Codes and designs

CODES AND DESIGNS

J.H. van Lint

Department of Mathematics, Technological University, Eindhoven, Netherlands

1. INTRODUCTION

We denote by $V(n,q)$ the set of all n-tuples from a q-symbol alphabet $\mathbb{F}$ (i.e. $V(n,q) = \mathbb{F}^n$). If q is a prime power we take $\mathbb{F} = \mathbb{F}_q$ and interpret $V(n,q)$ as n-dimensional vector space over $\mathbb{F}_q$. In any case we distinguish an element of $\mathbb{F}$ and denote it by 0. The elements of $V(n,q)$ are called *words* (or vectors) and are denoted by underlined symbols. The word $(0,0,\ldots,0)$ is denoted by $\underline{0}$. The (Hamming) *distance* $d(\underline{x},\underline{y})$ of two words $\underline{x}$ and $\underline{y}$ is defined by

$$d(\underline{x},\underline{y}) := \#\{i \mid 1 \le i \le n,\ x_i \neq y_i\}\ .$$

The *weight* $w(\underline{x})$ of the word $\underline{x}$ is $d(\underline{x},\underline{0})$. A subset C of $V(n,q)$ is called a *code*. We say that C is e-*error-correcting* if $d(\underline{x},\underline{y}) \ge 2e + 1$ for all pairs $\underline{x} \in C$, $\underline{y} \in C$, with $\underline{x} \neq \underline{y}$. The minimum distance of C, defined by $d := \min\{d(\underline{x},\underline{y}) \mid \underline{x} \in C,\ \underline{y} \in C,\ \underline{x} \neq \underline{y}\}$ determines the error correcting capability $e := \lfloor \frac{d-1}{2} \rfloor$ of the code. The set $S_e(\underline{x}) := \{\underline{y} \in V(n,q) \mid d(\underline{x},\underline{y}) \le e\}$ is called the sphere of radius e around $\underline{x}$. If the set of spheres $S_e(\underline{c})$, where $\underline{c}$ runs through C, forms a partition of $V(n,q)$ then C is called a *perfect code*.

The following numbers play an important role in our investigations:

$$B(\underline{x},k) := \#\{\underline{c} \in C \mid d(\underline{x},\underline{c}) = k\} \qquad (1.1)$$

for $\underline{x} \in V(n,q)$, $0 \le k \le n$, i.e. $B(\underline{x},k)$ is the number of code words at distance k from $\underline{x}$. The distance of $\underline{x}$ and C is defined by

$$\rho(\underline{x}) := \min\{k \mid 0 \le k \le n,\ B(\underline{x},k) \neq 0\} . \qquad (1.2)$$

In recent years many designs (i.e. t-designs; cf. (2.3)) have been found by considering the words of fixed weight in some special (often linear) code. Well known examples of such codes are the perfect codes (Hamming codes, Golay codes). The codes which have the property display a high degree of regularity. This has led to a number of definitions of classes of codes which could possibly yield unknown designs. One of these is the class of *uniformly packed* codes. These codes were introduced in 1971 by N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev [9]. A few examples and elementary results were given by this author at the previous Advanced Study Institute on Combinatorics in 1974 (cf. [7]). The definition was then generalized and most of the theory necessary to understand these codes was given by J.M. Goethals and H.C.A. van Tilborg in 1975 [6]. In his thesis which appeared a few months ago, H.C.A. van Tilborg [12] gave an extensive treatment of the theory, many examples, but most important of all a proof that if q is a prime power and $e \ge 4$ then such codes do not exist! The main purpose of this paper is to give the reader some idea of these most recent results. For details the reader is referred to [12].

2. REGULAR CODES AND DESIGNS

(2.1) DEFINITION. A code is called *t-regular* if for all $\underline{x} \in V(n,q)$ with $\rho(\underline{x}) \le t$ and for all k ($0 \le k \le n$) the number $B(\underline{x},k)$ depends only on $\rho(\underline{x})$ and k. If in this definition t is maximal then we call the code *completely regular*.

