Some non-existence theorems for perfect codes over arbitrary alphabets

SOME NON-EXISTENCE THEOREMS FOR PERFECT CODES OVER ARBITRARY ALPHABETS

PROEFSCHRIFT

TER VERKRIJGING VAN DE GRAAD VAN DOCTOR IN DE
TECHNISCHE WETENSCHAPPEN AAN DE TECHNISCHE
HOGESCHOOL EINDHOVEN, OP GEZAG VAN DE RECTOR
MAGNIFICUS, PROF.Dr. P. VAN DER LEEDEN, VOOR
EEN COMMISSIE AANGEWEZEN DOOR HET COLLEGE VAN
DEKANEN IN HET OPENBAAR TE VERDEDIGEN OP
DINSDAG 18 JANUARI 1977 TE 16.00 UUR

door

HENRICUS FRANCISCUS HUBERTUS REUVERS

GEBOREN TE MAASTRICHT

Dit proefschrift is goedgekeurd

door de promotoren

Prof. dr. J.H. van Lint

en

Prof. dr. J.H. de Boer

DRUKKERIJ UITGEVERIJ BIJSTERVELD
EINDHOVEN

Voor Marian en de kleine Erik

aan mijn ouders

CONTENTS page

CHAPTER 1. INTRODUCTION 1

1.1. On error-correcting codes 1

1.2. On perfect codes and the sphere packing condition 2

1.3. On the number of code words of weight k for some small k 3

1.4. On t-designs 4

1.5. On t-designs in perfect codes 5

1.6. The polynomial condition 6

1.7. Some examples of perfect codes 11

1.8. A remark about perfect 1-codes 12

1.9. Summary of results 15

CHAPTER 2. SOME GENERAL RESULTS CONCERNING q 17

2.1. The general case $q = p^s$ $(e \geq 2)$ 17

2.2. The general case $q = p_1^s p_2^t$ $(e \geq 3)$ 19

2.3. Introduction to a result concerning the number of primes dividing q 20

2.4. Statement of a result concerning the number of primes dividing q 23

2.5. Application to the case e = 6 26

CHAPTER 3. SOME RESULTS CONCERNING THE CASE e = 2 27

3.1. First approach to the case e = 2 27

3.2. Second approach to the case e = 2 30

3.3. The special case $q = p^s$ 32

3.4. A remark about the special case $q = p_1^s p_2^t$ 33

3.5. Some remarks about the special case $q = 2^k p^s$ 34

3.6. The special case q < 30 or q = 35 37

3.7. The special case q = 30 53

CHAPTER 4. SOME GENERAL RESULTS CONCERNING n 71

4.1. A first remark about n 71

4.2. A second remark about n 72

page

4.3. The existence of an upper bound N(e,q) for n 74

4.4. An upper bound N(e,q) made explicit if e is odd 76

4.5. Application 81

CHAPTER 5. SOME RESULTS FOR SMALL VALUES OF e 82

5.1. The case e = 3 82

5.2. The case e = 4 83

5.3. The case e = 5 88

CHAPTER 6. SOME RESULTS CONCERNING PERFECT MIXED CODES 91

6.1. Preliminaries 91

6.2. A nonexistence theorem concerning mixed perfect 2-codes 93

6.3. A nonexistence theorem concerning mixed perfect 3-codes 99

APPENDIX 102

HISTORICAL SUMMARY 116

REFERENCES 120

SAMENVATTING 125

CURRICULUM VITAE 127

CHAPTER 1 : INTRODUCTION

1.1. On error-correcting codes

Let S be a set of q symbols. We shall take $S := \{0,1,2,\dots,q-1\}$. We call S an *alphabet*.

Let, for some $n \in \mathbb{N}$, V be the Cartesian product S^n. We call V a *space*, and the elements of V *words*.

Let C be a subset of V. Then we call C a *code*. The elements of C are called *code words* and n is called the *word length* of C.

C is called a *group code* if it is a group under coordinatewise addition (modulo q).

Let $\underline{x} \in V$. Then the *Hamming weight* $W_H(\underline{x})$ of $\underline{x}$ is the number of coordinate places in which $\underline{x}$ has a nonzero symbol.

The *support* of $\underline{x}$ is the vector supp $(\underline{x})$ which has zeros in exactly the same coordinate places in which $\underline{x}$ has zeros, and which has ones in the other coordinate places.

For any two words $\underline{x}$ and $\underline{y}$ in the space V, we define the *Hamming distance* $d_H(\underline{x},\underline{y})$ between $\underline{x}$ and $\underline{y}$ to be the number of coordinate places in which $\underline{x}$ and $\underline{y}$ have a different symbol, so

1.1.1. $$d_H(\underline{x},\underline{y}) = W_H(\underline{x} - \underline{y})$$

where subtraction means coordinatewise subtraction (mod q).

By $d_H(\underline{x},C)$ we denote the distance from $\underline{x}$ to the code.

For any $\underline{x} \in V$, let the *Hamming sphere* with radius e around $\underline{x}$ be defined by:

1.1.2. $$S_e(\underline{x}) := \{\underline{y} \in V \mid d_H(\underline{x},\underline{y}) \le e\} .$$

A code C is called *e-error-correcting* (for some $e \in \mathbb{N}$) if for any two distinct code words $\underline{x}$ and $\underline{y}$ we have $d_H(\underline{x},\underline{y}) \ge 2e + 1$, so if the spheres with radius e around the code words are disjoint.

If C is an e-error-correcting code, and if we change at most e coordinates of a code word $\underline{x}$, then the changed word is still nearer to $\underline{x}$ than to any other code word.

A code C is called *e-error-detecting* if, for any two distinct code words $\underline{x}$ and $\underline{y}$, we have $d_H(\underline{x},\underline{y}) \geq 2e$.

The numbers, n, e and q are called the *traditional parameters* of a code.

1.2. On perfect codes and the sphere packing condition

We call a code C a *perfect e-code* if the Hamming spheres with radius e around the code words form a partition of V.

Such a code is not only e-error-correcting, but the Hamming spheres fill the space V.

It was proved by Lenstra (see [19]) that a perfect code over a q-symbol alphabet cannot be a group code unless q is a power of a prime.

The case where q is a power of a prime was settled completely by Van Lint and Tietäväinen (see sections 1.7, 2.1 and the historical survey).

They proved that unknown perfect codes over GF(q) do not exist.

Examples of perfect codes can be found in section 1.7.

It is our purpose to prove nonexistence theorems for perfect codes with parameters n, e, q, where q is not necessarily a power of a prime. In this case we call S an *arbitrary alphabet*.

An obvious necessary condition for the existence of perfect codes is called the *sphere packing condition:*

1.2.1. $$\{1 + n(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{e}(q-1)^e\} \mid q^n$$

Here the left hand side is the number of words in a sphere with radius e, and q^n is the total number of words in the space V.

If, for instance, q is a prime power, say $q = p^s$, then we have the very strong condition that for some $a \in \mathbb{N}$

1.2.2. $$1 + n(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{e}(q-1)^e = p^a .$$

From now on the symbol p will denote a prime.

The sphere packing condition plays a basic rôle in our investigations.

1.3. *On the number of code words of weight* k *for some small* k

Assume that we have a perfect code with parameters n, e, q. We can assume without loss of generality that the word $\underset{\sim}{0}$ (having a zero in every coordinate place) is a code word.

In this case the minimum weight of a code word is 2e + 1.

Then each word of weight e + 1 is in exactly one Hamming sphere with radius e around a code word, and this code word must be of weight 2e + 1.

Therefore, since there are $\binom{n}{e+1}(q-1)^{e+1}$ words of weight e + 1, and since in a Hamming sphere with radius e around a code word of weight 2e + 1 there are $\binom{2e+1}{e+1}$ words of weight e + 1, we find that the number a_{2e+1} of code words of weight 2e + 1 must be:

1.3.1. $$a_{2e+1} = \frac{\binom{n}{e+1}(q-1)^{e+1}}{\binom{2e+1}{e+1}} .$$

Furthermore, since each word of weight e + 2 is in exactly one Hamming sphere with radius e around a code word, and this code word must be of weight 2e + 1 or 2e + 2, we find, counting the words of weight e + 2 at a distance e or e - 1 from such a code word, the following recurrence relation, which determines the number a_{2e+2} of code words of weight 2e + 2:

1.3.2. $$\binom{n}{e+2}(q-1)^{e+2} = \binom{2e+2}{e+2}a_{2e+2} + \binom{2e+1}{e+2}a_{2e+1} + \binom{2e+1}{e+1}e(q-2)a_{2e+1}$$

which yields:

1.3.3. $$a_{2e+2} = \frac{(n - e^2 - 3e - 1)(q-1) + e(e+1)}{2e+2}\, a_{2e+1}$$

In the same way we can determine the number a_{2e+3} of code words of weight $2e + 3$ by means of the following recurrence relation:

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

$$+ a_{2e+1}\{\binom{2e+1}{e+3} + \binom{2e+1}{e+2}(e-1)(q-2) + \binom{2e+1}{e+2}(n-2e-1)(q-1) +$$

$$+ \binom{2e+1}{e+1}\binom{e}{2}(q-2)^2\}$$

In this way we can go on.
So the numbers a_k depend on k, n, e and q.
For our purpose we shall only need these numbers for the case $e = 4$.
In the appendix (see A.1) we determine the numbers a_i for $e = 4$ and $9 \le i \le 13$.

1.4. *On t-designs*

For the sections 1.4 and 1.5 we refer to [41], chapter 2, section 4.
We say that a word $\underline{y} \in V$ *covers* another word $\underline{x}$ if we have:

1.4.1. $$\forall_{i \in \{1,2,\dots,n\}}[x_i \neq 0 \Rightarrow x_i = y_i]$$

So if under coordinatewise multiplication we have $\underline{y}\cdot\text{supp}(\underline{x}) = \underline{x}$.
Now we define a (q-ary) *design of type t-(n, k, λ)* in V to be a collection D of words of weight k in V, such that every word of weight t in V is covered by exactly λ members of D.
This definition generalizes the concept of binary t-designs (see [27]) to the concept of *q-ary t-designs*.
If in V there exists a q-ary design of type t-(n, k, λ), then trivially λ must be an integer. But moreover:

1.4.2. For $0 \le i \le t$ we have $\lambda_i \in \mathbb{Z}$, where

$$\lambda_i := \frac{\lambda\binom{n-i}{t-i}(q-1)^{t-i}}{\binom{k-i}{t-i}}$$

This is true because a q-ary design of type t-(n, k, λ) defines q-ary designs of type i-(n, k, λ_i) for $0 \le i \le t$, which is not difficult to understand.

Remark that for a design D of type t-(n, k, λ) we have

1.4.3. $\lambda_0 = |D|$

The following remark may be useful for a better understanding of the proof of theorem 1.5.1:

Consider a q-ary design D of type t-(n, k, λ), and consider a set of $a + b$ positions where $a + b \le t$.

Let us choose coordinates $x_1, x_2, \dots, x_b$ on the b positions, all different from 0.

Then, because D defines q-ary designs of type i-(n, k, λ_i) for $i \le t$, it is immediately clear that the number of words in D which have 0 in the prescribed a positions, and $x_1, x_2, \dots, x_b$ in the prescribed b positions, depends only on the numbers a and b.

1.5. *On t-designs in perfect codes*

Let us consider a perfect code C with parameters n, e, q.

Let $\underline{x} \in V$ and let $d_H(\underline{x}, C) = r$ (so $r \le e$).

Finally, let $B(\underline{x}, k)$ be the number of code words at distance k from $\underline{x}$ (so unless $k \ge r$ we have $B(\underline{x}, k) = 0$).

Then the numbers $B(\underline{x}, k)$ depend only on r, k, n, e and q.

This follows from theorem 2.4.4 and its preliminaries in [41] and has nothing to do with the question whether or not V is a linear space, and whether or not C is a linear subspace of V.

Now we are ready to prove the following theorem:

1.5.1. THEOREM. Let C be a perfect code with parameters n, e, q and suppose that $\underline{0} \in C$. Then, for $0 \le k \le n$, the code words of weight k form a q-ary design of type $(e + 1)$ - $(n, k, \lambda(k))$.

PROOF. First we prove the case $k = 2e + 1$.
Let $\underline{x} \in V$ and $W_H(\underline{x}) = e + 1$. Then it is clear from the triangle inequality that $d_H(\underline{x},C) = e$ and $\underline{x}$ has distance e to exactly one code word of weight $2e + 1$. Clearly this code word must cover $\underline{x}$, and $\underline{x}$ is covered by no other code word of weight $2e + 1$.
So the code words of weight $2e + 1$ form a q-ary design of type $e + 1 - (n, 2e + 1, 1)$.
Now assume that, for all $k < w$, the code words of weight k form a q-ary design of type $e + 1 - (n, k, \lambda(k))$, for some $w \leq n$.
Let $\underline{x}$ be any word in V such that $w_H(\underline{x}) = e + 1$.
Then, since the code words of weight k form a q-ary design of type $i - (n, k, \lambda(k,i))$ for all $i \leq e + 1$, we see that the number of code words of weight k at a given distance from $\underline{x}$, is a constant independent of $\underline{x}$ (see the end of section 1.4).
So the number A of code words of weight $\leq w - 1$ at distance $w - e - 1$ from $\underline{x}$ is independent of $\underline{x}$.
Moreover, since $d_H(\underline{x},C) = e$ if $w_H(\underline{x}) = e + 1$, the numbers $B(\underline{x},i)$ $(0 \leq i \leq n)$ are independent of $\underline{x}$, so $B := B(\underline{x}, w - e - 1)$ is independent of $\underline{x}$.
So the number of code words of weight w at distance $w - e - 1$ from $\underline{x}$ is $B - A$, for all $\underline{x}$ with $w_H(\underline{x}) = e + 1$.
Hence, since these code words are exactly those of weight w which cover $\underline{x}$, they form a q-ary design of type $e + 1 - (n, w, B - A)$.
So we have proved the theorem by induction.

REMARK. The proof of the preceding theorem strongly resembles the proof of theorem 2.4.7 in [41], but is not exactly the same.
For our purpose, we shall only need the results on t-designs in perfect codes for the case $e = 4$ (see A.1 in the appendix).

1.6. *The polynomial condition*

A class of orthogonal polynomials, the so-called *Krawtchouk polynomials*, is defined by:

1.6.1. $$K_m(n,X) := \sum_{i=0}^{m} (-1)^i \binom{n-X}{m-i}\binom{X}{i}(q-1)^{m-i} , \quad \text{for } m \in \mathbb{N}$$

We refer to [35] and [41]. An important property of Krawtchouk polynomials is the following identity:

1.6.2. $$\sum_{m=0}^{e} K_m(n,X) = K_e(n-1, X-1) .$$

From algebraic considerations (see [10], [19] and [27]) it follows that if there exists a perfect code with parameters n, e, q, then

1.6.3. $$P_e(X) := K_e(n-1, X-1) = \sum_{i=0}^{e} (-1)^i \binom{n-X}{e-i}\binom{X-1}{i}(q-1)^{e-i}$$

has e distinct integral zeros.
This is a very strong condition for the existence of perfect codes. We call it the *polynomial condition*. Like the sphere packing condition it plays a basic rôle in our investigations.
Usually the condition is called *Lloyd's Theorem*. The polynomial $P_e(X)$ is called the *Lloyd polynomial*.
Since there are many proofs in the literature, and we shall use the condition as a tool, we shall omit the proof.
Mostly the proofs deal with the case that C is a linear subspace of a linear space V over a finite field GF(q), where q is a prime power.
It was first proved by Lenstra ([19]) that this is not necessary at all.
A nice proof was given by Cvetkovic / Van Lint ([9]).

In [27] one can find another representation of $P_e(X)$:

1.6.4. $$P_e(X) = (-1)^e \sum_{j=0}^{e} (-1)^j q^j \binom{n-X}{j}\binom{n-j-1}{e-j} .$$

Now we shall introduce the theorem and give the symmetric expressions obtained from the coefficients of the Lloyd polynomial, and from the values of $P_e(0)$ and $P_e(1)$.

1.6.5. THEOREM. If there exists a perfect code with parameters n, e, q, then the polynomial $P_e(X)$ has e distinct integral zeros $x_1, x_2, \ldots, x_e$, which belong to the set $\{0,1,2,\ldots,n\}$, and we have:

1.6.6. $$\sum_{i=0}^{e} x_i = \frac{e(n-e)(q-1)}{q} + \frac{e(e+1)}{2} \in \mathbb{Z}$$

1.6.7. $$\sum_{1 \le i < j \le e} x_i x_j = \frac{e(e-1)(q-1)}{2q^2}\{(n-e)^2(q-1)+(n-e)(qe+q-1)\} + $$
$$+ \frac{(e-1)e(e+1)(3e+2)}{24} \in \mathbb{Z}$$

1.6.8. $$\prod_{i=1}^{e} x_i = \frac{e!}{q^e}\{1 + n(q-1) + \binom{n}{2}(q-1)^2 + \ldots + \binom{n}{e}(q-1)^e\} \in \mathbb{Z}$$

1.6.9. $$\prod_{i=1}^{e}(x_i - 1) = (n-1)(n-2)\ldots(n-e)\frac{(q-1)^e}{q^e} \in \mathbb{Z}$$

Combining 1.6.8 with the sphere packing condition 1.2.1 we find:

1.6.10 $$\prod_{i=1}^{e} x_i \mid e!q^n$$

In the special case that q is a prime power, say $q = p^s$, we find for some $t \in \mathbb{N}$ the very strong condition:

1.6.11. $$\prod_{i=1}^{e} x_i = A(e,p)p^t ,$$

where $A(e,p)$ is defined by

1.6.12. $$A(e,p) = \frac{e!}{p^u}$$

and $u \in \mathbb{N}$ is chosen in such a way that $p^u \,\|\, e!$

So there must be positive integers a_i and t_i $(1 \le i \le e)$ such that

1.6.13. $\prod_{i=1}^{e} a_i = A(e,p)$,

and

1.6.14. $x_i = a_i p^{t_i}$

However, it is clear that if there are many distinct primes dividing q, then the formula 1.6.10 becomes much less effective.

For odd e, say $e = 2m+1$, it turns out to be very effective to use a substitution θ, first introduced by Van Lint in [23] for the case $e = 3$. Let

1.6.15. $\theta := qX - n(q-1)$.

Remark that if $\theta = 0$, then $X = \frac{n(q-1)}{q}$, and that $\frac{n(q-1)}{q}$ resembles the arithmetical mean of the zeros x_i of $P_e(X)$ (see 1.6.6).
Then since

1.6.16. $\sum_{e=0}^{\infty} P_e(X)Z^e = (1 + (q-1)Z)^{n-X}(1-Z)^{X-1}$,

we find, if we take

1.6.17. $F_e(\theta) := P_e(X)$,

the following power series which generates the *transformed Lloyd polynomials* $F_e(\theta)$:

1.6.18. $\sum_{e=0}^{\infty} F_e(\theta)Z^e =$

$$(1 + (q-1)Z)^{-\theta/q}(1-Z)^{(\theta/q)-1}\{(1 + (q-1)Z)^{1/q}(1-Z)^{q-1/q}\}^n$$

We shall need this generating power series for lemma 1.6.23.

We conclude this section with some remarkable properties of $F_e(\theta)$. It is known that the polynomials $F_e(\theta)$ can be expressed in a determinant form (see [7], [9]).

For instance we have, transforming $P_3(X)$ and $P_5(X)$ respectively by hand:

1.6.19. $$3!F_3(\theta) = (n-1)(n-2)(n-3) - 3(n-2)(n-3)(n-\theta) + 3(n-3)(n-\theta)(n-\theta-q) - (n-\theta)(n-\theta-q)(n-\theta-2q) .$$

1.6.20. $$\begin{aligned} 5!F_5(\theta) = {} & (n-1)(n-2)(n-3)(n-4)(n-5) - \\ & 5(n-2)(n-3)(n-4)(n-5)(n-\theta) + \\ & + 10(n-3)(n-4)(n-5)(n-\theta)(n-\theta-q) - \\ & 10(n-4)(n-5)(n-\theta)(n-\theta-q)(n-\theta-2q) + \\ & + 5(n-5)(n-\theta)(n-\theta-q)(n-\theta-2q)(n-\theta-3q) - \\ & (n-\theta)(n-\theta-q)(n-\theta-2q)(n-\theta-3q)(n-\theta-4q) \end{aligned}$$

In general we have the following

1.6.21. LEMMA. $F_e(\theta) = \det(a_{ij})_{0\le i,j\le e}$, where

1.6.22. $$\begin{aligned} & a_{0i} = \binom{e}{i} \quad \text{for } i = 0,1,\dots,e \\ & a_{ii} = n - i + 1 \quad \text{for } i = 1,\dots,e \\ & a_{i\;i+1} = n - \theta - (i+1)q \quad \text{for } i = 0,1,\dots,e \\ & a_{ij} = 0 \quad \text{if } j \neq i \text{ and } j \neq i+1 \text{ and } i \neq 0 . \end{aligned}$$

Finally, let us consider $F_e(\theta)$ as a polynomial in n, say

1.6.23. $$F_e(\theta) = \sum_{k=0}^{e} a_k(\theta) n^k$$

Then we have the following

1.6.24. **LEMMA.** If $e = 2m + 1$, then for $k > m$ the coefficients $a_k(\theta)$ are all zero.

PROOF. Define ξ and η by

1.6.25. $\xi := \frac{q-1}{2}$ and $\eta := \frac{q-1\ q-2}{3}$

Then we find

1.6.26. $\{(1 + (q-1)z)^{1/q}(1 - z)^{q-1/q}\}^n = \{1 + z^2(-\xi + \eta z + \ldots)\}^n =$

$$= \sum_{j=0}^{n} \binom{n}{j} z^{2j}(-\xi + \eta z + \ldots)^j$$

So from 1.6.18 we see that $F_e(\theta)$ is the coefficient of z^e in

1.6.27. $(1 - (\theta - 1)z + \ldots)\left(\sum_{j=0}^{n} \binom{n}{j} z^{2j}(-\xi + \eta z + \ldots)^j\right)$

So, as a polynomial in n, $F_e(\theta)$ is of degree $\le e/2$. □

1.7. *Some examples of perfect codes*

The concept of perfect codes would never have been studied if there would not exist examples.

First we have the *trivial* perfect codes with only one code word, and the so-called *repetition codes* with $q = 2$ and word length $n = 2e+1$, consisting of an all-zero code word and an all-one code word. Repetition codes are also called trivial.

Secondly we have the perfect *Hamming codes* with $e = 1$ and $n = \frac{q^m - 1}{q - 1}$ which exist for all prime powers q. These codes are described in [27].

Finally there are the two *Golay codes* with parameters

$n = 11,\ e = 2,\ q = 3$

$n = 23,\ e = 3,\ q = 2$

respectively.

A description of these two codes can also be found in [27].
The uniqueness of perfect codes with the Golay parameters was proved by Snover (for the binary code, see [34]) and by Delsarte - Goethals (for the ternary code, see [11]).

1.8. A remark about perfect 1-codes

Let C be a perfect code with parameters n, e = 1, and q.
From the sphere packing condition 1.2.1 we find that

1.8.1. $\{1 + n(q - 1)\} \mid q^n$

So if $q = p_1^{s_1} \ldots p_r^{s_r}$ is the prime decomposition of q, then

1.8.2. $1 + n(q - 1) = p_1^{k_1} \ldots p_r^{k_r}$

for some positive integers k_i $(i = 1,\ldots,r)$.
From the polynomial condition 1.6.5 we find that $P_1(X)$ (cfr. 1.6.3) must have an integral zero x, such that

1.8.3. $qx - 1 - n(q - 1) = 0$

hence we have

1.8.4. $q \mid \{1 + n(q - 1)\}$

Hence we find from 1.8.1, 1.8.2 and 1.8.4 that $s_i \leq k_i \leq ns_i$, and

1.8.5. $$n = \frac{p_1^{k_1} \ldots p_r^{k_r} - 1}{p_1^{s_1} \ldots p_r^{s_r} - 1}$$

Indeed there exist perfect codes if r = 1 and n is of the form 1.8.5, as we mentioned in the preceding section.
It was shown by Block and Hall (see [13]) that there does not exist a

perfect 1-code of length 7 on 6 symbols (which was the next open case). The proof made use of the non-existence of a pair of orthogonal 6 × 6 Latin squares.

A *Latin square* of size k is a matrix such that every row and every column is a permutation of the numbers 1,2,...,k.

A pair of Latin squares is called *orthogonal* if by taking the entries from the place (i,j) from both squares, thus forming k^2 pairs of entries, one gets k^2 distinct pairs.

In the same way as Block and Hall did, we considered the question of the existence of a single-error-correcting code of length 11 on 10 symbols. Indeed we found more generally:

1.8.6. THEOREM. Let us suppose that there exists a perfect single-error-correcting code of length $n = q + 1$ over a q-symbol alphabet. Then there must be $(q - 2)^2$ pairs (A_i, B_i) of orthogonal q × q Latin squares such that, if for some $(k,\ell) \in \{1,2,\ldots q\}^2$ we have $((A_i)_{k,\ell}, (B_i)_{k,\ell}) = ((A_j)_{k,\ell}, (B_j)_{k,\ell})$, then i = j.

PROOF. First we claim that in $V(4,q) := \{(x_1,x_2,x_3,x_4) \mid x_i \in \{1,2,\ldots q\}\}$ there must be $(q - 2)^2$ disjoint 1-codes of length 4 on q symbols, each with q^2 code words.

Indeed, suppose there exists a perfect 1-code C of length $n = q + 1$ on q symbols, hence

$$1.8.7. \qquad |C| = \frac{q^{q+1}}{1 + (q+1)(q-1)} = q^{q-1} \ .$$

Then each of the q^{q-1} (q - 1)-tuples of q symbols is the initial (q - 1)-tuple of exactly one of the q^{q-1} code words. For if any would occur twice, then the corresponding code words would be at a distance at most two, contradicting that C is single-error-correcting.

Then all q^{q-3} (q - 3)-tuples of q symbols are initial (q - 3)-tuple of exactly q^2 code words in C.

