Nonexistence Theorems for Perfect Codes over Finite Fields

André Jönsson

Bachelor's thesis
2012

Abstract

In this survey, we consider the trivial perfect codes which are the binary repetition codes of odd length and all codes that only contain one code word. We also take into account, the Hamming codes as well as the two perfect Golay codes. We then prove that there do not exist any perfect codes over finite fields others than the ones above, using Lloyd's theorem.

Contents

1 Introduction

When transferring information there is a risk that errors occur, that a message gets distorted on its way to the receiver. Coding theory is about coding your information according to different specific applications such as discovering and correcting possible errors with the goal of designing efficient and reliable data transmission.

In this bachelor's thesis, the focus is on the existence of perfect block codes, or rather the nonexistence. Perfect codes are efficient when it comes to correcting errors because they are in a sense as small as possible. Herein, I give an account for the results in this area, mainly achieved by Jacobus Hendricus van Lint and Aimo Tietäväinen during the 1970's. A lot of the material is taken from articles written by these two mathematicians to whom I express my gratitude. Some rearrangements of their work have been made and also efforts to make this thesis more self-contained. A complete list of the articles and books utilised, can be found in the reference list. I would also like to thank my supervisor Kjell Elfström.

2 Codes

An *alphabet* is a finite set F. The elements of an alphabet are called *letters.* A *code word* is a finite sequence of letters and a *code* a finite set of code words. If all code words of a code have equal length n, we call the code a *block code* of length n.

From now on we shall assume that all codes are block codes and that the set F is a finite field with q elements where the number q is a power of a prime number p. We can then regard the code words as vectors in the vector space F^n and codes as subsets of F^n.

Definition 2.1 Two codes C and C' belonging to F^n are said to be *equivalent* if there exists a permutation π of the set $\{1, \dots, n\}$, such that

$$C' = \{(x_{\pi(1)}, \dots, x_{\pi(n)});\ x \in C\}.$$

Definition 2.2 The weight $w(x)$ of a code word $x = (x_1, \dots, x_n)$ in F^n is the number of coordinates in x that are not equal to zero. The weight $w(C)$ of a code C in F^n is defined as

$$w(C) = \min\{w(x);\ x \in C,\ x \neq 0\}.$$

Definition 2.3 The *Hamming distance* $d(x, y)$ between two vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ in a vector space F^n is defined as the number of coordinates where $x_i \neq y_i$.

Sometimes it is not certain that any other letter will do as a replacement if we find an error in a word and therefore the Hamming distance may not always be the most appropriate measurement. It is, nevertheless, the measurement we will use.

Definition 2.4 The *separation* $d(C)$ for a code C in a vector space is defined as the minimal Hamming distance between two different words in the code.

$$d(C) = \min\{d(x, y);\ x, y \in C,\ x \neq y\}.$$

We observe that equivalent codes have equal weight and equal separation.

Definition 2.5 Let us also give the definition of the distance $d(x, C)$ between a vector x and the code C as

$$d(x, C) = \min\{d(x, y) \mid y \in C\}$$

along with letting C_i denote the set

$$C_i = \{x \in F^n \mid d(x, C) = i\}$$

where $i = 0, 1, 2, \ldots$.

Definition 2.6 For any vector x in F^n, we define the *ball* $B(x, e)$ of radius e centered at x to be the set

$$B(x, e) = \{y \in F^n;\ d(x, y) \leq e\}.$$

Theorem 2.7

1. A code C can detect a maximum of e errors in each word if $d(C) \geq e + 1$.
2. A code C can correct a maximum of e errors in each word if $d(C) \geq 2e + 1$.

Proof

1. $d(C) \geq e + 1$ indicates that two different code words always differ in at least $e + 1$ locations. A received word with a minimum of one and a maximum of e letters therefore cannot be a code word and will be detected as faulty.
2. Suppose x is a received word that differs from a code word y in a maximum of e locations. If $d(C) \geq 2e+1$, there cannot be any other code word z that differs from x in a maximum of e locations. That would mean that $d(y, z) \leq 2e$. One may therefore correct x to y. ■

2.1 Perfect Codes

Lemma 2.8 Let us assume we have a ball $B(x, e)$ centered in $x \in F^n$ with radius e. If F then has q elements, the number of words contained in the ball $B(x, e)$ is exactly

$$\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{e}(q-1)^e.$$

Proof The number of words that differ from x in i positions where $0 \leq i \leq e$, is $\binom{n}{i}(q-1)^i$. ■

Theorem 2.9 (The *ball-packing* or *Hamming bound*) Suppose F has q elements and that the code C in F^n contains M words with the separation $2e + 1$. Then we have

$$M\left[\binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{e}(q-1)^e\right] \leq q^n. \tag{1}$$

If we have equality in (1) we get what is called a *perfect code* according to the following definition.

Definition 2.10 Let e be a positive integer. A code C is called a *perfect e-(Hamming-)error-correcting code* if

1. $F^n = \cup_{x \in C} B(x, e)$
2. $\min\{d(x, y);\ x \in C,\ y \in C,\ x \neq y\} \geq 2e + 1$

A perfect code entails the existence of exactly one code word for each word x in F^n with a maximum distance e from x. By interpreting the equality in (1), we realize that the M balls of radius e centered on the different code words $x_1, \dots, x_n$ will cover the whole space without overlapping each other. One may also describe the equality in (1) as every vector being at most at a distance e from exactly one code word.

Example 2.11 Consider the binary repetition code, consisting of the two vectors $(0, 0, \dots, 0)$ and $(1, 1, \dots, 1)$ of length n. If $n = 2e + 1$ is odd, then this is a perfect code with parameters $n = 2e + 1$ and $q = 2$.

This kind of codes are called *trivial* perfect codes, as well as codes which contain only one code word. The latter have parameters $n = e$ and q where q is a prime power.

2.2 Linear Codes

Definition 2.12 A code C in F^n is called *linear* if it is a subspace of F^n. If we assume that C has dimension k, then it is called an $[n, k]$-code.

We observe that for a linear code C the separation equals the weight.

Definition 2.13 The *dual code* $C^\perp$ of a linear $[n, k]$-code C is defined to be the set of vectors of F^n which are perpendicular to every code word of C, i.e. where the scalar product between these is zero.

$$C^\perp = \{y \in F^n;\ \langle x, y \rangle = 0 \quad \forall x \in C\}.$$

Definition 2.14 A *generator matrix* for a linear code C is a matrix, the rows of which are a basis for C. A *control matrix* for C is a generator matrix for $C^\perp$.

2.3 Hamming Codes

Definition 2.15 Let C be a linear $[n, k]$-code in F^n with separation $2e + 1 = 3$. If C has a control matrix H, such that every vector in F^{n-k} can be obtained by multiplying some column of H by an element in F, then the code is called a Hamming code.

Theorem 2.16 Hamming codes are perfect.

Proof If two columns of H are linearly dependent, there must be a code word, the weight of which is 2 or less. Since this contradicts the assumptions, every two columns in H must be linearly independent. The products ay where $a \neq 0$ is an element of F and y a column of H must therefore be distinct. This means that F^{n-k} contains $(q-1)n$ non-zero vectors and since F^{n-k} contains q^{n-k} vectors we conclude that $(q-1)n + 1 = q^{n-k}$. According to theorem 2.9 the code is perfect. ■

The equality $(q-1)n + 1 = q^{n-k}$ can be written as $n = 1 + q + q^2 + \cdots + q^{n-k-1}$ and now it is not hard to see that there always exists a Hamming code with the parameters $e = 1$, and n and q satisfying the equality.

2.4 Golay Codes

Let C be the $[12,6]$-code over $\mathbf{Z}_3$ with generator matrix

$$G = \left[\begin{array}{cccccc|cccccc}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 \\
0 & 0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 1 & 0
\end{array}\right].$$

We observe that $\langle x, y\rangle = 0$, if x and y are two rows of G. Therefore $\langle x, x\rangle = 0$ for every $x \in C$. Since the elements of $\mathbf{Z}_3$ can be written 0 or ± 1, this implies that the weight $w(x)$ of each code word x is divisible by 3. We will show that there is no code word with weight equal to 3. Such a word must be of type $(3 \mid 0)$, $(2 \mid 1)$, $(1 \mid 2)$ or $(0 \mid 3)$ where the first number is the number of non-zero letters among the first six letters of the code word and the second number the number of non-zero letters among the last six letters of the code word. Since each code word is orthogonal to all the rows of G the types $(3 \mid 0)$, $(2 \mid 1)$ can be ruled out. On the other hand, a code word must be a linear combination of the rows of G, and this is impossible for words of the types $(1 \mid 2)$ or $(0 \mid 3)$. The weight of the code therefore equals 6. If we remove the seventh column from G, we get a generator matrix for an $[11,6]$-code over $\mathbf{Z}_3$ with separation $2e+1=5$. This code is called the Golay code $\mathcal{G}_{11}$. The parameters are $e=2$, $q=3$ and $n=11$, and since the number of code words is 3^6, a simple computation together with theorem 2.9 will reveal that $\mathcal{G}_{11}$ is perfect.

Golay also constructed a perfect binary $[23,12]$-code $\mathcal{G}_{23}$ with separation 7. This code has the parameters $e=3$, $q=2$ and $n=23$.

