Binary uniformly packed codes

EINDHOVEN UNIVERSITY OF TECHNOLOGY

Department of Mathematics

Memorandum 1975-12

October 1975

Binary Uniformly Packed Codes

by

H.C.A. van Tilborg

University of Technology
Department of Mathematics
PO Box 513, Eindhoven
The Netherlands

§ 1. Introduction

It will be shown in this paper that uniformly packed, binary codes, with $e \geq 3$, do not exist except for the extended Golay code of length 24. For $e = 1$ and 2 there are infinite sequences of uniformly packed codes known (see [2], tables I and II).

§ 2. Notations and definitions

C a code in a binary vectorspace V,

n length of the code (= dimension of V),

d minimum distance of C (= $\min\{d(\underline{c}_1,\underline{c}_2) \mid \underline{c}_1 \in C, \underline{c}_2 \in C, \underline{c}_1 \neq \underline{c}_2\}$),

e error correcting capability (= $[\frac{d-1}{2}]$),

C_k $:= \{\underline{x} \in V \mid d(\underline{x},C) = k\}$, $0 \leq k \leq n$,

$B(\underline{x},i)$ $:= |\{\underline{c} \in C \mid d(\underline{x},\underline{c}) = i\}|$, $\underline{x} \in V$, $0 \leq i \leq n$,

$\rho(\underline{x})$ $:= \min\{k \mid B(\underline{x},k) \neq 0\}$, $\underline{x} \in V$.

A code C is called *uniformly packed* with parameters (λ,μ) if for all $\underline{x} \in V$ with $\rho(\underline{x}) \geq e$ the following holds: either

(2.1) $B(\underline{x},e) = 1$ and $B(\underline{x},e+1) = \lambda$, or $B(\underline{x},e) = 0$ and $B(\underline{x},e+1) = \mu$.

(2.2) $$P_k^{(n)}(x) := \sum_{i=0}^{k} (-2)^i \binom{n-i}{k-i}\binom{x}{i} = \sum_{i=0}^{k} (-1)^i \binom{x}{i}\binom{n-x}{k-i}$$ Krawtchouk polynomials.

B_j characteristic numbers of the code C, $0 \leq j \leq n$, (see [2]),

$N(C)$ $:= \{j \mid 1 \leq j \leq n, B_j \neq 0\}$,

$F_C(x)$ *characteristic polynomial of* C defined by

(2.3) $$\frac{2^n}{|C|} \prod_{j \in N(C)} \left(1 - \frac{x}{j}\right).$$

r *external distance* of C := degree of $F_C(x)$,

α_i $(i = 0,1,\ldots,r)$ defined by $F_C(x) = \sum_{k=0}^{r} \alpha_k P_k^{(n)}(x)$.

§ 3. Known results

Lemma 3.1. For every code C one has

$$(3.1) \qquad \forall_{\underline{x} \in V} \left[\sum_{k=0}^{r} \alpha_k B(\underline{x},k) = 1 \right] .$$

Proof. [2], corollary 1.1, page 7. □

Theorem 3.2. (Lloyd). C is uniformly packed with parameters (λ,μ) iff

$$(3.2) \qquad F_C(x) = \sum_{k=0}^{e-1} P_k^{(n)}(x) + \left(1 - \frac{\lambda}{\mu}\right) P_e^{(n)}(\lambda) + \frac{1}{\mu} P_{e+1}^{(n)}(x) .$$

Proof. [2], theorem 12, page 17. □

Corollary 3.3. Necessary conditions for the existence of a uniformly packed code with parameters (λ,μ) are

$$(3.3) \text{ i)} \quad |C| \left\{ \sum_{k=0}^{e-1} \binom{n}{k} + \left(1 - \frac{\lambda}{\mu}\right) \binom{n}{e} + \frac{1}{\mu} \binom{n}{e+1} \right\} = 2^n$$

$$(3.4) \text{ ii)} \quad Q(x) := \sum_{k=0}^{e-1} P_k^{(n)}(x) + \left(1 - \frac{\lambda}{\mu}\right) P_e^{(n)}(x) + \frac{1}{\mu} P_{e+1}^{(n)}(x)$$

has $e+1$ distinct integer zeros in $[1,n]$.