So, considering a fixed initial (q - 3)-tuple, we see that the q^2 code words of C that begin with the fixed initial (q - 3)-tuple have 4-symbol-tails that form in V(4,q) a 1-code D on q symbols, of length 4, with q^2 code words.

Moreover, considering a second fixed initial $(q - 3)$-tuple, differing from the first in at most two coordinates, we must find a 1-code D' on q symbols, of length 4, with q^2 code words and such that D and D' have no code word in common.
Hence, considering all fixed initial $(q - 3)$-tuples that differ from the first in at most one coordinate, since each pair of them disagrees in at most two coordinates, we must find $1 + (q - 3)(q - 1) = (q - 2)^2$ disjoint single-error-correcting codes of length 4 on q symbols with q^2 code words, proving the claim.

Now consider such a code of length 4. Then each of the q^2 2-tuples out of q elements is initial 2-tuple of exactly one code word. For if any would occur twice, then the corresponding code words would be at a distance at most two apart, contradicting the one-error-correcting-capability of the code.
Thus, such a code is equivalent with a pair (A,B) of $q \times q$ matrices by the correspondence:
(k,ℓ,m,n) is a code word iff $A_{k,\ell} = m$ and $B_{k,\ell} = n$.
Moreover, if any one of A and B, say A, would have the same symbol twice in any row or column, say $A_{k\ell} = A_{km}$, then the code words $(k,\ell,A_{k\ell},B_{k\ell})$ and (k,m,A_{km},B_{km}) would be at a distance at most two, which is impossible. So A and B are Latin squares.
Furthermore, if for some pair of pairs $((k,\ell), (m,n))$ we would have $(A_{k\ell}, B_{k\ell}) = (A_{mn}, B_{mn})$, then again we would have two code words at a distance two, which is impossible. So A and B form a pair of orthogonal Latin squares.
Finally, since all $(q - 2)^2$ codes are disjoint, taking from any two codes D and D' the code words defined by an initial 2-tuple (k,ℓ), they must be different, so they must have different tails, so the $(q - 2)^2$ pairs of orthogonal Latin squares are distinct in the sense of the theorem. □

1.9. Summary of results

The rest of our investigations is devoted to the question of the existence of parameters n, e, q that fit a perfect code. We shall neglect trivial cases

In chapter 2 we shall explain how, by combining the sphere packing condition and the polynomial condition, some results can be established about the number of primes dividing q.
After two theorems by Van Lint / Tietävälnen and by Tietävälnen, who consider $q = p^s$ and $q = p_1^s p_2^t$ respectively, we shall introduce a generalization and apply it to the case $e = 6$.
This generalization states that in most of the cases, q must have at least e distinct prime divisors.

In chapter 3 we give the zeros x_1 and x_2 of $P_2(X)$ in a parameter form and derive some partial results on q. Here too we use the combination of the sphere packing condition and the polynomial condition.

In chapter 4 we shall derive an upper bound N(e,q) for n in the case that e is odd, using the polynomial condition only.
For this purpose we consider the transformed Lloyd polynomials $F_e(\theta)$ and find two values θ_0 and θ_1 of θ, such that for $n > N(e,q)$

1.9.1. $F_e(\theta_0) > 0$ and $F_e(\theta_1) < 0$

while in the interval (θ_0, θ_1) there does not exist an integer.
The existence of such an upper bound N(e,q) for n in the case that e is even, is established but not made explicit.

In chapter 5 we shall derive our main theorems.
Here we shall prove the non-existence of unknown nontrivial perfect codes with $e = 3$ or $e = 4$ or $e = 5$.
For the case $e = 3$ and for the case $e = 5$ we generalize an early theorem

by Van Lint about the case $e = 3$ and $q = p^s$.
For the case $e = 4$ we use the *resolvent of Lagrange* to transform the Lloyd polynomial $P_4(X)$ into a polynomial of the third degree, which in some sense can be treated as the "odd" polynomials $P_3(X)$ and $P_5(X)$. Again we find two values where the polynomial takes a different sign, whereas between them there does not exist an integer.

Finally, we have added to our text the chapter 6, which shows how our methods can also serve for non-existence theorems concerning *mixed perfect codes*.

CHAPTER 2 :SOME GENERAL RESULTS CONCERNING q

2.1. *The general case* $q = p^s$ $(e \geq 2)$

Since a few years it is known that there do not exist perfect e-codes over an alphabet GF(q), where $q = p^s$, except the two Golay codes, if $e \geq 2$.

The proof was given by Van Lint and Tietäväinen (see our "historical summary").

The approach of Tietäväinen is the following lemma, which we shall use later on for the case $e = 2$.

2.1.1. **LEMMA.** Suppose there exists an unknown perfect code with parameters n,e,q. Let the zeros of the Lloyd polynomial $P_e(X)$ be ordered in such a way that $x_1 < x_2 < \ldots < x_e$.

Then we have:

2.1.2. Either $x_e < 2x_1$ or $n < 5e^2$.

PROOF. Assume $x_e \geq 2x_1$. Then we have also

2.1.3. $$x_1 x_e \leq \frac{2}{9}(x_1 + x_e)^2$$

and hence from the *geometrical-arithmetical mean inequality*

2.1.4. $$x_1 x_2 \ldots x_e \leq \frac{8}{9}\left(\frac{x_1 + \ldots + x_e}{e}\right)^e$$

Furthermore, from the formulas 1.6.6 and 1.6.8 it follows that

2.1.5. $$\frac{n(n-1)\ldots(n-e+1)(q-1)^e}{q^e} < x_1 \ldots x_e$$

and that

2.1.6. $$\left(\frac{x_1 +\dots+ x_e}{e}\right)^e < \left(\frac{q-1}{q}\right)^e n^e$$

So, combining the formulas 2.1.4, 2.1.5 and 2.1.6, we find

2.1.7. $$\frac{n(n-1)\dots(n-e+1)(q-1)^e}{q^e} < \frac{8}{9}\left(\frac{q-1}{q}\right)^e n^e$$

from which it is easily derived that

2.1.8. $n < 5e^2$.

With the help of lemma 2.1.1 we can prove our goal as follows:
In the case $q = p^s$, it follows from 1.6,12, 1.6.13 and 1.6.14 that for $1 \le i \le e$

2.1.9. $x_i = a_i p^{t_i}$

where $a_i \in \mathbb{N}$, $t_i \in \mathbb{N}$, and either for some pair (i,j) we have $a_i = a_j$, or $p > e$ and the numbers a_i from a permutation of the numbers $1,2,\dots e$. Hence in any case, except for the case $e = 2$ and $q = 3^s$ which shall be treated in section 3.3, we have:

2.1.10. $x_e \ge 2x_1$

Then from lemma 2.1.1 we have 2.1.2,

2.1.11. $n < 5e^2$.

But on the other hand we find from 1.6.9, since $q = p^s$,

2.1.12. $p^{es} \mid (n - 1)\dots(n - e)$

Therefore, one of the numbers $n - i$ $(1 \le i \le e)$ must be divisible by p^t, where

2.1.13. $$t > es - \frac{e}{p} - \frac{e}{p^2} - \frac{e}{p^3} \dots = es - \frac{e}{p-1}$$

Hence we find

2.1.14. $n > q^{e/2}$

Now, combining 2.1.11 and 2.1.14, we see that there is only a finite number of possible parameters (n, e, p^s). These were ruled out by a computer investigation (see the Historical Summary). Therefore we have the following

2.1.15. THEOREM. (Van Lint - Tietävӓinen). The Golay codes are the only perfect e-codes with $e \geq 2$ over an alphabet $GF(q)$, where $q = p^s$.

2.2. *The general case* $q = p_1^s p_2^t$ $(e \geq 3)$

Recently, the following theorem was proved by A. Tietävӓinen:

2.2.1. THEOREM. There does not exist a perfect e-code with $e \geq 3$ and q of the form $q = p_1^s p_2^t$.

We shall give an outline of the proof, which illustrates again how one can treat q with few prime divisors.

The proof makes use of three inequalities which contradict each other for large n.

The first inequality is the following about the zeros of the Lloyd polynomial $P_e(X)$, ordered in such a way that $x_1 < x_2 < \ldots < x_e$:

2.2.2. $|x_i - x_j| > \gcd(x_i, x_j)$.

Remark that from 1.2.1 and 1.6.8 it follows that for $1 \leq i \leq e$

2.2.3. $x_i = d_i p_1^{a_i} p_2^{b_i}$

where a_i, b_i are unspecified positive integers, and $d_i \in \mathbb{N}$ and

2.2.4. $d_1 d_2 \ldots d_e \mid e!$

From 2.2.3, 2.2.4 and lemma 2.1.1 it follows that, if $e > 2$, a pair (x_i, x_j) must exist which has a common divisor which is large with respect to x_i.

Furthermore we have the following inequality, which can be found in [27], page 115:

2.2.5. $$x_1 > \frac{(n-e)(q-1)+e}{q-1+e}$$

The third inequality is obtained from 1.6.6 and 1.6.7:

2.2.6. $$\sum_{i=1}^{e} \sum_{j=1}^{e} (x_i - x_j)^2 < \frac{3e^2(e-1)(n-e)}{q}$$

These three inequalities contradict each other if

2.2.7 $$n > q^{e/4}$$

which can be established from 1.6.9. We refer to [40].

The inequality 2.2.5 will also be important for our investigations in the case $e = 2$. It follows from the fact that the terms in the alternating sum 1.6.3 decrease in absolute value if X is smaller than the bound mentioned in 2.2.5.

Remark that if $e = 2$ then x_1 and x_2 need not have a large common divisor at all.

In the following two sections we shall see that in general a perfect e-code is not possible if q has less than e prime divisors.

2.3. *Introduction to a result concerning the number of primes dividing q*

As an introduction to the section 2.4 we have the following theorem which is unimportant after section 5.2.

2.3.1. THEOREM. If a perfect four-error-correcting code on q symbols does exist, then either q is divisible by at least four distinct primes, or gcd $(q,30) > 1$.

PROOF. By calculation of the coefficients of $P_4(X)$ (see 1.6.6, 1.6.7) we have the following expressions in the zeros x_1, x_2, x_3, x_4, which must be integers:

2.3.2. $$x_1 + x_2 + x_3 + x_4 = \frac{4(n-4)(q-1)}{q} + 10$$

2.3.3. $$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 &= 4(n - 4)^2 + 20(n - 4) + 30 \\ &\quad - \frac{4(n-4)}{q^2}\{(2q-1)(n-3) + 4\} \end{aligned}$$

2.3.4. $$\begin{aligned} x_1^3 + x_2^3 + x_3^3 + x_4^3 &= 4(n-4)^3 + 30(n-4)^2 + 90(n-4) + 100 \\ &\quad + \frac{n-4}{q^3}\{(n-4)^2(12q^2 - 12q + 4) + \\ &\quad (n-4)(24q^2 + 42q - 36) + (12q^2 + 54q + 24)\} \end{aligned}$$

Now let p be a prime such that $p \geq 5$ and let $s \in \mathbb{N}_0$ be such that $p^s \parallel q$. Then from 2.3.2 we see

2.3.5. $$p^s \mid n - 4$$

Then from 1.6.9 it follows that

2.3.6. $$p^{4s} \mid n - 4$$

Hence we have from 2.3.2, 2.3.3 and 2.3.4:

2.3.7. $$\begin{aligned} x_1 + x_2 + x_3 + x_4 &\equiv 10 \pmod{p^{3s}} \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 &\equiv 30 \pmod{p^{2s}} \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 &\equiv 100 \pmod{p^{s}} \end{aligned}$$

Now let $q = p_1^{s_1} \dots p_r^{s_r}$ and gcd $(q,30) = 1$. Then from 1.6.10 we find, since gcd $(q,30) = 1$, for some $k_i \in \mathbb{N}_0$

2.3.8. $\quad x_1x_2x_3x_4 = 24\, p_1^{k_1} \dots p_r^{k_r}$

Now suppose that the smallest zero, x_1, would be at most 24. Then from lemma 2.1.1 we see that either

2.3.9. $\quad n < 80$

contradicting 2.3.6 since gcd $(q,30) = 1$, or

2.3.10. $\quad x_4 \le 48$

from which it would follow that

2.3.11. $\quad x_1 + x_2 + x_3 + x_4 \le 24 + 46 + 47 + 48$

contradicting 2.4.7 since gcd $(q,30) = 1$ and since $P_4(1) \ne 0$.
Hence x_1 is greater than 24 and all zeros are divisible by some p_i dividing q.
So if q is divisible by no more than three primes, then there exist x_i and x_j $(i \ne j)$ which are divisible by the same prime $p(p \mid q)$.
So in that case it would follow from 2.3.7 that the other two zeros, x and y, satisfy

2.3.12. $\quad x + y \equiv 10 \pmod p$

$$x^2 + y^2 \equiv 30 \pmod p$$

$$x^3 + y^3 \equiv 100 \pmod p$$

Then, successively, the following congruences (modulo p) would hold:

2.3.13. $\quad (x + y)^2 = x^2 + y^2 + 2xy \equiv 100$

2.3.14. $\quad 30 + 2xy \equiv 100$, so $xy \equiv 35$

2.3.15. $(x + y)^3 = x^3 + y^3 + 3xy(x + y) \equiv 1000$

2.3.16. $100 + 3.35.10 \equiv 1000 \equiv 1150$

so p would divide 150, contradicting gcd $(q,30) = 1$. □

In section 5.2 we shall see that perfect 4-codes do not exist at all.

2.4. Statement of a result concerning the number of primes dividing q

We have the following theorem, which generalizes in some sense what was done (by Van Lint and Tietäväinen) in the sections 2.1 and 2.2:

2.4.1. THEOREM. Let us assume that there exists a perfect e-code on q symbols, where $q = p_1^{s_1} \dots p_k^{s_k}$ and (for $i \in \{1,2,\dots,k\}$) $p_i > e$ and $p_i \nmid e!\,(1 + 1/2 +\dots+ 1/e)$. Then $k \geq e$.

PROOF. Since for all i we have $p_i > e$, it follows from 1.6.6 and 1.6.9 that

2.4.2. $q^e \mid n - e$

Now in lemma 2.4.11 we shall see:

2.4.3. $$\sum_{i=1}^{e} \prod_{j\neq i}^{e} x_j \equiv \sum_{i=1}^{e} \prod_{j\neq i}^{e} j \equiv e!(1 + 1/2 +\dots+ 1/e) \left(\mathrm{mod}\ \frac{n-e}{q^{e-1}}\right)$$

Hence from 2.4.2 and 2.4.3 we have

2.4.4. $$\sum_{i=1}^{e} \prod_{j\neq i}^{e} x_j \equiv e!(1 + 1/2 +\dots+ 1/e) \quad (\mathrm{mod}\ q)$$

Then from the conditions on p_i we find for $i \in \{1,2,\dots,k\}$

2.4.5. $$\sum_{i=1}^{e} \prod_{j\neq i}^{e} x_j \not\equiv 0 \quad (\mathrm{mod}\ p_i)$$

So at most one of $x_1, x_2, \dots x_e$ is divisible by p_i.
Furthermore, since from 2.4.2

2.4.6. $\quad n > q^e$

and since from the conditions on p_i we have

2.4.7. $\quad q > e$

and since for the smallest zero of $P_e(X)$ we have the inequality 2.2.5, it follows immediately that for $1 \leq i \leq e$

2.4.8. $\quad x_i > e!$

Hence, since from the conditions $p_i > e$ and from 1.6.10 we have

2.4.9. $$\prod_{i=1}^{e} x_i = e!\, p_1^{a_1} \dots p_k^{a_k} \quad (a_i \in \mathbb{N}_0, \;\; i = 1,2,\dots,k)$$

we find that any zero x_i is divisible by at least one of the primes $p_1, p_2 \cdots p_k$.
Then, since from 2.4.5 we concluded that a given prime p_i divides at most one of the zeros $x_1, \dots, x_e$, we may conclude

2.4.10. $\quad k \geq e$

So we have proved theorem 2.4.1 when we have proved lemma 2.4.11.

2.4.11. LEMMA. Let us assume that there exist a perfect e-code with $q = p_1^{s_1} \dots p_k^{s_k}$, where $p_i > e$ for $i \in \{1,2,\dots,k\}$. Then

$$\sum_{i=1}^{e} \prod_{j\neq i}^{e} x_j \equiv \sum_{i=1}^{e} \prod_{j\neq i}^{e} j \quad (\text{modulo } \frac{n-e}{q^{e-1}}).$$

PROOF. Since for all i we have $p_i > e$, it follows from 1.6.6 and 1.6.9 tha

2.4.12. $\quad q^e \mid n - e$

Now, for briefness, let us define

2.4.13. $s := n - e$

Then, in accordance with the definition 1.6.3 of the Lloyd polynomial $P_e(X)$, we have

2.4.14. $$e!P_e(X) = \sum_{i=0}^{e} (-1)^i \binom{e}{i} (q-1)^i (s+e-X)(s+e-1-X)\dots (s+i+1-X)(X-i)(X-i+1)\dots(X-1)$$

Then, because

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

we see that there exists $Q_e(X) \in \mathbb{Z}[X]$ such that

2.4.16. $$\frac{e!P_e(X)}{q^e} = (-1)^e (X-1)(X-2)\dots(X-e) + \frac{s}{q^e} Q_e(X)$$

Now, considering $Q_e(X)$ as a polynomial in s and X, say

2.4.17. $$Q_e(X) := \sum_{i,j=0}^{e} a_{ij} s^i X^j$$

we see from 2.4.14 and 2.4.16 that for the coefficient of s^0 we have:

2.4.18. $$\sum_{j=0}^{e} a_{0j} X^j = \sum_{i=0}^{e-1} (-1)^e \binom{e}{i} (q-1)^i \sum_{j=i+1}^{e} \prod_{\substack{m \neq j \\ m=1}}^{e} (X-m)$$

Therefore we have

2.4.19. $$a_{01} = \sum_{i=0}^{e-1} (-1)^e \binom{e}{i} (q-1)^i \sum_{j=i+1}^{e} \frac{e!}{j} (1 + 1/2 + \dots + \widehat{1/j} + \dots + 1/e)$$

where $\widehat{1/j}$ means that $1/j$ must be replaced by 0.
Now in the appendix (see A.3) we shall prove:

2.4.20. $$\sum_{i=0}^{e-1} (-1)^i \binom{e}{i} \sum_{j=i+1}^{e} \frac{e!}{j} (1 + 1/2 + \ldots + \widehat{1/j} + \ldots + 1/e) = 0$$

and therefore we have from 2.4.19 and 2.4.20

2.4.21. $a_{01} \equiv 0 \pmod q$

Since by 2.4.12 clearly

2.4.22. $s \equiv 0 \pmod q$

we see from 2.4.17 and 2.4.21 that the coefficient of X in $Q_e(X)$ has a divisor q.
Then it follows from 2.4.13 and 2.4.16 that lemma 2.4.11 holds. □

2.5. *Application to the case* e = 6

In the case $e = 6$ we derive from theorem 2.4.1 the following

2.5.1. THEOREM. If a perfect 6-code exists with q symbols, where $q = p_1^{s_1} \ldots p_k^{s_k}$, then either $k \geq 6$, or q has at least one prime factor 2,3,5 or 7.

Since, from the theorems 2.1.15 and 2.2.1, q must in any case be divisible by at least three primes, the first open case with $e = 6$ is $q = 30$.
The smallest q with no factors 2,3,5 or 7 which is possible for a perfect 6-code is $q = 11\cdot13\cdot17\cdot19\cdot23\cdot29$.

CHAPTER 3 : SOME RESULTS CONCERNING THE CASE $e = 2$

3.1. First approach to the case $e = 2$

In this section we shall derive a parameter representation for the zeros x_1 and x_2 of the Lloyd polynomial $P_2(X)$, defined in 1.6.3. This representation is stated in the following lemma:

3.1.1. LEMMA. Assume that there exists a perfect double-error-correcting code with parameters n and q.
Then if $q = 2q'$ and q' is odd and $n - 2$ is odd we have for some $u \in \mathbb{N}$

3.1.2. $$2x_1 = q'(u^2 - 1) + u + 3$$

$$2x_2 = q'(u^2 - 1) - u + 3$$

In all other cases we have for some $v \in \mathbb{N}$

3.1.3. $$x_1 = qv^2 + qv + v + 2$$

$$x_2 = qv^2 + qv - v + 1$$

PROOF. Define

3.1.4. $$t := q(x_1 - x_2)$$

Then from the polynomial condition 1.6.5 we know that t must be an integer. Furthermore, from 1.6.6, 1.6.8 and 3.1.4 we see that

3.1.5. $$t^2 = q^2 + 4(n - 2)(q - 1)$$

Again, combining 1.6.6 and 3.1.5 we find

3.1.6. $$t^2 + (x_1 + x_2 - 3)^2 = (q + x_1 + x_2 - 3)^2$$

Now first assume that q is odd (so from 3.1.5 t is odd). Then we have, as is well-known:

3.1.7. $$\begin{aligned} t = q(x_1 - x_2) &= d(u^2 - v^2) \\ x_1 + x_2 - 3 &= d(2uv) \\ x_1 + x_2 - 3 + q &= d(u^2 + v^2) \end{aligned}$$

where u and v are relatively prime positive integers and d is the common divisor, which clearly must divide q.

Furthermore, if q is odd we find from 1.6.6 and 1.6.9

3.1.8. $q \mid (x_1 + x_2 - 3)$

So in 3.1.7 we find d = q and without loss of generality:

3.1.9. $u^2 + v^2 = 2uv + 1$

3.1.10. $$\begin{aligned} x_1 - x_2 &= 2v + 1 \\ x_1 + x_2 &= 2qv(v + 1) + 3 \end{aligned}$$

from which 3.1.3 is derived immediately.

Now if $4 \mid q$, it also follows from 1.6.6 and 1.6.9 that 3.1.8 holds, so d = q.

Then, if we assume, instead of 3.1.7,

3.1.11. $x_1 + x_2 - 3 = q(u^2 - v^2) = q(u^2 + v^2) - q$

we find

3.1.12. $2v^2 = 1$

which is impossible. So 3.1.7 holds and finally we have 3.1.3.

This is not true if q = 2q', q' is odd and n - 2 is odd. In this case we see from 1.6.6 and 1.6.9 that $x_1 + x_2 - 3$ is odd and

3.1.13. $q' \mid (x_1 + x_2 - 3)$

hence, from 3.1.6 we have d = q' and for some $u,v \in \mathbb{N}$ which are relatively prime:

3.1.14. $$x_1 - x_2 = uv$$

$$x_1 + x_2 - 3 = q'(u^2 - v^2)$$

$$x_1 + x_2 - 3 + 2q' = q'(u^2 + v^2)$$

From 3.1.14 it follows that

3.1.15. $$u^2 + v^2 = u^2 - v^2 + 2$$

So we have $v = 1$ and

3.1.16. $$x_1 - x_2 = u$$

$$x_1 + x_2 = q'(u^2 - 1) + 3$$

from which 3.1.2 is derived immediately.

Remark that if $n - 2$ is even, then in any case we have 3.1.3.

In 3.1.16 we have that u is even. So u in lemma 3.1.1, formula 3.1.2, is even. Note that if u would be odd, say $u = 2v + 1$, then 3.1.2 would be reduced to 3.1.3. $\square$

We can find a more extensive parametrisation as follows:

Again suppose $2 \nmid q$ or $4 \mid q$, so by 1.6.6 and 1.6.9

3.1.17. $$q^2 \mid (n - 2)$$

Now define $\eta \in \mathbb{N}$ by

3.1.18. $$n - 2 := \eta q^2$$

Then by combination of 1.6.6, 3.1.10 and 3.1.18 we have

3.1.19. $$v(v + 1) = \eta(q - 1)$$

If $q = 2q'$ and q' is odd, then we find in the same way

3.1.20. $$u^2 - 1 = \eta'(q - 1) ,$$

where

3.1.21. $\quad n - 2 := \eta' q'^2$

Now we can substitute 3.1.19 and 3.1.20 in 3.1.3 and 3.1.2 respectively, to find a more extensive parametrisation.

3.2. Second approach to the case e = 2

The approach in this section found its inspiration in Van Lint's approach to the special case q = 10, cfr. [28] . We shall say something about the prime divisors of the zeros x_1 and x_2 of the Lloyd polynomial $P_2(X)$, using the parameter representations in the preceding section and a combination of the polynomial and sphere packing conditions.
Assume that there exists a perfect double-error-correcting code of word length n with $q = p_1^{s_1} \ldots p^{s_\ell}$.
Then by the sphere packing condition 1.2.1 we have

3.2.1. $$1 + n(q - 1) + \binom{n}{2}(q - 1)^2 = p_1^{k+\alpha_1} \ldots p^{k+\alpha_\ell}$$

where α_i $(i = 1,\ldots,\ell)$ is a nonnegative integer and k is defined by

3.2.2. $$\alpha_1 \ldots \alpha_\ell = 0 .$$

The formula 3.2.1 can also be written in the following form:

3.2.3. $$(q - 1)((q - 1)n + q + 1)(n - 2) = 2(p_1^{k+\alpha_1} \ldots p_\ell^{k+\alpha_\ell} - q^2)$$

Now let us define for $i = 1,\ldots,\ell$

3.2.4. $$\beta_i = k + \alpha_i - 2s_i$$

Then we find from 1.6.8 and 3.2.1

3.2.5. $$x_1 x_2 = 2p_1^{\beta_1} \ldots p_\ell^{\beta_\ell}$$

3.2.6. $$\beta_i \geq 0 \quad \text{if} \quad p_i \neq 2 \quad (\text{and } \beta_i \geq -1 \quad \text{if} \quad p_i = 2)$$

The formula 3.2.5 is useful in combination with lemma 3.1.1 to show the nonexistence of double-error-correcting perfect codes for some special values of q.
For this purpose we gather the relevant results in the following

3.2.7. LEMMA. Under the assumptions mentioned above, let $x_1 < x_2$. Then we have:

a) $x_1 x_2 = 2p_1^{\beta_1} \ldots p_\ell^{\beta_\ell}$

b) if $p_i \neq 2$ then $x_1 + x_2 \equiv 3 \pmod{p_i^{s_i}}$

c) unless $p = 2$ or $p = 3$, x_1 and x_2 cannot have a prime factor p in common.

d) Let s be a prime factor of $q - 1$.
Then either $x_1 \equiv 1 \pmod{s}$ and $x_2 \equiv 2 \pmod{s}$
or $x_1 \equiv 2 \pmod{s}$ and $x_2 \equiv 1 \pmod{s}$

e) $q(x_1 - x_2)^2 - 2(x_1 + x_2) = q - 6$

f) $p_1^{k+\alpha_1} \ldots p_\ell^{k+\alpha_\ell} \equiv 1 \pmod{q-1}$

g) $x_1 > \dfrac{(n-1)(q-1) + 2}{q+1}$

h) $x_2 < 2x_1$

PROOF.

a) This is exactly 3.2.5.

b) This can be seen from 3.1.2 and 3.1.3.

c) This follows readily from b)

d) This follows from 3.1.19 and 3.1.20 respectively, and the formulas 3.1.2 and 3.1.3 respectively. For example we find that s divides either v or v + 1.

e) This follows from the formulas 1.6.6 and 1.6.8, or from 3.1.10 and 3.1.16.

f) This follows from 3.2.1 and

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

g) This is known from [27], page 115. See also section 2.2.

h) From theorem 2.1.15 we may assume $q \geq 6$. Hence this follows from g) and from the fact that $x_2 < n$, if $n > 3$. See also lemma 2.1.1.