2.5 Nonexistence

The remainder of this work is dedicated to show that there are no perfect codes over fields with parameters other than those of

1. the trivial perfect codes with $n=e$, or $q=2$, $n=2e+1$,
2. perfect single error-correcting codes with the parameters of Hamming codes,
3. codes with the parameters of the two perfect Golay codes $\mathcal{G}_{11}$ and $\mathcal{G}_{23}$.

3 Krawtchouk Polynomials and Lloyd's Theorem

Let us begin this chapter by defining the tridiagonal matrix $Q_e = Q_e(a,b,s)$ by

$$Q_e(a,b,s) = \begin{bmatrix}
a & b & 0 & \dots & 0 & 0 \\
1 & a+(s-1) & b-s & \dots & 0 & 0 \\
0 & 2 & a+2(s-1) & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \dots & a+(e-1)(s-1) & b-(e-1)s \\
0 & 0 & 0 & \dots & e & a+e(s-1)
\end{bmatrix}$$

and

$$P_e = P_e(a,b,s) = \left[\begin{array}{ccccc|c} &&&&& 1\\ &&&&& 1\\ && Q_{e-1}(a,b,s) &&& \vdots\\ &&&&& 1\\ &&&&& 1\\ \hline 0 & 0 & \cdots & 0 & e & 1 \end{array}\right].$$

Let us also denote the determinants of Q_e and P_e by $\tilde{Q}_e$ and $\tilde{P}_e$, respectively. By developing by the last row, we will find that

$$\tilde{Q}_e = (a + e(s-1))\tilde{Q}_{e-1} - e(b - (e-1)s)\tilde{Q}_{e-2}.$$

By adding all columns to the last one and developing by the last row, we find

$$\tilde{Q}_e = (a + es)\tilde{Q}_{e-1} - e(a+b)\tilde{P}_{e-1}. \tag{2}$$

Developing P_e by the last row, yields

$$\tilde{P}_e = \tilde{Q}_{e-1} - e\tilde{P}_{e-1}. \tag{3}$$

Now apply (3) with $e+1$ instead of e, combine with (3) and eliminate the $\tilde{Q}$-terms by using (2). Then we get

$$\tilde{P}_{e+1} = (a + es - e - 1)\tilde{P}_e - e(b - es)\tilde{P}_{e-1}. \tag{4}$$

This recurrence relation relates the determinants to well-known polynomials.

3.1 Krawtchouk Polynomials

Definition 3.1 The *Krawtchouk polynomial* K_k is defined by

$$K_k(n,u) = \sum_{j=0}^{k} (-1)^j (q-1)^{k-j} \binom{u}{j} \binom{n-u}{k-j}.$$

Lemma 3.2 The generating function for Krawtchouk polynomials is

$$\sum_{k=0}^{\infty} K_k(n,u) z^k = (1-z)^u (1 + (q-1)z)^{n-u}. \tag{5}$$

Proof The right-hand side is equal to

$$\left(\sum_{j=0}^{\infty} \binom{u}{j} (-1)^j z^j \right) \left(\sum_{i=0}^{\infty} \binom{n-u}{i} (q-1)^i z^i \right),$$

and we see that the coefficient for z^k is

$$\sum_{j=0}^{k} \binom{u}{j} (-1)^j \binom{n-u}{k-j} (q-1)^{k-j}. \blacksquare$$

Lemma 3.3 It is true, that

$$(k+1)K_{k+1}(n,u) = (k+(q-1)(n-k)-qu)K_k(n,u) - (q-1)(n+1-k)K_{k-1}(n,u),$$

when $k \geq 1$.

Proof If we differentiate the left-hand side of (5) and multiply by $(1-z)(1+(q-1)z)$, we get

$$\begin{aligned}&(1-z)(1+(q-1)z)\sum_{k=1}^{\infty} kK_k(n,u)z^{k-1} = (1-z)(1+(q-1)z)\sum_{k=0}^{\infty}(k+1)K_{k+1}(n,u)z^k \\ &= \sum_{k=0}^{\infty}(k+1)K_{k+1}(n,u)z^k + (q-2)\sum_{k=1}^{\infty} kK_k(n,u)z^k - (q-1)\sum_{k=1}^{\infty}(k-1)K_{k-1}(n,u)z^k. \quad (6)\end{aligned}$$

If we do the same with the right-hand side, we get

$$\begin{aligned}&(1-z)(1+(q-1)z)(-u(1-z)^{u-1}(1+(q-1)z)^{n-u}+(q-1)(n-u)(1-z)^u(1+(q-1)z)^{n-u-1}) \\ &= -u(1+(q-1)z)(1-z)^u(1+(q-1)z)^{n-u} + (q-1)(n-u)(1-z)(1-z)^u(1+(q-1)z)^{n-u} \\ &= (-u(1+(q-1)z)+(q-1)(n-u)(1-z))\sum_{k=0}^{\infty} K_k(n,u)z^k \\ &= (n(q-1)-qu))\sum_{k=0}^{\infty} K_k(n,u)z^k - n(q-1)\sum_{k=1}^{\infty} K_{k-1}(n,u)z^k. \quad (7)\end{aligned}$$

Identification of coefficients in (6) and (7) gives

$$\begin{aligned}&(k+1)K_{k+1}(n,u) \\ &= (n(q-1)-qu-(q-2)k)K_k(n,u) - (n(q-1)-(q-1)(k-1))K_{k-1}(n,u) \\ &= (k+(q-1)(n-k)-qu)K_k(n,u) - (q-1)(n+1-k)K_{k-1}(n,u)\end{aligned}$$

when $k \geq 1$. ■

3.2 Lloyd's Theorem

Definition 3.4 *Lloyd's polynomial* ψ_e of degree e is defined by

$$\psi_e(n,x) = K_e(n-1,x-1).$$

Using lemma 3.3 along with this definition of Lloyd polynomials, we find that

$$(e+1)\psi_{e+1}(n,x) = (e+(q-1)(n-e)-qx+1)\psi_e(n,x) - (q-1)(n-e)\psi_{e-1}(n,x). \quad (8)$$

Lemma 3.5 Let $s = q-1$. Then we have

$$\tilde{P}_e(qy-ns, ns, s) = (-1)^e e!\psi_e(n,y). \quad (9)$$

Proof For $e = 1$ and $e = 2$, it is easy to check the assertion using the definitions. By substitutions of the appropriate values of a and b in (4) and using (8), we see that the polynomials on both sides of (9) satisfy the same recurrence relation. ■

Definition 3.6 The square matrix A_k of size q^k is defined as follows. Number the rows and columns by the q-ary system from 0 to $q^k - 1$. The entry $A_k(i,j)$ is 1 if the representations of i and j differ in exactly one digit, otherwise $A_k(i,j) = 0$.

From this definition of A_k, it is clear that

$$A_{k+1} = I_q \times (A_k - I_{q^k}) + J_q \times I_{q^k} \tag{10}$$

where I_m denotes the identity matrix of size m, J_m denotes the "all-one"-matrix of size m and × indicates the Kronecker product.

Lemma 3.7 The matrix A_k has the eigenvalues $-k + jq$ with multiplicities

$$\binom{k}{j}(q-1)^{k-j}$$

where $j = 0, 1, \ldots, k$.

Proof (Induction) First, look at the case $k = 1$. We have $A_1 = J_q - I_q$. By adding all of the rows to the last one in $\det(A_1 - \lambda I_q)$ and thereafter subtracting the last column from the remaining columns, we get a triangular determinant. The product of the diagonal elements in this determinant is $(-1-\lambda)^{q-1}(q-1-\lambda)$. Now, let the column vector x be an eigenvector of A_k, belonging to the eigenvalue λ. Then by (10), we have

$$A_{k+1}(x^t, x^t, \ldots, x^t)^t = (\lambda + q - 1)(x^t, x^t, \ldots, x^t)^t \tag{11}$$

where x^t is repeated q times on both sides. If $(c_1, \ldots, c_q)^t$ is eigenvector of J_q with eigenvalue 0 (which has multiplicity $q - 1$), then

$$A_{k+1}(c_1 x^t, \ldots, c_q x^t)^t = (\lambda - 1)(c_1 x^t, \ldots, c_q x^t) \tag{12}$$

since $\sum c_i = 0$. The induction step now follows from (11) and (12) and well-known properties of binomial coefficients. ■

Lemma 3.8 Let A be an $(m \times m)$-matrix of the form

$$A = \begin{bmatrix} A_{11} & A_{12} & \ldots & A_{1k} \\ A_{21} & A_{22} & \ldots & A_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{k1} & A_{k2} & \ldots & A_{kk} \end{bmatrix}.$$

Let each element A_{ij} in A be an $(m_i \times m_j)$-matrix where $i = 1, 2, \ldots, k$ and $j = 1, 2, \ldots, k$. Suppose, for each i and j, that the matrix A_{ij} has constant row sums b_{ij} and let these be entries in another matrix B. Then each eigenvalue of B is also an eigenvalue of A.