Proof. Substitution of $x = 0$ in (3.2) and (2.3) yields i), while ii) follows from (3.2) and the definition of $F_C(x)$ in (2.3). □

Theorem 3.5. For the parameters (λ,μ) of an uniformly packed code, the following inequalities hold

$$(3.5) \qquad 0 \le \lambda < \frac{n-e}{e+1} ,$$

$$(3.6) \qquad 1 \le \mu \le \frac{n+1}{e+1} .$$

Proof. See [2], page 20, formula (28) and (29). □

Lemma 3.7.

$$(3.7) \qquad \sum_{i=0}^{k} P_i^{(n)}(x) = P_k^{(n-1)}(x-1) .$$

Proof. See [3], corollary 5.4.18, page 110. □

§ 4. Side trip

The next theorem places this paper in the context in which it should be placed.

Theorem 4.1. Let C be an e-error correcting code. Then C is uniformly packed iff its external distance is $e+1$.

Proof. The implication to the right is covered by (3.2). So assumed that $r = e+1$. It follows from (3.1) that $\rho(\underline{x}) \le e+1$ for all $\underline{x} \in V$. Let $\underline{x} \in V$ with $\rho(\underline{x}) = e$, i.e. $B(\underline{x},0) = \ldots = B(\underline{x},e-1) = 0$ and $B(\underline{x},e) > 0$. Since $d \ge 2e+1$, it follows that $B(\underline{x},e) = 1$. Now (3.1) reads $\alpha_e + \alpha_{e+1}B(\underline{x},e+1) = 1$, i.e. $B(\underline{x},e+1)$ is constant (let us say λ, with $\alpha_e + \lambda\alpha_{e+1} = 1$). Let $\underline{x} \in V$ with $\rho(\underline{x}) > e$. Then it follows from $\rho(x) \le e+1$, that $\rho(\underline{x}) = e+1$, i.e. $B(\underline{x},0) = B(\underline{x},1) = \ldots = B(\underline{x},e) = 0$. Now (3.1) reads $\alpha_{e+1}B(\underline{x},e+1) = 1$, i.e. $B(\underline{x},e+1)$ is constant (let us say μ). The theorem follows from definition (2.1). □

§ 5. Basic tools

Let $Q(x)$ be defined as in (3.4). Using lemma (3.7) one can rewrite $Q(x)$ as

$$(5.1) \qquad \frac{1}{\mu}\{\mu P_e^{(n-1)}(x-1) + P_{e+1}^{(n)}(x) - \lambda P_e^{(n)}(x)\} .$$

Theorem 5.2. Let x_i, $i = 1,\ldots,e+1$ be the zeros of $Q(x)$ then

$$(5.2) \text{ i) } \sum_{i=1}^{e+1} x_i = \frac{(n+\mu-\lambda)(e+1)}{2} ,$$

$$(5.3) \text{ ii) } \sum_{1\le i<j\le e+1} x_i x_j = \frac{(e+1)e}{24}\{3n^2 + 3(2\mu-2\lambda-1)n + 6\mu + 2e - 2\} ,$$

$$(5.4)\ \text{iii)}\quad \sum_{1\le i<j\le e+1} (x_j - x_i)^2 = \frac{e(e+1)^2}{4}\{n + (\mu-\lambda)^2 - 2\mu - 2\,\frac{e-1}{3}\}$$

$$(5.5)\ \text{iv)}\quad \prod_{i=1}^{e+1} x_i = \frac{\mu(e+1)!}{2^{e+1}} \cdot \frac{2^n}{|C|} = \frac{\mu(e+1)!}{2^{e+1}}\{\sum_{i=0}^{e} \binom{n}{i} + \frac{1}{\mu}(\binom{n}{e+1} - \lambda\binom{n}{e})\}$$

$$(5.6)\ \text{v)}\ 2^{e+1}\sum_{i=1}^{e+1}(x_i - 1) = (n-1)(n-2)\ldots(n-e+1)\{n^2 - en + (e+1)(\mu-\lambda-2)n - e(e+1)(\mu-2\lambda-2)\}$$

$$(5.7)\ \text{vi)}\quad 2^{e+1}\sum_{i=1}^{e+1}(x_i - 2) = (n-2)(n-3)\ldots(n-e+1)\ \times$$

$$\times\ \{n(n-1)(n-e-\lambda-e\lambda) + (e+1)(n-1)((\mu-4)(n-e) + 4\lambda e) - 2e(e+1)((\mu-2)(n-e) + 2\lambda(e-1))\}\ .$$