3.3. *The special case* $q = p^s$

The case $q = p^s$ was already done by Van Lint in [23], and is also easily treated with lemma 3.2.7.

First, from a) we have

3.3.1. $$x_1 x_2 = 2p^k$$

Then since from h) $x_2 < 2x_1$ we see that

3.3.2. $$p = 3$$

so for some positive integers a and b we have

3.3.3. $$\{x_1, x_2\} = \{2.3^a, 3^b\}$$

Then from b) we see that if $s \geq 2$, then $x_1 + x_2$ has exactly one factor 3, so for some $\ell \in \mathbb{N}$

3.3.4. $$x_1 = 6 \text{ and } x_2 = 3^{\ell} \quad (\ell \geq 2),$$

or

$$x_1 = 3 \text{ and } x_2 = 2.3^{\ell} \quad (\ell \geq 1) .$$

Hence, since $x_2 < 2x_1$ we have

3.3.5. $$x_1 = 6 \text{ and } x_2 = 9 .$$

If $s = 1$ we find from e)

3.3.6. $\quad 3(x_1 - x_2)^2 - 2(x_1 + x_2) = -3$

Then we see from 3.3.3 and 3.3.6 that $x_1 + x_2$ has exactly one factor 3, so again we have 3.3.5. Hence in any case

3.3.7. $\quad x_1 + x_2 = 15$

Comparing this with 1.6.6 we find

3.3.8. $\quad n(q - 1) = 8q - 2,$

so

3.3.9. $\quad (q - 1) \mid 6$

Hence $q = 3$ and from 3.3.8 $n = 11$. Then we find the parameters of the ternary Golay code.

This result is part of theorem 2.1.15.

3.4. *A remark about the special case* $q = p_1^s p_2^t$

Let assume the existence of a double-error-correcting code with parameters n and $q = p_1^s p_2^t$, where gcd $(q,6) = 1$.

We shall use the results stated in lemma 3.2.7.

From a) and c) it follows that for some positive integers a and b

3.4.1. $\quad \{x_1,x_2\} = \{2p_1^a,p_2^b\}$ or $\{x_1,x_2\} = \{p_1^a,2p_2^b\}$.

Hence it follows from b) that

3.4.2. $\quad$ Either $2p_1^a \equiv 3 \pmod{p_2}$ or $p_1^a \equiv 3 \pmod{p_2}$

Therefore we have the following theorem:

3.4.3. THEOREM. There does not exist a perfect 2-error-correcting code on q symbols if $q = p_1^s p_2^t$ and gcd $(q,6) = 1$ and $p_1 \equiv 1 \pmod{p_2}$.

PROOF. Assuming the existence of such a code, we would have a contradiction with 3.4.2. □

For example, an alphabet with $5^s 11^t$ symbols is impossible for a perfect 2-code.

3.5. *Four remarks about the special case* $q = 2^k p^s$

Suppose that there exists a perfect 2-code with $q = 2^k p^s$. In this section we shall show that p must satisfy some conditions.
We shall refer to lemma 3.2.7.
First we mention a theorem which was proved by Bassalygo, Zinoviev, Leontiev and Feldman (see [6]).

3.5.1. THEOREM. There does not exist a perfect 2-code on q symbols if $q = 2^k 3^s$.

Like Tietävainen's proof of theorem 2.1.15, the proof makes use of a refinement of the arithmetical-geometrical mean inequality.
This refinement was introduced by Lagrange.
Like Tietävainen, Bassalygo c.s. needed a lower bound for x_2 / x_1.
In the case they treated this meant that a lower bound had to be found for $|A \log 2 - B \log 3|$, where A and B are bounded since x_1 and x_2 have an upper bound n.

Hence without loss of generality we may assume $p \neq 3$. Then from a) in lemma 3.2.7 we find for some positive integers a and b

3.5.2. $\quad x_1 x_2 = 2^a p^b$

Hence from c) we find for some positive integers c, d, such that $c + d = a$

3.5.3. $\quad \{x_1, x_2\} = \{2^c, 2^d p^b\}$

Furthermore we have $c \geq 2$ because

3.5.4. $$P_2(1) = \frac{(n-1)(n-2)}{2}(q-1)^2 > 0$$

3.5.5. $$P_2(2) = \frac{(n-2)(n-3)}{2}(q-1)^2 - (n-2)(q-1) > 0$$

Now we are ready to prove the next two theorems.

3.5.6. THEOREM. There does not exist a perfect 2-code on q symbols if $q = 2^kp^s$ and, for some $t \in \mathbb{N}$, $p = 2^t - 1$. For instance, q cannot be 2^k7^s or 2^k31^s.

PROOF. From b) and 3.5.3 follows

3.5.7. $$2^c \equiv 3 \pmod{p}$$

Now if $p = 2^t - 1$, then 3 is not among the residues of $2^c \pmod{p}$. □

3.5.8. THEOREM. There does not exist a perfect 2-code on q symbols if $q = 2^kp^s$ and $k \geq 2$ and $p \equiv 1 \pmod{4}$.
For instance, if $k \geq 2$ it is impossible that $q = 2^k5^s$.

PROOF. Assume $k \geq 2$. If x_1 and x_2 are both even then we find a contradiction to e), considering this equation modulo 4.
Hence since $c \geq 2$ we find $d = 0$, so $c = a$ and $a \geq 2$ and from 3.5.3 it follows that

3.5.9. $$\{x_1, x_2\} = \{2^a, p^b\}$$

Therefore the equation e) becomes

3.5.10. $$2^{k-1}p^s(2^a - p^b)^2 - (2^a + p^b) = 2^{k-1}p^s - 3$$

Then since $a \geq 2$ and $p \equiv 1 \pmod{4}$ we have a contradiction, considering the equation 3.5.10 modulo 4 . □

Finally, for the fourth theorem we need to look back at section 3.2. If $p_1 = 2$ we find, because in 3.5.3 we have $c \geq 2$, from 3.2.5 and the fact that x_1 and x_2 are integers

3.5.11. $\beta_1 \geq 1$

So from 3.2.4 we have $k + \alpha_1 \geq 3$. Hence from 3.2.3 we find:

3.5.12. $(q - 1)((q - 1)n + q + 1)(n - 2) \equiv 0 \pmod 8$.

Now we are ready to prove the following theorem.

3.5.13. **THEOREM.** There does not exist a perfect 2-code on q symbols if $q = 2p^s$ and $p \equiv 1 \pmod 8$, nor if $q = 2p^{2t}$ and $p \equiv 5 \pmod 8$. For instance q cannot be of the form 2.17^s or 2.25^t.

PROOF. Like in the theorem, assume that $k = 1$, so $q = 2p^s$. Now we distinguish between two cases:

i) n is even. Then from 3.5.12 it follows that $n \equiv 2 \pmod 8$. Hence from 1.6.6 we find

3.5.14. $x_1 + x_2 \equiv 3 \pmod 8$

So in 3.5.3 we find $d = 0$, $c = a$ and

3.5.15. $\{x_1, x_2\} = \{2^a, p^b\}$

Now if $a = 2$, then from h) we see that $p^b = 3, 5$ or 7. So from 3.5.1 and 3.5.6 we have $p^b = 5$, so $x_1 = 4$ and $x_2 = 5$. This contradicts e). So $a \geq 3$ and from 3.5.14 we see

3.5.16. $p^b \equiv 3 \pmod 8$.

So we have a contradiction if $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$.

ii) n is odd. Then from 3.5.12 it follows that

3.5.17. $((q - 1)n + q + 1) \equiv 0 \pmod 8$

Hence we have the following possibilities:

3.5.18. $n \equiv 1 \pmod 8$ and $2q \equiv 0 \pmod 8$

$n \equiv 3 \pmod 8$ and $4q \equiv 2 \pmod 8$

$n \equiv 5 \pmod 8$ and $6q \equiv 4 \pmod 8$

$n \equiv 7 \pmod 8$ and $8q \equiv 6 \pmod 8$

These are all contradictions except the third. So $n \equiv 5 \pmod 8$. Then from 1.6.6 we have, by the substitution $n = 5 + 8t$:

3.5.19. $(2p^s - 1)(3 + 8t) + 3p^s = p^s(x_1 + x_2)$

From 3.5.19 we see immediately:

3.5.20. If $p^s \equiv 1 \pmod 8$ then $x_1 + x_2 \equiv 6 \pmod 8$

If $p^s \equiv 5 \pmod 8$ then $x_1 + x_2 \equiv 2 \pmod 8$

So from 3.5.3 we find $d = 1$ and

3.5.21. $\{x_1, x_2\} = \{2^c, 2p^b\}$

By substitution in e) we find:

3.5.22. $p^s(2^c - 2p^b)^2 - (2^c + 2p^b) = p^s - 3$

Now we see as above that $x_1 > 4$, so $c \geq 3$. Hence we find

3.5.23. $4 - 2p^b \equiv p^s - 3 \pmod 8$

This is a contradiction if $p \equiv 1 \pmod 8$, and if $p \equiv 5 \pmod 8$ and $s = 2t$. □

3.6. *The special case* $q \leq 30$ *or* $q = 35$

In this section we shall treat the cases $q \leq 30$ and $q = 35$. The following values are impossible for q because they are prime powers:

3.6.1. q cannot be 2,3,4,5,7,8,9,11,13,16,17,19,23,25,27,29 , The following values are impossible because of the theorems 3.5.1, 3.5.6 and 3.5.8 respectively:

3.6.2. q cannot be 6,12,18,24

q cannot be 14,28

q cannot be 20

Now, before we shall treat the remaining values 10,15,21,22,26 and 35 we shall treat the case $q = 6$ in an elementary way, using the sphere packing condition only.

3.6.3. THEOREM. A perfect 2-code on 6 symbols does not exist.

PROOF. Assume that there exists such a code. Then by the sphere packing condition 1.2.1 we have for some $k,\ell \in \mathbb{N}_0$:

3.6.4. $$1 + n\cdot 5 + \binom{n}{2}\cdot 25 = 2^k 3^\ell$$

Using the substitution $x = 10n - 3$ we have the diophantine equation

3.6.5. $$x^2 - 1 = 2^{k+3}3^\ell$$

which reduces by $x = 2y + 1$ to

3.6.6. $$y(y + 1) = 2^{k+1}3^\ell$$

Hence we have the following two possibilities

3.6.7. Either $y = 3^\ell$ and $y + 1 = 2^{k+1}$ (A)

or $y = 2^{k+1}$ and $y + 1 = 3^\ell$ (B)

Now we shall treat both cases (A) and (B)

(A) $$2^{k+1} - 1 = 3^\ell$$

Now unless $\ell = 0$ (so $k = 0$ and from 3.6.5 $x = 3$) we find that $k + 1$ must be even, say $k + 1 = 2s$. Then we have

3.6.8. $$(2^s + 1)(2^s - 1) = 3^\ell$$

which is a contradiction since $2^s + 1$ and $2^s - 1$ have no factor 3 in common.

(B) $\qquad 3^{\ell} - 1 = 2^{k+1}$

Now unless $k = 0$ (so $\ell = 1$ and from 3.6.5 $x = 5$) we find that ℓ must be even, say $\ell = 2t$. Then we have

3.6.9. $\qquad (3^t + 1)(3^t - 1) = 2^{k+1}$

Hence we see that $t = 1$, $\ell = 2$ and $k = 2$, so from 3.6.5: $x = 17$.
So $x = 3$ or $x = 5$ or $x = 17$. Furthermore by definition $x = 10n - 3$. This is only possible if $n = 2$. But for a non-trivial perfect 2-code we must have $n \geq 5$. □

In the following all unannounced symbols stand for unspecified positive integers. We shall repeatedly refer to lemma 3.2.7.
As above we shall neglect trivial perfect codes.

3.6.10. THEOREM. (cfr. Van Lint, [28]). A perfect 2-code does not exist if $q = 10$.

PROOF. Assume that there exists such a code.
Since $q = 10$ is among the values of $q = 2p^s$, $p \equiv 5 \pmod 8$ we have as in the proof of theorem 3.5.13 (cfr. 3.5.21)

3.6.11. $\qquad \{x_1, x_2\} = \{2^c, 2\cdot 5^b\}$

Comparing this with 3.2.5 we have the more detailed

3.6.12. $\qquad \{x_1, x_2\} = \{2^{\beta_1}, 2\cdot 5^{\beta_2}\}$

where from 3.2.4 and 3.2.2

3.6.13. $\qquad \beta_i = k + \alpha_i - 2 \quad$ and $\quad \alpha_1\alpha_2 = 0$

Now since from b) we have $x_2 < 2x_1$ we find from 3.6.12 and 3.6.13

3.6.14. $\alpha_2 = 0$ and $\alpha_1 > 0$

Hence we have from f)

3.6.15. $2^{\alpha_1} \equiv 1 \pmod{9}$,

so

3.6.16. $\alpha_1 = 6t$ where $t > 0$.

Now from 3.6.12, 3.6.13, 3.6.14 and 3.6.16 we find, replacing $k - 2$ by u:

3.6.17. $\{x_1, x_2\} = \{2^{u+6t}, 2 \cdot 5^u\}$

where $u \geq 1$ since $x_1 > 2$. Hence we find by substitution in e)

3.6.18. $5(2 \cdot 5^u - 2^{u+6t})^2 - (2 \cdot 5^u + 2^{u+6t}) = 2$

Then since $t > 0$ (see 3.6.16) we find

3.6.19. $4 \cdot 5^{2u+1} - 2 \cdot 5^u \equiv 2 \pmod{16}$

$$2 \cdot 5^{2u+1} - 5^u \equiv 1 \pmod{8}$$

$$10 - 5^u \equiv 1 \pmod{8}$$

$$5^u \equiv 1 \pmod{8}$$

so u must be even, say

3.6.20. $u = 2v$

Furthermore we see from 3.6.18

3.6.21. $2^{u+6t} \equiv 3 \pmod{5}$,

so

3.6.22. $u + 6t = 3 + 4w$

contradicting 3.6.20. So $q = 10$ is impossible. □

Maybe the following case provides the best example of the method used in this section.

3.6.23. THEOREM. A perfect 2-code does not exist if $q = 15$.

PROOF. Assume that there exists such a code. Then for the integral zeros x_1 and x_2 of the Lloyd polynomial $P_2(X)$ we have from 3.2.2, 3.2.4 and 3.2.5:

3.6.24. $$x_1x_2 = 2\cdot 3^{\beta_1}5^{\beta_2}$$

3.6.25. $$\beta_i = k + \alpha_i - 2 \quad \text{and} \quad \alpha_1\alpha_2 = 0$$

From lemma 3.2.7 h) it follows that $\beta_1 > 0$.
From c) it follows that x_1 and x_2 are not both divisible by 5.
From b) it follows, since $\beta_1 > 0$, that x_1 and x_2 are both divisible by 3.
Since $\alpha_1\alpha_2 = 0$ it follows from f) that if $\alpha_i > 0$ then

3.6.26. $$p_i^{\alpha_i} \equiv 1 \pmod 7$$

so $\alpha_i = 6s$. Therefore, replacing $k - 2$ by u, we have four possibilities:

3.6.27. $$\alpha)\ \{x_1,x_2\} = \{x,y\}\ , \quad x = 2\cdot 3^{\beta}5^{u+6s}\ , \quad y = 3^{\gamma}\ , \quad \beta + \gamma = u$$

$$\beta)\ \{x_1,x_2\} = \{x,y\}\ , \quad x = 3^{\beta}5^{u+6s}\ , \quad y = 2\cdot 3^{\gamma},\ \beta + \gamma = u$$

$$\gamma)\ \{x_1,x_2\} = \{x,y\}\ , \quad x = 2\cdot 3^{\beta}5^{u}\ , \quad y = 3^{\gamma}\ , \ \beta + \gamma = u + 6s$$

$$\delta)\ \{x_1,x_2\} = \{x,y\}\ , \quad x = 3^{\beta}5^{u}\ , \quad y = 2\cdot 3^{\gamma},\ \beta + \gamma = u + 6s$$

Now from h) it follows that α) and β) are impossible, because in these cases we would have $x > 2y$.
Now we distinguish between the cases γ) and δ) and we will use the equation e) which becomes in our case

3.6.28. $15(x_1 - x_2)^2 - 2(x_1 + x_2) = 9$

γ) in this case we have by substitution in 3.6.28

3.6.29. $15(2\cdot 3^\beta 5^u - 3^\gamma)^2 - 2(2\cdot 3^\beta 5^u + 3^\gamma) = 9$

where β and γ are positive and $\beta + \gamma = u + 6s \geq 6$ since $s > 0$.
Hence we find from 3.6.29

3.6.30. $-2(2\cdot 3^\beta 5^u + 3^\gamma) \equiv 9 \pmod{27}$

Now suppose $u = 0$. Then, keeping in mind that $x_2 < 2x_1$, we have a contradiction to 3.6.30. So $u > 0$ and since $\beta > 0$ we have $\gamma \geq 3$, because otherwise we would have a contradiction to h).
Now it follows from 3.6.30 that

3.6.31. $\beta = 2$

Hence since $\beta + \gamma \geq 6$ we have $\gamma \geq 4$. Therefore we find from 3.6.30

3.6.32. $-4\cdot 5^u \equiv 1 \pmod{9}$,

so

3.6.33. $u + 1 = 6t$

where $t > 0$ since $u > 0$. Furthermore we have from 3.6.29, since $u > 0$,

3.6.34. $-2\cdot 3^\gamma \equiv 4 \pmod{5}$,

so

3.6.35. $\gamma = 1 + 4v$

Then since $\beta + \gamma = u + 6s$ it follows from 3.6.31 and 3.6.33 that

3.6.36. $\gamma = 6t + 6s - 3$

so we have from 3.6.35 and 3.6.36

3.6.37. $6t + 6s = 4(v + 1)$

so $v + 1$ must be divisible by 3 and

3.6.38. $6t + 6s = 12w$

Now it follows from 3.6.31, 3.6.33, 3.6.36 and 3.6.38 that

3.6.39. $\{x_1, x_2\} = \{18 \cdot 5^{6t-1}, 3^{12w-3}\}$

Finally we shall use d) i.e.

3.6.40. $x_1 + x_2 \equiv 3 \pmod 7$

Since 27 ≡ -1 (mod 27) it follows from 3.6.39 and 3.6.40 that

3.6.41. $4 \cdot 5^{6t-1} + (-1)^{4w-1} \equiv 3 \pmod 7$,

so

3.6.42. $5^{6t-1} \equiv 1 \pmod 7$,

so

3.6.43. $6t - 1 = 6z$

which yields a contradiction. So the case γ) is impossible.

δ) In this case we have by substitution in 3.6.28

3.6.44. $15(3^\beta 5^u - 2 \cdot 3^\gamma)^2 - 2(3^\beta 5^u + 2 \cdot 3^\gamma) = 9$

where β and γ are positive and $\beta + \gamma = u + 6s \geq 6$.
Hence we find from 3.6.44

3.6.45. $-2(3^\beta 5^u + 2 \cdot 3^\gamma) \equiv 9 \pmod{27}$

In the same way as after 3.6.30 we find $\gamma \geq 3$ so from 3.6.45 we have

3.6.46. $\beta = 2$

Hence since $\beta + \gamma \geq 6$ we have $\gamma \geq 4$ and we find from 3.6.45

3.6.47. $-2 \cdot 5^u \equiv 1 \pmod 9$,

so

3.6.48. $u = 4 + 6t$

Furthermore we have from 3.6.44 since $u > 0$

3.6.49. $-4\cdot 3^{\gamma} \equiv 4 \pmod{5}$,

so

3.6.50. $\gamma = 2 + 4v$

Then since $\beta + \gamma = u + 6s$ it follows from 3.6.46, 3.6.48 and 3,6,50 that

3,6.51. $2 + 4v = 2 + 6s + 6t$

3.6.52. $6s + 6t = 12w$

Now it follows from 3.6.46, 3.6.48, 3.6.50, 3.6.51 and 3.6.52 that

3.6.53. $\{x_1,x_2\} = \{9\cdot 5^{4+6t}, 2\cdot 3^{2+12w}\}$

Finally we will use d), i.e.

3.6.54. $x_1 + x_2 \equiv 3 \pmod{7}$

which becomes, using 3.6.53:

3,6.55, $2\cdot 5^{4} + 2\cdot 3^{2} \equiv 3 \pmod{7}$

3.6.56. $1 \equiv 3 \pmod{7}$

which yields a contradiction. So the case δ) is also impossible.

By careful observation of the above proof we see that our considerations modulo 5 are in this case superfluous. In general there is not so much coincidence. For the following theorems we shall give the proofs in a more concise form.

3.6.57. THEOREM. A perfect 2-code does not exist if $q = 21$.

PROOF. Assume that there exists such a code with $q = 21$.
Then we have from 3.2.2, 3.2.4 and 3.2.5

3.6.58. $x_1x_2 = 2\cdot 3^{\beta_1}7^{\beta_2}$

3.6.59. $\beta_i = k + \alpha_i - 2$ and $\alpha_1\alpha_2 = 0$

From lemma 3.2.7 h) it follows that $\beta_1 > 0$, so from b) it follows that x_1 and x_2 are both divisible by 3 but not both by 7.
Since $\alpha_1\alpha_2 = 0$ it follows from f) that if $\alpha_i > 0$, then

3.6.60. $p_i^{\alpha_i} \equiv 1 \pmod{5}$, so $\alpha_i = 4s$

Hence if we replace $k - 2$ by u and if we set $\{x_1,x_2\} = \{x,y\}$ then from h) it follows that there are only two possibilities:

3.6.61. $x = 2\cdot 3^{\beta}7^{u}$, $y = 3^{\gamma}$, $\beta + \gamma = u + 4s$ (α)

$x = 3^{\beta}7^{u}$, $y = 2\cdot 3^{\gamma}$, $\beta + \gamma = u + 4s$ (β)

where $\beta > 0$, $\gamma > 0$, $\beta + \gamma \geq 4$. We shall distinguish between (α) and (β)

(α) In this case we find by substitution in e)

3.6.62. $21(2\cdot 3^{\beta}\, 7^{u} - 3^{\gamma})^2 - 2(2\cdot 3^{\beta}7^{u} + 3^{\gamma}) = 15$

If $\gamma = 1$ then by h) we have a contradiction since $\beta \geq 1$. So $\gamma \geq 2$ and we see by considering 3.6.62 (modulo 9)

3.6.63. $\beta = 1$.

Now, if $u = 0$, then since $\beta = 1$ we have $x = 6$, so from h) $y = 9$. But then we have a contradiction to e). So $u > 0$ and from 3.6.62

3.6.64. $-2\cdot 3^{\gamma} \equiv 1 \pmod{7}$

3.6.65. $\gamma = 1 + 6v$

Now from d) it follows

3.6.66. $x + y \equiv 3 \pmod 4$

since from 3.6.63 and 3.6.65 we have

3.6.67. $\{x,y\} = \{6\cdot 7^u, 3^{1+6v}\}$

we find a contradiction to 3.6.66. So the case (α) is impossible.

(β) In this case we find by substitution in e)

3.6.68. $21(3^\beta 7^u - 2\cdot 3^\gamma)^2 - 2(3^\beta 7^u + 2\cdot 3^\gamma) = 15$

Now if $\gamma = 1$, then by h) we see, since $\beta > 0$, that $y = 6$ and $x = 9$. But then we have a contradiction to e). So $\gamma \geq 2$. Therefore we see by considering 3.6.68 (modulo 9)

3.6.69. $\beta = 1$

3.6.70. $-6\cdot 7^u \equiv 6 \pmod 9$

3.6.71. $7^u \equiv 2 \pmod 3$

which yields a contradiction. So (β) is also impossible. □

In the following example we shall see that sometimes we need considerations with congruences modulo a prime which does not divide q nor q - 1.

3.6.72. THEOREM. A perfect 2-code with $q = 22$ does not exist.

PROOF. Assume that there exists such a code. Then we find from 3.2.5

3.6.73. $x_1 x_2 = 2^{\beta_1+1} 11^{\beta_2}$

Hence we see from c) that for some $a,b \in \mathbb{N}_0$

3.6.74. $\{x_1,x_2\} = \{2^a, 2^b 11^{\beta_2}\}$, where $a + b = \beta_1 + 1$

Hence we have by substitution in e):

3.6.75. $11(2^a - 2^b 11^{\beta_2})^2 - (2^a + 2^b 11^{\beta_2}) = 8$

From h) we see that $\beta_2 > 0$, so again using h) we see that $a \geq 3$. Therefore, by considering 3.6.75 (modulo 8), we see that b cannot be 1 or 2. Furthermore, if $b > 3$, then by h) we see that $a > 3$ and we find a contradiction by considering 3.6.75 (modulo 16). So $b = 0$ or $b = 3$.