Proof Let $Bx = \lambda x$ where $x = (x_1, x_2, \ldots, x_k)^t$ and define y by

$$y^t = (x_1, x_1, \ldots, x_1, x_2, x_2, \ldots, x_2, \ldots, x_k, x_k, \ldots, x_k)$$

where each x_i is repeated m_i times. By definition of B, it is obvious that $Ay = \lambda y$. ■

Theorem 3.9 (Lloyd's theorem) If a perfect e-error-correcting code of block length n over $GF(q)$ exists, then the polynomial $\psi_e(n, x)$ has e distinct integral zeros among the integers $1, 2, \ldots, n$.

Proof It is a well-known fact that the zeros of the Krawtchouk polynomials are simple. Assume C to be a perfect e-error-correcting code of block length n over an alphabet $\{0, 1, \ldots, q-1\}$ of q symbols. Consider the matrix A_n, defined as in definition 3.6. Let's reorder the rows and columns of A_n as follows. First, take the rows and columns with a number corresponding to an element of C. Then take, successively, those with numbers corresponding to elements of C_i as in definition 2.5 where $i = 1, 2, \ldots, e$. Since C is a perfect code, the matrix A_n now has the form of a tridiagonal matrix A as in lemma 3.8 with

$$B = \begin{bmatrix} 0 & ns & 0 & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 1 & q-2 & (n-1)s & 0 & 0 & \ldots & 0 & 0 & 0 & 0 \\ 0 & 2 & 2(q-2) & (n-2)s & 0 & \ldots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \ldots & 0 & e-1 & (e-1)(q-2) & (n-e+1)s \\ 0 & 0 & 0 & 0 & 0 & \ldots & 0 & 0 & e & ns-e \end{bmatrix}$$

where $s = q-1$. Now, apply lemma 3.8. The eigenvalues of A_n were determined in lemma 3.7. In $\det(B - xI_{e+1})$, we substitute $x = ns - yq$ which leads to the problem of determining $\tilde{P}_e(qy - ns, ns, s)$. Then Lloyd's theorem follows from lemma 3.5. ■

4 Nonexistence Theorems for Perfect Codes

Throughout this chapter, we will let $GF(q)$ denote a finite field with q elements where q is a prime power, as always. We will also let the n-dimensional vector space over $GF(q)$ be denoted by $V(n, q)$.

4.1 Preceding Lemmas

Lemma 4.1 If there exists a perfect e-error-correcting code of block length n over $GF(q)$, then there exists an integer k such that

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^{n-k}. \tag{13}$$

The cardinality of the code equals q^k.

Proof The number of vectors in the ball $B(x, e)$ is $\sum_{i=0}^{e} \binom{n}{i} (q-1)^i$. If the code is perfect, this number must be a divisor of the cardinality q^n of $V(n, q)$. Hence, for some integer m, we have

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i = p^m.$$

Since $\sum_{i=0}^{n} \binom{n}{i} (q-1)^i = q^n$ we get, by subtraction,

$$q^n - p^m \equiv 0 \pmod{(q-1)}$$

which implies that p^m is a power of q, i.e. $p^m = q^{n-k}$. Therefore a necessary condition for the existence of a perfect e-error-correcting code over $GF(q)$ with block length n is

$$\sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^{n-k}$$

which is (13). We also see that q^k is the cardinality of the code. ■

Lemma 4.2 If there exists a perfect e-error-correcting code of block length n over $GF(q)$, with $e < n$, there are positive integers $x_1, \ldots, x_e$ such that $1 \leq x_1 < x_2 < \cdots < x_e \leq n-1$,

$$x_1 + \cdots + x_e = \frac{e(n-e)(q-1)}{q} + \frac{e(e+1)}{2}, \tag{14}$$

$$x_1 \cdots x_e = e! q^{n-k-e}, \tag{15}$$

and

$$x_1 \geq \frac{(n-e+1)(q-1)+e}{(q-1)+e}. \tag{16}$$

Proof According to Lloyd's theorem, the distinct zeros $x_1, \ldots, x_e$ of $\psi_e(n,x)$ are integers. By lemma 4.1 and definition 3.4, we have

$$\psi_e(n,0) = \sum_{i=0}^{e} (-1)^i \binom{n}{e-i} \binom{-1}{i} (q-1)^{e-i} = \sum_{i=0}^{e} \binom{n}{i} (q-1)^i = q^{n-k}.$$

The coefficient of x^e in $\psi_e(n,x)$ is

$$\sum_{i=0}^{e} (-1)^i \frac{(-1)^{e-i}}{(e-i)!} \frac{1}{i!} (q-1)^{e-i} = \frac{(-1)^e}{e!} \sum_{i=0}^{e} \binom{e}{i} (q-1)^i = \frac{(-1)^e q^e}{e!}.$$

Analogously, we find the coefficient of x^{e-1} to be

$$\sum_{i=0}^{e} \frac{(-1)^e (q-1)^{e-i}}{(e-i)! i!} \left[-\sum_{j=0}^{e-i-1} (n-j) - \sum_{j=1}^{i} j \right] = \frac{(-1)^{e-1}}{e!} q^{e-1} \left[e(n-e)(q-1) + \frac{e(e+1)q}{2} \right].$$

From the coefficients of x^e, x^{e-1} and x^0 in $\psi_e(n,x)$, the sum and product of the zeros are found.

To prove (16), we first remark that if a is a positive integer, then $\binom{a}{i} \geq 0$ because a negative factor in the numerator of

$$\binom{a}{i} = \frac{a(a-1)\cdots(a-i+1)}{i!}$$

only occurs if some other factor is 0. Next, we remark that if all terms in the sum defining $\psi_e(n,x)$ are zero for some value of x, then $n = e$ which contradicts the assumptions. Assuming x to be an integer, this sum is therefore an alternating sum with non-negative terms which decrease in absolute value if

$$x < \frac{(n-e+1)(q-1)+e}{(q-1)+e}. \blacksquare$$

Lemma 4.3 Given a code of block length n and cardinality q^k, there exists a critical ball of integral radius t which includes K code words where

$$K \geq q^{k-n} \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

By a suitable translation of the code, this critical ball may be centered at $(0,0,\ldots,0)$. A critical ball is a ball containing a maximum number of code words.

Proof There are q^n balls of radius t centered at the points in the space. Let K_i be the number of code words in the ith ball where $i = 1, \dots, q^n$, let and $K = \max K_i$. Each of the code words appears in

$$V = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

of the balls. The number of pairs (c, B) where c is a code word and B a ball containing c, can be counted in two different ways,

$$\sum_{i=1}^{q^n} K_i = q^k V.$$

Since

$$\sum_{i=1}^{q^n} K_i \le q^n K,$$

this yields

$$K \ge q^{k-n} V = q^{k-n} \sum_{i=0}^{t} \binom{n}{i} (q-1)^i.$$

If the word at the center of the critical ball is subtracted from each of the code words, the center of the critical ball is translated into the null vector 0, and the minimum distance of the code is unchanged. ■

Lemma 4.4 The eigenvalues of the $(q \times q)$-matrix

$$A = \begin{bmatrix} 0 & 1 & 1 & & 1 \\ 1 & 0 & 1 & & 1 \\ 1 & 1 & 0 & & 1 \\ & & & \ddots & \\ 1 & 1 & 1 & & 0 \end{bmatrix}$$

are $q-1$ and -1 where the latter has the multiplicity $q-1$.

Proof This follows directly from lemma 3.7. ■

Lemma 4.5 The function $f : \mathbf{R}^q \to \mathbf{R}$ defined by $f(x) = xAx^t$ is concave on the set

$$M = \{x \in \mathbf{R}^q;\ \sum_{k=0}^{q-1} x_k = 1\}.$$

Proof Let $e_0, \dots, e_{q-1}$ be an orthonormal basis of eigenvectors for the matrix A where the vector e_k belongs to the eigenvalue λ_k. Choose $\lambda_0 = q-1$ and $e_0 = (1, \dots, 1)/\sqrt{q}$. We can write x and y in M as $x = \sum_{k=0}^{q-1} u_k e_k$ and $y = \sum_{k=0}^{q-1} v_k e_k$. Suppose $a \ge 0$, $b \ge 0$ and $a + b = 1$. Then we have

$$f(ax + by) = \sum_{k=0}^{q-1} \lambda_k (au_k + bv_k)^2$$

and

$$af(x) + bf(y) = a \sum_{k=0}^{q-1} \lambda_k u_k^2 + b \sum_{k=0}^{q-1} \lambda_k v_k^2.$$

It is true, that x, y and $ax+by$ belong to M. If $x=\sum_{k=0}^{q-1} u_k e_k$ is in M, then it is also true, that $u_0=\langle e_0,x\rangle = 1/\sqrt{q}$. This implies that

$$u_0 = v_0 = au_0 + bv_0 = 1/\sqrt{q},$$

whence

$$\lambda_0(au_0+bv_0)^2 = a\lambda_0 u_0^2 + b\lambda_0 v_0^2.$$

Because of this, we get

$$af(x)+bf(y)-f(ax+by) = \sum_{k=1}^{q-1} \lambda_k(au_k^2+bv_k^2-(au_k+bv_k)^2) \leq 0,$$

since t^2 is a convex function of t and $\lambda_k \leq 0$, $k=1,\ldots,q-1$. ■

Let C be a code consisting of K code words $c^{(1)},\ldots,c^{(K)}$. With the *total distance* between pairs of code words, we mean

$$d_{\text{tot}} = \sum_{i=1}^{K}\sum_{j=1}^{K} d(c^{(i)},c^{(j)}) = \sum_{i=1}^{K}\sum_{j=1}^{K}\sum_{k=1}^{n} d(c_k^{(i)},c_k^{(j)}) = \sum_{k=1}^{n}\sum_{i=1}^{K}\sum_{j=1}^{K} d(c_k^{(i)},c_k^{(j)}).$$