Proof. Since the coefficient of x^{e+1} in $Q(x)$ equals $\frac{(-2)^{e+1}}{\mu(e+1)!}$ it follows that

$$(5.8)\qquad Q(x) = \frac{(-2)^{e+1}}{\mu(e+1)!}\prod_{i=1}^{e+1}(x - x_i)\ .$$

Now (5.2) and (5.3) are easily derivable by regarding the coefficients of x^{e+1} and x^e, resp. x^{e+1} and x^{e-1} in $Q(x)$, using of course the formulas (5.1) and (2.2). Now (5.4) is easily computed, since

$$\sum_{i<j}(x_i - x_j)^2 = e\sum_i x_i^2 - 2\sum_{i<j} x_i x_j\ .$$

The formulas (5.5), (5.6) and (5.7) follow directly, if one substitutes $x=0$, $x=1$ resp. $x=2$ in (5.1) and (5.8). □

It turns out that we need more information on the distribution of the zeros of $Q(x)$.
Since Krawtchouk polynomials (after the right normalization) belong to the classical polynomials ([4], section 2.82), we may apply the standard results in this theory.

Lemma 5.9. The zeros of $P_k^{(n)}(x)$ are real, distinct and located in the interior of $[1,n]$.

Proof. [4], theorem 3.3.1, page 44. □

Lemma 5.10. Let $u_1 < u_2 < \dots < u_k$ be the zeros of $P_k^{(n)}(x)$ and $v_1 < v_2 < \dots < v_{k+1}$ the zeros of $P_{k+1}^{(n)}(x)$. Then

$$1 < v_1 < u_1 < v_2 < u_2 < \dots < v_k < u_k < v_{k+1} < n \,.$$

Proof. [4], theorem 3.3.2, page 46. □

Lemma 5.11. The polynomials $P_k^{(n)}(x)$ satisfy the relation

$$(5.11) \qquad (k+1)P_{k+1}^{(n)}(x) = (n-2x)P_k^{(n)}(x) - (n-k+1)P_{k-1}^{(n)}(x) \,.$$

Proof. [1], formula (4.11), page 59. □

We remark that (5.10) follows from (5.11) and an induction argument.

Lemma 5.12. Let $u_1 < u_2 < \dots < u_k$ be the zeros of $P_k^{(n)}(x)$ then

$$(5.12) \qquad u_i + u_{k-i} = n, \quad i = 1,2,\dots,k \,.$$

Proof. From (2.2) it follows that $P_k^{(n)}(x) = (-1)^k P_k^{(n)}(n-x)$. □

The lemmas above enable us to prove a theorem, which turns out to be essential in this paper.

Theorem 5.13. Let $u_1 < u_2 < \dots < u_e$ be the zeros of $P_e^{(n-1)}(x-1)$, and $v_1 < v_2 < \dots < v_{e+1}$ the zeros of $P_{e+1}^{(n-1)}(x-1)$. Then

$$Q(x) = \sum_{k=0}^{e-1} P_k^{(n)}(x) + \left(1 - \frac{\lambda}{\mu}\right)P_e^{(n)}(x) + \frac{1}{\mu} P_{e+1}^{(n)}(x)$$

has distinct real zeros $x_1 < x_2 < \dots < x_{e+1}$, such that

i) $\quad 0 < x_1 < u_1 < x_2 < u_2 < \dots < x_e < u_e < x_{e+1} < n$

ii) $\quad x_1 > v_1 \qquad$ if $\mu - \lambda - 1 \ge 0$

$\quad x_{e+1} < v_{e+1} \qquad$ if $\mu - \lambda - 1 \le 0$.