α) Let us suppose $b = 0$, so from 3.6.74 and 3.6.75

3.6.76. $\{x_1, x_2\} = \{2^a, 11^{\beta_2}\}$

and

3.6.77. $11(2^a - 11^{\beta_2})^2 - (2^a + 11^{\beta_2}) = 8$

From 3.6.77 we find

3.6.78. $2^a \equiv 3 \pmod{11}$, so

3.6.79. $a = 8 + 10u$

Hence since $a \geq 8$ we find again from 3.6.77

3.6.80. $11^{2\beta_2+1} - 11^{\beta_2} \equiv 8 \pmod{16}$,

so

3.6.81. $\beta_2 = 1 + 4t$

Now from d) we see

3.6.82. $2^a \equiv 1 \pmod{21}$ and $11^{\beta_2} \equiv 2 \pmod{21}$,

or

$2^a \equiv 2 \pmod{21}$ and $11^{\beta_2} \equiv 1 \pmod{21}$.

Since from 3.6.79 a is even, we see

3.6.83. $2^a \equiv 1 \pmod{3}$

So from 3.6.82.

3.6.84. $2^a \equiv 1 \pmod{21}$

3.6.85. $a = 6w$

So from 3.6.82 and 3.6.84 we have

3.6.86. $11^{\beta_2} \equiv 2 \pmod{21}$

3.6.87. $\beta_2 = 5 + 6z$

Now by combination of 3.6.79 and 3.6.85,
and 3.6.81 and 3.6.87 respectively, we see

3.6.88. $a = 18 + 30v$

$\beta_2 = 5 + 12s$

3.6.89. $\{x_1, x_2\} = \{2^{18+30v}, 11^{5+12s}\}$

Now since we have the following congruences modulo 13:

3.6.90. $2^{18+30v} \equiv \pm 1 \pmod{13}$

3.6.91. $11^{5+12s} \equiv -6 \pmod{13}$

we see that we have a contradiction by substitution in 3.6.77, considering the equation modulo 13.

β) Now let us suppose that $b = 3$, so, from 3.6.74 and 3.6.75

3.6.92. $\{x_1, x_2\} = \{2^a, 8 \cdot 11^{\beta_2}\}$

3.6.93. $11(2^a - 8 \cdot 11^{\beta_2})^2 - (2^a + 8 \cdot 11^{\beta_2}) = 8$

Like in the case α) we have

3.6.94. $a = 18 + 30v$

But in this case we have instead of 3.6.86

3.6.95. $8\cdot 11^{\beta_2} \equiv 2 \pmod{21}$

3.6.96. $\beta_2 = 2 + 6z$

Hence we find from 3.6.92, 3.6.94 and 3.6.96

3.6.97. $\{x_1,x_2\} = \{2^{18+30v}, 8\cdot 11^{2+6z}\}$

Now since we have the following congruences modulo 5:

3.6.98. $2^{18+30v} \equiv \pm 1 \pmod{5}$

3.6.99. $8\cdot 11^{2+6z} \equiv 3 \pmod{5}$

we see that we have a contradiction by substitution in 3.6.77, considering the equation modulo 5. □

3.6.100. THEOREM. A perfect 2-code does not exist if $q = 26$.

PROOF. Assume that there exists such a code.
Since $q = 26$ is among the values of $q = 2p^s$, $p \equiv 5 \pmod{8}$, we have as in the proof of theorem 3.5.13 (cfr. 3.5.21)

3.6.101. $\{x_1,x_2\} = \{2^c, 2\cdot 13^b\}$

Comparing this with 3.2.5, 3.2.2 and 3.2.4 we have the more detailed

3.6.102. $\{x_1,x_2\} = \{2^{\beta_1}, 2\cdot 13^{\beta_2}\}$

where $\beta_i = k + \alpha_i - 2$ and $\alpha_1\alpha_2 = 0$.

Now since from h) we have $x_2 < 2x_1$, we find from 3.6.12 and 3.6.13

3.6.103. $\alpha_2 = 0$ and $\alpha_1 > 0$

Hence it follows from f) that

3.6.104. $2^{\alpha_1} \equiv 1 \pmod{25}$,

so

3.6.105. $\alpha_1 = 20s$ and $s > 0$

Now from 3.6.101, 3.6.102, 3.6.103 and 3.6.105 we have, replacing $k - 2$ by u.

3.6.106. $\{x_1, x_2\} = \{2^{u+20s}, 2\cdot 13^u\}$

where $u > 0$ since $x_1 > 2$. Hence we find by substitution in e)

3.6.107. $13(2^{u+20s} - 2\cdot 13^u)^2 - (2^{u+20s} + 2\cdot 13^u) = 10$

Then since $s > 0$ (see 3.6.105) we find

3.6.108. $4\cdot 13^{2u+1} - 2\cdot 13^u \equiv 10 \pmod{16}$

$$\begin{aligned} 2\cdot 13^{2u+1} - 13^u &\equiv 5 \pmod{8} \\ 26 - 13^u &\equiv 5 \pmod{8} \\ 13^u &\equiv 5 \pmod{8} \end{aligned}$$

so u must be odd, say

3.6.109. $u = 2v + 1$

Furthermore, we see from 3.6.107

3.6.110. $2^{u+20s} \equiv 3 \pmod{13}$,

so

3.6.111. $u + 20s = 4 + 12t$

contradicting 3.6.109. So $q = 26$ is impossible. □

We see that the proof for the case $q = 26$ is completely analogous to the proof for the case $q = 10$. Yet we cannot find a general nonexistence proof for the case $q = 2p$ ($p \equiv 5 \pmod{8}$), since we need explicit congruences.

In the next theorem we meet the first value of q which has no factor 2 or 3.

3.6.112. THEOREM. There does not exist a perfect 2-code if $q = 35$.

PROOF. Assume that there exists such a code. Then we have from 3.2.2, 3.2.4 and 3.2.5, and c) in lemma 3.2.7

3.6.113. $\{x_1,x_2\} = \{2\cdot 5^{\beta_1}, 7^{\beta_2}\}$ or $\{x_1,x_2\} = \{5^{\beta_1}, 2\cdot 7^{\beta_2}\}$

where $\beta_i = k + \alpha_i - 2$ and $\alpha_1\alpha_2 = 0$.
Furthermore, since from h) $x_2 < 2x_1$ we have

3.6.114. $\beta_2 \geq 2$ or $\{x_1,x_2\} = \{7,10\}$

In the latter case it should follow from b) that

3.6.115. $7 \equiv 3 \pmod{5}$

which is not true. So we have

3.6.116. $\beta_2 \geq 2$.

Now if $\alpha_2 > 0$ then since $\alpha_1\alpha_2 = 0$ we have $\beta_2 > \beta_1$, contradicting h).
So we find

3.6.117. $\alpha_2 = 0$.

Hence from f) we have

3.6.118. $5^{\alpha_1} \equiv 1 \pmod{17}$

3.6.119. $\alpha_1 = 16s$, where $s \geq 0$

Then, replacing $k - 2$ by u we have from 3.6.113, 3.6.117 and 3.6.119

3.6.120. Either $\{x_1,x_2\} = \{2\cdot 5^{u+16s}, \quad 7^u\}$ (a)

or $\{x_1,x_2\} = \{ \quad 5^{u+16s}, 2\cdot 7^u\}$ (b)

where from 3.6.116 it follows that $u + 16s \geq 2$

We shall treat the cases (a) and (b) separately.

a) In this case we have by substitution in e)

3.6.121. $35(2\cdot 5^{u+16s} - 7^u)^2 - 2(2\cdot 5^{u+16s} + 7^u) = 29$

So since $u + 16s \geq 2$ we find

3.6.122. $5\cdot 7^{2u+1} - 2\cdot 7^u \equiv 4 \pmod{25}$

So since $49 \equiv -1 \pmod{25}$ we have

3.6.123. $10(-1)^u - 2\cdot 7^u \equiv 4 \pmod{25}$

3.6.124. $u = 3 + 4v$

Furthermore we have from 3.6.121, since from 3.6.124 we have u is odd,

3.6.125. $3(4 + 4 + 1) - 2(10 + 7) \equiv 5 \pmod{8}$

which is a contradiction. So the case (a) is impossible.

b) In this case we have by substitution in e)

3.6.126. $35(5^{u+16s} - 2\cdot 7^u)^2 - 2(5^{u+16s} + 2\cdot 7^u) = 29$

so since $u + 16s \geq 2$ we find

3.6.127. $10\cdot 4\cdot 7^{2u} - 4\cdot 7^u \equiv 4 \pmod{25}$

3.6.128. $10(-1)^u - 7^u \equiv 1 \pmod{25}$

But this is a contradiction since the left hand side of 3.6.128 is (mod 25) equal to 8, 11, 22, 9 respectively if $u \equiv 1, 2, 3, 0 \pmod{4}$. □

The next open cases are $q = 30$, which will be treated in section 3.7, and $q = 33$.
The impatient reader may try to treat the case $q = 33$ in some way like $q = 15$ or $q = 21$.

Remark that the case $q = 34$ is ruled out by theorem 3.5.13, so after $q = 33$ the first open case is $q = 38$ (for $q = 36$ see theorem 3.5.1). But at this moment we shall make a stop.

3.7. *The special case* $q = 30$

In our investigations the case $q = 30$ is often the first open case. The reason is that 30 has three small distinct prime divisors (cfr. chapter 2).

In 3.6 the case $q = 30$ was left out because otherwise the paragraph would become too lengthy.

Nevertheless, in the following we shall refer to the results in lemma 3.2.7. The outcome is the following non-existence theorem:

3.7.1. THEOREM. A perfect 2-code on 30 symbols does not exist.

PROOF. Assume that there exists such a code. Then from a) in lemma 3.2.7 we find that for some $a,b,c \in \mathbb{N}_0$ we have

3.7.2. $$x_1x_2 = 2^a3^b5^c$$

Now if two of a,b,c are equal to zero, then we have a contradiction to h). So at most one of them can be zero. Now first we shall treat the cases $a = 0$, $b = 0$, and $c = 0$, respectively.

i) Let us suppose $a = 0$. Then $b > 0$ and $c > 0$.
Then it follows from b) and c) that for some $b_1,b_2 \in \mathbb{N}$ with $b_1 + b_2 = b$ we have

3.7.3. $$\{x_1,x_2\} = \{3^{b_1},3^{b_2}5^c\}$$

Then we have by substitution in e)

3.7.4. $$15(3^{b_1} - 3^{b_2}5^c)^2 - (3^{b_1} + 3^{b_2}5^c) = 12$$

Now since $3^{b_2}5^c \geq 15$, we have from h) that $b_1 \geq 2$. Therefore we see by considering 3.7.4 modulo 9:

3.7.5. $\quad b_2 = 1$

So 3.7.4 becomes

3.7.6. $\quad 15(3^{b_1} - 3 \cdot 5^c)^2 - (3^{b_1} + 3 \cdot 5^c) = 12$

Now by considering 3.7.6 modulo 5 we see that

3.7.7. $\quad 3^{b_1} \equiv 3 \pmod 5$

3.7.8. $\quad b_1 = 1 + 4t$

so since $b_1 \geq 2$ we find $b_1 \geq 5$. Hence we find from 3.7.6:

3.7.9. $\quad 3 \cdot 5^c \equiv 15 \pmod{27}$

$$5^c \equiv 5 \pmod 9$$

3.7.10. $\quad c = 1 + 6s$

Hence since from 3.7.8 and 3.7.10 b_1 and c are both odd we see by considering 3.7.6 modulo 8:

3.7.11. $\quad -(3 - 15)^2 - (3 + 15) \equiv 4 \pmod 8)$

which yields a contradiction. So it is impossible that a = 0.

ii) Let us suppose that b = 0. Then a > 0 and c > 0. Then it follows from c) that for some $a_1, a_2 \in \mathbb{N}_0$ with $a_1 + a_2 = a$ we have

3.7.12. $\quad \{x_1, x_2\} = \{2^{a_1}, 2^{a_2}5^c\}$

Then we have by substitution in e)

3.7.13. $\quad 15(2^{a_1} - 2^{a_2}5^c)^2 - (2^{a_1} + 2^{a_2}5^c) = 12$

Now from 3.5.4 and 3.5.5 we find $a_1 \geq 2$.

If $a_2 = 0$ we therefore have from 3.7.13

3.7.14. $2 \equiv 0 \pmod 4$

which is a contradiction. If $a_2 = 1$ we have also 3.7.14.

If $a_2 \geq 3$ then from h) we see that $a_1 \geq 3$, so we have a contradiction to 3.7.13, considering the equation modulo 8. Hence we find:

3.7.15. $a_2 = 2$

so 3.7.13 becomes

3.7.16. $15(2^{a_1} - 4 \cdot 5^c)^2 - (2^{a_1} + 4 \cdot 5^c) = 12$

From 3.7.16 we have

3.7.17. $2^{a_1} \equiv 3 \pmod 5$

3.7.18. $a_1 = 3 + 4s$

so a_1 is odd. So from d) we have

3.7.19. $2^{a_1} \equiv 2 \pmod{29}$

$4 \cdot 5^c \equiv 1 \pmod{29}$

3.7.20. $c = 5 + 14t$

Furthermore we see from 3.7.16

3.7.21. $2^{a_1} + 2^c \equiv 0 \pmod 3$

which yields a contradiction, since following 3.7.18 and 3.7.20 a_1 and c are both odd. So it is impossible that $b = 0$.

iii) Let us suppose that $c = 0$. Then $a > 0$ and $b > 0$ and it follows that for some $a_1, a_2, b_1, b_2 \in \mathbb{N}_0$ chosen in a way that $a_1 + a_2 = a$ and $b_1 + b_2 = b$ we have

3.7.22. $\{x_1, x_2\} = \{2^{a_1}3^{b_1}, 2^{a_2}3^{b_2}\}$

Furthermore, since $b > 0$ it follows from b) that

3.7.23. $b_1 b_2 > 0$

and from h) it follows that

3.7.24. $a_1 \neq a_2$ and $b_1 \neq b_2$

By substitution in e) we find

3.7.25. $15(2^{a_1}3^{b_1} - 2^{a_2}3^{b_2})^2 - (2^{a_1}3^{b_1} + 2^{a_2}3^{b_2}) = 12$

So since b_1 and b_2 are positive we find

3.7.26. $2^{a_1}3^{b_1} + 2^{a_2}3^{b_2} \equiv 15 \pmod{27}$

Therefore, and since we have 3.7.23 and 3.7.24, we have without loss of generality

3.7.27. $b_1 = 1$ and $b_2 \geq 2$

So from 3.7.22 we find

3.7.28. $\{x_1, x_2\} = \{3 \cdot 2^{a_1}, 3^{b_2}2^{a_2}\}$

Now since $b_2 \geq 2$ we see from h) that $a_1 \geq 1$.
Now suppose $a_1 < 3$. Then by h) and 3.7.27 $\{x_1, x_2\}$ is one of the following pairs:

3.7.29. $\{x_1, x_2\} = \{6, 9\}$ or $\{9, 12\}$ or $\{12, 18\}$

Then we have a contradiction by substitution in e). So we have

3.7.30. $a_1 \geq 3$

Then we find from 3.7.25 and 3.7.27

3.7.31. $-(2^{a_2}3^{b_2})^2 - (2^{a_2}3^{b_2}) \equiv 4 \pmod{8}$

Therefore we see that we have two subcases:

3.7.32. Either $a_2 = 0$ and b_2 is odd (A)

or $a_2 = 2$ (B)

(A) In this subcase we have from 3.7.28

3.7.33. $\{x_1, x_2\} = \{3 \cdot 2^{a_1}, 3^{b_2}\}$

3.7.34. $b_2 = 1 + 2s$

From 3.7.27 and 3.7.34 we have $b_2 \geq 3$. So from 3.7.26 and 3.7.27 we have

3.7.35. $2^{a_1} \equiv 5 \pmod{9}$

3.7.36. $a_1 = 5 + 6t$

From 3.7.33 we see by substitution in e)

3.7.37. $3 \cdot 2^{a_1} + 3^{b_2} \equiv 3 \pmod{5}$

Since b_2 and a_1 are both odd (see 3.7.34 and 3.7.36) this is only possible if

3.7.38. $a_1 = 1 + 4u$

3.7.39. $b_2 = 3 + 4v$

Now we have from d) in 3.2.7

3.7.40. Either $3^{b_2} \equiv 1 \pmod{29}$ or $3^{b_2} \equiv 2 \pmod{29}$

Since b_2 is odd we find that we must have the latter congruence, so

3.7.41. $b_2 = 17 + 28w$

But 3.7.41 contradicts 3.7.39, so the subcase (A) is impossible.

(B) In this subcase we have following 3.7.28

3.7.42. $\{x_1,x_2\} = \{3\cdot 2^{a_1}, 4\cdot 3^{b_2}\}$

Hence by substitution in e) we have

3.7.43. $15(3\cdot 2^{a_1} - 4\cdot 3^{b_2})^2 - (3\cdot 2^{a_1} + 4\cdot 3^{b_2}) = 12$

From 3.7.27 we have $b_2 \geq 2$. Now if $b_2 = 2$ then we have from h)

3.7.44. $\{x_1,x_2\} = \{24,36\}$ or $\{x_1,x_2\} = \{48,36\}$

but these pairs contradict e) in lemma 3.2.7. So we have $b_2 \geq 3$, and we find from 3.7.26 and 3.7.27

3.7.45. $2^{a_1} \equiv 5 \pmod{9}$

3.7.46. $a_1 = 5 + 6t$

So $a_1 \geq 5$. Therefore it follows from 3.7.43 that

3.7.47. $4\cdot 3^{b_2} \equiv 4 \pmod{16}$

$3^{b_2} \equiv 1 \pmod{4}$

3.7.48. $b_2 = 2s$

Furthermore we have from 3.7.43:

3.7.49. $3\cdot 2^{a_1} + 4\cdot 3^{b_2} \equiv 3 \pmod{5}$

Since a_1 is odd and b_2 is even (see 3.7.46, 3.7.48) this is only possible if

3.7.50. $a_1 = 3 + 4u$ and $b_2 = 4v$

Now again we find from d)

3.7.51. Either $4\cdot 3^{b_2} \equiv 1 \pmod{29}$ or $4\cdot 3^{b_2} \equiv 2 \pmod{29}$

But from these two congruences it would follow that, respectively

3.7.52. Either $b_2 = 22 + 28w$ or $b_2 = 11 + 28w$

and we see that 3.7.52 contradicts 3.7.50. Hence the subcase (B) is also impossible. Therefore we see that it is impossible that $c = 0$.

Now we have seen in the cases i), ii), iii):

3.7.53. $abc > 0$

Hence we have from 3.7.2, and b) and c) im lemma 3.2.7, some $a_1, a_2 \in \mathbb{N}_0$ with $a_1 + a_2 = a$ and some $b_1, b_2 \in \mathbb{N}$ with $b_1 + b_2 = b$ such that

3.7.54. $\{x_1, x_2\} = \{2^{a_1}3^{b_1}, 2^{a_2}3^{b_2}5^{c}\}$

Now we shall first show that a_1 and a_2 are both positive. Assume $a_1a_2 = 0$, so either $a_1 = 0$ and by 3.7.53 $a_2 > 0$, or $a_2 = 0$ and by 3.7.53 $a_1 > 0$.

1) Let us assume $a_1 = 0$ and $a_2 > 0$. Then we have $2^{a_2}3^{b_2}5^{c} \geq 30$, so from h) it follows that $b_1 \geq 3$.

Furthermore we have by substitution in e)

3.7.55. $15(2^{a_2}3^{b_2}5^c - 3^{b_1})^2 - (2^{a_2}3^{b_2}5^c + 3^{b_1}) = 12$

So since $b_1 \geq 3$ we see from 3.7.55

3.7.56. $2^{a_2}3^{b_2}5^c \equiv 15 \pmod{27}$

so we have

3.7.57. $b_2 = 1$

3.7.58. $2^{a_2}5^c \equiv 5 \pmod{9}$

Again it follows from 3.7.55 that

3.7.59. $3^{b_1} \equiv 3 \pmod{5}$

3.7.60. $b_1 = 1 + 4s$

Hence b_1 is odd. Therefore we have from 3.7.55, since $a_2 > 0$

3.7.61. $3 - 2^{a_2}3\ 5^c - 3 \equiv 0 \pmod{4}$

so $a_1 \geq 2$. Again from 3.7.55 we find

3.7.62. $-1 - 2^{a_2}3\ 5^c - 3 \equiv 4 \pmod{8}$

so $a_2 \geq 3$. Then we find from 3.7.55 and 3.7.60

3.7.63. $-9 - 2^{a_2}3\ 5^c - 3 \equiv 12 \pmod{16}$

3.7.64. $a_2 = 3$

So from 3.7.57 and 3.7.64 we have

3.7.65. $\{x_1,x_2\} = \{3^{b_1}, 24\cdot 5^c\}$

Now from d) in lemma 3.2.7 we find

3.7.66. Either $3^{b_1} \equiv 1 \pmod{29}$ and $24\cdot 5^c \equiv 2 \pmod{29}$

or $3^{b_1} \equiv 2 \pmod{29}$ and $24\cdot 5^c \equiv 1 \pmod{29}$

Now since from 3.7.60 b_1 is odd, the latter congruences must hold. Hence we find

3.7.67. $b_1 = 17 + 28v$

3.7.68. $c = 6 + 14w$

In particular we find $c \geq 2$. Hence we find from 3.7.55

3.7.69. $15\cdot 3^{2b_1} - 3^{b_1} \equiv 12 \pmod{25}$

Now it is straightforward to check that if b_1 is odd, then

3.7.70. $15\cdot 3^{2b_1} \equiv 10 \pmod{25}$

So from 3.7.69 and 3.7.70 we find

3.7.71. $3^{b_1} \equiv 23 \pmod{25}$

3.7.72. $b_1 = 13 + 20t$

Now by substitution of 3.7.65 in e) we have

3.7.73. $15(3^{b_1} - 24\cdot 5^c)^2 - (3^{b_1} + 24\cdot 5^c) = 12$

Furthermore modulo 31 we have:

3.7.74. $5^c \equiv 5, -6$ or 1

3.7.75. $3^{b_1} \equiv \pm 4, \quad \pm 11 \quad \text{or} \quad \pm 7$

because from 3.7.72 $b_1 \equiv 3 \pmod 5$). Now it is straightforward to check that 3.7.74 and 3.7.75 contradict 3.7.73. So the subcase 1) is impossible.

2) Now suppose $a_2 = 0$ and $a_1 > 0$. Then we have by substitution in e) from 3.7.54:

3.7.76. $15(2^{a_1}3^{b_1} - 3^{b_2}5^c)^2 - (2^{a_1}3^{b_1} + 3^{b_2}5^c) = 12$

So since b_1 and b_2 are positive

3.7.77. $2^{a_1}3^{b_1} + 3^{b_2}5^c \equiv 15 \pmod{27}$

Hence at least one of b_1, b_2 is equal to 1. Therefore we shall treat the (partly overlapping) subcases α) and β) where $b_1 = 1$, $b_2 = 1$ respectively.

α) Suppose $b_1 = 1$, so

3.7.78. $\{x_1, x_2\} = \{3 \cdot 2^{a_1}, 3^{b_2}5^c\}$

and by substitution in e)

3.7.79. $15(3 \cdot 2^{a_1} - 3^{b_2}5^c)^2 - (3 \cdot 2^{a_1} + 3^{b_2}5^c) = 12$

so

3.7.80. $3 \cdot 2^{a_1} \equiv 3 \pmod 5$

3.7.81. $a_1 = 4s$

so $a_1 \geq 4$ and from 3.7.79

3.7.82. $-(3^{2b_2}5^{2c}) - 3^{b_2}5^{c} \equiv 12 \pmod{16}$

So by checking all 16 possibilities we find

3.7.83. Either $b_2 = 1 + 4u$ and $c = 2 + 4v$

or $b_2 = 3 + 4v$ and $c = 4v$

Let us suppose $b_2 = 1$. Then from d) we find:

3.7.84. Either $3 \cdot 5^{c} \equiv 1 \pmod{29}$ and $3 \cdot 2^{a_1} \equiv 2 \pmod{29}$

or $3 \cdot 5^{c} \equiv 2 \pmod{29}$ and $3 \cdot 2^{a_1} \equiv 1 \pmod{29}$

Since, from 3.7.83, c is even we see that the latter congruences must hold. But then this contradicts 3.7.81. So $b_2 > 1$.
Hence from 3.7.83 we find $b_2 \geq 3$.
Therefore, and since in this subcase $b_1 = 1$ we find from 3.7.77

3.7.85. $2^{a_1} \equiv 5 \pmod{9}$

3.7.86. $a_1 = 5 + 6t$

which yields a contradiction to 3.7.81. So the case α) is impossible, so $b_1 > 1$.

β) So in the case 2) we have $b_2 = 1$ and $b_1 > 1$ and

3.7.87. $\{x_1, x_2\} = \{3^{b_1}2^{a_1}, 3 \cdot 5^{c}\}$

Now first suppose $b_1 = 2$. Then from b) in lemma 3.2.7 we find

3.7.88. $9 \cdot 2^{a_1} \equiv 3 \pmod{5}$

3.7.89. $a_1 = 1 + 4s$

From d) we have

3.7.90. Either $9\cdot 2^{a_1} \equiv 1$ (mod 29) or $9\cdot 2^{a_1} \equiv 2$ (mod 29

3.7.91. Either $a_1 = 18 + 28v$ or $a_1 = 19 + 28v$

which contradicts 3.7.89. So $b_1 \geq 3$.

By substitution of 3.7.87 in e) we have

3.7.92. $15(3^{b_1}2^{a_1} - 3\cdot 5^c)^2 - (3^{b_1}2^{a_1} + 3\cdot 5^c) = 12$

so since $b_1 \geq 3$ we find

3.7.93. $3\cdot 5^c \equiv 15$ (mod 27)

3.7.94. $5^c \equiv 5$ (mod 9)

3.7.95. $c = 1 + 6s$

Now from d) it follows that

3.7.96. Either $3\cdot 5^c \equiv 1$ (mod 29) or $3\cdot 5^c \equiv 2$ (mod 29)

By checking all possible values of c (mod 14) we find

3.7.97. $3\cdot 5^c \equiv 2$ (mod 29) and $c = 10 + 14t$

which is a contradiction to 3.7.95. So β) is impossible.