We shall say that a vector $\underline{x} \in V(n,q)$ is *covered* by a vector $\underline{y} \in V(n,q)$ if for every nonzero coordinate x_i we have $x_i = y_i$.

(2.2) DEFINITION. A q-ary $t-(n,k,\lambda)$ *design* is a collection S of vectors of weight k in $V(n,q)$ with the property that every vector $\underline{x} \in V(n,q)$ of weight t is covered by exactly λ vectors $\underline{y} \in S$.

(2.3) LEMMA. If S is a q-ary $t-(n,k,\lambda)$ design then

i) S is also a q-ary $i-(n,k,\lambda_i)$ design for $0 \le i \le t-1$, where

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

ii) If $w(\underline{x}) = i$ and we consider j zero coordinates of $\underline{x}$ where $i+j \le t$ then the number of vectors $\underline{y} \in S$ which cover $\underline{x}$ and which also have zero coordinates at the j prescribed positions depends only on i and j.

PROOF.

i) Let $\underline{x} \in V(n,q)$, $w(\underline{x}) = i$. Then $\underline{x}$ is covered by $\binom{n-i}{t-i}(q-1)^{t-i}$ vectors $\underline{x}'$ of weight t. Each of these vectors $\underline{x}'$ is covered by exactly λ vectors $\underline{y}$ in S. For each vector $\underline{y} \in S$ which covers $\underline{x}$ there are $\binom{k-i}{t-i}$ vectors $\underline{x}'$ of weight t which cover $\underline{x}$ and which are covered by $\underline{y}$.

ii) This follows from i) by a straightforward inclusion-exclusion argument. □

The connection between design theory and coding theory is now established by the following theorem.

(2.5) THEOREM. Let C be a t-regular code with $\underline{0} \in C$. Let the minimum distance d of C satisfy $d \geq 2t$. Then for each k $(0 \leq k \leq n)$ the collection of code words of weight k is a q-ary t-design.

PROOF. The proof is by induction. First consider k = d. Let $\underline{x} \in V(n,q)$, $w(\underline{x}) = t$. Since $d \geq 2t$ we have $\rho(\underline{x}) = t$ by the triangle inequality. Now the regularity of C implies that $B(\underline{x}, d-t)$ is independent of $\underline{x}$. Again using the triangle inequality we see that $\underline{c} \in C$ and $d(\underline{x},\underline{c}) = d - t$ iff $w(\underline{c}) = d$ and $\underline{c}$ covers $\underline{x}$. Therefore the words of weight d form a q-ary $t-(n,d,\lambda(d))$ design for some $\lambda(d)$.

Now assume that the theorem has been proved for all $k < w$. Then by lemma 2.3ii) there are numbers $a(k,\ell)$, $(d \leq k < w,\ 0 \leq \ell \leq n)$ such that for any $\underline{x} \in V(n,q)$ with $w(\underline{x}) = t$ exactly $a(k,\ell)$ code words of weight k have distance ℓ to $\underline{x}$. It follows that the number of code words of weight $< w$ with distance $w - t$ to $\underline{x}$ does not depend on the choice of $\underline{x}$. Since we also know that $B(\underline{x}, w-t)$ is independent of the choice of $\underline{x}$ the result again follows from the triangle inequality for Hamming distance. □

3. RECENT RESULTS ON PERFECT CODES

Since perfect codes are completely regular they yield interesting designs and in fact the known non-trivial perfect codes are connected to even nicer designs than theorem 2.5 promises. It has been known for some years that if q is a prime power then there are no unknown perfect codes. The situation for other q is still far from being completely understood. We shall briefly report on the state of affairs at present. We consider perfect codes in V(n,q) with $d = 2e + 1$.

i) For e = 1 and e = 2 there are some isolated results. The situation is not understood at all.

ii) The case $e \geq 2$, $q = 2^a 3^b$ was settled in 1975 by L.A. Bassaligo, V.A. Zinoviev, V.K. Leontiev and N.I. Feldman [2].

iii) $e \geq 3$, $q = p_1^r p_2^s$ was settled recently by A. Tietäväinen [11].

iv) $3 \leq e \leq 5$, q arbitrary was settled by H.F. Reuvers [8]. He also has some results concerning $e = 2$ and $q = p_1^r p_2^s$ but the problem seems very hard.

v) E. Bannai [1] has just shown that for each $e \geq 3$ there are at most finitely many unknown perfect codes.