For a fix k, let $p_m^{(k)}$ denote the number of occurrences of the m:th letter in the alphabet amongst the letters $c_k^{(1)},\ldots,c_k^{(K)}$. The vector

$$p^{(k)} = (p_0^{(k)},\ldots,p_{q-1}^{(k)})/K \tag{17}$$

will then be a probability vector and

$$\sum_{i=1}^{K}\sum_{j=1}^{K} d(c_k^{(i)},c_k^{(j)}) = \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} p_i^{(k)}p_j^{(k)}A_{ij} = K^2 p^{(k)}A(p^{(k)})^t,$$

where A is the said matrix above. We get

$$d_{\text{tot}} = K^2\sum_{k=1}^{n} p^{(k)}A(p^{(k)})^t.$$

Now, let p be a probability vector which maximises pAp^t. Since there are $K(K-1)$ pairs of different code words, it is true for the average distance between these code words, that

$$d_{\text{av}} = \frac{K^2}{K(K-1)}\sum_{k=1}^{n} p^{(k)}A(p^{(k)})^t \leq \frac{nK^2}{K(K-1)}pAp^t.$$

Consequently, regarding the minimal distance between different code words, we get

$$d_{\text{min}} \leq \frac{nK^2}{K(K-1)}pAp^t.$$

This inequality is called “the Plotkin bound on minimum distance”.

We now use lemma 4.5 to determine the maximum of pAp^t. According to this lemma,

$$f(p) = pAp^t - 2\frac{q-1}{q}\left(\sum_{i=0}^{q-1} p_i - 1\right)$$

is a concave function of $p \in M = \{p \in \mathbf{R}^q;\ \sum_{i=0}^{q-1} p_i = 1\}$. We see that $p = (1,\ldots,1)/q$ is a critical point of f. Since the function f is concave on M, it will assume its maximum value when $p = (1,\ldots,1)/q$. Therefore, also pAp^t will assume its maximum value when $p = (1,\ldots,1)/q$ and then we get

$$pAp^t = \frac{q-1}{q}.$$

By defining $\bar{A} = (q-1)/q$, the following lemma emerges.

Lemma 4.6

$$d_{\mathrm{min}} \le d_{\mathrm{av}} \le \frac{\bar{A}n}{1-K^{-1}}.$$

Lemma 4.7 If each of K code words has a weight that is no greater than $(q-1)xn/q$ where $0 \le x \le 1$, then the distance between some pair of these K code words must be no greater than

$$\frac{(q-1)(2-x)xn}{q(1-K^{-1})}.$$

Proof With $p^{(k)}$ defined as in (17), we get

$$d_{\mathrm{tot}} = K^2 \sum_{k=1}^{n} p^{(k)} A (p^{(k)})^t,$$

and

$$d_{\mathrm{min}} \le \frac{d_{\mathrm{tot}}}{K^2 - K}.$$

The total weight of code words is $\sum_{k=1}^{n} KA^{(0)}(p^{(k)})^t$ where $A^{(0)}$ is the first row in the matrix A. According to the assumptions, the total weight is at most

$$\frac{K(q-1)xn}{q} = K\bar{A}xn,$$

and we get

$$\sum_{k=1}^{n} A^{(0)}(p^{(k)})^t \le \bar{A}xn.$$

Now, we want probability vectors $p^{(1)},\ldots,p^{(n)}$ that maximise $\sum_{k=1}^{n} p^{(k)}A(p^{(k)})^t$ under the condition $\sum_{k=1}^{n} A^{(0)}(p^{(k)})^t \le \bar{A}xn$. We will perform this construction in two steps. First, we maximise $p^{(k)}A(p^{(k)})^t$ under the condition $A^{(0)}(p^{(k)})^t = \bar{A}x_k$ and thereafter we choose maximising x_k, $k = 1,\ldots,n$, under the condition $\sum_{k=1}^{n} x_k \le nx$. When

$$\sum_{i=0}^{q-1} p_i^{(k)} = 1, \quad A^{(0)}(p^{(k)})^t = \bar{A}x_k \tag{18}$$

it is true, that

$$p^{(k)}A(p^{(k)})^t = \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} p_i^{(k)} p_j^{(k)} A_{ij} = f(p^{(k)})$$

where

$$f(p^{(k)}) = \sum_{i=0}^{q-1}\sum_{j=0}^{q-1} p_i^{(k)} p_j^{(k)} A_{ij} + \lambda\left(\bar{A}x_k - \sum_{i=0}^{q-1} A_{0i}p_i^{(k)}\right) + \mu\left(1 - \sum_{i=0}^{q-1} p_i^{(k)}\right).$$

Here, the Lagrange multipliers, λ and μ, are any constants. Now, we differentiate with respect to $p_m^{(k)}$, $m = 0, \ldots, q-1$ and set the partial derivatives equal to zero. Since $A_{mm} = 0$, we get for each m,

$$\sum_{i=0}^{q-1} p_i^{(k)} A_{im} + \sum_{j=0}^{q-1} p_j^{(k)} A_{mj} - \lambda A_{0m} - \mu = 0,$$

which is equivalent to

$$2\sum_{i=0}^{q-1} p_i^{(k)} A_{im} = \lambda A_{0m} + \mu.$$

If we let $\lambda = 2(1-x_k)$ and $\mu = 2x_k\bar{A}$, we see that

$$p^{(k)} = \frac{x_k}{q}(1, \ldots, 1) + (1-x_k)(1, 0, \ldots, 0)$$

is a critical point which satisfies (18). Since f is a concave function on the set M where $M = \{p \in \mathbf{R}^q;\ \sum_{i=0}^{q-1} p_i = 1\}$, we know that $p^{(k)}$ has to maximise $p^{(k)}A(p^{(k)})^t$ under the condition (18). The maximum value is

$$p^{(k)}A(p^{(k)})^t = x_k(2-x_k)\bar{A}.$$

What is left, is to choose $x_1, \ldots, x_n$ such that $\sum_{k=1}^n \bar{A}x_k(2-x_k)$ is maximised under the condition $\sum_{k=1}^n x_k \leq nx$. If we now set $x_k = x$, $k = 1, \ldots, n$, we get a critical point and since $x(2-x)$ is a concave function of x, the sum will assume its maximum value under the condition in this point. The total distance will then be $K^2x(2-x)\bar{A}n$ and the average distance for a pair of different code words is

$$\frac{K^2x(2-x)\bar{A}n}{K(K-1)} = \frac{x(2-x)(q-1)n}{q(1-K^{-1})}. \blacksquare$$

Lemma 4.8 If $e < n$, then $\psi_e(n,n) \neq 0$.

Proof It is true, that

$$\psi_e(n,n) = (-1)^e\binom{n-1}{e} \neq 0, \quad \text{if} \quad n > e \geq 1. \blacksquare$$

Lemma 4.9

$$\sum_{i=0}^{e-j}\binom{n-x-j}{e-i-j}\binom{x-1}{i} = \binom{n-j-1}{e-j}. \tag{19}$$

Proof Taylor expansion gives

$$\begin{aligned}(1+z)^{n-j-1} &= \sum_{k=0}^{\infty}\binom{n-j-1}{k}z^k = (1+z)^{n-x-j}(1+z)^{x-1}\\ &= \left(\sum_{k=0}^{\infty}\binom{n-x-j}{k}z^k\right)\left(\sum_{i=0}^{\infty}\binom{x-1}{i}z^i\right)\\ &= \sum_{k=0}^{\infty}\sum_{i=0}^{k}\binom{n-x-j}{k-i}\binom{x-1}{i}z^k.\end{aligned}$$

Identifying coefficients of z^{e-j} completes the proof. $\blacksquare$

Lemma 4.10 It is true, that

$$\psi_e(n,x) = (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{n-x}{j} \binom{n-j-1}{e-j}. \tag{20}$$

Proof

$$\begin{aligned}
\psi_e(n,x) &= \sum_{i=0}^{e} (-1)^i \binom{n-x}{e-i} \binom{x-1}{i} \sum_{j=0}^{e-i} \binom{e-i}{j} q^j (-1)^{e-i-j} \\
&= (-1)^e \sum_{j=0}^{e} (-1)^j q^j \sum_{i=0}^{e-j} \binom{n-x}{e-i} \binom{e-i}{j} \binom{x-1}{i} \\
&= (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{n-x}{j} \sum_{i=0}^{e-j} \binom{n-x-j}{e-i-j} \binom{x-1}{i} \\
&= (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{n-x}{j} \binom{n-j-1}{e-j}. \blacksquare
\end{aligned}$$

Lemma 4.11 If there exists a perfect e-error-correcting code of block length n over $GF(q)$ when $e < n$, then

$$q \le \frac{n-1}{e}.$$

Proof Since there exists a perfect e-error-correcting code and since $e < n$, Lloyd's theorem, along with lemma 4.8, tells us that $\psi_e(n,x)$ has its zeros in the set $\{1,\ldots,n-1\}$ and according to lemma 4.8, we have

$$\psi_e(n,n) = (-1)^e \binom{n-1}{e} \neq 0.$$

Lemma 4.10 gives

$$\begin{aligned}
\psi_e(n,n-1) &= (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{1}{j} \binom{n-j-1}{e-j} = (-1)^e \left(\binom{n-1}{e} - q \binom{n-2}{e-1} \right) \\
&= (-1)^e \binom{n-1}{e} \left(1 - \frac{qe}{n-1}\right) = \psi_e(n,n) \left(1 - \frac{qe}{n-1}\right)
\end{aligned}$$

and since either $\psi_e(n,n-1) = 0$ or $\psi_e(n,n-1)$ and $\psi_e(n,n)$ have the same sign, we know that

$$1 - \frac{qe}{n-1} \ge 0. \blacksquare$$

Extensive computer searches have been made to be able to exclude some cases of our parameters. We present the way to cover these cases in an appendix. The ranges covered are presented in the following lemma.