So 2) is impossible, and in 1) and 2) we have proved that we have

3.7.98. $a_1 a_2 > 0$

Now we see that for positive integers a_1, b_1, a_2, b_2 and c

3.7.99. $\{x_1, x_2\} = \{2^{a_1}3^{b_1}, 2^{a_2}3^{b_2}5^c\}$

By substitution in e) we have

3.7.100. $15(2^{a_1}3^{b_1} - 2^{a_2}3^{b_2}5^c)^2 - (2^{a_1}3^{b_1} + 2^{a_2}3^{b_2}5^c) = 12$

Now by considering 3.7.100 modulo 9 we see that at least one of b_1,b_2 must be equal to 1.

Furthermore, by considering 3.7.100 modulo 8 we see that one of the following possibilities must hold

3.7.101. Either $a_1 = a_2 = 1$, or one of a_1,a_2 equals 2 and the other is at least 3.

Therefore we have six cases:

(1) $b_1 = 1$ and $a_1 = a_2 = 1$ $b_2 \geq 1$

(2) $b_1 = 1$ and $a_2 = 2$ and $a_1 \geq 3$ and $b_2 \geq 1$

(3) $b_1 = 1$ and $a_1 = 2$ and $a_2 \geq 3$ and $b_2 \geq 1$

(4) $b_2 = 1$ and $a_1 = a_2 = 1$ and $b_1 > 1$

(5) $b_2 = 1$ and $a_2 = 2$ and $a_1 \geq 3$ and $b_1 > 1$

(6) $b_2 = 1$ and $a_1 = 2$ and $a_2 \geq 3$ and $b_1 > 1$

(1) In this case we find from 3.7.99

3.7.102. $\{x_1,x_2\} = \{6, 2\cdot 3^{b_2}5^c\}$

which is impossible because of h) in lemma 3.2.7

(2) In this case we find from 3.7.99 and 3.7.100

3.7.103. $\{x_1,x_2\} = \{3\cdot 2^{a_1}, 4\cdot 3^{b_2}5^c\}$

3.7.104. $15(3\cdot 2^{a_1} - 4\cdot 3^{b_2}5^c)^2 - (3\cdot 2^{a_1} + 4\cdot 3^{b_2}5^c) = 12$

Now if $b_2 \geq 3$ we have

3.7.105. $3\cdot 2^{a_1} \equiv 15 \pmod{27}$

3.7.106. $2^{a_1} \equiv 5 \pmod{9}$

3.7.107. $a_1 = 5 + 6t$

Furthermore, in any case we have

3.7.108. $3\cdot 2^{a_1} \equiv 3 \pmod{5}$

3.7.109. $a_1 = 4s$

Hence 3.7.107 contradicts 3.7.109. So $b_2 \leq 2$

Now since from 3.7.109 $a_1 \geq 4$ we see from 3.7.104

3.7.110. $4\cdot 3^{b_2}5^{c} \equiv 4 \pmod{16}$

3.7.111. $3^{b_2}5^{c} \equiv 1 \pmod{4}$

3.7.112. $b_2 = 2u$

So since $b_2 \leq 2$ we find

3.7.113. $b_2 = 2$

Hence we find from 3.7.104

3.7.114. $3\cdot 2^{a_1} + 36\cdot 5^{c} \equiv 15 \pmod{27}$

3.7.115. $2^{a_1} + 3\cdot 5^{c} \equiv 5 \pmod{9}$

But since from 3.7.109 a_1 is even, so

3.7.116. $2^{a_1} \equiv 4,\ 7 \text{ or } 1 \pmod{9}$

we find a contradiction to 3.7.115. So (2) is impossible.

(3) In this case we find from 3.7.99

3.7.117. $\{x_1,x_2\} = \{12, 2^{a_2}3^{b_2}5^c\}$

where $a_2 \geq 3$ and $b_2 \geq 1$ and $c \geq 1$. This contradicts h)

(4) In this case we find from 3.7.99 and 3.7.100

3.7.118. $\{x_1,x_2\} = \{2\cdot 3^{b_1}, 6\cdot 5^c\}$

3.7.119. $15(2\cdot 3^{b_1} - 6\cdot 5^c)^2 - (2\cdot 3^{b_1} + 6\cdot 5^c) = 12$

From 3.7.119 it follows that

3.7.120. $2\cdot 3^{b_1} \equiv 3 \pmod{5}$

3.7.121. $b_1 = 2 + 4t$

Now from d) it follows that

3.7.122. Either $2\cdot 3^{b_1} \equiv 1 \pmod{29}$ or $2\cdot 3^{b_1} \equiv 2 \pmod{29}$

so

3.7.123. Either $b_1 = 11 + 28v$ or $b_1 = 28w$

and we see that 3.7.123 contradicts 3.7.121. Hence (4) is impossible.

(5) In this case we find from 3.7.99 and 3.7.100

3.7.124. $\{x_1,x_2\} = \{2^{a_1}3^{b_1}, 12\cdot 5^c\}$

3.7.125. $15(2^{a_1}3^{b_1} - 12\cdot 5^c)^2 - (2^{a_1}3^{b_1} + 12\cdot 5^c) = 12$

Now if $a_1 \geq 4$ then we see from 3.7.125

3.7.126. $12\cdot 5^c \equiv 4 \pmod{16}$

3.7.127. $3\cdot 5^c \equiv 1 \pmod{4}$

which is a contradiction. So $a_1 \le 3$. Then since in (5) we have $a_1 \ge 3$ we find

3.7.128. $a_1 = 3$

Hence we find from 3.7.125

3.7.129. $8\cdot 3^{b_1} \equiv 3 \pmod{5}$

3.7.130. $b_1 = 4s$

Now following d) we must have

3.7.131. Either $8\cdot 3^{b_1} \equiv 1 \pmod{29}$ or $8\cdot 3^{b_1} \equiv 2 \pmod{29}$

but it is straightforward to show that this is impossible if 3.7.130 holds. So the case (5) is impossible.

(6) In this case we find from 3.7.99 and 3.7.100

3.7.132. $\{x_1, x_2\} = \{4\cdot 3^{b_1}, 3\cdot 2^{a_2}5^c\}$

3.7.133. $15(4\cdot 3^{b_1} - 3\cdot 2^{a_2}5^c)^2 - (4\cdot 3^{b_1} + 3\cdot 2^{a_2}5^c) = 12$

Hence we find

3.7.134. $4\cdot 3^{b_1} \equiv 3 \pmod{5}$

3.7.135. $b_1 = 3 + 4s$

Now if $a_2 \ge 4$ then it follows from 3.7.133 that

3.7.136. $4\cdot 3^{b_1} \equiv 4 \pmod{16}$

3.7.137. $3^{b_1} \equiv 1 \pmod{4}$

3.7.138. $b_1 = 2t$

contradicting 3.7.135. So $a_2 \le 3$. Since in the case (6) we have $a_2 \ge 3$ we find

3.7.139. $a_2 = 3$

Hence we find from 3.7.132 and 3.7.133

3.7.140. $\{x_1,x_2\} = \{4 \cdot 3^{b_1}, 24 \cdot 5^c\}$

3.7.141. $15(4 \cdot 3^{b_1} - 24 \cdot 5^c)^2 - (4 \cdot 3^{b_1} + 24 \cdot 5^c) = 12$

Now since, from 3.7.135, $b_1 \ge 3$ we find

3.7.142. $24 \cdot 5^c \equiv 15 \pmod{27}$

3.7.143. $8 \cdot 5^c \equiv 5 \pmod{9}$

3.7.144. $c = 4 + 6t$

So c is even. Hence

3.7.145. $5^c \equiv 1 \pmod{8}$

3.7.146. $24 \cdot 5^c \equiv 24 \pmod{64}$

Furthermore, from 3.7.135 we find

3.7.147. $3^{b_1} \equiv 11 \pmod{16}$

3.7.148. $4 \cdot 3^{b_1} \equiv 44 \pmod{64}$

and

3.7.149. $3^{2b_1} \equiv 1 \pmod{4}$

3.7.150. $16 \cdot 3^{2b_1} \equiv 16 \pmod{64}$

Hence from 3.7.141, 3.7.146. 3.7.148 and 3.7.150 we have

3.7.151. $15\cdot 16 - 44 - 24 \equiv 12 \pmod{64}$

which is a contradiction. So (6) is also impossible. Hence we have proved the theorem. □

CHAPTER 4 :SOME GENERAL RESULTS CONCERNING n

4.1. A first remark about n

4.1.1. LEMMA. Let n, $q = p_1^{a_1} \dots p_\ell^{a_\ell}$, e be the traditional parameters of a perfect code C.
Let $1 + n(q-1) + \dots + \binom{n}{e}(q-1)^e = p_1^{k_1} \dots p_\ell^{k_\ell}$ (cfr. 1.2.1). Then for all $i \in \{1,2,\dots,\ell\}$ such that $k_i - e\,a_i > 0$ and $p_i > e$, $n - e$ must have exactly ea_i factors p_i.

PROOF. Let $p_i > e$ and let $n - e$ have exactly b_i factors p_i. Then, modulo $p_i^{b_i}$, we have:

4.1.2. $$p_1^{k_1} \dots p_\ell^{k_\ell} = 1 + n(q-1) + \dots + \binom{n}{e}(q-1)^e \equiv \sum_{i=0}^{e} \binom{e}{i}(q-1)^i = q^e$$

so we have

4.1.3. $$p_i^{b_i} \mid (q^e - p_1^{k_1} \dots p_\ell^{k_\ell})$$

Now from 1.6.8 we find

4.1.4. $$\prod_{i=1}^{e} x_i = \frac{e!}{q^e} p_1^{k_1} \dots p_\ell^{k_\ell} \in \mathbb{Z}$$

Hence we find $k_i \geq ea_i$, and we see from 4.1.3 that $b_i \leq ea_i$ if $k_i > ea_i$, that means: if

4.1.5. $$p_i \nmid \prod_{j=1}^{e} x_j \ .$$

Furthermore, from 1.6.6 and 1.6.9 we see, since $p_i > e$, that $b_i \geq ea_i$.
Thus $b_i = ea_i$. □

4.2. *A second remark about* n

4.2.1. LEMMA. Assume that there exists a perfect e-code with $e \geq 2$ and $q \geq 2$ and $n \leq 1000$.
Then this code is one of the two Golay codes.

PROOF. From 1.6.9 we see that if p is prime and $p \mid q$, then

4.2.2. $$p^e \mid (n-1)(n-2)\ \dots\ (n-e)$$

Hence there exists an $i \in \{1,2,\dots,e\}$ such that

4.2.3. $$p^s \mid n - i$$

where s is defined by

4.2.4. $$s := e - [\frac{e}{p}] - [\frac{e}{p^2}] - \dots$$

Then since

4.2.5. $$s > e(\frac{p-2}{p-1})$$

we find from 4.2.3

4.2.6. $$n > p^{e(\frac{p-2}{p-1})}$$

Now first assume $e \geq 3$. Then since q must be divisible by at least three distinct primes (if q does not belong to a triple of Golay parameters), cfr. 2.2.1, it must be divisible by a prime p which is at least 5, so we find from 4.2.6

4.2.7. $$n > 5^{3/4e}$$

Then if $n \leq 1000$ we find $e \leq 5$.
The cases $e = 3$ and $e = 4$ are treated, independent of this section, in 5.1 and 5.2. We only have the binary Golay code.

If $e = 5$ then, for the same reason as above, q must be divisible by a prime p which is at least 5, and we find from 1.6.9 that for a certain $i \in \{1,2,3,4,5\}$

4.2.8. $\quad p^5 \mid (n - i)$

so we have

4.2.9. $\quad n > 5^5 > 1000$

contradicting our assumptions.

So e must be 2. In this case we see from 1.6.6 that

4.2.10. $\quad q \mid 2(n - 2)$

Now first assume that q is odd. Then from 4.2.10 and 1.6.9 we find

4.2.11. $\quad q^2 \mid (n - 2)$

so if $n \le 1000$ then $q \le 31$. But the odd q with $q \le 31$ were treated in chapter 3 and we only found the ternary Golay code.

Now assume

4.2.12. $\quad q = 2^k q'$ where q' is odd.

Then from 4.2.10 we find

4.2.13. $\quad 2^{k-1} q' \mid (n - 2)$

Then if $k \ge 2$ we find from 4.2.13 and 1.6.9 that 4.2.11 holds, so if $n \le 1000$ then $q \le 31$. But the q with $k \ge 2$ and $q \le 31$ were treated in chapter 3. No perfect code was found.

If $k = 1$ we find from 4.2.13 amd 1.6.9

4.2.14. $\quad q'^2 \mid (n - 2),$

so

4.2.15. $\quad q^2 \mid 4(n - 2)$

So if $n \le 1000$ then $q \le 63$. Furthermore, since from 2.1.15 q is not a prime power, and since q has exactly one factor 2, and since the cases $q \le 30$ were already treated in chapter 3, we have

4.2.16. $q = 34, 38, 42, 46, 50, 54, 58, 62$

In the appendix (see A.4) we shall explain how these last cases are treated.

4.3. The existence of an upper bound N(e,q) *for* n

The following lemma follows from a well-known result of C.L. Siegel from number theory (cfr. [33], [37]).

4.3.1. LEMMA. Let $p(X)$ be a polynomial such that if $a \in \mathbb{Z}$, then $p(a) \in \mathbb{Z}$. Assume that $p(X)$ is not of the form $s(uX + t)^k$, where s, u, and t are real constants and $k \in \mathbb{N}$. For $n \in \mathbb{N}$, let q_n be the largest prime factor of $p(n)$. Then $\forall_{N \in \mathbb{N}} \exists_{M \in \mathbb{N}} \forall_{n \in \mathbb{N}} [n > M \to q_n > N]$.

With the help of lemma 4.3.1 we can prove the following theorem.

4.3.2. THEOREM. Assume that there exists a perfect code with parameters n, $e \geq 2$ and q. Then n is bounded by a number $N(e,q)$ depending only on e and q.

PROOF. Let the polynomial $p(X)$ be defined by:

4.3.4. $$p(X) := \sum_{i=0}^{e} \binom{X}{i} (q-1)^i$$

Then if $a \in \mathbb{Z}$ we have $p(a) \in \mathbb{Z}$. Moreover, assume that for some constants s and t and $k \in \mathbb{N}$ we have

4.3.5. $$p(X) = s(uX + t)^k$$

Then $k = e$, and since from 4.3.4 and 4.3.5

4.3.6. $$p(0) = 1 = st^k = st^e$$

we find

4.3.7. $p(X) = (rX + 1)^e, \quad \text{where } r := \frac{u}{t}$

From 4.3.4 and 4.3.7 we have:

4.3.8. $p(1) = q = (1 + r)^e$

4.3.9. $p(2) = q^2 = (1 + 2r)^e$

Then, comparing 4.3.8 and 4.3.9, we find

4.3.10. $(1 + 2r + r^2)^e = (1 + 2r)^e$

so $r = 0$, whence from 4.3.8 we have $q = 1$, which is not possible. So, since $p(X)$ is not of the form 4.3.5, we can apply lemma 4.3.1. Now take $Q > q$. Then there is a number $M = N(e,q)$ such that for $n > M$ we have for the largest prime factor q_n of $p(n)$

4.3.11. $q_n > Q > q$

But since from the polynomial condition 1.2.1 we find

4.3.12. $p(n) \mid q^n$

formula 4.3.11 is a contradiction. Hence we have $n < M$. □

Explicit lower bounds for q_n are known: there exist effectively computable constants c, depending only on the polynomial $p(X)$, such that for large n

4.3.13. $q_n > c \log \log n$

In particular, if $p(X)$ is of degree 2, we have for $\varepsilon > 0$ and large n the following inequality:

4.3.14. $q_n \geq (0.25 + \varepsilon)\log \log n$

This was found recently by Langevin (see [18]), using a result of Stark about the diophantine equation $X^3 - Y^2 = k$.

However, these bounds are not of practical value for our purpose. For instance, assume the existence of a perfect code with $e = 2$ and, say, $q = 3^s5^t$.

Now let us derive an upper bound for n, using 4.3.14.

For this purpose we define the polynomial $p(X)$ of degree 2 by

4.3.15. $$p(X) := 1 + X(q - 1) + \frac{X(X - 1)}{2}(q - 1)^2$$

where $q = 3^s5^t$.

Then it follows from the sphere packing condition that

4.3.16. $$p(n) = 3^u5^v, \quad \text{so} \quad q_n \le 5$$

But on the other hand we have for large n the inequality 4.3.14, from which it follows that

4.3.17. $$q_n > 5 \quad \text{if} \quad \log \log n > 20$$

We conclude that we find the following upper bound for n, which is very large indeed:

4.3.18. $$n \le \exp(\exp(20))$$

4.4. An upper bound N(e,q) *made explicit if* e *is odd*

For a better understanding of this section, the reader is invited to read again the second half of section 1.6, about the transformed Lloyd polynomial $F_e(\theta)$.

Let $e = 2m + 1$. Then by combination of 1.6.23 and 1.6.24 we may write:

4.4.1. $$F_e(\theta) = \sum_{k=0}^{m} a_k(\theta) n^k$$

Using only the terms with $j = m$, we find from 1.6.27:

4.4.2. $$a_m(\theta) = \frac{(-1)^{m-1}}{m!} \xi^{m-1} (m\eta + \xi(\theta - 1)) ,$$

where ξ and η are defined in 1.6.25.

So if we define

4.4.3. $$\theta_0 := e - \frac{(e-1)(q+1)}{3}$$

we see that $a_m(\theta)$ changes sign in θ_0, that means

4.4.4. $$a_m(\theta_0) = 0$$

4.4.5. $$|a_m(\theta_0 + 1/3)| = |a_m(\theta_0 - 1/3)| = \frac{(q-1)^m}{m!}\{\frac{(e-1)q-2e}{2^m}\}$$

Now let us define:

4.4.6. $$M(e,q) := \frac{1}{(m-1)!}\binom{e+1}{m} e^{m+2} 2^e q$$

Then we have the following lemma:

4.4.7. **LEMMA.** For $n > M(e,q)$ as defined in 4.4.6, and $q \geq 30$, the signs of $F_e(\theta_0 + 1/3)$ and $F_e(\theta_0 - 1/3)$ are different.

PROOF. Using 1.6.21 and 1.6.22 we see that

4.4.8. $$\begin{aligned} e!F_e(\theta) = {} & (n-1)(n-2)\ \dots\ (n-e) - e(n-2)\ \dots\ (n-e)(n-\theta) + \\ & + \binom{e}{2}(n-3)\ \dots\ (n-e)(n-\theta)(n-\theta-q) - \dots \\ & + (-1)^{e-1}e(n-e)(n-\theta)\ \dots\ (n-\theta-(e-2)q) + \\ & + (-1)^e(n-\theta)(n-\theta-q)\ \dots\ (n-\theta-(e-1)q) \end{aligned}$$

Hence for the coefficients $a_k(\theta)$ of n^k in $F_e(\theta)$ we have if $|\theta| < \frac{eq}{3}$:

4.4.9. $$e!\,|a_k(\theta)| < (e+1)\binom{e}{m}\binom{e}{k}\left(\frac{4}{3}eq\right)^{e-k}$$

Now define b_k to be the right hand side of 4.4.9. Then since

4.4.10. $$\frac{b_k}{b_{k+1}} = \frac{(k+1)(\frac{4}{3}\,eq)}{e-k}$$

we find that if

4.4.11. $$n > \frac{b_{m-2}}{b_{m-1}} = \frac{(m-1)(\frac{4}{3}\,eq)}{m+3}$$

then we have for $k = 0,1,\dots,m-2$

4.4.12. $$b_{m-1}n^{m-1} > b_k n^k$$

So from 4.4.9 we have, if $|\theta| < \frac{eq}{3}$ and 4.4.11 holds,

4.4.13. $$\sum_{k=0}^{m-1} |a_k(\theta)|\; n^k < mb_{m-1}n^{m-1},$$

i.e.

4.4.14. $$\sum_{k=0}^{m-1} |a_k(\theta)|\; n^k < m\,\frac{(e+1)}{e!}\binom{e}{m}\binom{e}{m-1}(\tfrac{4}{3}\,eq)^{m+2}n^{m-1}$$

Now, since obviously $F_e(\theta_0 + 1/3)$ and $F_e(\theta_0 - 1/3)$ have different signs if for $|\theta| < \frac{eq}{3}$

4.4.15. $$\sum_{k=0}^{m-1} |a_k(\theta)|\, n^k < |a_m(\theta_0 + 1/3)|\, n^m$$

we see from 4.4.5 and 4.4.14 that this is true if 4.4.11 holds and

4.4.16. $$m(e+1)\binom{e}{m}\binom{e}{m-1}(\tfrac{4}{3}\,eq)^{m+2} < \frac{(q-1)^m}{m!}\left\{\frac{(e-1)q-2e}{2^m}\right\} n$$

Now we can check that this inequality reduces to the bound $M(e,q)$ for n, mentioned in 4.4.6, if we keep in mind the following inequalities:

4.4.17. $\frac{q}{q-1} \le \frac{30}{29}$ and $29 > 4 \cdot 5$

$(e - 1)q - 2e > q$ if $q \ge 6$

$m^2 < m(m + 1)$

Here the first inequality is equivalent with $q \ge 30$, which is necessary if we want an unknown perfect code (cfr. 2.2). □

Now assume that there exists a perfect code with parameters n, q, e, and $e = 2m + 1$. Let s and p be defined by

4.4.18. $s := \gcd(q,e)$

4.4.19. $p := \frac{q}{s}$

Then from 1.6.6 we have

4.4.20. $p \mid (n - e)$

Therefore if θ is a zero of the transformed Lloyd polynomial $F_e(\theta)$, we see from 1.6.15 and the polynomial condition 1.6.5 that for some integer w we have

4.4.21. $\theta = e + pw$

Now we are able to prove:

4.4.22. LEMMA. Assume that there exists a perfect code with parameters $n,q,e = 2m + 1$, where $n > M(e,q)$. Then θ_0, as defined in 4.4.3, is a zero of $F_e(\theta)$.
Furthermore we have:

4.4.23. $3p \mid (1 - e)(q + 1)$

4.4.24. $m \ge 9$

PROOF. From lemma 4.4.7 we see that there must be a zero θ of $F_e(\theta)$ between $\theta_0 - 1/3$ and $\theta_0 + 1/3$, which from the polynomial condition must be of the form 4.4.21.
Therefore we have

4.4.25. $\theta_0 - 1/3 < e + pw < \theta_0 + 1/3$

From 4.4.3 we see that 4.4.25 is equivalent to

4.4.26. $(1 - e)(q + 1) - 1 < 3pw < (1 - e)(q + 1) + 1$

4.4.27. $3pw = (1 - e)(q + 1)$

Thus we have 4.4.23 and, comparing 4.4.27 with 4.4.3

4.4.28. $\theta = e + pw = \theta_0$

Finally 4.4.24 follows from 4.4.23, as will be explained in the appendix (see A.5).

Like the coefficient $a_m(\theta)$ we can calculate the coefficient $a_{m-1}(\theta)$. This will be done in the appendix (see A.6).
We find the following inequality:

4.4.29. $$|a_{m-1}(\theta_0)| > \frac{(q-1)^{m-3} q^5 m^3}{2^{m-1} 5 \cdot 9 \cdot (m-1)!} \qquad (\text{for } q \geq 30,\ m \geq 9)$$

Now, finally, we are ready to prove what was the purpose of this section, with the help of lemma 4.4.22.

4.4.30. THEOREM. For $n > M(e,q)$ as defined in 4.4.6, there does not exist a perfect e-code if $e = 2m + 1$ $(m \in \mathbb{N})$.

PROOF. Assume the existence of such a code with $n > M(e,q)$. Then from 4.4.1
4.4.4 and lemma 4.4.22 we find

4.4.31. $$F_e(\theta_0) = \sum_{k=0}^{m-1} a_k(\theta_0) n^k = 0$$

Like in the proof of lemma 4.4.7 we have for $|\theta| < \frac{eq}{3}$

4.4.32. $$\sum_{k=0}^{m-2} |a_k(\theta)| n^k < (m-1)\frac{(e+1)}{e!} \binom{e}{m}\binom{e}{m-2}\left(\frac{4}{3}eq\right)^{m+3} n^{m-2}$$

Since obviously we have a contradiction with 4.4.31 if for $|\theta| < \frac{eq}{3}$

4.4.33. $$\sum_{k=0}^{m-2} |a_k(\theta)| n^k < |a_{m-1}(\theta_0)|$$

we see from 4.4.29 and 4.4.32 that we have a contradiction if

4.4.34. $$(m-1)(e+1)\binom{e}{m}\binom{e}{m-2}(\frac{4}{3}\, eq)^{m+3} < \frac{e!(q-1)^{m-3} q^5 m^3 n}{2^{m-1} 5 \cdot 9\ (m-1)!}$$

so, as is not difficult to see, if $n > M(e,q)$. □

4.5. *Application*

As an application of theorem 4.4.30 we mention:

4.5.1. THEOREM. Assume that there exists a perfect e-code with q symbols and that all prime divisors of q are greater than e.
Then e cannot be odd if $e > 1$.

PROOF. If all prime divisors of q are greater than e then it follows from 1.6.6 amd 1.6.9 that

4.5.2. $$q^e \mid (n - e)$$

Furthermore, if we have an unknown perfect code with $e > 2$ then from the sections 2.1 and 2.2 we see that the number of these prime divisors is at least 3, so

4.5.3. $$q > e^3$$

Hence from 4.5.2 and 4.5.3 we have

4.5.4. $$n > qe^{6m}$$

Now it is straightforward to show that 4.5.4 contradicts the upper bound $M(e,q)$ for n, mentioned in 4.4.6, which is valid if e is odd and at least 3.

CHAPTER 5 : SOME RESULTS FOR SMALL VALUES OF e

5.1. The case $e = 3$

5.1.1. **THEOREM.** The only non-trivial perfect 3-code is the binary Golay code of length 23.