In all the cases above no unknown perfect code turned up and hence the results are negative for those readers interested in t-designs.

4. UNIFORMLY PACKED CODES

We now consider a class of codes which in some sense are one step away from being perfect. For the code C in V(n,q) we shall now require that it is e-error-correcting, that every $\underline{x}$ has $\rho(x) \leq e + 1$, and that it is completely regular. We first need a lemma.

(4.1) LEMMA. Let C be an e-error-correcting code in V(n,q). Then for any $\underline{x} \in V(n,q)$ we have

$$\text{i)} \quad \rho(\underline{x}) = e \quad \Rightarrow B(\underline{x}, e+1) \leq \frac{(n-e)(q-1)}{e+1},$$

$$\text{ii)} \quad \rho(\underline{x}) = e+1 \Rightarrow B(\underline{x}, e+1) \leq \frac{n(q-1)}{e+1}.$$

PROOF.

i) Assume w.l.o.g. that $\underline{x} = 0$ and that the code word $\underline{c}$ has $w(\underline{c}) = e$. Then a code word with weight $e+1$ must have 0's in the nonzero positions of $\underline{c}$. Furthermore two such code words cannot have the same nonzero coordinate in the same position. The result follows by double counting.

ii) The proof is analogous. □

(4.2) DEFINITION. An e-error-correcting code C in V(n,q) is called *uniformly packed* with parameters λ and μ, iff for all $\underline{x} \in V(n,q)$

$$\rho(\underline{x}) = e \quad \Rightarrow B(\underline{x}, e+1) = \lambda \ ,$$

$$\rho(\underline{x}) = e+1 \Rightarrow B(\underline{x}, e+1) = \mu \ ,$$

where $\lambda < \dfrac{(n-e)(q-1)}{e+1}$, $\mu \geq 1$.

Clearly the definition implies that $\rho(\underline{x}) \leq e+1$ for all $\underline{x}$. The conditions of (4.2) uniquely determine the number of code words.

(4.3) THEOREM. Let C be an e-error-correcting uniformly packed code in V(n,q) with parameters λ and μ. Then

$$|C|\{\sum_{i=0}^{e-1} \binom{n}{i}(q-1)^i + (1-\frac{\lambda}{\mu})\binom{n}{e}(q-1)^e + \frac{1}{\mu}\binom{n}{e+1}(q-1)^{e+1}\} = q^n. \quad (4.4)$$

PROOF. The result follows immediately form (4.2) if we count the number of pairs $(\underline{x},\underline{c})$ with $\underline{c} \in C$ and $e \leq d(\underline{x},\underline{c}) \leq e+1$ in two ways.

□

Note that if we take $\lambda = \dfrac{(n-e)(q-1)}{e+1}$ then (4.4) implies that C is perfect. This is why we have excluded this possibility in (4.2). Except for the extended Golay code all known uniformly packed codes have e = 1 or e = 2 (cf. the tables in [6] and [12]). The reader interested in examples is referred to chapter 4 of [12]. Many of the more interesting examples are based on the following theorem which can be proved using the group algebra approach to coding. This would take too along to explain here so we just state the theorem.

(4.5) THEOREM. Let C be an e-error-correcting linear code. Then C is uniformly packed iff in the dual code $C^{\perp}$ exactly e + 1 nonzero weights occur.