Proof. By virtue of lemma (5.12), we rewrite Q(x)

$$Q(x) = \frac{1}{\mu}\{P_{e+1}^{(n-1)}(x-1) + (\mu-\lambda-1)P_e^{(n-1)}(x-1) + \lambda P_{e-1}^{(n-1)}(x-1)\} . \tag{5.14}$$

According to (5.11)

$$(e+1)P_{e+1}^{(n-1)}(u_i-1) = -(n-e)P_{e-1}^{(n-1)}(n_i-1) .$$

Hence

$$Q(u_i) = \frac{1}{\mu}\{P_{e+1}^{(n-1)}(u_i-1) + \lambda P_{e-1}^{(n-1)}(u_i-1)\} = \frac{1}{\mu}\{\lambda - \frac{n-e}{e+1}\}P_{e-1}^{(n-1)}(u_i-1).$$

Since $P_{e-1}^{(n-1)}(x)$ and $P_e^{(n-1)}(x)$ are both positive in $x = 0$, we can deduce from (5.10) that the sign of $P_{e-1}^{(n-1)}(u_i - 1)$ is $(-1)^{i+1}$ and consequently, by (3.5), that the sign of $Q(u_i)$ is $(-1)^i$. Moreover, since

$$Q(0) = \sum_{i=0}^{e} \binom{n}{i} + \frac{1}{\mu}(\binom{n}{e+1} - \lambda\binom{n}{e}) > 0$$

and

$$Q(n) = \frac{(-1)^{e+1}}{\mu}\{\binom{n}{e+1} + \lambda\binom{n}{e} - \binom{n}{e} + \binom{n}{e-1} - \ldots + (-1)^e\binom{n}{0}\} ,$$

i.e. the sign of Q(n) is $(-1)^{e+1}$, it follows that part i) of this theorem is proved.

Since, by lemma (5.10), $P_{e+1}^{(n-1)}(x-1)$, $P_e^{(n-1)}(x-1)$ and $P_{e-1}^{(n-1)}(x-1)$ are positive on $[0,v_1]$, $x_1 > v_1$ for $\mu - \lambda - 1 \geq 0$. Similarly these polynomials have sign $(-1)^{e+1}$, $(-1)^e$, resp. $(-1)^{e-1}$ on $[v_{e+1},n]$. Consequently, for $\mu - \lambda - 1 \leq 0$, Q(x) has sign $(-1)^{e+1}$ on $[v_{e+1},n]$, i.e. $x_{e+1} < v_{e+1}$. □

There is one more crucial theorem in this paper. In order to state this, we need a definition.

Definition 5.15. For any $n \in \mathbb{N}$, $A(n)$:= the largest odd factor of n, i.e. $n = A(n).2^{\ell}$ for some ℓ.

<u>Theorem 5.16.</u> Let C be a uniformly packed code with parameters (λ,μ). Then

$$(5.16)\ \text{i)}\quad \prod_{i=1}^{e+1} A(x_i) = \frac{A(\mu)A((e+1)!)}{A(|C|)}$$

$$(5.17)\ \text{ii)}\quad \prod_{i=1}^{e+1} A(x_i) \le A((e+1)!)\frac{n+1}{e+1} .$$

<u>Proof.</u> Statement (5.16) follows directly from the first equality in (5,5), while, in turn, it self implies (5.17), since

$$\frac{A(\mu)A((e+1)!)}{A(|C|)} \le A(\mu)A((e+1)!) \le \mu A((e+1)!) \le \frac{n+1}{e+1} A((e+1)!) ,$$

(here use (3.6)). □

<u>Lemma 5.18.</u> The zeros of $P_k^{(n)}(x)$ all lie in the interior of the interval

$$(5.19)\qquad \left[\frac{n - \sqrt{k(k-1)n/2}}{2} , \frac{n + \sqrt{k(k-1)n/2}}{2}\right] \quad \text{for } k \ge 2 .$$

