1$</td>
<td>$7^1$</td>
<td>$8^1$</td>
<td>$4^2$</td>
<td>$\infty$</td>
</tr>
<tr>
<td>4</td>
<td>$5^2$</td>
<td>$6^6$</td>
<td>$5^1$</td>
<td>$6^1$</td>
<td>$7^1$</td>
<td>$8^1$</td>
<td>$6^6$</td>
<td>$5^2$</td>
</tr>
<tr>
<td>5</td>
<td>$6^2$</td>
<td>$6^6$</td>
<td>$6^6$</td>
<td>$6^1$</td>
<td>$7^1$</td>
<td>$8^1$</td>
<td>$6^6$</td>
<td>$6^6$</td>
</tr>
<tr>
<td>6</td>
<td>$3^6$</td>
<td>$4^6$</td>
<td>$5^6$</td>
<td>$6^6$</td>
<td>$7^1$</td>
<td>$8^1$</td>
<td>$6^6$</td>
<td>$5^6$</td>
</tr>
<tr>
<td>7</td>
<td>$8^2$</td>
<td>$8^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$8^9$</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>$9^2$</td>
<td>$10^4$</td>
<td>$9^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>$10^2$</td>
<td>$10^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>$8^{14}$</td>
<td>$9^{12}$</td>
<td>$10^{12}$</td>
<td>$11^{12}$</td>
<td></td>
<td></td>
<td>$10^9$</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>$12^2$</td>
<td>$12^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$12^9$</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>$13^2$</td>
<td>$14^3$</td>
<td>$13^7$</td>
<td></td>
<td></td>
<td></td>
<td>$14^9$</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>$14^2$</td>
<td>$14^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>$12^{11}$</td>
<td>$13^{12}$</td>
<td>$14^{12}$</td>
<td>$15^{12}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>$16^2$</td>
<td>$16^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$16^9$</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>$17^2$</td>
<td>$18^3$</td>
<td>$17^7$</td>
<td></td>
<td></td>
<td></td>
<td>$18^{10}$</td>
<td>$17^8$</td>
</tr>
<tr>
<td>17</td>
<td>$18^2$</td>
<td>$18^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$18^9$</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>$19^2$</td>
<td>$18^5$</td>
<td>$19^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>$20^2$</td>
<td>$20^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$20^9$</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>$21^2$</td>
<td>$22^3$</td>
<td>$21^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>$19^{11}$</td>
<td>$20^{12}$</td>
<td>$21^{12}$</td>
<td>$22^{12}$</td>
<td></td>
<td></td>
<td>$22^9$</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>$20^{11}$</td>
<td>$21^{12}$</td>
<td>$22^{12}$</td>
<td>$23^{12}$</td>
<td></td>
<td></td>
<td>$24^{10}$</td>
<td>$23^8$</td>
</tr>
<tr>
<td>23</td>
<td>$24^2$</td>
<td>$24^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$24^9$</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>$25^2$</td>
<td>$26^3$</td>
<td>$25^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>$26^2$</td>
<td>$26^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$26^9$</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>$27^2$</td>
<td>$26^5$</td>
<td>$27^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>$28^2$</td>
<td>$28^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$28^9$</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>$29^2$</td>
<td>$30^3$</td>
<td>$29^7$</td>
<td></td>
<td></td>
<td></td>
<td>$30^{10}$</td>
<td>$29^8$</td>
</tr>
<tr>
<td>29</td>
<td>$30^2$</td>
<td>$30^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$30^9$</td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>$27^{11}$</td>
<td>$28^{12}$</td>
<td>$29^{12}$</td>
<td>$30^{12}$</td>
<td>$31^{12}$</td>
<td></td>
<td></td>
<td>$32^9$</td>
</tr>
<tr>
<td>31</td>
<td>$32^2$</td>
<td>$32^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>$33^2$</td>
<td>$34^4$</td>
<td>$33^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>$30^{11}$</td>
<td>$31^{12}$</td>
<td>$32^{12}$</td>
<td>$33^{12}$</td>
<td>$34^{12}$</td>
<td></td>
<td></td>
<td>$34^9$</td>
</tr>
<tr>
<td>34</td>
<td>$35^2$</td>
<td>$34^5$</td>
<td>$35^7$</td>
<td></td>
<td></td>
<td></td>
<td>$36^{10}$</td>
<td>$35^8$</td>
</tr>
<tr>
<td>35</td>
<td>$36^2$</td>
<td>$36^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$36^9$</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>$37^2$</td>
<td>$38^4$</td>
<td>$37^8$</td>
<td>$38^3$</td>
<td></td>
<td></td>
<td>$38^9$</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>$38^2$</td>
<td>$38^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>$35^{11}$</td>
<td>$36^{12}$</td>
<td>$37^{12}$</td>
<td>$38^{12}$</td>
<td>$39^{12}$</td>
<td></td>
<td></td>
<td>$40^9$</td>
</tr>
<tr>
<td>39</td>
<td>$40^2$</td>
<td>$40^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$42^{10}$</td>
<td>$41^8$</td>
</tr>
<tr>
<td>40</td>
<td>$41^2$</td>
<td>$42^4$</td>
<td>$41^7$</td>
<td></td>
<td></td>
<td></td>
<td>$42^9$</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>$42^2$</td>
<td>$42^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$42^9$</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>$39^{11}$</td>
<td>$40^{12}$</td>
<td>$41^{12}$</td>
<td>$42^{12}$</td>
<td>$43^{12}$</td>
<td>$39^{12}$</td>
<td>$40^9$</td>
<td>$41^8$</td>
</tr>
</tbody>
</table>