In [4] Delsarte considered n-subsets S of the set of points of a (k - 1)-dimensional projective space PG(k - 1,q), having the property that the intersection of S with any hyperplane consists of $n - w_1$ or $n - w_2$ points. Many such sets S are known. Using such a set S one immediately finds a linear code of length n and dimension k over $\mathbb{F}_q$ having the two weights w_1 and w_2 by considering the characteristic functions of hyperplanes in the space and restricting to S. Delsarte called these codes *two weight projective codes*. By theorem 4.5 the dual of such a code is uniformly packed with e = 1. So in this case the codes are constructed using known combinatorial designs.

5. GENERALIZATION OF LLOYD'S THEOREM TO UNIFORMLY PACKED CODES

In the case where q is a power of a prime the group-algebra methods of [6] and [12] led to a generalization of Lloyd's theorem for perfect codes. Recently D.M. Cvetković and J.H. van Lint [3] gave a simple proof of Lloyd's theorem. We shall now show that the same method can be used to prove the generalization to uniformly packed codes for all q. In order to state the theorem we first need a few definitions.

(5.1) DEFINITION. The *Krawtchouk polynomial* K_k is defined by

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

The polynomial ψ_e defined by

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

is called Lloyd's polynomial of degree e.

Several recurrence relations for Krawtchouk polynomials are known (cf. [10], [5] (4.11)). From these we find

$$(e+1)\psi_{e+1}(n,x) = \{e + (q-1)(n-e) - qx + 1\}\psi_e(n,x) - \\ + (q-1)(n-e)\psi_{e-1}(n,x) \ . \tag{5.2}$$

The theorem which we wish to prove now follows.

(5.3) THEOREM. Let C be an e-error-correcting uniformly packed code with parameters λ and μ. Then the polynomial $Q(x)$ defined by

$$\mu Q(x) := \psi_{e+1}(n,x) + (\mu - \lambda - 1)\psi_e(n,x) + \\ + \lambda\psi_{e-1}(n,x) \tag{5.3}$$

has $e+1$ distinct integral zeros in the interval $[1,n]$.

The fact that these zeros are distinct follows from well known properties of Krawtchouk polynomials. The interesting fact and the basis of the known non-existence theorems is that the zeros are integers. The proof of theorem 5.3 is based on the following more or less trivial lemma.

(5.5) LEMMA. Let A be a matrix of size m by m which has the form

$$A = \begin{pmatrix} A_{00} & A_{01} & \cdots & A_{0k} \\ A_{10} & A_{11} & \cdots & A_{1k} \\ & & & \\ A_{k0} & A_{k1} & \cdots & A_{kk} \end{pmatrix}$$

where A_{ij} has size m_i by m_j $(i = 0,1,\ldots,k;$ $j = 0,1,\ldots,k)$.

Suppose that for each i and j the matrix A_{ij} has constant row sums with sum b_{ij}. Let the matrix B have entries b_{ij}. Then each eigenvalue of B is also an eigenvalue of A.

PROOF. Let $B\underline{x} = \lambda\underline{x}$, where $\underline{x} = (x_0, x_1, \ldots, x_k)^T$. Define $\underline{y}$ by

$$\underline{y}^T := (x_0, x_0, \ldots, x_0, x_1, x_1, \ldots, x_1, \ldots, x_k, x_k, \ldots, x_k)$$

where each x_i is repeated m_i times. By definition of B it is obvious that $A\underline{y} = \lambda\underline{y}$. □

(5.6) DEFINITION. The square matrix A_n of size q^n is defined as follows. Rows and columns are indexed by the elements of $V(n,q)$ and $A(\underline{x},\underline{y}) = 1$ if $d(\underline{x},\underline{y}) = 1$, $A(\underline{x},\underline{y}) = 0$ otherwise.

From the definition of A_n we see that

$$A_{n+1} = I_q \times (A_n - I_{q^n}) + J_q \times I_{q^n}, \tag{5.7}$$

where I_m denotes the identity matrix of size m, J_m the all one matrix of size m and $\times$ indicates the Kronecker product.

(5.8) LEMMA. The matrix A_n has the eigenvalues

$$-n + jq \quad (j = 0, 1, \ldots, n)$$

with multiplicities $\binom{n}{j}(q-1)^j$.