<u>Proof.</u> Let $u_1 < u_2 < \ldots < u_k$ be the zeros of $P_k^{(n)}(x)$. Since $Q(x)$ in (5.1) equals $P_{e+1}^{(n-1)}(x-1)$ for $\lambda = 0$, $\mu = 1$, we deduce from (5.4), after replacing $e+1$ by k and $n-1$ by n, that

$$\sum_{1\le i<j\le k} (u_j - u_i)^2 = \frac{(k-1)k^2}{4}\{n - \frac{2(k-2)}{3}\} .$$

Now

$$\sum_{1\le i<j\le k} (u_j - u_i)^2 = (u_k - u_1)^2 + \sum_{i=2}^{k-1} \{(u_k - u_i)^2 + (u_i - u_1)^2\} +$$

$$\sum_{2\le i<j\le k-1} (u_j - u_j)^2 \ge (u_k - u_1)^2 + (k-2)\{(u_k - \frac{u_k + u_1}{2})^2 + (\frac{u_k + u_1}{2} - u_1)^2\}$$

$$+ 0 = \frac{k}{2}(u_k - u_1)^2 .$$

Hence

$$(u_k - u_1)^2 \le \frac{k(k-1)}{2}\{n - \frac{2(k-2)}{3}\} < \frac{k(k-1)n}{2} .$$

The lemma now follows from the observation that $u_1 + u_k = n$ (by (5.12)). □

Lemma 5.19. Let $f < m$ be integers. Consider f distinct integers z_i, $i = 1,2,\ldots,f$. Let $F(m,f)$ be the product of the powers of 2 in these numbers. Then

$$(5.19) \qquad F(m,f) \le \tfrac{1}{2}\left(\frac{2m}{f}\right)^f .$$

Proof. Let $\alpha := \lceil {}^2\log \frac{m}{f} \rceil$ and $\frac{m}{f} = 2^{\alpha-\theta}$, $0 \le \theta < 1$, (here $\lceil x \rceil$ denotes the smallest integer k such that $k \ge x$). These are exactly ℓ multiples of 2^α, which are at less then or equal to m, where $\ell = \lfloor \frac{m}{2^\alpha} \rfloor \le \frac{f}{2^\theta}$.
$F(m,f)$ is maximal if one takes for $z_1,z_2,\ldots,z_f$ these ℓ multiples of 2^α and $f-\ell$ multiples of $2^{\alpha-1}$. Hence

$$ {}^2\log F(m,f) \le (f-\ell)(\alpha-1) + \ell\alpha + \lfloor \tfrac{\ell}{2} \rfloor + \lfloor \tfrac{\ell}{4} \rfloor + \ldots \le $$

$$ f(\alpha-1) + 2\ell - 1 \le f(\alpha - 1 + 2^{1-\theta}) - 1 \le f(\alpha - \theta + 1) - 1 $$

(since $2^x - x \le 1$ for $0 \le x \le 1$). □

§ 6. Main theorem

Theorem 6.1. There are no uniformly packed codes for $e \ge 3$ except for the extended Golay of length 24.

Proof A. Upper bounds on n for $e \ge 4$. According to theorem (5.13) there are at least e roots of $Q(x)$ in the interval (v_1, v_{e+1}), where v_1 and v_{e+1} are the smallest, resp. largest, zero of $P^{(n-1)}_{e+1}(x-1)$. According to (5.18) this implies that all these zeros lie in

$$(6.2) \qquad \left[\frac{n+1-\sqrt{\frac{e(e+1)(n-1)}{2}}}{2}, \frac{n+1+\sqrt{\frac{e(e+1)(n-1)}{2}}}{2}\right].$$

Let α_i be defined by $x_i = A(x_i)2^{\alpha_i}$.
We renumber the zeros x_i as $y_1,y_2,\ldots,y_{e+1}$, in such a way that $y_1,\ldots,y_e$ are all in the interval given by (6.2) and that $\alpha_1 \le \alpha_2 \le \ldots \le \alpha_e$.