Continued on the next page
Table 5.1 – continued from previous page

<table>
<thead>
<tr>
<th>$q$</th>
<th>$k=2$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>$q-1$</th>
<th>$q-2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$4^9$</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$4^9$</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$4^9$</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>$43^{11}$</td>
<td>$44^{12}$</td>
<td>$45^{12}$</td>
<td>$46^{12}$</td>
<td>$47^{12}$</td>
<td>$48^{10}$</td>
<td>$47^8$</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>$4^8$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$4^9$</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>$4^2$</td>
<td>$4^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$5^9$</td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>$51^{11}$</td>
<td>$52^{12}$</td>
<td>$53^{12}$</td>
<td>$54^{12}$</td>
<td>$55^{12}$</td>
<td>$56^{10}$</td>
<td>$59^8$</td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>$56^{2}$</td>
<td>$56^{3}$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$56^9$</td>
<td></td>
</tr>
<tr>
<td>56</td>
<td>$57^{2}$</td>
<td>$58^{3}$</td>
<td>$57^7$</td>
<td></td>
<td></td>
<td></td>
<td>$56^9$</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>$54^{11}$</td>
<td>$55^{12}$</td>
<td>$56^{12}$</td>
<td>$57^{12}$</td>
<td>$58^{12}$</td>
<td>$56^{10}$</td>
<td>$59^8$</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>$59^{2}$</td>
<td>$58$</td>
<td>$59^7$</td>
<td></td>
<td></td>
<td></td>
<td>$60^{10}$</td>
<td>$59^8$</td>
</tr>
<tr>
<td>59</td>
<td>$60^2$</td>
<td>$60^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$60^9$</td>
<td></td>
</tr>
<tr>
<td>60</td>
<td>$61^2$</td>
<td>$61^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$60^9$</td>
<td></td>
</tr>
<tr>
<td>61</td>
<td>$62^2$</td>
<td>$62^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$62^9$</td>
<td></td>
</tr>
<tr>
<td>62</td>
<td>$59^{11}$</td>
<td>$60^{12}$</td>
<td>$61^{12}$</td>
<td>$62^{12}$</td>
<td>$63^{12}$</td>
<td>$60^{10}$</td>
<td>$63^8$</td>
<td></td>
</tr>
<tr>
<td>63</td>
<td>$64^{2}$</td>
<td>$64^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$64^9$</td>
<td></td>
</tr>
<tr>
<td>64</td>
<td>$65^{2}$</td>
<td>$66^3$</td>
<td>$65^7$</td>
<td></td>
<td></td>
<td></td>
<td>$66^{10}$</td>
<td>$65^8$</td>
</tr>
<tr>
<td>65</td>
<td>$66^2$</td>
<td>$66^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$66^9$</td>
<td></td>
</tr>
<tr>
<td>66</td>
<td>$63^{11}$</td>
<td>$64^{12}$</td>
<td>$65^{12}$</td>