Lemma 4.12 If there exists an unknown perfect e-error-correcting code of block length n over $GF(q)$, then

$$q > 100 \quad \text{or} \quad n > 10000 \quad \text{or} \quad e > 1000.$$

4.2 Cases e $\leq$ 7

Theorem 4.13 For $q \geq 2$ where q is a prime power, there are no unknown perfect 2-error-correcting codes over the alphabet $GF(q)$ with block length $n > 2$.

Proof Assume $q = e = 2$. By replacing $n - k$ by k in (13), we get

$$n^2 + n + 2 = 2^{k+1}$$

where $k > 2$. The right-hand side, and consequently the left-hand side, is divisible by 8. This shows that $n \equiv 2 \pmod 8$ or $n \equiv 5 \pmod 8$. Now (14) yields $x_1 + x_2 = n + 1 \not\equiv 0 \pmod 8$. Therefore at least one of x_1 and x_2 is not divisible by 8 and according to (15), $x_1 x_2 = 2^{k-1}$. Hence $x_1 \leq 4$ and according to (16), $x_1 \geq (n+1)/3$ which results in $n \leq 11$. According to lemma 4.12 there are no unknown perfect codes in this case.

Now assume $q \geq 3$ and suppose that there does exist a perfect 2-error-correcting code of block length n over $GF(q)$ where $q = p^\alpha$ is a prime power. By Lloyd's theorem, the polynomial

$$2\psi_2(n, x) = (qx)^2 - [(2n-1)q - (2n-4)](qx) + 2\psi_2(n, 0)$$

has two integral zeros x_1 and x_2 where $1 \leq x_i \leq n - 1$, $i = 1, 2$. According to lemma 4.1, we have $\psi_2(n, 0) = q^k$ for some integer k. Hence the equation

$$(qx)^2 - [2n(q-1) - q + 4](qx) + 2q^k = 0 \tag{21}$$

has two integral roots x_1 and x_2. If we consider (13) as a quadratic equation in n, we find

$$2(q-1)n = q - 3 + \sqrt{8q^k + q^2 - 6q + 1}. \tag{22}$$

With this, (21) implies that

$$x_1 x_2 = 2q^{k-2}$$

and

$$q(x_1 + x_2) = 1 + \sqrt{8q^k + q^2 - 6q + 1}. \tag{23}$$

By substitution, we see that $x = 1$ is a zero of ψ_2 only if $n = 1$ or $n = 2$. If $x = 2$ is a zero of ψ_2, then $n = 2$ or $(n-3)(q-1) = 2$, i.e., $n = 5$, $q = 2$ corresponding to the repetition code of block length 5 or $n = 4$, $q = 3$ in which case (13) is not satisfied. We may therefore assume that x_1 and x_2 are both divisible by the prime p. Let us write

$$x_1 = p^\lambda, \qquad x_2 = 2p^\mu \tag{24}$$

where $\lambda > 0$, $\mu > 0$ and $\lambda + \mu = (k-2)\alpha$ where $q = p^\alpha$. We also remark that $k \geq 3$ since otherwise (22) would yield $n \leq 2$. We now substitute (24) in (23) and eliminate the square root which results in

$$8q^{k-1} + q - 6 = q(p^\lambda + 2p^\mu)^2 - 2(p^\lambda + 2p^\mu). \tag{25}$$

Considering the highest power of p which divides both the right-hand side and the left-hand side of this equation makes it obvious that p must be 2 or 3. If $p = 2$, the right-hand side is divisible by 4 while the left-hand side is only divisible by 4 if $q = 2$. If $p = 3$ and $q > 3$, reduction of both sides modulo 9 yields

$$3 \equiv 3^\lambda + 2 \cdot 3^\mu \pmod 9$$

and this implies that $\lambda = 1$ and $\mu > 1$. Then we can reduce (25) to the form

$$q^{k-1} = 2q + q \cdot 3^{2\mu} - 3^{\mu}$$

which is impossible since the left-hand side is divisible by a higher power of 3 than the right-hand side. If $p = q = 3$, then $\alpha = 1$ and $\lambda + \mu = k - 2$. Now (25) yields $\lambda = 2$ and $\mu = 1$. The roots of $\psi_2(n, x)$ are then $x_1 = 9$ and $x_2 = 6$. An easy computation shows that in this case $n = 11$. The only non-trivial perfect 2-error-correcting code when $q \geq 3$ therefore has the parameters of $\mathcal{G}_{11}$. ■

Theorem 4.14 The only perfect 3-error-correcting codes over $GF(q)$ when $n > 3$ are those with parameters $q = 2$ and either $n = 7$ or $n = 23$.

Proof Assume first that $q = 2$. Then (13) yields $(n + 1)(n^2 - n + 6) = 3 \cdot 2^{k+1}$ for some integer k. This may also be written $(n + 1)((n + 1)^2 - 3(n + 1) + 8) = 3 \cdot 2^{k+1}$. If $n + 1$ is divisible by 16, then the highest power of 2 which divides $n^2 - n + 6$ is 2^3, i.e. $n^2 - n + 6$ divides 24, and then $n + 1 < 16$. Therefore $n + 1$ is not divisible by 16 and hence $n + 1$ divides 24. This leaves only the following possible values for n: $n = 7$, corresponding to the repetition code and $n = 23$ corresponding to the binary Golay code.

Now, let us assume that $q \geq 3$ and $n > 3$. From Lloyd's theorem, we look at $\psi_3(n, x)$ and use the notations

$$(q - 1)n = t, \qquad qx = t + \theta.$$

Then we have

$$\begin{aligned} -6\psi_3(n, x) &= \theta^3 + 3(q - 3)\theta^2 + (2q^2 - 9q + 18 - 3t)\theta - [(2q - 7)t + 6] \\ &= \theta^3 + 3(q - 3)\theta^2 + (2q^2 - 9q + 18)\theta - 6 - (3\theta + 2q - 7)t \\ &= \Gamma(\theta). \end{aligned} \tag{26}$$

Note that by (13), we have

$$1 + \binom{n}{1}(q - 1) + \binom{n}{2}(q - 1)^2 + \binom{n}{3}(q - 1)^3 = q^k.$$

Using elementary algebra, it then follows that

$$\frac{1}{6}(n - 1)(n - 2)(n - 3) \equiv 0 \pmod{q}.$$

If we write $n = qv + r$ where $r = 1, 2$ or 3, then

$$n - v - 1 \leq n - v - 1 + \frac{3 - r}{q} < n - v - \frac{r - 1}{q} \leq n - v,$$

i.e., there are no integers x, satisfying

$$t + 3 - q < qx < t + 1. \tag{27}$$

By (26), we have

$$\Gamma(3 - q) = (q - 1)(q - 2)(n - 3) > 0$$

and

$$\Gamma(1) = 2(q - 1)(q - 2)(1 - n) < 0.$$

Hence Γ has a zero in the interval $(3 - q, 1)$, i.e., $\psi_3(n, x)$ has a zero in the interval (27), and this zero is not an integer. Since the condition of Lloyd's theorem is not satisfied, there are no perfect 3-error-correcting codes for $q \geq 3$ when $n > 3$. ■

Using equality in (1) it follows at once, that all non-trivial 1-error-correcting codes must have the parameters of a Hamming code. Therefore we have now covered the cases $e = 1$, $e = 2$ and $e = 3$, and continue with the case $e \geq 4$. We also exclude the trivial case $n = e$. Then, replacing $n - k$ in lemma 4.1 by k, it follows that $k < n$ and that $k > e$ since $\binom{n}{i} > \binom{e}{i}$ when $i \neq 0$. Summarizing: from now on, we have

$$n > k > e \geq 4. \tag{28}$$

From (14) it also follows that

$$e(n - e) \equiv 0 \pmod{q}. \tag{29}$$

Theorem 4.15 If $e \geq 4$ and $q = p^\alpha$ where $p > e$, then there are no non-trivial perfect e-error-correcting codes over $GF(q)$.