By lemma (5.19)

(6.3) $$A(y_1.y_2.\cdots.y_{e-1}) = \frac{y_1.y_2.\cdots.y_{e-1}}{2^{\alpha_1+\alpha_2+\cdots+\alpha_{e-1}}} \geq \frac{\left[\dfrac{n+1-\sqrt{\frac{e(e+1)(n-1)}{2}}}{2}\right]^{e-1}}{F\left(\sqrt{\frac{e(e+1)(n-1)}{2}},\ e-1\right)} \geq$$

$$\geq 2\left(\frac{e-1}{4}\right)^{e-1}\left[\frac{n+1-\sqrt{\frac{e(e+1)(n-1)}{2}}}{\sqrt{\frac{e(e+1)(n-1)}{2}}}\right]^{e-1} .$$

Substituting (6.3) in (5.17) results in

(6.4) $$2\left(\frac{e-1}{4}\right)^{e-1}\left[\frac{n+1-\sqrt{\frac{e(e+1)(n-1)}{2}}}{\sqrt{\frac{e(e+1)(n-1)}{2}}}\right]^{e-1} \leq \frac{n+1}{e+1}\, A((e+1)!) ,$$

which implies

$$\frac{e-1}{4}\left(\sqrt{\frac{2(n-1)}{e(e+1)}} - 1\right) \leq (n+1)^{\frac{1}{e-1}}\left(\frac{A((e+1)!)}{2(e+1)}\right)^{\frac{1}{e-1}} ,$$

$$\sqrt{\frac{2(n-1)}{e(e+1)}} \leq 1 + \frac{4}{e-1}\ (n+1)^{\frac{1}{e-1}}\left(\frac{A((e+1)!)}{2(e+1)}\right)^{\frac{1}{e-1}} ,$$

$$\sqrt{\frac{2(n-1)}{e(e+1)}} \leq \frac{8}{e-1}\ (n+1)^{\frac{1}{e-1}}\left(\tfrac{1}{2}e!\right)^{\frac{1}{e-1}} ,$$

(6.5) $$(n-1) \leq \frac{16e(e+1)}{e-1}\ (n+1)^{\frac{2}{e-1}}(e+1)^2 ,$$

(6.6) $$(n-1)(n+1)^{\frac{-2}{e-1}} \leq 24(e+1)^3, \quad e \geq 3 .$$

For $n \geq \frac{9}{2}e(e+1) + 5$, it follows from (6.2) that at least e zeros of Q(x) are in $(\frac{1}{3}n, \frac{2}{3}n)$. This implies that all these zeros have different odd part.

Hence by (5.17)

(6.7) $$(n+1)\frac{A((e+1)!)}{e+1} \geq 1.3.5.7 \ldots (2e-1) .$$

Since the asymptotic behavior of this lower bound roughly behaves like 2^e (or more), it is easy to verify that this lower bound contradicts (6.6) for $e \geq 13$.

Hence $n \le \frac{9}{2} e(e+1) + 5$ for $e \ge 13$.
For $e = 4,5,\ldots,12$, we repeat this whole argument, except that we use (6.4) instead of (6.6).
It turns out that for $e = 7,8,\ldots,12$ we obtain again a contradiction with (6.7).
Hence

(6.8) $$n \le \frac{9}{2} e(e+1) + 5 \text{ for } e \ge 7 .$$

For $e = 4,5.6.$ we find respectively.

(6.9) $$n \le 11.000, \; n \le 1450 \text{ and } n \le 1050 .$$

B. Lower bound on n. All cases $e \ge 4$. We define $p_2(n)$ and $p_3(n)$ as the second, resp. third degree polynomial, between the brackets in the right hand side of (5.6), resp. (5.7).
Making use of (3.5) and (3.6) it immediately follows that $p_2(n) \le 2n^2$ and $p_3(n) \le 2n^3$. Let $n-i$ be the factor in $(n-1)(n-2)\ldots(n-e+1)$ divisible by the highest power of 2, say 2^a. Let 2^b and 2^c be the powers of 2 in $p_2(n)$ resp. $p_3(n)$. We denote this by $2^a \| (n-i)$, etc... Clearly