<td>$66^{12}$</td>
<td>$67^{12}$</td>
<td>$66^9$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>67</td>
<td>$68^2$</td>
<td>$68^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$68^9$</td>
<td></td>
</tr>
<tr>
<td>68</td>
<td>$69^{2}$</td>
<td>$70^4$</td>
<td>$69^7$</td>
<td></td>
<td></td>
<td></td>
<td>$70^9$</td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>$66^{11}$</td>
<td>$67^{12}$</td>
<td>$68^{12}$</td>
<td>$69^{12}$</td>
<td>$70^{12}$</td>
<td>$72^{10}$</td>
<td>$71^8$</td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>$67^{11}$</td>
<td>$68^{12}$</td>
<td>$69^{12}$</td>
<td>$70^{12}$</td>
<td>$71^{12}$</td>
<td>$72^9$</td>
<td></td>
<td></td>
</tr>
<tr>
<td>71</td>
<td>$72^2$</td>
<td>$72^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$72^9$</td>
<td></td>
</tr>
<tr>
<td>72</td>
<td>$73^{2}$</td>
<td>$74^4$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$74^9$</td>
<td></td>
</tr>
<tr>
<td>73</td>
<td>$74^{2}$</td>
<td>$74^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$74^9$</td>
<td></td>
</tr>
<tr>
<td>74</td>
<td>$75^{2}$</td>
<td>$75^5$</td>
<td>$75^7$</td>
<td></td>
<td></td>
<td></td>
<td>$76^9$</td>
<td></td>
</tr>
<tr>
<td>75</td>
<td>$76^2$</td>
<td>$76^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$78^{10}$</td>
<td>$77^8$</td>
</tr>
<tr>
<td>76</td>
<td>$77^{2}$</td>
<td>$78^4$</td>
<td>$77^7$</td>
<td></td>
<td></td>
<td></td>
<td>$78^{10}$</td>
<td>$77^8$</td>
</tr>
<tr>
<td>77</td>
<td>$74^{11}$</td>
<td>$75^{12}$</td>
<td>$76^{12}$</td>
<td>$77^{12}$</td>
<td>$78^{12}$</td>
<td>$78^{10}$</td>
<td>$77^8$</td>
<td></td>
</tr>
<tr>
<td>78</td>
<td>$75^{11}$</td>
<td>$76^{12}$</td>
<td>$77^{12}$</td>
<td>$78^{12}$</td>
<td>$79^{12}$</td>
<td>$78^{10}$</td>
<td>$77^8$</td>
<td></td>
</tr>
<tr>
<td>79</td>
<td>$80^2$</td>
<td>$80^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$80^9$</td>
<td></td>
</tr>
<tr>
<td>80</td>
<td>$81^2$</td>
<td>$82^4$</td>
<td>$81^7$</td>
<td></td>
<td></td>
<td></td>
<td>$82^9$</td>
<td></td>
</tr>
<tr>
<td>81</td>
<td>$82^2$</td>
<td>$82^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$82^9$</td>
<td></td>
</tr>
<tr>
<td>82</td>
<td>$83^{2}$</td>
<td>$82^{5}$</td>
<td>$83^7$</td>
<td></td>
<td></td>
<td></td>
<td>$84^{10}$</td>
<td>$83^8$</td>
</tr>
<tr>
<td>83</td>
<td>$84^{2}$</td>
<td>$84^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$84^9$</td>
<td></td>
</tr>
<tr>
<td>84</td>
<td>$85^{2}$</td>
<td>$86^4$</td>
<td>$85^7$</td>
<td></td>
<td></td>
<td></td>
<td>$84^9$</td>
<td></td>
</tr>
</tbody>
</table>