Proof By using lemma 4.10 with $x = 0$ and replacing $n - k$ by k in lemma 4.1, we find

$$\sum_{j=0}^{e} (-1)^j q^j \binom{n}{j} \binom{n-j-1}{e-j} = (-1)^e q^k \tag{30}$$

where $k > e$. Since $p > e$, we find from (29), that $q \mid (n - e)$. Furthermore, in the binomial coefficients in (30), the factor p does not occur in the denominator but for every $j < e$, the factor $(n - e)$ occurs in the numerator of $\binom{n-j-1}{e-j}$. Since $q \mid (n - e)$ and $p > e$, it follows that $p \nmid (n - i)$ where $0 \leq i < e$. Now assume $q = p^\alpha$. If p^γ is the highest power of p dividing $n - e$, then $p^{\alpha j + \gamma}$ is the highest power of p dividing the jth term on the left-hand side of (30) when $j = 0, 1, \ldots, e - 1$ whereas $p^{\alpha e}$ is the highest power of p dividing the last term. Since $k > e$, we must have $\gamma = \alpha e$. This implies that the first term on the right-hand side of (14) is divisible by q^{e-1} whereas the second term contains a factor p only if $e + 1 = p$. It is therefore not possible that all the zeros of $\psi_e(n, x)$ are divisible by p^2 and if $p \neq e + 1$, then it is even impossible that all the zeros are divisible by p. Hence, according to (15), at least one of the zeros is a divisor of $(e + 1)!$. It follows that $x_1 \leq (e + 1)!$ and since $q^e \mid (n - e)$, we have $n - e \geq (e + 1)^e$. Substituting these inequalities in (16), we find $(e + 1)! \geq 1 + \frac{1}{2}(e + 1)^e$ which is false for $e \geq 3$. ■

Van Lint proved, partly by means of computer programs covering a finite number of cases, that there are no perfect codes when $e = 4$ and $p \leq e$ [5] and that there are no perfect codes when $5 \leq e \leq 7$ [10]. Combining these results with lemma 4.12 and theorems 4.13, 4.14 and 4.15 gives us the following corollary.

Corollary 4.16 If there exists an unknown perfect e-error-correcting code of block length n over $GF(q)$, the two following conditions must hold.

1. $e \geq 8$.
2. $q > 100$ or $n > 10000$ or $e > 1000$.

4.3 Finalising

Lemma 4.17 (Refinement of the arithmetic-mean–geometric-mean inequality) Let $y_1, \ldots, y_s$ and p be positive integers such that $y_{i+1}/y_i \geq p$ where $i = 1, \ldots, s - 1$. Then

$$y_1 y_2 \cdots y_s \leq R^{s-1} \left(\frac{y_1 + y_2 + \cdots + y_s}{s} \right)^s \tag{31}$$

where $R = 4p/(p + 1)^2$.

Proof (Induction) The assertion (31) is trivial for $s = 1$. Suppose now, that $h \geq 1$, $y_1 \leq y_2 \leq \cdots \leq y_h$,

$$y_1 y_2 \cdots y_h \leq R^{h-1} \left(\frac{y_1 + y_2 + \cdots + y_h}{h} \right)^h$$

and that $y_{h+1}/y_h \geq p$. Let $(y_1 + y_2 + \cdots + y_h)/h = Y$ and $y_{h+1} = zY$ where $z \geq p$. Then

$$y_1 y_2 \cdots y_{h+1} \leq R^{h-1} z Y^{h+1}. \tag{32}$$

Let

$$f(x) = xY^{h+1} \left(\frac{hY + xY}{h+1} \right)^{-h-1} = x(h+1)^{h+1}(h+x)^{-h-1}.$$

Then f decreases on $[1, \infty)$ and hence

$$f(z) \leq f(p) = p \left(1 + \frac{p-1}{h+1} \right)^{-h-1} \leq 4p(p+1)^{-2} = R.$$

Consequently,

$$zY^{h+1} \leq R \left(\frac{hY + y_{h+1}}{h+1} \right)^{h+1} = R \left(\frac{y_1 + y_2 + \cdots + y_{h+1}}{h+1} \right)^{h+1}.$$

Combining this with (32), we get the assertion (31) in case $s = h + 1$. ■

For a positive integer m, define $A(m) = p^{-u}m$, where p^u is the highest power of p dividing m. Let $x_1, \ldots, x_e$ be positive integers. Write $x_j \sim x_h$ if $A(x_j) = A(x_h)$. This relation $\sim$ defines a partition of the set $\{x_1, \ldots, x_e\}$ into disjoint subsets $X_1, \ldots, X_r$.

Lemma 4.18 If a perfect e-error-correcting code of block length n exists over $GF(q)$, then

$$e - r \geq [e/p] \frac{\log p}{\log e} \tag{33}$$

where $[a]$ denotes the largest integer not exceeding a. If $p = 2$ and $e \geq 8$, we also have

$$r < e + 1 - \frac{5e \log 2}{4 \log e}. \tag{34}$$

Proof It follows from (15), that

$$A(x_1 x_2 \cdots x_e) = A(e!). \tag{35}$$

For a real number a, let $Q(a)$ be the product of the positive integers not exceeding a and not divisible by p. Then

$$\begin{aligned} A(e!) &\leq Q(e) \cdot [e/p]! \\ &\leq Q(e) \left(\frac{e}{p} \right)^{[e/p]} \\ &= Q(e) \cdot e^{[e/p](1 - \frac{\log p}{\log e})}. \end{aligned} \tag{36}$$

On the other hand, $A(x_1 x_2 \cdots x_e)$ is greater than or equal to the product of those r least positive integers which are not divisible by p. Hence

$$A(x_1 x_2 \cdots x_e) \geq Q(e) \cdot e^{r - e + [e/p]}. \tag{37}$$

Collecting the results (35), (36) and (37), we get the assertion (33).

In the case $p = 2$ we use (35) and, clearly,

$$A(e!) = Q(e)[e/2]! \cdot 2^{-[e/4]-[e/8]-\cdots} < Q(e)[e/2]! \cdot 2^{-e/4} \tag{38}$$

since $e \geq 8$. Furthermore,

$$2^{-e/4}[e/2]! < 2^{-5e/4}e^{[e/2]+1} = e^{[e/2]+1-(5e\log 2)/(4\log e)}$$

and combining this with (35) and (38), we get

$$A(x_1x_2\cdots x_e) < Q(e)e^{[e/2]+1-(5e\log 2)/(4\log e)}.$$

On the other hand, we know that

$$A(x_1x_2\cdots x_e) \geq 1\cdot 3\cdot 5\cdots(2r-1) = Q(2r)$$

and therefore, counting the numbers of factors, we get

$$r < \left[\frac{e+1}{2}\right] + \left[\frac{e}{2}\right] + 1 - \frac{5e\log 2}{4\log e} = e + 1 - \frac{5e\log 2}{4\log e}. \blacksquare$$

Lemma 4.19 Let R be defined as in lemma 4.17 and

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

If a perfect e-error-correcting code of block length n exists over $GF(q)$, then

$$R^{e-r} > (n-b)^{-e}e!\binom{n}{e} = \prod_{j=0}^{e-1}\left(1 + \frac{b-j}{n-b}\right).$$

Proof Let X_i be any one of the sets $X_1, \ldots X_r$ and let $s(i)$ be the cardinality of X_i. Let also R_i be defined as

$$R_i = \left(\prod_{x\in X_i} x\right)\Big/\left(\sum_{x\in X_i}\frac{x}{s(i)}\right)^{s(i)}.$$

Now we may apply lemma 4.17 which results in

$$R_i \leq R^{s(i)-1}.$$

From this, it follows that

$$R_1R_2\cdots R_r \leq \prod_{i=1}^{r} R^{s(i)-1} = R^{e-r}$$

or

$$x_1x_2\cdots x_e \leq R^{e-r}\prod_{i=1}^{r}\left(\sum_{x\in X_i}\frac{x}{s(i)}\right)^{s(i)}$$

which, by the arithmetic-mean–geometric-mean inequality, implies that

$$x_1x_2\cdots x_e \leq R^{e-r}\left(\frac{x_1+x_2+\cdots+x_e}{e}\right)^e.$$

Using lemmas 4.1 and 4.2, we find

$$q^{-e}e!\sum_{i=0}^{e}\binom{n}{i}(q-1)^i \le R^{e-r}\left(\frac{(n-e)(q-1)}{q}+\frac{e+1}{2}\right)^e$$

and, consequently,

$$R^{e-r} > (n-b)^{-e}e!\binom{n}{e} = \prod_{j=0}^{e-1}\left(1+\frac{b-j}{n-b}\right)$$

where

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

Theorem 4.20 There are no unknown perfect binary codes.

Proof **In the case $\mathbf{n \ge \frac{2}{3}(e^2+e)}$**: Assume, towards a contradiction, that there does exist an unknown perfect binary code of length $n \ge \frac{2}{3}(e^2+e)$. By corollary 4.16, we may restrict ourselves to $e \ge 8$ and by lemma 4.19, it then follows directly that

$$(8/9)^{e-r} > (n+1)^{-e}e!\binom{n}{e} = \prod_{i=1}^{e}\left(1-\frac{i}{n+1}\right) > 1-\frac{e^2+e}{2(n+1)}. \tag{39}$$

Combining (39), (34) and our assumptions $n \ge \frac{2}{3}(e^2+e)$ and $e \ge 8$, we get

$$(8/9)^{(5e\log 2)/(4\log e)-1} > 1/4.$$

This implies that

$$\frac{e\log 2}{\log e} < \frac{4}{5}\left(\frac{\log 4}{\log(9/8)}+1\right) < \frac{41}{4}$$

and hence, we have $e < 64$. It then follows, from lemma 4.12, that $n > 10000$ which, along with the fact that $e < 64$, implies

$$1-\frac{e^2+e}{2(n+1)} > 3/4 > (8/9)^3. \tag{40}$$

Since $e \ge 8$, (34) gives us the inequality $e-r \ge 3$ and using this inequality along with (40) in (39) will result in the impossible inequality $(8/9)^3 > (8/9)^3$.