PROOF. The proof is by induction. For $n = 1$ we have $A_1 = J_q - I_q$ and then the assertion is well known. Suppose $A_n\underline{x} = \lambda\underline{x}$. Let

$$\underline{x}' := (c_1\underline{x}^T, c_2\underline{x}^T, \ldots, c_q\underline{x}^T)^T,$$

where $c_1 + c_2 + \ldots + c_q = 0$. Then by (5.7) $A_{n+1}\underline{x}' = (\lambda - 1)\underline{x}'$. On the other hand, if we take $c_1 = c_2 = \ldots = c_q = 1$ then by (5.7) we

find $A_{n+1}\underline{x}^t = (\lambda + q - 1)\underline{x}^t$. The result now follows from well known addition properties of binomial coefficients. []

Now we assume that C is a uniformly packed code in V(n,q) with parameters λ and μ. We reorder the rows and columns of A_n in such a way that those indexed by an element of C come first, then the rows and columns indexed by elements of V(n,q) with distance 1 to the code, etc. Then A_n has the form of the matrix A in lemma 5.5 with $k = e + 1$ and where A_{ij} has rows (resp. columns) indexed by the elements of V(n,q) with distance i (resp. j) to C. We find (writing $q - 1 =: s$)

$$B = \begin{pmatrix} 0 & ns & 0 & & & 0 \\ 1 & q-2 & (n-1)s & 0 & & \\ 0 & 2 & 2(q-2) & (n-2)s & & \\ & 0 & & & & \\ & & & e-1 & (e-1)(q-2) & (n-e+1)s \\ & & & & e & e(q-2)+\lambda(e+1) \\ 0 & & & & 0 & \mu(e+1) \end{pmatrix} \quad (5.9)$$

We now have to determine the eigenvalues of the tridiagonal matrix B. This is done with the same method which was used in [3].

(5.10) DEFINITION. The matrix $Q_e = Q_e(a,b,s)$ is the tridiagonal matrix given by

$$Q_e(a,b,s) := \begin{pmatrix} a & 0 & 0 & 0 & & 0 \\ 1 & a+(s-1) & b-s & 0 & & 0 \\ 0 & 2 & a+2(s-1) & b-2s & 0 & 0 \\ 0 & 0 & & & & \\ & & & & & b-(e-1)s \\ 0 & & & 0 & e & a+e(s-1) \end{pmatrix}.$$

Furthermore we define

$$P_e = P_e(a,b,s) := \left(\begin{array}{c|c} Q_{e-1}(a,b,s) & \begin{matrix}1\\1\end{matrix} \\ \hline 0\ 0\ \ldots\ 0\ e & 1 \end{array}\right) .$$

The determinants of these matrices are denoted by $\bar{Q}_e$, resp. $\bar{P}_e$.

Developing by the last row we find from (5.10)

$$\bar{Q}_e = (a + e(s-1))\bar{Q}_{e-1} - e(b-(e-1)s)\bar{Q}_{e-2} . \tag{5.11}$$

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

$$\bar{Q}_e = (a+es)\bar{Q}_{e-1} - e(a+b)\bar{P}_{e-1} . \tag{5.12}$$

Developing P_e by the last row yields

$$\bar{P}_e = \bar{Q}_{e-1} - e\bar{P}_{e-1} . \tag{5.13}$$

Now apply (5.13) with $e+1$ instead of e, combine with (5.13) and eliminate the $\bar{Q}$-terms using (5.12). This yields

$$\bar{P}_{e+1} = (a+es-e-1)\bar{P}_e - e(b-es)\bar{P}_{e-1} . \tag{5.14}$$

(5.15) LEMMA. Let $s := q-1$. Then we have

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

PROOF. For $e = 1$ and $e = 2$ the assertions can be checked directly from the definitions. By substitution of the appropriate values of a and b in (5.14) and using (5.2) we see that the polynomials on both sides in the lemma satisfy the same recurrence relation. □