Continued on the next page
### Table 5.1 – continued from previous page

<table>
<thead>
<tr>
<th>$q$</th>
<th>$k=2$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>$q-1$</th>
<th>$q-2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>85</td>
<td>$86^2$</td>
<td>$86^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td>$82^{11}$</td>
<td>$83^{12}$</td>
<td>$84^{12}$</td>
<td>$85^{12}$</td>
<td>$86^{12}$</td>
<td>$87^{12}$</td>
<td>$86^9$</td>
<td></td>
</tr>
<tr>
<td>87</td>
<td>$88^2$</td>
<td>$88^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$88^9$</td>
<td></td>
</tr>
<tr>
<td>88</td>
<td>$89^2$</td>
<td>$90^4$</td>
<td>$89^5$</td>
<td></td>
<td></td>
<td></td>
<td>$90^{10}$</td>
<td>$89^8$</td>
</tr>
<tr>
<td>89</td>
<td>$90^2$</td>
<td>$90^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$90^9$</td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>$91^2$</td>
<td>$90^5$</td>
<td>$91^7$</td>
<td></td>
<td></td>
<td></td>
<td>$92^9$</td>
<td></td>
</tr>
<tr>
<td>91</td>
<td>$92^2$</td>
<td>$92^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>92</td>
<td>$93^2$</td>
<td>$94^4$</td>
<td>$93^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>93</td>
<td>$89^{11}$</td>
<td>$90^{12}$</td>
<td>$91^{12}$</td>
<td>$92^{12}$</td>
<td>$93^{12}$</td>
<td>$94^{12}$</td>
<td>$94^9$</td>
<td></td>
</tr>
<tr>
<td>94</td>
<td>$90^{11}$</td>
<td>$91^{12}$</td>
<td>$92^{12}$</td>
<td>$93^{12}$</td>
<td>$94^{12}$</td>
<td>$95^{12}$</td>
<td>$96^{10}$</td>
<td>$95^8$</td>
</tr>
<tr>
<td>95</td>
<td>$96^2$</td>
<td>$96^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$96^9$</td>
<td></td>
</tr>
<tr>
<td>96</td>
<td>$97^2$</td>
<td>$98^4$</td>
<td>$97^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>97</td>
<td>$98^2$</td>
<td>$98^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$98^8$</td>
<td></td>
</tr>
<tr>
<td>98</td>
<td>$99^2$</td>
<td>$98^5$</td>
<td>$99^7$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>99</td>
<td>$100^2$</td>
<td>$100^3$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>$100^9$</td>
<td></td>
</tr>
<tr>
<td>100</td>
<td>$101^2$</td>
<td>$102^4$</td>
<td>$101^7$</td>
<td></td>
<td></td>
<td></td>
<td>$102^{10}$</td>
<td>$101^8$</td>
</tr>
</tbody>
</table>
Chapter 6

Conclusion

6.1 Summary

Maximum Distance Separable codes are combinatorially equivalent to many objects, so that advances in research in this area influence research in the other areas. MDS codes have many important applications in industry, security, and other areas, even everyday activities. The history of research in MDS codes and related areas is long, rich, and very diverse, especially for latin squares.

The main conjecture of linear MDS codes has been proven for the majority of cases, but many are still open. The main conjecture for general MDS codes is slightly different from the linear case, since we have to include non-linear codes, several of which have bounds lower than given in the main conjecture for the linear case. Most upper bounds that are known for general MDS codes only hold for certain cases, often progress is just one case at a time. The 2-dimensional case of MDS codes is especially important because of the equivalence to latin squares and finite nets, and research has been extensive.

6.2 Open questions

Since few upper bounds close to the main conjecture are known for general MDS codes, there are many open questions.

We especially want to know when the upper bounds hold with equality, or if they can still be improved. Many cases in which equality is unknown can be found in Table 5.1. There has been research into MDS codes over groups, rings, and other algebraic objects lately (see for example [78] and [24] or [23]), which might solve, at least in some cases, the question of existence.

It has been conjectured that for $k \geq 2$ and $q$ a prime power there are no non-linear MDS codes longer than a linear MDS code. This would imply that for $q$ a prime power, Theorem 3.5 also holds in the general case. See for example the remark after Theorem 4 by Silverman and Maneri in [42], in which they also state that this holds at least for $q \leq 5$ and $k \leq 3$. 

33
Using Table 5.1 we can easily find cases in which the upper bound on general MDS codes is still open, i.e. we do not know if the best known upper bound holds with equality. Some of them are the following:

1. $k = 2$ and $q$ is not a prime power
2. $k \geq 4$ and $36 \mid q$
3. $k = 4$ and $q$ is odd (current bound is $M(4,q) \leq q + 2$)
4. $k = q - 2$ and $q \not\equiv 4 \pmod{6}$
5. $k = q - 1$ and $q \equiv 0, 2 \pmod{6}$
6. $q = 7$ and $k = 4$ or $k = 5$

For linear MDS codes, the main conjecture is still open for $q$ not a prime and not meeting any of the other criteria in Theorem 3.5.

6.3 Conclusion

For linear MDS codes there has been a great advance in proving the main conjecture on the upper bounds lately.

For non-linear MDS codes there are not many theorems on the upper bound that hold in general, especially close to the main conjecture. Usually theorems only cover certain cases, often very few. Overall very little is known.

The partition weight enumerator together with other combinatorial techniques seems to be a good approach to improving upper bounds though.

Chapter 5, and especially Table 5.1 are very useful in determining where work is still needed.
Bibliography