PROOF. From the polynomial condition 1.6.5 we find that, assuming the existence of a perfect code with parameters $n, e = 3$, $q > 2$ the Lloyd polynomial $P_3(X)$ must have three distinct integral zeros.
Therefore application of the transformation θ (1.6.15) learns that the transformed polynomial $F_3(\theta)$, as given in 1.6.19, must have three integral zeros of the form

5.1.2. $\theta_i = qx_i - n(q - 1)$, where $x_i \in \mathbb{Z}$ $(i = 1,2,3)$

However, as is easily verified, we have

5.1.3. $3!F_3(1) = 2(q - 1)(q - 2)(1 - n) < 0$

5.1.4. $3!F_3(3 - q) = (q - 1)(q - 2)(n - 3) > 0$

Hence for one of the zeros θ_i we must have

5.1.5. $3 - q < \theta_i < 1$

So for the integer x_i associated with θ_i we have

5.1.6. $3 - q < qx_i - n(q - 1) < 1$

However, we see from 1.6.6 that

5.1.7. $q \mid 3(n - 3)$

So for some integers v, w, respectively, we find

5.1.8. if $3 \nmid q$ then $n = 3 + qv$

5.1.9. If for some $p \in \mathbb{N}$ $q = 3p$, then $n = 3 + pw$

So from 5.1.5, 5.1.6 and 5.1.8, 5.1.9 respectively we see that for some integers v', w', respectively, we must have:

5.1.10. If $3 \nmid q$ then $\theta_i = 3 + qv'$ and $3 - q < 3 + qv' < 1$

5.1.11. If $q = 3p$ then $\theta_i = 3 + pw'$ and $3 - q < 3 + pw' < 1$

Hence, since 5.1.10 is impossible we see that $q = 3p$ and, since $F_3(\theta_i) = 0$,

5.1.12. $F_3(3 - p) \cdot F_3(3 - 2p) = 0$

However, we see after simple calculation, since for nontrivial perfect codes we have $n > 7$, that

5.1.13. $F_3(3 - p) = - 10p^3 + p^2(27 - 9n) + p(9 - 3n) + 48 + 2n < 0$

5.1.14. $F_3(3 - 2p) = - 8p^3 + p(18 - 6n) + 48 + 2n < 0$

Now we find that 5.1.13 and 5.1.14 contradict 5.1.12.
So if a perfect code with parameters $n, e = 3$ and q does exist, then $q = 2$.
Furthermore, if $q = 2$, or more generally a prime power, it is known that the only perfect 3-code is the binary Golay code with $n = 23$, (cfr. [23]). □

5.2. *The case* $e = 4$

In the following we shall prove that there does not exist a perfect nontrivial four-error-correcting code.
In lemma 1 we make use of the well-known *cubic resolvent* of a polynomial of the fourth degree, which was first introduced by Lagrange.

5.2.1. LEMMA. Let $P(Z) := Z^4 + pZ^2 + rZ + s$ be a polynomial with integral zeros. Then the polynomial $Q(Z)$, defined by $Q(Z) := Z^3 - pZ^2 - 4sZ + 4ps - r^2$ has three integral zeros.

PROOF. Let $P(Z)$ have integral zeros z_1, z_2, z_3, z_4. Then we can write p, r, s as the symmetric expressions:

5.2.2. $$p = z_1z_2 + z_1z_3 + z_1z_4 + z_2z_3 + z_2z_4 + z_3z_4$$
$$-r = z_1z_2z_3 + z_1z_2z_4 + z_1z_3z_4 + z_2z_3z_4$$
$$s = z_1z_2z_3z_4$$

Now define $Q(Z) := (Z - y_1)(Z - y_2)(Z - y_3)$, where

5.2.3. $$y_1 := z_1z_2 + z_3z_4$$
$$y_2 := z_1z_3 + z_2z_4$$
$$y_3 := z_1z_4 + z_2z_3$$

Then, from 5.2.2 and 5.2.3, it is straightforward to show that

5.2.4. $$y_1 + y_2 + y_3 = p$$
$$y_1y_2 + y_1y_3 + y_2y_3 = -4s$$
$$y_1y_2y_3 = r^2 - 4ps$$

Then $Q(z)$ has the form as in the theorem, and its zeros y_1, y_2 and y_3 are integers. □

REMARK. cfr. the theorem in Van Der Waerden [42], where $Q(z)$ has zeros $y_1 + y_2$, $y_1 + y_3$ and $y_2 + y_3$.

By now we are ready to prove:

5.2.5. THEOREM. A non-trivial perfect four-error-correcting code does not exist.

PROOF. Assume there exists such a code with parameters $n, e = 4$, and q. Then by the transformation θ (1.6.15) and by

5.2.6. $$Z := 2\theta + 3q - 8$$

the Lloyd polynomial $P_4(X)$ is transformed into $P(Z)$ like in lemma 5.2.1, where p,r and s will not be mentioned.
Following the polynomial condition and the lemma 5.2.1 we find a polynomial $Q(Z)$ like in lemma 5.2.1, with three integral zeros. Since the coefficient of $(n-4)^3$ in $Q(Z)$ is independent of Z we substitute

5.2.7. $2Y := Z + 24(q-1)(n-4)$

and find that $F(Y)$ must have three integral zeros, where

5.2.8. $F(Y) := a_2(Y)(n-4)^2 + a_1(Y)(n-4) + a_0(Y)$,

and

5.2.9.
$$a_2(Y) = 3Y + 11q^2 + 16q - 16$$
$$a_1(Y) = -24(q-1)(Y+5q^2)(Y+q^2+4q-4)$$
$$a_0(Y) = (Y-3q^2)(Y+3q^2)(Y+5q^2)$$

Hence if we define y_0 by

5.2.10. $y_0 := -\frac{1}{3}(11q^2 + 16q - 16)$

then we find

5.2.11.
$$a_2(y_0) = 0$$
$$a_2(y_0 - \tfrac{1}{3}) = -32(q-1)^2$$

and for $y = y_0$ and $y = y_0 - \frac{1}{3}$ we find

5.2.12.
$$72q^4(q-1) < a_1(y) < 88q^4(q-1)$$
$$0 < a_0(y) < 8q^6$$

and hence:

5.2.13. $F(y_0) > 72q^4(q - 1)(n - 4) > 0$

5.2.14. $F(y_0 - \frac{1}{3}) < - 32(q - 1)^2(n-4)^2 + 88(q - 1)q^4(n-4) + 8q^6$

so, as is easily established:

5.2.15. $F(y_0 - \frac{1}{3}) < 0$ if $n - 4 \geq \frac{14}{5}\frac{q^4}{q-1}$

So we see from 5.2.13 and 5.2.15 that, if $n - 4 \geq \frac{14}{5}\frac{q^4}{q-1}$, there must be an integral zero of $F(Y)$ in the open interval $(y_0 - 1/3, y_0)$. Hence, since from 5.2.10 it is clear that this interval does not contain an integer, we find

5.2.16. $n - 4 < \frac{14}{5}\frac{q^4}{q-1}$

Now we shall see in the following two lemmas that this is also impossible Hence we have proved the theorem.

5.2.17. LEMMA. Suppose that there exists a perfect four-error-correcting code with word length n such that

$$n - 4 < \frac{14}{5}\frac{q^4}{q-1},$$

and let $q = 2^k 3^\ell q'$ and $\gcd(6,q') = 1$.
Then we have the following diagram of possibilities:

$\ell \backslash k$	$k = 0$	$k = 1$	$k = 2$	$k \geq 3$
$\ell=0$	$q < 4$	$q < 46$	$q < 718$	$q < 7$
$\ell\geq1$	$q < 10$	$q < 136$	$q < 2152$	$q < 18$

PROOF. Like in section 2.3 we find that the following expressions in the zeros x_1, x_2, x_3 and x_4 of $P_4(x)$ must be integers:

5.2.18. $$x_1 + x_2 + x_3 + x_4 = \frac{4(n-4)(q-1)}{q} + 10$$

5.2.19. $$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4(n-4)^2 + 20(n-4) + 30 - \frac{4(n-4)}{q^2}\{(2q-1)(n-3)+4\}$$

5.2.20. $$x_1^3 + x_2^3 + x_3^3 + x_4^3 = 4(n-4)^3 + 30(n-4)^2 + 90(n-4) + 100 -$$

$$\frac{n-4}{q^3}\{(n-4)^2(12q^2-12q+4) + (n-4)(24q^2+42q-36) + (12q^2+54q+24)\}$$

5.2.21. $$(x_1 - 1)(x_2 - 1)(x_3 - 1)(x_4 - 1) = \frac{(n-1)(n-2)(n-3)(n-4)}{q^4}(q-1)^4$$

Then if $3 \mid q$ we see from 5.2.18 that $3 \mid (n-4)$.
So $\{(n-4)^2(12q^2 - 12q + 4) + (n-4)(24q^2+42q-36) + (12q^2 + 54q + 24)\}$
has exactly one factor 3.
Then since $27 \mid q^3$, we see from 5.2.20 that $9 \mid n - 4$.

Furthermore, if $8 \mid q$ we see from 5.2.18 that $2 \mid (n-4)$.
So $\{(2q-1)(n-3) + 4\}$ is odd.
Then, since $64 \mid q^2$, we see from 5.2.19 that $4 \mid (n-4)$.

Hence, since from 5.2.18 and 5.2.21

5.2.22. $$q \mid 4(n-4) \quad \text{and} \quad q^4 \mid (n-1)(n-2)(n-3)(n-4)$$

We can make the following diagram of possibilities, with A chosen in such a way that $q^4 \mid A(n-4)$

5.2.23.

$\ell \backslash^{k}$	$k = 0$	$k = 1$	$k = 2$	$k \geq 3$
$\ell = 0$	$A = 1$	$A = 16$	$A = 256$	$A = 2$
$\ell \geq 1$	$A = 3$	$A = 48$	$A = 768$	$A = 6$

Now in each of the cases listed in the diagram we have the condition

5.2.24. $$\frac{q^4}{A} \leq n - 4 < \frac{14}{5}\,\frac{q^4}{q-1}$$

Which yields

5.2.25. $\quad q < \frac{14}{5} A + 1$

So by combination of 5.2.23 and 5.2.25 we have the diagram of possibilities listed in 5.2.17. □

5.2.26. LEMMA. The values of q listed in 5.2.17 are also impossible.

PROOF. This will be proved in the appendix (see A.2). □

5.3. *The case* e = 5

5.3.1. THEOREM. There does not exist a non-trivial perfect 5-code.

PROOF. Assuming the existence of a perfect code with parameters n, e = 5, and q, we find from section 2.2 that q must have at least three distinct prime divisors, so

5.3.2. $\quad q \geq 30$

Now define $\lambda \in \mathbb{Q}$ such that

5.3.3. $\quad \lambda := \frac{q}{5}$

so by 5.3.2

5.3.4. $\quad \lambda \geq 6$

In the appendix (see A.7) we shall show that we may assume

5.3.5. $\quad n \geq 80\lambda$

Now from the polynomial condition 1.6.5 we find that the Lloyd polynomial $P_5(X)$ must have five distinct integral zeros.
Therefore, application of the transformation θ (1.6.15) learns that the transformed polynomial $F_5(\theta)$, which was made explicit in 1.6.20, must have five integral zeros of the form

5.3.6. $\quad \theta_i = qx_i - n(q-1), \quad$ where $x_i \in \mathbb{Z} \quad (i = 1,2,3,4,5)$

Now we calculate $F_5(-6\lambda)$ and $F_5(-7\lambda)$ and find:

5.3.7. $$5!F_5(-6\lambda) = n^2(250\lambda^3 - 1475\lambda^2 + 560\lambda - 55) +$$
$$+ n(3300\lambda^4 - 6510\lambda^3 + 7220\lambda^2 - 90\lambda + 224)$$
$$+ (3024\lambda^5 - 5400\lambda^4 + 4800\lambda^3 - 3600\lambda^2 - 3600\lambda - 120)$$

5.3.8. $$5!F_5(-7\lambda) = n^2(-125\lambda^3 - 1325\lambda^2 + 545\lambda - 55) +$$
$$+ n(2150\lambda^4 - 5330\lambda^3 + 9180\lambda^2 - 520\lambda + 224) +$$
$$+ (4368\lambda^5 - 8400\lambda^4 + 8400\lambda^3 - 8400\lambda^2 - 4200\lambda - 120)$$

Now it can be seen immediately that the following inequalities follow from, respectively, 5.3.4, and 5.3.4 and 5.3.5:

5.3.9. $$F_5(-6\lambda) > 0$$
$$F_5(-7\lambda) < 0$$

Hence we have for one of the zeros θ_i (cfr. 5.3.6), say θ'

5.3.10. $-7\lambda < \theta' < -6\lambda$

Now we see from 1.6.6 that

5.3.11. $q \mid 5(n - 5)$

So for some integers v, w, respectively we find:

5.3.12. If $5 \nmid q$ then $n = 5 + qv$

5.3.13. If $\lambda \in \mathbb{N}$ then $n = 5 + \lambda w$

Hence from 5.3.6, 5.3.10 and 5.3.12, 5.3.13 respectively, we find for some integers v', w' respectively:

5.3.14. If $5 \nmid q$ then $\theta' = 5 + qv'$ and $-7\lambda < 5 + qv' < -6\lambda$

5.3.15. If $\lambda \in \mathbb{N}$ then $\theta' = 5 + \lambda w'$ and $-7\lambda < 5 + \lambda w' < -6\lambda$

Now, since from 5.3.2 we have $q \geq 30$, there is no $v' \in \mathbb{Z}$ such that

5.3.16 $\quad -7q < 25 + 5qv' < -6q$

so 5.3.14 is impossible. Therefore 5.3.15 must hold and we see that

5.3.17. $\quad \lambda \in \mathbb{N}$

and

5.3.18. $\quad \theta' = 5 - 7\lambda$

On the other hand, we calculate $F_5(5 - 7\lambda)$ and find

5.3.19. $$5!F_5(5 - 7\lambda) = n^2(-125\lambda^3 + 550\lambda^2 - 205\lambda + 20) + n(2150\lambda^4 + 1670\lambda^3 - 4720\lambda^2 + 1740\lambda - 176) + (4368\lambda^5 - 10.750\lambda^4 - 5225\lambda^3 + 12.350\lambda^2 - 4075\lambda + 380)$$

Now it is straightforward to show from 5.3.4 and 5.3.5

5.3.20. $\quad F_5(5 - 7\lambda) < 0$

but we shall omit the calculations.

Now 5.3.20 and 5.3.18 contradict each other since θ' was defined to be a zero of $F_5(\theta)$.

Therefore we have proved that a perfect 5-code does not exist.

CHAPTER 6 :SOME RESULTS CONCERNING PERFECT MIXED CODES

6.1. *Preliminaries*

For $i = 1,2,\ldots n$, let S_i be a set of q_i symbols, say

6.1.1. $\quad S_i := \{0,1,2,\ldots,q_i-1\}$

where q_i is an integer at least equal to 2.
Then a *mixed code* C is a subset of the cartesian product $V:=S_1 \times S_2 \times \ldots \times S_n$.
The Hamming metric in V is defined as in section 1.1.
C is called a *mixed perfect e-code* if the spheres $S_e(\underline{c})$, with $\underline{c}$ running through C, form a partition of V.
Several mixed perfect 1-codes are known with $q_i = p^{a_i}$ $(i = 1,2,\ldots n)$.
We refer to [15], [21].

In this chapter, our purpose is to prove some non-existence theorems concerning mixed perfect 2- and 3-codes with the help of four necessary conditions.
First, the *sphere packing condition* becomes for mixed perfect 2-codes:

6.1.2. $$1 + \sum_{i=1}^{n} (q_i - 1) + \sum_{i<j}^{n} (q_i - 1)(q_j - 1) \mid q_1 q_2 \ldots q_n \ .$$

Furthermore, the following two conditions were derived by O. Heden (see [14]) in a paper which generalizes the polynomial condition to the case of mixed perfect codes:

6.1.3. LEMMA. If a mixed perfect e-code exists and for some i we have $p \nmid q_i$, then $p \mid |S_e(\underline{0})|$.

Here, obviously, $|S_e(\underline{0})|$ is the left hand side of 6.1.2. (It is also possible to prove that $p \mid |C|$, but we shall not do that here.)

6.1.4. LEMMA. If a mixed perfect e-code exists and for some i we have $p \mid q_i$, then p divides at least n - e + 1 of the number q_i.

We shall quote from [14] the *polynomial condition* for mixed perfect codes:

Suppose that there exists a mixed perfect e-code of length n. Without loss of generality we can assume that the cardinalities q_i of the alphabets increase (weakly) with i.
Let us define the numbers $n_1, n_2 \dots n_k$ by

6.1.5.
$$\begin{array}{lllll} q_1 & = q_2 & = \dots = q_{n_1} & & \\ q_{n_1+1} & = q_{n_1+2} & = \dots = q_{n_1+n_2} & & \\ \vdots & \vdots & & & \\ q_{n_{k-1}+1} & = q_{n_{k-1}+2} & = \dots = q_{n_{k-1}+n_k} & = q_n & . \end{array}$$

Furthermore, let us define the set S by

6.1.6.
$$S := \{(s_1, s_2 \dots, s_k) \mid s_i \in \mathbb{Z} \text{ and } 0 \le s_i \le n_i \text{ for } i = 1,2,\dots,k \text{ and } s_1 + s_2 + \dots + s_k \le e\},$$

and let us define the polynomials $a_{(s_1,\dots,s_k)}(X_1, X_2 \dots X_k)$ by

6.1.7.
$$\sum_{0 \le s_i \le n_i} a_{(s_1,\dots,s_k)}(X_1, X_2 \dots X_k) Z_1^{s_1} \dots Z_k^{s_k} =$$
$$= \prod_{i=1}^{k} (1 + (q_i - 1)Z_i)^{n_i - X_i} (1 - Z_i)^{X_i}$$

Finally, let us define the polynomial $p(X_1, X_2 \dots X_k)$ by

6.1.8.
$$p(X_1, X_2 \dots X_k) := \sum_{(s_1, s_2 \dots s_k) \in S} a_{(s_1,\dots,s_k)}(X_1, X_2 \dots X_k)$$

Then there exist at least $|S| - 1$ distinct k-tuples $(x_1,x_2,\dots x_k)$ such that for $i = 1,2,\dots,k$

6.1.9. $\quad x_i \in \mathbb{Z}$ and $0 \le x_i \le n_i$

and

6.1.10. $\quad p(x_1,x_2\dots x_k) = 0$.

6.2. A nonexistence theorem concerning mixed perfect 2-codes

We have the following result concerning mixed perfect double-error-correcting codes:

6.2.1. THEOREM. A mixed perfect 2-code does not exist if, for $i = 1,2,\dots,n$, $q_i \mid 6$, unless this code is a trivial one or the ternary Golay code.

PROOF. Assume the existence of such a code. Since we exclude trivial cases we may assume $n \ge 5$.
From theorem 2.1.15 we know that it is not possible that for all i $q_i = 2$, or that all q_i are equal to 3 (unless we have the ternary Golay code)
Therefore, there exists an i such that $2 \mid q_i$ and there exists an i such that $3 \mid q_i$.
So from lemma 6.1.4 at least $n - 1$ of the numbers q_i are divisible by 2, and at least $n - 1$ of them are divisible by 3.
Furthermore, we know from theorem 3.6.3 that it is not possible that all q_i are equal to 6.
Therefore we can without loss of generality distinguish between 3 cases:

a) $q_1 = 2$ and for $i = 2,3,\dots n$ $q_i = 6$

b) $q_1 = 3$ and for $i = 2,3,\dots n$ $q_i = 6$

c) $q_1 = 2$, $q_2 = 3$ and for $i = 3,\dots n$ $q_i = 6$.

a) In this case the sphere packing condition 6.1.2 becomes:

6.2.2. $\quad 25n^2 - 55n + 34 = 2^{k+1}3^{\ell}$, where $|S_2(\underline{0})| = 2^k 3^{\ell}$

From 6.1.3 we find $k \geq 1$ and $\ell \geq 1$ so

6.2.3. $\quad n(n + 5) \equiv 2 \pmod{12}$

6.2.4. $\quad n \equiv 2 \pmod{12}$ or $n \equiv 5 \pmod{12}$

From the generalized polynomial condition of Heden (see [14]) the followin two quadratic equations must both have two integral solutions:

6.2.5. $$36Y^2 - (60n - 84)Y + 25(n - 1)(n - 2) = 0$$

6.2.6. $$36Y^2 - (60n - 60)Y + 25(n - 1)(n - 2) + 20(n - 1) + 4 = 0$$

Remark that if we substitute $y = 0$ in 6.2.6 then we find from 6.2.2, $2 \mid |S_2(\underline{0})|$.

But the case we treat is much easier: there must be two integral solutions y_1 and y_2 to equation 6.2.6, for which we have

6.2.7. $$y_1 + y_2 = \frac{60(n - 1)}{36} = \frac{5(n - 1)}{3} \in \mathbb{Z}$$

so we find

6.2.8. $\quad 3 \mid (n - 1)$

contradicting 6.2.4. So the case a) is impossible.

b) In this case the sphere packing condition 6.1.2 becomes:

6.2.9. $$25n^2 - 45n + 26 = 2^{k+1}3^{\ell}, \quad \text{where } |S_2(\underline{0})| = 2^k 3^{\ell}$$

From 6.1.3 we find $k \geq 1$, $\ell \geq 1$, so

6.2.10. $\quad n(n + 3) \equiv 10 \pmod{12}$

6.2.11. $\quad n \equiv a \pmod{12}$ where $a = 2$ or $a = 7$ or $a = 10$ or $a = 11$.

From the generalized polynomial condition of Heden the following two quadratic equations must both have two integral solutions:

6.2.12. $$36Y^2 - (60n - 84)Y + 25(n - 1)(n - 2) = 0$$

6.2.13. $$36Y^2 - (60n - 48)Y + 25(n - 1)(n - 2) + 30(n - 1) + 6 = 0$$

Remark that if we substitute $y = 0$ in 6.2.13, then we find from 6.2.9, $2|s_2(\underline{0})|$.

In the case b) we do not need this consideration.

Now let us denote the zeros of equation 6.2.12 by y_{01} and y_{02}, and those of equation 6.2.13 by y_{11} and y_{12}.

Then we find from 6.2.12 and 6.2.13 respectively:

6.2.14. $$y_{01} + y_{02} = \frac{60n - 84}{36} = \frac{5n - 7}{3} \in Z$$

6.2.15. $$y_{11} + y_{12} = \frac{60n - 48}{36} = \frac{5n - 4}{3} \in Z$$

so we find

6.2.16. $n \equiv 2 \pmod 3$

Therefore we find from 6.2.11

6.2.17. $n \equiv 2 \pmod{12}$ or $n \equiv 11 \pmod{12}$

Furthermore, we find from 6.2.12 and 6.2.13 respectively

6.2.18. $$y_{01} \cdot y_{02} = \frac{25(n-1)(n-2)}{36} \in Z$$

6.2.19. $$y_{11} \cdot y_{12} = \frac{25(n-1)(n-2) + 30n - 24}{36} \in Z$$

From 6.2.18 and 6.2.19 we derive

6.2.20. $36 \mid (30n - 24)$

6.2.21. $6 \mid (5n - 4)$

So n must be even. Therefore it follows from 6.2.17 that

6.2.22. $n \equiv 2 \pmod{12}$

Using 6.2.22 we find from 6.2.15

6.2.23. $y_{11} + y_{12} \equiv 2 \pmod 4$

Now we shall use our consideration that from 6.2.9 and 6.2.13 it follows that

6.2.24. $y_{11} \cdot y_{12} = 2^{k-1} 3^{\ell-2}$

so $\ell \geq 2$ and, as we knew, $k \geq 1$.

From 6.2.24 it follows that for some $a_1, b_1, a_2, b_2 \in \mathbb{N}_0$

6.2.25. $y_{11} = 2^{a_1} 3^{b_1}$

$$y_{12} = 2^{a_2} 3^{b_2}$$

Furthermore, from 6.2.15 and 6.2.19 we find the following equality:

6.2.26. $3(y_{11} - y_{12})^2 = y_{11} + y_{12} - 2$

Hence we find

6.2.27. $3 \mid (y_{11} + y_{12} - 2)$

Therefore we must distinguish between two cases:

α) $b_1 = b_2 = 0$ and a_1 and a_2 are both even

β) $b_1 = 0$, $b_2 > 0$ and a_1 is odd

α) This subcase is impossible in view of 6.2.23.

β) In this subcase, let us first suppose $y_{11} = 2$. Then, from 6.2.26, y_{12} must be a root of

6.2.28. $3X^2 - 13X + 12 = 0$

so we find

6.2.29. $y_{11} = 2$ and $y_{12} = 3$

contradicting 6.2.23.

So $y_{11} > 2$. Therefore we find from 6.2.23 that $a_2 = 1$, so

6.2.30. $y_{11} = 2^{a_1}$

$y_{12} = 2\cdot3^{b_2}$

Now since a_1 is odd, say

6.2.31. $a_1 = 1 + 2s \geq 3$

we have from 6.2.26

6.2.32. $3\cdot4\cdot3^{2b_2} \equiv 2\cdot3^{b_2} - 2 \pmod{8}$

6.2.33. $b_2 = 1 + 2t$

Hence we have from 6.2.26

6.2.34. $3\cdot4\cdot3^{2+4t} \equiv 2^{a_1} + 2\cdot3^{1+2t} - 2 \pmod{16}$

6.2.35. $12 \equiv 2^{a_1} + 4 \pmod{16}$

6.2.36. $a_1 = 3$

So $y_{11} = 8$. Then, from 6.2.26, y_{12} must be a root of

6.2.37. $3X^2 - 49X + 186 = 0$

so $y_{12} = 6$. Hence we have

6.2.38. $y_{11} = 8$ and $y_{12} = 6$

In combination with 6.2.15 this yields

6.2.39. $5n = 46$

which is a contradiction. So the case b) is impossible too.

c) In this case the sphere packing condition 6.1.2 becomes:

6.2.40. $25n^2 - 85n + 82 = 2^{k+1}3^{\ell}$, where $|S_2(\underline{0})| = 2^k3^{\ell}$

From 6.1.3 we have $k \geq 1$, $\ell \geq 1$, so

6.2.41. $n(n - 1) \equiv 2 \pmod{12}$

6.2.42. $n \equiv 2 \pmod{12}$ or $n \equiv 11 \pmod{12}$

From the generalized polynomial condition of Heden the following four quadratic equations must have eight rational solutions and at least seven of them must be integral.