Now consider the matrix B of (5.9). We shall calculate

$$\prod_{i=1}^{e+1} (x_i - 1) = \frac{(q-1)^{e-1}}{q^{e+1}}(n-1)(n-2)\ldots(n-e+1)p_2(n) \quad , \quad (6.4)$$

where

$$p_2(n) = (n-e)(n-e-1)(q-1)^2 +$$

$$+ (\mu - \lambda - 1)(n-e)(e+1)(q-1) + \lambda e(e+1) \quad .$$

These expressions are obtained easily by calculating a few of the coefficients of $Q(x)$ and $Q(1)$. In a similar way (calculating one more coefficient) an expression for $\sum_{i<j} (x_i - x_j)^2$ can be obtained which then gives an upper bound for the difference between the smallest and largest zero. (This bound has shortened the nonexistence proofs for perfect codes considerably).

Since the Krawtchouk polynomials are orthogonal polynomials the familiar theorems on interlacing of zeros can be used. Let $a_1 < a_2 < \ldots < a_e$ be the zeros of $\psi_e(n,x)$ and let $b_1 < b_2 < \ldots < b_{e+1}$ be the zeros of $\psi_{e+1}(n,x)$. One can then show that

$$0 < x_1 < a_1 < x_2 < a_2 < \ldots < a_e < x_{e+1} \quad , \quad (6.5)$$

$$x_{e+1} \leq n \text{ iff } \mu - \lambda - 1 \leq \frac{n-e-1}{e+1} + \frac{\lambda e}{n-e} \quad , \quad (6.6)$$

Furthermore, at least e zeros of $Q(x)$ are in the interval (b_1, b_{e+1}) and the method described above gives the following upper bound for $b_{e+1} - b_e$.

$$f := f(n,q,e) := q(b_{e+1} - b_1) \leq$$

$$\leq \sqrt{\frac{e(e+1)}{6}\{12n(q-1) + (e+2)q^2 - 12(q-1)(e+1)\}} \quad . \quad (6.7)$$

The essential idea of the proof is to derive a lower bound for n and an upper bound for n such that these bounds yield a contradiction for all but finitely many parameter sets n,q,e.

(6.8) LEMMA. If an e-error-correcting, uniformly packed code exists in V(n,q), then

$$n \geq \begin{cases} q^{\frac{e+1}{6}} & \text{for } e \geq 5,\ q \neq 2\ , \\ q.2^{-1/3} & \text{for } e = 4,\ q \neq 2\ , \\ 2^{\frac{e+7}{7}} & \text{for } q = 2\ . \end{cases} \tag{6.9}$$

PROOF. The proof is based on (6.4). In the proof we shall use the following notation

$$k = T(k).p^{ex(k)}, \quad \text{where } (T(k),p) = 1\ . \tag{6.10}$$

Let $\ell := \max\{ex(n-k) \mid k = 1,2,\ldots,e-1\}$. We have

$$c := ex((n-1)(n-2)\ldots(n-e+1)) \leq \ell + \frac{e-3}{p-1}\ ,$$

so

$$n \geq p^{\ell} \geq p^{c-\frac{e-3}{p-1}}\ .$$

Let $b := ex(p_2(n))$. From (6.6) it follows that $p_2(n) < q^2n^2$, i.e. $n \geq p^{\frac{b-2a}{2}}$. These two lower bounds for n, combined with the fact that $b + c \geq a(e+1)$, which follows from (6.4), and a few simple calculations establish the first inequality of the lemma. The others are proved in a similar way. □

If $y_1,y_2,\ldots,y_k$ are distinct integers in the interval $[1,A]$ and we assume that they are divisible by the highest possible powers of p a simple counting argument shows that

$$p^{ex(y_1y_2\ldots y_k)} \leq p^{\frac{k-1}{p-1}}\left(\frac{A}{k}\right)^k\ .$$

A similar result holds if $y_1, y_2, \ldots, y_k$ are in an interval $(t, t+A]$ if we exclude one of the integers y_i which could possibly be divisible by a very high power of p.