In the case $\mathbf{n < \frac{2}{3}(e^2+e)}$: Suppose, again towards a contradiction, that there does exist an unknown code of cardinality 2^k and length $n < \frac{2}{3}(e^2+e)$. Since the trivial codes are excluded, we know that $k \ge 2$ and consequently, by lemma 4.6 with the insertion $q = 2$,

$$d_{\min} \le \frac{n}{2(1-1/4)} = \frac{2n}{3}. \tag{41}$$

On the other hand, by the definition of e-error-correcting codes, $d_{\min} \ge 2e+1$ which, together with the inequality (41), implies

$$n \ge 3e+2. \tag{42}$$

Let $t = e + 2$ in lemma 4.3. If we then use the insertion $q = 2$ in lemma 4.1, we will get

$$\begin{aligned}
K &\geq 2^{k-n}\left(\sum_{i=0}^{e}\binom{n}{i} + \binom{n}{e+1} + \binom{n}{e+2}\right) \\
&= 1 + \left(\binom{n}{e+1} + \binom{n}{e+2}\right) \Big/ \sum_{i=0}^{e}\binom{n}{i} \\
&> 1 + \binom{n+1}{e+2} \Big/ \left(\binom{n}{e}\left(1 + \frac{e}{n-e+1} + \left(\frac{e}{n-e+1}\right)^2 + \cdots\right)\right) \\
&= 1 + \frac{(n+1)(n-e)(n-2e+1)}{(e+1)(e+2)(n-e+1)} \\
&> 1 + \frac{n(n-2e)}{(e+1)(e+2)}
\end{aligned}$$

and hence

$$\frac{1}{1-K^{-1}} = 1 + \frac{1}{K-1} < 1 + \frac{(e+1)(e+2)}{n(n-2e)}.$$

Using the insertion $q = 2$ in lemma 4.7 and choosing $x = 2(e+2)/n$, we thereby get

$$d_{\min} < \frac{2(e+2)(n-e-2)}{n}\left(1 + \frac{(e+1)(e+2)}{n(n-2e)}\right)$$

and by combining this with $d_{\min} \geq 2e + 1$, we obtain

$$3n^3 - (2e^2 + 14e + 8)n^2 + (6e^3 + 26e^2 + 32e + 8)n - (2e^4 + 14e^3 + 36e^2 + 40e + 16) > 0. \quad (43)$$

If $e \leq 100$, our assumption $n < \frac{2}{3}(e^2 + e)$ tells us that $n < 10000$ and we have the case considered by lemma 4.12. Therefore, we may restrict ourselves to the case $e > 100$. Hence

$$(2e+8)n^2 + \left(\frac{2e^3}{3} - \frac{49e^2}{3} - 32e - 8\right)n + 12e^3 + 36e^2 + 40e + 16 > 0$$

and combining this inequality with the inequality (43), we find

$$F(n) = 3n^3 - (2e^2 + 12e)n^2 + \left(\frac{20e^3}{3} + \frac{29e^2}{3}\right)n - (2e^4 + 2e^3) > 0.$$

Since the zeros of F are $e/3$, $3e$ and $\frac{2}{3}(e^2 + e)$ and also since $n > 3e$ by (42), it must be true, that $n > \frac{2}{3}(e^2 + e)$. ■

Theorem 4.21 There are no unknown perfect codes over finite fields.

Proof **In the case $\mathbf{n \geq \frac{1}{2}e^2 + e}$:** Assume, towards a contradiction, that there does exist an unknown perfect code with parameters e, $n \geq \frac{1}{2}e^2 + e$ and q where $q = p^\alpha$ is a prime power. By theorems 4.20 and 4.15 and corollary 4.16, we may restrict ourselves to

$$q \geq 3, \quad e \geq p, \quad e \geq 8.$$

Since $e \geq p$ and $e - r$ is an integer, (33) implies

$$e - r \geq 1. \quad (44)$$

Let $c = [b] + 1$ where b is defined as in lemma 4.19. Then

$$\begin{aligned}\prod_{j=0}^{e-1}\left(1+\frac{b-j}{n-b}\right) &= \prod_{j=0}^{c-1}\left(1+\frac{b-j}{n-b}\right)\prod_{j=c}^{e-1}\left(1+\frac{b-j}{n-b}\right)\\ &> \left(1+\sum_{j=0}^{c-1}\frac{b-j}{n-b}\right)\left(1+\sum_{j=c}^{e-1}\frac{b-j}{n-b}\right)\\ &= 1-\frac{e(e-2b-1)}{2(n-b)}-\frac{c(2b-c+1)(e-c)(c+e-2b-1)}{4(n-b)^2}\\ &\geq 1-\frac{e(e-2b-1)}{2(n-b)}-\frac{(2b+1)^2(2e-2b-1)^2}{4\cdot 16(n-b)^2}\end{aligned}$$

using the arithmetic-mean–geometric-mean inequality. Further using lemma 4.19 and recalling the assumption $n \geq \frac{1}{2}e^2 + e$, we obtain

$$\begin{aligned}R^{e-r} &> 1-\frac{e^2+e}{2(q-1)n-(q-2)e+q}-\frac{e^2(q-2)(e+1)^2q}{16(2(q-1)n-(q-2)e+q)^2}\\ &> 1-\frac{1}{q-1}-\frac{(q-2)q}{16(q-1)^2}\\ &> \frac{15}{16}-\frac{1}{q-1}.\end{aligned}\tag{45}$$

If $p \geq 5$, then this inequality, together with (44), implies that

$$\frac{5}{9} \geq R^{e-r} > \frac{11}{16}$$

which is a contradiction. Suppose now that $p = 3$. In the case that $q \geq 9$, (45) implies that

$$\frac{3}{4} > \frac{13}{16}$$

which is also a contradiction. Therefore, we look at the case when $q = 3$. Then according to lemma 4.18, (45) takes the form

$$[e/3]\frac{\log 3}{\log e} < \frac{\log(64/29)}{\log(4/3)}.$$

Hence $e \leq 26$ and it follows, by lemma 4.12, that $n > 1000$. These two inequalities imply that

$$1-\frac{e^2+e}{2(q-1)n-(q-2)e+q}-\frac{e^2(q-2)(e+1)^2q}{16(2(q-1)n-(q-2)e+q)^2} > \frac{3}{4}$$

in the case when $q = 3$. Substituting this and the equality $R = 3/4$ in (45) and also recalling that $e - r \geq 1$, we get an impossibility.

Suppose finally that $p = 2$, whence $q \geq 4$. According to (34)

$$e-r > \frac{5e\log 2}{4\log e}-1$$

when $p = 2$. Because of the assumption $e \geq 8$, we therefore know that $e - r \geq 3$ and using similar arguments as in the case $p = 3$, we see that $q = 4$. Thus, we may write the inequality (45) in the form

$$e\frac{\log 2}{\log e} < \frac{4\log(18/11)}{5\log(9/8)}+1 < 5.$$

Hence $e < 32$ and, according to lemma 4.12, $n > 1000$. Consequently by (45), we get the impossibility

$$\left(\frac{8}{9}\right)^3 > 1 - \frac{e^2+e}{6n-2e+4} - \frac{e^2(e+1)^2}{2(6n-2e+4)^2} > 1 - \frac{1}{5} - \frac{1}{50}.$$

In the case $\mathbf{n < \frac{1}{2}e^2 + e}$: Suppose, again towards a contradiction, that there does exist an unknown code with parameters e, $n < \frac{1}{2}e^2 + e$ and q such that $q \geq 3$ and $e \geq 8$. Then, by the definition of e-error-correcting codes, we know that

$$n \geq d_{\min} \geq 2e+1. \tag{46}$$

Let $t = e+1$ in lemma 4.3. Then lemma 4.1 tells us that

$$\begin{aligned} K &\geq q^{k-n}\left(\sum_{i=0}^{e}\binom{n}{i}(q-1)^i + \binom{n}{e+1}(q-1)^{e+1}\right) \\ &= 1 + \binom{n}{e+1}(q-1)^{e+1}\left(\sum_{i=0}^{e}\binom{n}{i}(q-1)^i\right)^{-1} \\ &= 1 + \binom{n}{e+1}(q-1)^{e+1}\binom{n}{e}^{-1}(q-1)^{-e}\left(1+\frac{e}{(n-e+1)(q-1)}+\cdots\right)^{-1} \\ &> 1 + \frac{(n-e)((n-e+1)(q-1)-e)}{(e+1)(n-e+1)} \end{aligned} \tag{47}$$

and (46) tells us that

$$K > 1 + \frac{(q-2)(n-e)}{e+1}.$$

Consequently,

$$\frac{1}{1-K^{-1}} = 1 + \frac{1}{K-1} < 1 + \frac{e+1}{(q-2)(n-e)}.$$

By choosing

$$x = \frac{(e+1)q}{(q-1)n}$$

in lemma 4.7, we therefore get

$$d_{\min} < \frac{(e+1)(2(q-1)n-(e+1)q)}{(q-1)n}\left(1+\frac{e+1}{(q-2)(n-e)}\right). \tag{48}$$

By repeating the method above, but instead choosing $t = e+2$, $q = 3$ and

$$x = \frac{3(e+2)}{2n},$$

we get

$$d_{\min} < \frac{(e+2)(4n-3e-6)}{2n}\left(1+\frac{(e+2)^2}{(2n-e)(2n-3e+2)}\right) \tag{49}$$

when $q = 3$. Consider first the case $q \geq 5$. We want to show that the inequalities (46) and (48) imply

$$F(n) = n^2 - \left(\frac{1}{2}e^2 + 3e\right)n + e^3 + 2e^2 > 0. \tag{50}$$

Since the zeros of F are $2e$ and $\frac{1}{2}e^2+e$ and since (46) tells us that $n > 2e$, n must be greater than $\frac{1}{2}e^2+e$ which contradicts the assumption $n < \frac{1}{2}e^2+e$ when $q \geq 5$.