6.2.43. $36Z^2 - (60n - 96)Z + 25n^2 - 85n + 82 = 0$

6.2.44. $36Z^2 - (60n - 132)Z + 25n^2 - 115n + 130 = 0$

6.2.45. $36Z^2 - (60n - 120)Z + 25n^2 - 105n + 110 = 0$

6.2.46. $36Z^2 - (60n - 156)Z + 25n^2 - 135n + 170 = 0$

Remark that if we substitute $z = 0$ in 6.2.43, then we find $2 \mid S_2(\underline{0})|$ from 6.2.40.

But, like in the case a), we do not need this consideration in the case c)

First, let us suppose that the equation 6.2.43 has two integral zeros z_{11} and z_{12}. Then we find from 6.2.43

6.2.47. $z_{11} + z_{12} = \dfrac{60n - 96}{36} = \dfrac{5n - 8}{3} \in \mathbb{Z}$

6.2.48. $n \equiv 1 \pmod 3$

contradicting 6.2.42. So z_{11} and z_{12} cannot both be integers.

So the equations 6.2.44, 6.2.45, and 6.2.46 must each have two integral solutions, so also the equation 6.2.44.

Let us denote the zeros of equation 6.2.44 by z_{21} and z_{22}.

Then we find from 6.2.44

6.2.49. $z_{21} + z_{22} = \dfrac{60n - 132}{36} = \dfrac{5n - 11}{3} \in Z$

6.2.50. $n \equiv 1 \pmod 3$

contradicting 6.2.42. So the case c) is also impossible.

Now we have concluded the proof of theorem 6.2.1.

6.3. A nonexistence theorem concerning mixed perfect 3-codes

As a consequence of the fact that the Lloyd polynomial $P_3(X)$ defined in 1.6.3, cannot have three integral zeros if $q > 2$ (cfr. section 5.1), we have the following nonexistence theorem:

6.3.1. **THEOREM.** There do not exist nontrivial mixed perfect 3-codes for which, for $i = 2,3,\dots,n$, q_i is a constant q, and $q > 2$.

PROOF. Assume there exists such a code. Then, from theorem 5.1.1, we may assume without loss of generality that $q \neq q_1$.
Now let a_{ij} (X,Y) be defined by

6.3.2. $$\sum_{i,j=0}^{\infty} a_{ij}(X,Y) z_1^i z_2^j = (1 + (q_1 - 1)z_1)^{1-X}(1 - z_1)^X$$
$$(1 + (q - 1)z_2)^{n-1-Y}(1 - z_2)^Y$$

and let $P(X,Y)$ be defined by

6.3.3. $$\sum_{i=0}^{1} \sum_{j=0}^{3-i} a_{ij}(X,Y) := P(X,Y)$$

Then we find from the generalized polynomial condition of Heden that both $P(0,Y)$ and $P(1,Y)$ must have three integral zeros.
On the other hand we find from 6.3.2 and 1.6.16:

6.3.4. $$P(1,Y) = a_{03}(X,Y) = P_3(Y + 1)$$

so $P(1,Y)$ cannot have three integral zeros unless $q = 2$. □

Now what about $q = 2$? In addition to 6.3.1 we have the following theorem:

6.3.5. **THEOREM.** The only nontrivial mixed perfect 3-code for which, for $i = 2,3,\dots,n$, q_i is equal to 2, is the binary Golay code of length 23.

PROOF. Assume that there exists such a code. Then we have $n > 3$ and in view of lemma 6.1.4 we must have for some $k \in \mathbb{N}$

6.3.6. $$q_1 = 2^k$$

Now in view of theorem 5.1.1 we may assume wothout loss of generality that $k > 1$.

By the generalized polynomial condition of Heden we find that both $P(0,Y)$ and $P(1,Y)$ must have three integral zeros.

By straightforward calculation we find for the zeros of $P(0,Y)$:

6.3.7. $$y_{01} + y_{02} + y_{03} = \frac{3\cdot 2^{k+2} + 12(n-1)}{8}$$

6.3.8. $$y_{01}y^{0}_{2} + y_{01}y_{03} + y_{02}y_{03} = \frac{3\cdot 2^{k+2}n + 6n^2 - 18n + 16}{8}$$

6.3.9. $$y_{01}\cdot y_{02}\cdot y_{03} = \frac{3\cdot 2^{k+1}n + 3\cdot 2^{k}(n-1)(n-2) + (n-1)(n-2)(n-3)}{8}$$

Now the right hand side of 6.3.9 is exactly $\frac{3}{4}\,S_3(\underline{0})$, so by the sphere packing condition we must have for some $\ell \in \mathbb{N}_0$

6.3.10. $$y_{01}\cdot y_{02}\cdot y_{03} = 3\cdot 2^{\ell}$$

Now from 6.3.7 and the fact that y_{01}, y_{02} and y_{03} are integers we find that n must be odd (since $k > 1$).

From 6.3.8 we find

6.3.11. $$4 \mid n(n-3)$$

so we have

6.3.12. $$n \equiv 3 \pmod 4$$

Then since $k > 1$ we see from 6.3.7 that $y_{01} + y_{02} + y_{03}$ is odd.

So from 6.3.10 we find

6.3.13. $P(0,1)\cdot P(0,3) = 0$

On the other hand we find by straightforward calculation:

6.3.14. $6\cdot P(0,1) = n^3 - 12n^2 + 41n - 42 + 3\cdot 2^k (n^2 - 5n + 6)$

6.3.15. $6\cdot P(0,3) = n^3 - 24n^2 + 173n - 378 + 3\cdot 2^k (n^2 - 13n + 38)$

Hence we find

6.3.16. $6\cdot P(0,1) = (n - 2)(n - 3)(n - 7 + 3\cdot 2^k)$

6.3.17 $6\cdot P(0,3) \geq 48\cdot (2^k - 1)$ if $n \geq 11$

keeping in mind 6.3.12, we find combining 6.3.13 with 6.3.16 and 6.3.17 respectively, since $n > 3$:

6.3.18. $6\cdot P(0,3) = 0$

6.3.19. $n = 7$

6.3.20. $- 12\cdot 2^k = 0$

which is obviously a contradiction. □

Remark that theorem 6.3.1 (without the restriction $q > 2$) would hold for arbitrary e if one could prove the nonexistence of ordinary perfect codes using the Lloyd polynomial only.

This means that, with alphabets like above, the generalized polynomial condition reduces to the ordinary polynomial condition.

APPENDIX

A.1. For the case $e = 4$ we determine the numbers a_i of code words of weight i f
$i = 9,10,11,12,13.$
For this purpose we need 1·3·1, 1·3·3, 1·3·4 and the following two recurrence relations:

A.1.1.

$$a_{12}\binom{12}{8} = \binom{n}{8}(q-1)^8 - a_{11}\{\binom{11}{8} + \binom{11}{7}4(q-2)\} -$$

$$a_{10}\{\binom{10}{8} + \binom{10}{7}3(q-2) + \binom{10}{7}(n-10)(q-1) + \binom{10}{6}6(q-2)^2\}$$

$$- a_9\{\binom{9}{8} + \binom{9}{7}2(q-2) + \binom{9}{7}(n-9)(q-1) + \binom{9}{6}3(q-2)^2 +$$

$$+ \binom{9}{6}3(q-2)(n-9)(q-1) + \binom{9}{5}4(q-2)^3\}$$

A.1.2.

$$a_{13}\binom{13}{9} = \binom{n}{9}(q-1)^9 - a_{12}\{\binom{12}{9} + \binom{12}{8}4(q-2)\} -$$

$$a_{11}\{\binom{11}{9} + \binom{11}{8}3(q-2) + \binom{11}{8}(n-11)(q-1) + \binom{11}{7}6(q-2)^2\}$$

$$- a_{10}\{\binom{10}{9} + \binom{10}{8}2(q-2) + \binom{10}{8}(n-10)(q-1) + \binom{10}{7}3(q-2)^2 +$$

$$+ \binom{10}{7}3(q-2)(n-10)(q-1) + \binom{10}{6}4(q-2)^3\} -$$

$$a_9\{1 + \binom{9}{8}(q-2) + \binom{9}{8}(n-9)(q-1) + \binom{9}{7}(q-2)^2 +$$

$$+ \binom{9}{7}2(q-2)(n-9)(q-1) + \binom{9}{7}\binom{n-9}{2}(q-1)^2 + \binom{9}{6}(q-2)^3 +$$

$$+ \binom{9}{6}3(q-2)^2(n-9)(q-1) + \binom{9}{5}(q-2)^4\}$$

Now let us define s, t, u, v by

A.1.3. $$s := \frac{10\ a_{10}}{a_9} \qquad t := \frac{11 \cdot 10\ a_{11}}{a_9}$$

$$u := \frac{12 \cdot 11 \cdot 10\ a_{12}}{a_9} \qquad v := \frac{13 \cdot 12 \cdot 11 \cdot 10\ a_{13}}{a_9}$$

Then we find from the recurrence relations above:

A.1.4. $$a_9 = \frac{\binom{n}{5}(q-1)^5}{\binom{9}{5}}$$

A.1.5. $$s = (n-29)(q-1) + 20$$

A.1.6. $$t = (n-5)(n-6)(q-1)^2 - 4(q-1)(n-29) - 28(q-1)(q-2)(n-29) - 28(q-1)(n-9) - 252(q-2)^2 - 644(q-2) - 92$$

A.1.7. $$u = (n-5)(n-6)(n-7)(q-1)^3 - t(32q-60) - s\{32(q-1)(n-10) + 336(q-2)^2 + 96(q-2) + 12\} - (n-9)(q-1)(672q-1248) - 1344(q-2)^3 - 672(q-2)^2 - 192(q-2) - 24$$

A.1.8. $$v = (n-5)(n-6)(n-7)(n-8)(q-1)^4 - u(36q-68) - t\{432(q-2)^2 + 108(q-2) + 12 + 36(n-11)(q-1)\} - s\{2016(q-2)^3 + 864(q-2)^2 + 216(q-2) + 24 + {} + 108(n-10)(q-1) + 864(n-10)(q-1)(q-2)\} - \{24 + 216(q-2) + 864(q-2)^2 + 2016(q-2)^3 + 3024(q-2)^4 + 216(q-1)(n-9) + 1728(q-1)(q-2)(n-9) + {} + 6048(q-1)(q-2)^2(n-9) + 432(q-1)^2(n-9)(n-10)\}\ .$$

Now, since the code words of a given weight k form a design of type $S - (n,k,\lambda)$ (see section 1.5), where λ can be determined by 1.4.2, 1.4.3 and the numbers a_k mentioned above, we have from 1.4.2 the following conditions for the existence of perfect 4-codes:

A.1.9.

$$9\cdot8\cdot7\cdot6\cdot5 \mid n(n-1)(n-2)(n-3)(n-4)(q-1)^5 \qquad (1)$$

$$8\cdot7\cdot6\cdot5 \mid (n-1)(n-2)(n-3)(n-4)(q-1)^4 \qquad (2)$$

$$7\cdot6\cdot5 \mid (n-2)(n-3)(n-4)(q-1)^3 \qquad (3)$$

$$6\cdot5 \mid (n-3)(n-4)(q-1)^2 \qquad (4)$$

$$5 \mid (n-4)(q-1) \qquad (5)$$

$$10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid n(n-1)(n-2)(n-3)(n-4)(q-1)^5\, s \qquad (6)$$

$$9\cdot8\cdot7\cdot6\cdot5 \mid (n-1)(n-2)(n-3)(n-4)(q-1)^4\, s \qquad (7)$$

$$8\cdot7\cdot6\cdot5 \mid (n-2)(n-3)(n-4)(q-1)^3\, s \qquad (8)$$

$$7\cdot6\cdot5 \mid (n-3)(n-4)(q-1)^2\, s \qquad (9)$$

$$6\cdot5 \mid (n-4)(q-1)\, s \qquad (10)$$

$$5 \mid s \qquad (11)$$

$$11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid n(n-1)(n-2)(n-3)(n-4)(q-1)^5\, t \qquad (12)$$

$$10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-1)(n-2)(n-3)(n-4)(q-1)^4\, t \qquad (13)$$

$$9\cdot8\cdot7\cdot6\cdot5 \mid (n-2)(n-3)(n-4)(q-1)^3\, t \qquad (14)$$

$$8\cdot7\cdot6\cdot5 \mid (n-3)(n-4)(q-1)^2\, t \qquad (15)$$

$$7\cdot6\cdot5 \mid (n-4)(q-1)\, t \qquad (16)$$

$$6\cdot5 \mid t \qquad (17)$$

$$12\cdot11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid n(n-1)(n-2)(n-3)(n-4)(q-1)^5\, u \qquad (18)$$

$$11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-1)(n-2)(n-3)(n-4)(q-1)^4\, u \qquad (19)$$

$$10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-2)(n-3)(n-4)(q-1)^3\, u \qquad (20)$$

$$9\cdot8\cdot7\cdot6\cdot5 \mid (n-3)(n-4)(q-1)^2\, u \qquad (21)$$

$$8\cdot7\cdot6\cdot5 \mid (n-4)(q-1)\, u \qquad (22)$$

$$7\cdot6\cdot5 \mid u \qquad (23)$$

$$13\cdot12\cdot11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid n(n-1)(n-2)(n-3)(n-4)(q-1)^5\, v \qquad (24)$$

$$12\cdot11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-1)(n-2)(n-3)(n-4)(q-1)^4\, v \qquad (25)$$

$$11\cdot10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-2)(n-3)(n-4)(q-1)^3\, v \qquad (26)$$

$$10\cdot9\cdot8\cdot7\cdot6\cdot5 \mid (n-3)(n-4)(q-1)^2\, v \qquad (27)$$

$$9\cdot8\cdot7\cdot6\cdot5 \mid (n-4)(q-1)\, v \qquad (28)$$

$$8\cdot7\cdot6\cdot5 \mid v \qquad (29)$$

A.2. In this section we shall explain how, using the conditions A.1.9, we have excluded those parameters (n,q) for a 4-error-correcting perfect code, which are given by

A.2.1. $q = 2^k 3\ q'$ and $\gcd(6,q') = 1$ and

$\ell \backslash k$	$k = 0$	$k = 1$	$k = 2$	$k \geq 3$
$\ell = 0$	$q < 4$	$q < 46$	$q < 718$	$q < 7$
$\ell \geq 1$	$q < 10$	$q < 136$	$q < 2152$	$q < 18$

A.2.2. $n - 4 < \frac{14}{5} \frac{q^4}{q-1}$

Thus we finish the proof of theorem 5.2.5 by proving lemma 5.2.26. First we exclude the numbers q with only one or two distinct prime divisors, since these are impossible (see section 2.2).
Therefore we need to look only at the part of the diagram A.2.1 which is indicated below:

A.2.3.

$\ell \backslash k$	$k = 0$	$k = 1$	$k = 2$	$k \geq 3$
$\ell = 0$			$q < 718$	
$\ell \geq 1$		$q < 136$	$q < 2152$	

For instance, for the case $k = 1$, $\ell \geq 1$, the remaining q are:

A.2.4. $q = 30,\ 42,\ 54,\ 66,\ 78,\ 90,\ 102,\ 114,\ 126$.

Now let us take for example $q = 30$. In this case it follows from 5.2.23 that for some $m \in \mathbb{N}$

A.2.5. $n - 4 = m3^3 5^4$

and from A.2.2 that

A.2.6. $m \leq 4$

Now from A.1.9 (2) it follows that

A.2.7. $16 \mid (n-1)(n-2)(n-3)(n-4)$

Since from A.2.5 we see that $n - 4 \equiv 3m \pmod 8$ we find from A.2.7 and A.2.6 that m must be 2, so

A.2.8. $n - 4 = 2 \cdot 3^3 \cdot 5^4$

Finally, it follows from A.1.9 (3) that

A.2.9. $7 \mid (n-2)(n-3)(n-4)$

contradicting A.2.8, because from A.2.8 it follows that $n - 4 \equiv 3 \pmod 7)$ So we may exclude $q = 30$. In the same way we excluded all other cases separately by hand.

A.3. We shall show that the following identity holds:

$$\text{A.3.1.} \qquad \sum_{i=0}^{e-1} (-1)^i \binom{e}{i} \sum_{j=i+1}^{e} 1/j(1 + 1/2 + \dots + \widehat{1/j} + \dots + 1/e) = 0$$

where $\widehat{1/j}$ means that $1/j$ must be replaced by 0.

For this purpose we remark that for $i = 1,2,\dots,e-1$.

$$\text{A.3.2.} \qquad \binom{e}{i} = \binom{e-1}{i-1} + \binom{e-1}{i}$$

So the left hand side of A.3.1 is equal to

$$\text{A.3.3.} \qquad \sum_{i=0}^{e-2} (-1)^{i+1} \binom{e-1}{i} \sum_{j=i+2}^{e} a_j + \sum_{i=0}^{e-1} (-1)^i \binom{e-1}{i} \sum_{j=i+1}^{e} a_j$$

where a_j is defined by

$$\text{A.3.4.} \qquad a_j := 1/j(1 + 1/2 + \dots + \widehat{1/j} + \dots + 1/e)$$

Now clearly the expression A.3.3 is equal to

$$\text{A.3.5.} \qquad \sum_{i=0}^{e-1} (-1)^i \binom{e-1}{i} a_{i+1}$$

Hence, because

$$\text{A.3.6.} \qquad a_{i+1} = \frac{1 + 1/2 + \dots + 1/e}{i+1} - \frac{1}{(i+1)^2}$$

and because

$$\text{A.3.7.} \qquad \binom{e-1}{i} = \frac{i+1}{e} \binom{e}{i+1}$$

we find that the expression A.3.5 is equal to

$$\text{A.3.8.} \qquad (1 + 1/2 + \dots + 1/e)\, 1/e \sum_{i=0}^{e-1} (-1)^i \binom{e}{i+1} - 1/e \sum_{i=0}^{e-1} (-1)^i \binom{e}{i+1} \frac{1}{i+1}$$

Now, since

$$\text{A.3.9.} \qquad \sum_{i=0}^{e} (-1)^{i} \binom{e}{i} = 0$$

we see that the expression A.3.8 is equal to

$$\text{A.3.10.} \qquad (1 + 1/2 + \ldots + 1/e)1/e + 1/e \sum_{j=1}^{e} (-1)^{j} \binom{e}{j} 1/j$$

Finally to show that the expression A.3.10, and hence the left hand side of A.3.1, is equal to zero, we shall show:

$$\text{A.3.11.} \qquad \sum_{j=1}^{e} (-1)^{j+1} \binom{e}{j} 1/j = 1 + 1/2 + \ldots + 1/e$$

For this purpose we remark that for $j = 1, 2, \ldots, e$

$$\text{A.3.12.} \qquad (-1)^{j+1} \binom{e}{j} 1/j = \int_0^1 (-1)^{j+1} \binom{e}{j} x^{j-1} dx$$

so we have

$$\text{A.3.13.} \qquad \sum_{j=1}^{e} (-1)^{j+1} \binom{e}{j} 1/j = -\int_0^1 \frac{(1-x)^{e} - 1}{x} dx$$

Hence, since $- x = (1 - x) - 1$, we have

$$\text{A.3.14.} \qquad \sum_{j=1}^{e} (-1)^{j+1} \binom{e}{j} 1/j = \int_0^1 \sum_{k=0}^{e-1} (1 - x)^{k} dx$$

Finally, since

$$\text{A.3.15.} \qquad \int_0^1 (1 - x)^{k} dx = \frac{1}{k+1}$$

we find from A.3.14

A.3.16. $\sum_{j=1}^{e} (-1)^{j+1} \binom{e}{j} 1/j = 1 + 1/2 + \ldots + 1/e$. □

A.4. As an example, we shall explain why there does not exist a perfect double-error-correcting code with $q = 38$ and $n \leq 1000$. Assuming the existence of such a code, we find from 4.2.14:

A.4.1. $19^2 \mid (n - 2)$

So for $m = 1$ or $m = 2$ we have

A.4.2. $n = 2 + m \cdot 361$

Furthermore we have the sphere packing condition 1.2.1, which becomes in our case:

A.4.3. $1 + n(q - 1) + \binom{n}{2}(q - 1)^2 = 2^k 19^\ell$

for some pair $(k,\ell) \in \mathbb{N}_0^2$
Now for $m = 1$ and for $m = 2$ we can calculate the left hand side of A.4.3 with the help of, say, an electronic pocket calculator, and see that in each of both cases there is a prime unequal to 2 and unequal to 19 dividi it.
Hence we have a contradiction to A.4.3.

A.5. Let $m \in \mathbb{N}$, $q \in \mathbb{N}$, and let e, s and p be defined by:

A.5.1. $e := 2m + 1$

$s := \gcd(q,e)$

$q := ps$

Furthermore, assume that

A.5.2. $3p \mid (e - 1)(q + 1)$, so also $p \mid (e - 1)$

The purpose of this section is to show that there does not exist a q as above with at least three prime divisors, if $e < 19$ (or equivalently $m < 9$).

For this purpose we make the following list of q's with $q = ps$, $p \mid (e - 1)$, $s \mid e$, and the restrictions:

a) q is divisible by at least three distinct prime divisors

b) if $3 \nmid (e - 1)$ then $3 \nmid q$

c) if $9 \nmid (e - 1)$ then $3 \nmid p$

$m = 1$	$e - 1 = 2$	$p = 1,2$	$s = 1,3$	
$m = 2$	$e - 1 = 4$	$p = 1,2,4$	$s = 1,5$	
$m = 3$	$e - 1 = 6$	$p = 1,2$	$s = 1,7$	
$m = 4$	$e - 1 = 8$	$p = 1,2,4,8$	$s = 1,3,9$	
$m = 5$	$e - 1 = 10$	$p = 1,2,5,10$	$s = 1,11$	$q = 2\cdot 5\cdot 11$
$m = 6$	$e - 1 = 12$	$p = 1,2,4$	$s = 1,13$	
$m = 7$	$e - 1 = 14$	$p = 1,2,7,14$	$s = 1,3,5,15$	$q = 2\cdot 5\cdot 7$
$m = 8$	$e - 1 = 16$	$p = 1,2,4,8,16$	$s = 1,17$	

So we have only two possibilities for q. But in these cases we have $3 \nmid (e - 1)$. So from A.5.2 we should have $3 \mid (q + 1)$, which is not true.

<u>A.6.</u> The purpose of this section is to give a lower bound for the coefficient $a_{m-1}(\theta_0)$ of n^{m-1} in $F_e(\theta_0)$, where θ_0 is defined in 4.4.3, $F_e(\theta)$ is defined in 1.6.18, and $m \in \mathbb{N}$ is at least equal to 9.

We also assume that $q \geq 30$, which holds if q has at least three prime divisors.

Define ξ, η, λ and μ as follows:

A.6.1. $$\xi := \frac{(q-1)}{2}$$

$$\eta := \frac{(q-1)(q-2)}{3}$$

$$\lambda := \frac{(q-1)(2q^2-7q+7)}{8}$$

$$\mu := \frac{(q-1)(6q^3-29q^2+51q-34)}{30}$$

Then it follows from 1.6.18 that $a_{m-1}(\theta_0)$ is the coefficient of $z^e n^{m-1}$ in

A.6.2. $$\{1 - (\theta - 1)z + (\theta^2 + (q-4)\theta + 2)\frac{z^2}{2} - (\theta^3 + 3(q-3)\theta^2 + (2q^2 - 9q + 18)\theta - 6)\frac{z^3}{6} + \dots\} \cdot$$

$$\{\sum_{j=0}^{n} \binom{n}{j} z^{2j} (-\xi + \eta z - \lambda z^2 + \mu z^3 + \dots)^j$$

Hence we can calculate $a_{m-1}(\theta_0)$ from A.6.2, considering only terms with $j = m - 1, m$ (cfr. lemma 1.6.24).

The outcome is

A.6.3. $$a_{m-1}(\theta_0) = \frac{(-1)^m (\frac{q-1}{2})^{m-3} (q-1)^2 a}{16 \cdot 81 \cdot 5 \cdot (m-1)!}$$

where a is given by

A.6.4. $$a = -80m^3q^3 + 480m^3q^2 - 960m^3q + 640m^3 - 60m^2q^3 + 90m^2q^2 + 90m^2q - 60m^2 + 708mq^3 - 3582mq^2 + 6498mq - 4332m - 648q^3 + 3132q^2 - 5508q + 3672$$

Now since $m \geq 9$ and $q \geq 30$ we see from A.6.4 that

A.6.5. $$|a| > 80m^3q^3 + 60m^2q^3 - 720mq^3 - 480m^3q^2 - 90m^2q^2$$

Hence, since $m^3 \geq 9m^2$ and $m^2 \geq 9m$, we see:

A.6.6. $$|a| > 77m^3q^3 - 480m^3q^2 - 90m^2q^2$$

Since $q^3 \geq 30q^2$ we have

A.6.7. $$|a| > 61m^3q^3 - 90m^2q^2$$

Finally, since $m^3q^3 \geq 270m^2q^2$

A.6.8. $$|a| > 60m^3q^3$$

Now it follows from A.6.3 and A.6.8 that the following bound holds if $m \geq 9$ and $q \geq 30$:

A.6.9. $$|a_{m-1}(\theta_0)| > \frac{(q-1)^{m-1}m^3q^3}{2^{m-1}\cdot 27\cdot (m-1)!}$$

A.7. The purpose of this section is to show that, assuming the existence of a perfect 5-code, we may assume that

A.7.1. $n \geq 16q$

For this purpose we use the following conditions which are obtained immediately from 1.6.6 and 1.6.9:

A.7.2. $q \mid 5(n-5)$

A.7.3. $q^5 \mid (n-1)(n-2)(n-3)(n-4)(n-5)$

Now define $k, \ell, m \in \mathbb{N}$ and $q' \in \mathbb{N}$ with $\gcd(q', 30) = 1$ by

A.7.4. $q = 2^k 3^\ell 5^m q'$

Then, if $m \geq 2$ and A is in the distinct cases defined by the following diagram:

A.7.5.