We now come to the crucial part of the proof, i.e. the upper bound on n. Renumber the zeros of Q(x) in such a way that $x_1, x_2, \ldots, x_e$ are in (b_1, b_{e+1}) and $ex(x_1) \leq ex(x_2) \leq \ldots \leq ex(x_e)$. Then by (6.11) and (6.7) we have

$$p^{ex(x_1 x_2 \ldots x_{e-1})} \leq p^{\frac{e-2}{p-1}} \left(\frac{f}{q(e-1)}\right)^{e-1} .$$

Since b_{e+1} is larger than the largest zero of $\psi_2(n,x)$, which exceeds $\frac{(q-1)n}{q}$, we have

$$x_i \geq \frac{(q-1)n}{q} - (b_{e+1} - b_1) = \frac{(q-1)n - f}{q}, \quad (1 \leq i \leq e) .$$

Combining the last two inequalities we find a lower bound for $T(x_1, x_2, \ldots, x_{e+1})$. However, from (6.3) and (4.4) we find

$$T(x_1, x_2, \ldots, x_{e+1}) = T\left(\frac{(e+1)!\, q^{n-e-1}}{|C|}\right) .$$

Combining these results leads to an inequality

$$L(n,q,e) \leq R(n,q,e)$$

where, if n is as large as lemma 6.8 insures it should be, $L(n,q,e)$ behaves roughly like $(qn)^{\frac{e-1}{2}}$ and $R(n,q,e)$ behaves like $n(q-1)(e+1)!$ Clearly for $e \geq 4$ this yields a contradiction for sufficiently large n. In fact, a more detailed analysis showed that only a few thousand parameter sets n,e,q were possible. These were handled by computer. The most useful element in the program was the fact that the necessary conditions for the existence of t-designs (in (2.4) λ_i must be an integer) had to be satisfied. Attempts to modify the proof in such a way that e = 3 could also be treated were succesful for q = 2 only. The extended Golay code

turned out to be the only possibility.
The possibility of the existence of some 3-error-correcting uniformly packed codes with $q > 2$ remains open but it seems doubtful whether they exist.

REFERENCES

1. E. Bannai, On perfect codes in the Hamming schemes $H(n,q)$ with q arbitrary (submitted).
2. L.A. Bassalygo, V.A. Zinoviev, V.K. Leontiev and N.I. Feldman, Nonexistence of perfect codes over some alphabets (in russian), Problemy Peredachi Informatsii 11 (1975), 3-13.
3. D.M. Cvetković and J.H. van Lint, An elementary proof of Lloyd's theorem, Proc. Kon. Ned. Akad. v. Wet. (to appear).
4. P. Delsarte, Two-weight linear codes and strongly regular normed spaces, Discr. Math. 3 (1972), 47-64.
5. ---------, An algebraic Approach to the Association Schemes of Coding Theory, Philips Res. Repts. Suppl. 10 (1973).
6. J.M. Goethals and H.C.A. van Tilborg, Uniformly packed codes, Philips Res. Repts. 30 (1975), 9-36.
7. J.H. van Lint, Recent results on perfect codes and related topics, in Combinatorics I (M. Hall and J.H. van Lint eds.), Math. Centre Tracts 55 (1974).
8. H.F. Reuvers, Some nonexistence theorems for perfect error correcting codes, Thesis, Technological University Eindhoven (1977).
9. N.V. Semakov, V.A. Zinoviev and G.V. Zaitsev, Uniformly packed codes, Problemy Peredachi Informatsii 7 (1971), 38-50.
10. G. Szegö, Orthogonal polynomials, Amer. Math. Soc. Coll. Publ. 23 (1959).
11. A. Tietäväinen, Nonexistence of nontrivial perfect codes in case $q = p_1^r p_2^s$, $e \geq 3$, Discrete Math. (to appear).
12. H.C.A. van Tilborg, Uniformly packed codes, Thesis, Technological University Eindhoven, (1976).