So, if $q \geq 7$, then

$$1+\frac{e+1}{(q-2)(n-e)} \leq \frac{5n-4e+1}{5(n-e)}. \tag{51}$$

Furthermore, for all q, we have

$$\frac{2(q-1)n-(e+1)q}{(q-1)n} < \frac{2n-e-1}{n}.$$

Combining this inequality with the inequalities (46), (48) and (51), we get

$$(e+1)(2n-e-1)(5n-4e+1) > 5(n-e)n(2e+1)$$

or

$$5n^2-(3e^2+11e+3)n+4e^3+7e^2+2e-1>0.$$

Since

$$\left(\frac{1}{2}e^2-4e+3\right)n+e^3+3e^2-2e+1>0,$$

this implies (50).

If $q=5$, the inequalities (46) and (48) imply

$$12n^2-(7e^2+26e+7)n+10e^3+15e^2-5>0. \tag{52}$$

If $e \leq 40$, then the assumption $n < \frac{1}{2}e^2+e$ implies that $n < 1000$ and we have the case considered by lemma 4.12. Therefore, $e > 40$ and hence

$$(e^2-10e+7)n+2e^3+9e^2+5>0$$

which in turn, together with (52), implies (50).

Suppose now, that $q=4$. According to lemma 4.11, we then have $n > 4e$ and it follows that we may replace the assertion (50) with

$$F_1(n)=2n^2-(e^2+10e)n+4e^3+8e^2>0 \tag{53}$$

since the zeros of F_1 are $4e$ and $\frac{1}{2}e^2+e$. To prove (53), we use (47) and get

$$(1-K^{-1})^{-1} < 1+\frac{(e+1)(n-e+1)}{(n-e)(3n-4e+3)} \leq \frac{3n-3e+5}{3n-4e+3}.$$

Therefore,

$$2e+1 < \frac{(e+1)(6n-4e-4)(3n-3e+5)}{3n(3n-4e+3)}$$

or

$$9n^2-(6e^2+18e-9)n+12e^3+4e^2-28e-20>0. \tag{54}$$

Since we may suppose, as in case $q=5$, that $e>40$ we have

$$\left(\frac{3e^2}{2}-27e-9\right)n+6e^3+32e^2+28e+20>0$$

which in turn, together with (54), implies (53).

Suppose finally that $q = 3$. Combining the inequalities (46) and (49), we get

$$12n^3 - (6e^2 + 48e + 12)n^2 + (14e^3 + 63e^2 + 42e - 8)n - (6e^4 + 27e^3 + 42e^2 + 36e + 24) > 0. \quad (55)$$

Since we may suppose, as in case $q = 5$, that $e > 40$, we have

$$(6e + 12)n^2 + (e^3 - 21e^2 - 42e + 8)n + 15e^3 + 42e^2 + 36e + 24 > 0$$

and if we combine this inequality with (55), we obtain

$$F_2(n) = 12n^3 - (6e^2 + 42e)n^2 + (15e^3 + 42e^2)n - (6e^4 + 12e^3) > 0.$$

Now, since the zeros of F_2 are $\frac{1}{2}e$, $2e$ and $\frac{1}{2}e^2 + e$ and since (46) says that $n > 2e$, n must be greater than $\frac{1}{2}e^2 + e$ which contradicts the assumption $n < \frac{1}{2}e^2 + e$. ■

Appendix

The following program is testing when the parameters q, e and n satisfy the equation (13) regarding prime powers $q \leq 100$, $n \leq 10000$ and $e \leq \min(1000, n - 1)$. This program will not print the parameters for the trivial perfect codes nor for any Hamming codes.

```
#include <stdio.h>
#include <stdlib.h>
#include <gmp.h>
#define n_MAX 10000
#define e_MAX 1000
#define q_MAX 100

int isprime(long int p)
{
  ldiv_t result;
  long int a;

  a=3;
  result = ldiv(p,a);
  while (a <= result.quot)
    {
      if (result.rem == 0)
        return 0;
      a += 2;
      result = ldiv(p,a);
    }
  return 1;
}

unsigned long int prime()
{
  static long int p = 1;

  if (p == 1)
    return ((unsigned long int) (p = 2));
  if (p == 2)
    return ((unsigned long int) (p = 3));
  while (1)
    {
      p += 2;
      if (isprime(p))
        return (unsigned long int) p;
    }
}

int main()
{
  mpz_t q_pow;
  mpz_t s_term;
  mpz_t sum;
  unsigned long int e_max, e, n, p, q, q_1, tmp;
  int sgn;

  mpz_init(q_pow);
  mpz_init(s_term);
  mpz_init(sum);

  while ((p=prime()) <= q_MAX)
    {
      for(q = p; q <= q_MAX; q *= p)
        {
          q_1 = q - 1;
          for (n = 2; n <= n_MAX; n++)
            {
              mpz_set_ui(q_pow,(unsigned long int) 1);
              mpz_set_ui(sum,(unsigned long int) 1);
              mpz_set_ui(s_term,(unsigned long int) 1);
              e_max = e_MAX;
              if (e_max >= n)
                e_max = n - 1;
              for (e = 1; e <= e_max; e++)
                {
                  tmp = q_1*(n - e + 1);
                  mpz_mul_ui(s_term,s_term,tmp);
                  mpz_divexact_ui(s_term,s_term,e);
                  mpz_add(sum,sum,s_term);
                  while((sgn = mpz_cmp(q_pow,sum)) < 0)
                    mpz_mul_ui(q_pow,q_pow,q);
                  if((sgn == 0)
                     && (e > 1)
                     && !((q == 2) && (n == e + e + 1)))
                    printf("e=%lu, n=%lu, q=%lu\n",e,n,q);
                }
            }
        }
    }
  return 0;
}
```

A running of the program above, will give the output

```
e=3, n=23, q=2
e=2, n=90, q=2
e=2, n=11, q=3
```

where we can see that $e = 3$, $n = 23$, $q = 2$ and $e = 2$, $n = 11$, $q = 3$ represent the known Golay codes whilst $e = 2$, $n = 90$, $q = 2$ does not represent any perfect code, which is revealed in Lloyd's theorem.

References

[1] Raymond Hill, *A First Course in Coding Theory*, Clarendon Press (1988)

[2] J.H. van Lint, *Introduction to Coding Theory*, Springer (1999)

[3] Aimo Tietäväinen, *On the Nonexistence of Perfect Codes Over Finite Fields*, SIAM Journal on Applied Mathematics, Vol. 24, No 1 (1973)

[4] J.H. van Lint, *On the Nonexistence of Perfect 2- and 3-Hamming-Error-Correcting Codes over $GF(q)$*, Information and Control 16 (1970)

[5] J.H. van Lint, *Nonexistence Theorems for Perfect Error-Correcting Codes*, Computers in Algebra and Number Theory, (Proc. Sympos. Appl. Math., New York, 1970), pp. 89–95. SIAM-AMS Proc., Vol. IV, Amer. Math. Soc., Providence, R.I. (1971)

[6] J.H. van Lint and D.M. Cvetković, *An Elementary Proof of Lloyd's Theorem*, De Koninklijke Nederlandse Akademie van Wetenschappen, Series A, Vol. 80(1) (1976)

[7] J.H. van Lint, *A Survey of Perfect Codes*, Rocky Mountain Journal of Mathematics, Vol. 5, No 2 (1975)

[8] J.H. van Lint, *Coding Theory, Lecture Notes in Mathematics*, Springer (1971)

[9] Aimo Tietäväinen and Aarni Perko, *There are no Unknown Perfect Binary Codes*, Turun Yliopisto (1973)

[10] J.H. van Lint, *On the nonexistence of perfect 5-, 6- and 7-Hamming-error-correcting codes over $GF(q)$*, Technological University Eindhoven (1970)

[11] J.H. van Lint, *Report of the Discrete Mathematics Group*, Technological University Eindhoven (1967-1969)