$\ell \backslash k$	$k = 0$	$k = 1$	$k = 2$	$k \geq 3$
$\ell = 0$	$A = 1$	$A = 2^4$	$A = 2^8$	$A = 2^3$
$\ell = 1$	$A = 3^4$	$A = 2^4 3^4$	$A = 2^8 3^4$	$A = 2^3 3^4$
$\ell \geq 2$	$A = 3$	$A = 2^4 \cdot 3$	$A = 2^8 \cdot 3$	$A = 2^3 \cdot 3$

we find from A.7.2 and A.7.3

A.7.6. $q^5 \mid A(n-5)$

If $m = 1$ we find

A.7.7. $q^5 \mid 5^5 A(n-5)$

So in any case we find from A.7.6, A.7.7 and A.7.5

A.7.8. $n > \dfrac{q^5}{5^5 \cdot 2^8 3^4}$

so we have A.7.1 if

A.7.9. $q > 120 \sqrt[4]{5}$

Furthermore it follows from 4.2.9 that

A.7.10. $n \geq 3125$

So if q does not fulfil the inequality A.7.9, then A.7.1 follows from A.7.10. □

Historical Summary

During the past twenty years many attempts have been made to solve the question which we have considered: whether or not there are other examples of perfect codes than those mentioned in section 1.7. We shall give a summary of the history of progress in the approach to this question. A detailed survey was given by Van Lint in [29].

An important topic in the theory of perfect codes is the connection between group theory and the theory of perfect single-error-correcting codes which was introduced by Taussky & Todd (see [36]).
They consider an abelian group G with base elements $g_1, \dots, g_n$ of order q, and its subset S defined by

H.1. $$S := \{ag_i \mid i = 1,2,\dots,n,\ a = 0,1,\dots q-1\}$$

and ask for subsets H with minimal cardinality such that each group element g can be written in the form $g = h + s$ $(h \in H,\ s \in S)$.
We shall not go into this topic, but refer to [29].

The nonexistence proofs up to now concerning perfect e-codes with $e \geq 2$ can be divided into three classes: those which use the sphere packing condition only, those which combine the sphere packing condition and the polynomial condition, and those which use the polynomial condition only.

Early proofs belonging to the first class make use of the consideration that if e is odd and q = 2, then

H.2. $$e!(n+1) \mid \sum_{i=0}^{e} \binom{n}{i}(q-1)^i$$

So by the sphere packing condition $e!\ (n+1)$ must be a power of 2.
These are proofs by *Shapiro and Slotnick* (1959), *Leontiev* (1964), *Johnson* (1962) and *James, Stanton and Cowan* (1970).

It can be seen immediately from 1.4.2 that (90,2,2) does not fit a perfect code.

Details about these searches can be found in papers by *Cohen* (see [8]), *Mc Andrew* (see [31]) and *Van Lint* (see [22]).

The ranges covered were

H.5. $e = 2$, q odd, $3 \le q \le 125$, $3t \le k \le 40.000$ (Cohen)

$e \le 20$, $q = 2$, $n \le 2^{70}$ (Mc Andrew)

$e \le 1000$, $q \le 100$, $n \le 1000$ (Van Lint)

They use adapted Newton-Raphson procedures.

The most important step forward was made with proofs belonging to the second class by *Van Lint* and *Tietäväinen*.

First, the fruitful method of combining the sphere packing condition and the polynomial condition was introduced by *Van Lint* (1970) for the case $e = 2$.

For a general explanation of this method we refer to section 1.6.

In the same paper by *Van Lint* the case $e = 3$ was treated using the polynomial condition only.

Both for $e = 2$ and for $e = 3$ he proved that a perfect e-code over GF(q), $q = p^s$, cannot exist unless such a code has the Golay parameters. We refer to [23].

Van Lints method for the case $e = 3$ was generalized by the author to prove the nonexistence of perfect e-codes over arbitrary alphabets for $e = 3$ and $e = 5$ (see chapter 5).

The method for $e = 2$ was applied to the case $e = 4$ by *Tietäväinen* (1970). He proved that perfect 4-codes over GF(q), $q = p^s$, do not exist (see [38]).

The nonexistence of perfect 5- 6- and 7-codes over GF(q) was proved by *Van Lint* in [24].

Then, successively, the impossibility of unknown perfect codes over an alphabet GF(q), $q = p^s$, was established by *Van Lint* (1971) and *Tietäväinen* (1973).

Van Lint treated the case $p > e$. This is in a sense the easiest case,

In the first two proofs it was shown that, if $q = 2$ and e is odd, then n must be bounded by a bound depending on e only.
For this purpose the same theorem of Siegel was used that we use for the more general case where q is arbitrary.
We refer to [32], [20] and our section 4.3.
In the latter two proofs the nonexistence was established of perfect codes with $q = 2$, e odd, and (respectively) $5 \leq e \leq 29$, $e \leq 39$.
For the paper by James c.s. see [16].
The paper by *Johnson* ([17]) also contains proofs belonging to the third class: by factoring the Lloyd polynomials of degree 2 and 3 in the case $q = 2$ he proves the nonexistence of binary perfect 2- and 3- codes.

Other proofs belonging to the first class treat some small values of q in the case $e = 2$, starting from the equation

H.3. $$x^2 - (q^2 - 6q + 1) = 8q^k$$

which is related to the sphere packing condition 1.2.1.
The proofs use diophantine theory. They were given by *Alter* (1968), *Engelman* (1961) and *Cohen* (1964). See [1], [2], [12], [8].
The cases $7 \leq q \leq 9$ (Alter), $q = 5$ (Engelman) and $q \leq 6$ (Cohen) were excluded.
In the case $q = 6$ the proof is false, because in this case H.3 is not related to 1.2.1.
By approaching the solutions of H.3 with Newton's method, *Alter* proved that these solutions cannot be integral, but again this fact does not prove the nonexistence of perfect codes with parameters $e = 2$ and $q = 2s^2$.

Several computer searches have been made to find solutions of

H.4. $$\sum_{i=0}^{e} \binom{n}{i} (q - 1)^i = q^k$$

These were very extensive, but did not yield nontrivial solutions (n,e,q) except the Golay parameters and $(90,2,2)$.

which should be clear from our section 1.6.

In *Tietäväinen's* proof a sharpening of the arithmetical - geometrical mean inequality was used, which turned out to be very useful in later proofs (see [40], [6]).

Later on, simpler proofs were obtained by *Tietäväinen* (1974) and by *van Lint* (1975).

We refer to [26], [39] and [30], and to our chapter 2, where some generalizations can be found.

Subsequently, some nonexistence theorems were given for arbitrary q. Among these we mention proofs by *Tietäväinen* (1975), by *Bassalygo, Zinoviev, Leontiev and Feldman* (1975) and by *Van Lint* (1974), all belonging to the second class.

Van Lint proved the nonexistence of perfect codes with $e = 2$ and $q = 10$ (see [28]). In section 3.2 there are some more results of this kind given by the author.

Tietâväinen treated the case $q = p_1^s p_2^t$, $e \geq 3$, with a method described in our section 2.2. See [40]).

Finally, Bassalygo c.s. proved the nonexistence of perfect codes with $q = 2^k 3^s$ and $e \geq 2$, using estimates by Baker c.s. and a sharpening of the geometrical - arithmetical mean inequality by Lagrange.

We refer to [6] and our theorem 3.5.1.

A forthcoming paper by *Bannai* (1976) proves the existence of an upper bound N(e,q) for n for $e \geq 3$, as we did in our sections 4.3 and 4.4. This bound has not yet been made explicit.

For the purpose he uses Hermite polynomials to approximate the zeros of the Lloyd polynomials.

No use is made of the sphere packing condition. We refer to [4].

In this thesis there are some further contributions by the author. The most important is the proof of the nonexistence of perfect 4-codes over arbitrary alphabets in section 5.2.

In section 1.9 we give a survey of our results.

REFERENCES

[1] R. Alter, "On the non-existence of close-packed double-Hamming-error-correcting codes on q = 7 symbols".
Journal of Computer and System Sciences 2 (1968), 169-176.

[2] R. Alter, "On the nonexistence of perfect double-Hamming-error-correcting codes on q = 8 and q = 9 symbols".
Information and Control 13 (1968), 619-627.

[3] R. Alter, "On a diophantine equation related to perfect codes".
Mathematics of Computation 25 (1971), 621-624.

[4] E. Bannai, "On perfect codes in the Hamming Schemes H(n,q) with q arbitrary".
Columbus, Ohio State University, 1976. To appear in Journal of Combinatorial Theory.

[5] L.A. Bassalygo, V.A. Zinoviev, V.K. Leontiev, "Perfect codes over arbitrary alphabets".
Abstracts of papers, part 2, the third international symposium on Information theory (Tallinn 1973), 23-28.

[6] L.A. Bassalygo, V.A. Zinoviev, V.K. Leontiev, N.I. Feldman, "Nonexistence of perfect codes over some alphabets".
Problemy Peredači Informacii 11 (1975), 3-13.

[7] N. Biggs, "Perfect codes in graphs".
Journal of Combinatorial Theory B 15 (1973), 289-296.

[8] E.L. Cohen, "A note on perfect double-error-correcting codes on q symbols".
Information and Control 7 (1964), 381-384.

[9] D.M. Cvetkovic, J.H. van Lint. "An elementary proof of Lloyd's theorem".
Eindhoven, The Netherlands. Technological University Eindhoven, september 1976. Verschijnt in Proceedings van de Koninklijke Nederlandse Akademie van Wetenschappen.

[10] P. Delsarte, "The association schemes of coding theory".
Philips Research Reports. Supplements 10 (1973).

[11] P. Delsarte, J.M. Goethals, "Unrestricted codes with the Golay parameters are unique".
Discrete Mathematics 12 (1975), 211-224.

[12] C. Engelman, "On close-packed double-error-correcting codes on P symbols".
IRE Transactions on Information Theory 7 (1961), 51-52.

[13] S.W. Golomb, E.C. Posner, "Rook domains, Latin squares, Affine planes and Error-distributing codes".
IEEE Transactions on Information Theory, IT 10 (1964), 196-208.

[14] O. Heden, "A generalized Lloyd theorem and mixed perfect codes".
Matematiska Institutionen Stockholms Universitet, 1974.
Memorandum no. 8.

[15] M. Herzog, J. Schönheim, "Group partition, factorization and the vector covering problem".
Canadian Mathematical Bulletin 15 (1972), 207-214.

[16] L.O. James, R.G. Stanton, D.D. Cowan, "A problem in coding theory".
Proceedings of the Louisiana Conference on Combinatorics, Graph theory and Computing.
Baton Rouge, Louisiana State University, 1970, 167-179.

[17] S. Johnson, "On perfect error-correcting codes".
Santa Monica, California; Rand Corporation, 1962.
Memorandum RM-3403 PR.

[18] M. Langevin, "Plus grand facteur premier d'entiers consécutifs.
Séminaire Delange-Pisot-Poitou (Théorie des Nombres).
Paris, Secretariat Mathématique, 1975.

[19] H.W. Lenstra, jr., "Two theorems on perfect codes".
Discrete Mathematics 3 (1972), 125-132.

[20] V.K. Leontiev, "On a problem of close-packed codes". (Russian).
Diskretnyĭ analiz. Ibornik Trudov (Novosibirsk) 2 (1964), 56-58.

[21] B. Lindström, "Group partition and mixed perfect codes".
To appear in the Canadian Mathematical Bulletin.

[22] J.H. van Lint, "1967-1969 Report of the Discrete Mathematics group".
Eindhoven, The Netherlands; Technological University
Eindhoven, 1969. Report 69-WSK-04.

[23] J.H. van Lint, "On the nonexistence of perfect 2- and 3-error-correcting codes over GF(q)".
Information and Control 16 (1970), 396-401.

[24] J.H. van Lint, "On the nonexistence of perfect 5-, 6- and 7-error-correcting codes over GF(q)".
Eindhoven, The Netherlands; Technological University
Eindhoven, 1970. Report 70-WSK-06.

[25] J.H. van Lint, "On the nonexistence of certain perfect codes".
Computers in Number Theory.
London-New York, Academic Press, 1971; 277-282.

[26] J.H. van Lint, "Nonexistence theorems for perfect error-correcting codes".
Computers in algebra and number theory.
Providence, American Mathematical Society, 1971. SIAM-AMS Proceedings, vol. 4, 89-95.

[27] J.H. van Lint, "Coding theory".
Berlin etc.,Springer Verlag, 1973.
Lecture Notes in Mathematics, vol. 201.

[28] J.H. van Lint, "Recent results in perfect codes and related topics".
Combinatorics, vol. 1; ed. by M. Hall and J.H. van Lint.
Amsterdam, Mathematical Center, 1974.
Mathematical Center Tracts, nr. 55; 163-183.

[29] J.H. van Lint, "A survey of perfect codes".
Rocky Mountain Journal of Mathematics 5, (1975), 199-224.

[30] J.H. van Lint, H.C.A. van Tilborg, "Gelijkmatig verdeelde codes".
MC Syllabus 31. Amsterdam, Mathematische Centrum, 1976.

[31] M.H. Mc Andrew, "An algorithm for solving a Polynomic Congruence and its Application to Error-Correcting codes".
Mathematics of Computation 19 (1965), 68-72.

[32] H.S. Shapiro, D.S. Slotnick, "On the mathematical theory of error-correcting codes".
IBM Journal of Research Development 3 (1959), 25-34.

[33] C.L. Siegel, "Approximation Algebraischer Zahlen".
Gesammelte Abhandlungen, Band I.
Berlin etc., Springer Verlag, 1966; 1-47.

[34] S.L. Snover, "The uniqueness of the Nordstrom-Robinson and the Golay binary codes".
Pd.D. Thesis, Michigan State University, 1973.

[35] G. Szegö, "Orthogonal Polynomials".
Providence, American Mathematical Society, 1959.
American Mathematical Society Colloquium Publications, vol. 23.

[36] O. Taussky, J. Todd, "Covering Theorems for Groups".
Annales Societatis Polonicae Mathematicae 2 (1948), 303-305.

[37] A. Thue, "Ueber Annäherungswerte algebraischer Zahlen".
Journal der Reine und angewandte Matematik 135. (1909), 284-305.

[38] A. Tietäväinen, "On the nonexistence of perfect 4-Hamming-error-correcting codes".
Annales Academiae Scientiarum Fennicae ser.A.I (1970), nr. 485.

[39] A. Tietäväinen, "A short proof for the nonexistence of unknown perfect codes over GF(q).
Annales Academiae Scientarium Fennicae ser.A.I (1974), nr. 580.

[40] A. Tietäväinen, "Nonexistence of nontrivial perfect codes in case $q = p_1^s p_2^t$, $e \geq 3$.
To appear in Discrete Mathematics.

[41] H.C.A. van Tilborg, "Uniformly packed codes".
Thesis, Technological University Eindhoven, June 1976.

[42] B.L. van der Waerden, "Moderne Algebra I".
Berlin etc., Springer Verlag, 1964; § 58.

SAMENVATTING

In dit proefschrift is de (non-)existentie aan de orde van drietallen (n,e,q) van parameters voor zogenaamde *perfecte codes*.
Aan de hand van een tweetal voorwaarden worden non-existentiestellingen bewezen. De eerste van deze twee voorwaarden is de *sphere packing condition:*

S.1. $$1 + n(q - 1) + \dots + \binom{n}{e}(q - 1)^{e} \mid q^{n}$$

De tweede is de *polynomial condition:*

S.2. $$P_e(X) := \sum_{i=0}^{e} (-1)^{i} \binom{n-X}{e-i} \binom{X-1}{i} (q - 1)^{e-i}$$

heeft e verschillende gehele nulpunten in $\{1,2,\dots,n\}$.

Na het eerste hoofdstuk, dat een inleiding is tot het proefschrift, spitst het onderzoek zich toe op deze twee voorwaarden.

In hoofdstuk 2 wordt uiteengezet hoe men, door beide voorwaarden te combineren, iets kan zeggen over het aantal priemdelers van q.
Na twee stellingen, respectievelijk van Van Lint / Tietäväinen en Tietäväinen, over achtereenvolgens het geval $q = p^{s}$ en het geval $q = p_1^{s}p_2^{t}$, geraken wij tot een generalisatie en passen deze toe in het geval $e = 6$.
Deze generalisatie houdt in dat q "meestal" tenminste e verschillende priemdelers heeft.

In hoofdstuk 3 geven wij de nulpunten x_1 en x_2 van $P_2(X)$ in een parameterformule en leiden enkele deelresultaten aangaande q af.
Ook hier gebruiken wij de combinatie van beide boven genoemde noodzakelijke voorwaarden.

In hoofdstuk 4 wordt een bovengrens $N(e,q)$ voor n afgeleid in het geval dat e oneven is, met behulp van de polynoomvoorwaarde alleen.

Hiertoe beschouwen we een transformatie θ die de polynomen $P_e(x)$ overvoert in polynomen $F_e(\theta)$ die eveneens e verschillende gehele nulpunten moeten hebben.
Voor deze polynomen $F_e(\theta)$ vinden we dan twee waarden van θ waarin $F_e(\theta)$ voor $n > N(e,q)$ een verschillend teken heeft, terwijl in het interval begrensd door beide waarden van θ geen geheel getal voorkomt.

In hoofdstuk 5 komen wij tot onze voornaamste stellingen.
Hier bewijzen wij dat onbekende niet-triviale perfecte codes met $e = 3$, 4 of 5 niet bestaan.
In de gevallen $e = 3$ en $e = 5$ wordt hiertoe een bewijs van Van Lint (die zich beperkte tot het geval $q = p^s$) gegeneraliseerd.
Voor het geval $e = 4$ maken wij gebruik van de *resolvente van Lagrange* om van het vierdegraads *Lloyd polynoom* $P_4(X)$ te geraken tot een derdegraads polynoom die in zekere zin kan worden behandeld als de "oneven" polynomen $P_3(X)$ en $P_5(X)$.
Opnieuw vinden wij twee waarden x waarin het polynoom van teken verschilt, terwijl in het interval begrensd door beide waarden geen geheel getal voorkomt.

Tenslotte hebben wij aan onze tekst het zesde hoofdstuk toegevoegd, waarin men kan zien hoe onze methoden eveneens gebruikt kunnen worden om nonexistentiestellingen te bewijzen aangaande zogenaamde *mixed perfect codes*.

CURRICULUM VITAE

De ontwerper van dit proefschrift werd in 1951 geboren te Maastricht. Zijn enthousiasme voor de wiskunde werd hem bijgebracht door de wiskundeleraar aan het gymnasium der paters Carmelieten te Zenderen (O.), de heer G.A. Jansen.
Na het eindexamen gymnasium B in 1969 ging hij wiskunde studeren aan de Katholieke Universiteit in Nijmegen, waar hij colleges volgde van onder andere prof. dr. A.H.M. Levelt en prof. dr. J.H. de Boer, en in 1973 doctoraal examen deed.
Daarna begon hij, onbezoldigd, met het samenstellen van dit proefschrift, begeleid en geïnspireerd door prof. dr. J.H. van Lint, die hoogleraar is aan de Technische Hogeschool te Eindhoven.
Hiertoe werd hij in staat gesteld door een studentassistentschap en een toelage van het Ministerie van Onderwijs en Wetenschappen.
Sinds augustus 1976 is de ontwerper als docent wiskunde part-time in dienst van de Katholieke Leergangen te Tilburg en Sittard.

STELLINGEN

I

Het is niet zo eenvoudig een algemene nonexistentiestelling voor perfecte 2-codes met q symbolen te bewijzen, waar $q = 2p^k$ (p priem).
Van de andere kant zijn nonexistentiestellingen voor zulke codes eenvoudig te bewijzen als q een vooraf gegeven natuurlijk getal is, bijvoorbeeld $q = 33$ of $q = 38$.

Vergelijk dit met stelling 3.5.13 en de paragrafen 3.6 en 3.7 van dit proefschrift.

II

Indien e een gegeven klein oneven natuurlijk getal is ongelijk aan 1 (bijvoorbeeld $e = 7,9,11$), dan kan men een nonexistentiestelling voor perfecte e-codes bewijzen met een bewijs analoog aan dat van de stellingen 5.1.1 en 5.3.1 van dit proefschrift.

Vergelijk dit met de hoofdstukken 4 en 5 van dit proefschrift.

XII

Het is van belang nonexistentiestellingen voor perfecte codes zoveel mogelijk te bewijzen met behulp van de polynoomvoorwaarde alleen.
Hiermee bewijs men namelijk meteen wezenlijk sterkere nonexistentiestellingen op het gebied van de zogenaamde "mixed perfect codes".

Vergelijk dit met paragraaf 6.3 van dit proefschrift.

IV

Zij, voor $q \in \mathbb{N}$, de verzameling S gedefinieerd door $S := \{0,1,..,q\}$.
Zij $n \in \mathbb{N}$ en laat voor $\underline{x} = (x_1, x_2 ... x_n) \in S^n$ de uitspraak $P(\underline{x})$ gedefinieerd zijn door:

$$"\forall_{i\in\{1,2,...,n-1\}}[x_i = 0 \Rightarrow x_{i+1} = 0]"$$

Dan kan men een "code met variabele woordlengte" definiëren als een deelverzameling van $V := \{\underline{x} \in S^n \,/\, P(\underline{x})\}$.

a) Indien $q = 1$, dan bestaat er voor iedere $n \in \mathbb{N}$ een "perfecte e-foutenverbeterende code met variabele woordlengte".

b) Indien $q \neq 1$, dan zijn codes met variabele woordlengte zowel voor de wiskunde als voor de techniek de moeite van het bestuderen waard, en voor de taalwetenschap interessanter dan codes met vaste woordlengte.

V

De constructie der reële getallen, uitgaande van de rationele, volgens de methode van de Nederlandse wiskundige Pierre Baudet (1891-1921) biedt bepaalde voordelen boven de constructies van Cantor, Dedekind en Weierstrasz.

Vergelijk F. Schuh: "Het getalbegrip, in het bijzonder het onmeetbaar getal"; Groningen, Noordhoff, 1927.

VI

Bij het zoeken naar de oplossingen $(x,n) \in \mathbb{N}^2$ van niet-triviale diophantische vergelijkingen van het type $x^2 + d = p^n$ (d kwadraatvrij, p priem) lijkt het werken in een getallenlichaam $Q(\sqrt{-d})$ zinloos als $d < 0$, en in ieder geval zinvol als $d = 1,2,3,7$ of 11.
De diophantische vergelijking $x^2 + 7 = 11^n$ heeft geen andere oplossing $(x,n) \in \mathbb{N}^2$ dan $(2,1)$. Men kan hiervan een bewijs geven dat analoog is aan een bewijs in een (onder genoemd) artikel van Alter en Kubota.

Vergelijk: Hardy & Wright: "An introduction to the theory of numbers"; Oxford University Press, 1971.

Pierre Samuel: "Théorie Algébrique des Nombres"; Collection Méthodes, Hermann, Paris, 1967.

Ronald Alter & K.K. Kubota: "The diophantine equation $x^2 + 11 = 3^n$ and a related sequence", Journal of Number Theory 7 (1975), 5-10.

VII

Stel dat p een priemgetal is en q een willekeurig natuurlijk getal ongelijk aan 1. Indien

$$\forall_{(s,t) \in \mathbb{N}^2} [p \mid \sum_{i=0}^{q} s^i t^{q-i} \Rightarrow p \mid s]$$

(dit is bijvoorbeeld het geval als $p = q = 2$)
dan is de functie $f : \mathbb{Q} \to \mathbb{Q}$, gedefinieerd door $f(x) := x(x^q - p)$ injectief.

Vergelijk dit met problem E 2554 in the American Mathematical Monthly, oktober 1975, page 851.

VIII

Gedurende een bepaalde periode in de middeleeuwen beschreven monniken in langdradige verbale teksten de oplossing van lineaire vergelijkingen van het type $ax + b = 0$ met de methode van single, resp. double false:

i) is $ag + b = f$, dan is $x = \dfrac{g(f - b) - gf}{f - b}$.

ii) zijn g_1 en g_2 zó dat $ag_1 + b = f_1$ en $ag_2 + b = f_2$, dan is

$$x = \frac{f_1 g_2 - f_2 g_1}{f_1 - f_2} .$$

Niettegenstaande het feit dat de moderne algebraïsche methoden en de moderne notatie van algebraïsche vergelijkingen in die tijd niet in zwang waren, lijkt het onwaarschijnlijk dat de rechtstreekse oplossing van het probleem niet aan de meeste belangstellenden bekend was.

Vergelijk Christoph Scriba: "The concept of number"; B-I-Hochschulskripten 825/825a, Mannheim/Zürich, Bibliographisches Institut, 1968.

IX

Het maximale profijt dat men als wiskundige kan trekken uit deelname aan een filosofisch debat is een geoefend vermogen tot het handhaven van een verbale consistentie, met andere woorden: tot het vermijden van een contradictio in terminis.

H.F.H. Reuvers,   Eindhoven, 18 januari 1977.

Errata

On page	(after) formula	stands	which should be
8	1.6.12	and t_i	and nonnegative integers t_i
12	1.8.2	positive	nonnegative
18	2.1.9	$t_i \in \mathbb{N}$	$t_i \in \mathbb{N}_0$
20	2.2.7	in general	in "most" of the cases
30	3.2	$p_1^{s_1} \cdots p^{s_\ell}$	$p_1^{s_1} \cdots p_\ell^{s_\ell}$
30	3.2.1	$p_1^{k+\alpha_1} \cdots p^{k+\alpha_\ell}$	$p_1^{k+\alpha_1} \cdots p_\ell^{k+\alpha_\ell}$
34	3.5.2	positive	nonnegative
37	3.6	$q \leq 30$	$q < 30$
39	3.6.9	positive	positive or nonnegative
43	3.6.40	(mod 27)	(mod 7)
83	5.2.1	with integral zeros	with four integral zeros
117	H. 5	$3t \leq k \leq$	$3 \leq k \leq 40.000$
118	H. 3	be integral	be integral if $q = 2s^2$

The pages 117 and 118 should be read in reversed order.