(6.10) $$4.n^7 = n.n.2n^2.2n^3 \ge 2^a.2^a.2^b.2^c = 2^{2a+b+c} .$$

Since $2^a \| (n-i)$ and $(n-i)$ contains the highest power of 2, it follows that $2^x \| (n-1)(n-2)\ldots(n-i-1)(n-i+1)\ldots(n-e+1)$ where

$$x \le \left\lfloor\frac{e-2}{2}\right\rfloor + \left\lfloor\frac{e-2}{4}\right\rfloor + \left\lfloor\frac{e-2}{8}\right\rfloor + \ldots ,$$

which is at most $e-3$.
Hence $2^y \| (n-1)(n-2)\ldots(n-e+1) \cdot p_2(n)$ where $y \le a+b+e-3$ and similarly $2^z \| (n-2)(n-3)\ldots(n-e+1) \cdot p_3(n)$ where $z \le a+c+e-3$. However $2^{2(e+1)} \prod_{i=1}^{e+1} (x_i-1)(x_i-2)$ is clearly divisible by $2^{3(e+1)}$. We therefore obtain the inequality $3(e+1) < 2a+b+c+2(e-3)$. Together with (6.10) this yields

(6.11) $$4n^7 > 2^{e+9} , \text{ i.e.}$$
$$n \ge 2^{\frac{e+7}{7}} .$$

For $e \geq 103$ this inequality contradicts (6.8), which proves the theorem for $e \geq 103$.
For $e = 4,5,6,\dots,102$, we still have a finite number of possibilities given by (6.8) and (6.9). These possibilities were all checked on a computer. It turned out that none of them satisfied the necessary conditions. This means that the theorem is proved for all $e \geq 4$. The total computer time was roughly $1\frac{1}{4}$ hour on a Burroughs B6700.

Remark. In [2] (theorem 8 and corollary 12.2) it is shown that the code words of fixed weight in an uniformly packed code, containing $\underline{0}$, form an e-design. In the computer program we used the divisibility conditions for designs as the most powerfull tool to reject possibilities.

C. The case $e = 3$. For $n \leq 2300$ we have checked all possibilities on a computer and it turned out that only the extended Golay code of length 24 exists. In the sequel we have $n > 2300$.
By lemma (5.13) there are at least 3 roots in the interval (v_1,u_3) or (u_1,v_4). For this small value of e it is easy to calculate these zeros explicitly.

$$(6.12) \qquad \left|v_4 - \frac{n+1}{2}\right| = \left|v_1 - \frac{n+1}{2}\right| < \tfrac{1}{2}\sqrt{3n + n\sqrt{3}}$$

$$(6.13) \qquad \left|u_3 - \frac{n+1}{2}\right| = \left|u_1 - \frac{n+1}{2}\right| < \tfrac{1}{2}\sqrt{3}n .$$

Applying (5.16) and (5.19) as in part A one finds

$$(6.14) \qquad A(y_3)A(y_4) \cdot \tfrac{1}{2}\left(\frac{n + 1 - \sqrt{n(3 + \sqrt{3})}}{\tfrac{1}{2}\sqrt{n}(\sqrt{3} + \sqrt{3 + \sqrt{3}})}\right)^2 \leq 3A(\mu) .$$

We first treat the case that μ is even. Then by (3.6)

$$(6.15) \qquad A(\mu) \leq \frac{\mu}{2} \leq \frac{(n+1)}{8} .$$

For $n \geq 2300$ we now deduce from (6.14) $A(y_3)A(y_4) < 3$, i.e.

$$(6.16) \qquad A(y_3) = A(y_4) = 1 .$$

Suppose $y_3 = 2^{2k+1}$. Since $\left|y_3 - \frac{n+1}{2}\right| \leq \frac{1}{2}\sqrt{n(3+\sqrt{3})}$, it follows that $n < 2^{2k+2} + 2^{k+3}$ and $\sqrt{n} < 2^{k+1} + 1$. Consequently $\frac{1}{2}\sqrt{n}(\sqrt{3} + \sqrt{3+\sqrt{3}}) < 2^{k+2}$.

Hence as possible values of y_1 and y_2 one has $2^{2k+1} + 2^{k+1}$ or $2^{2k+1} - 2^{k+1}$ (at most one of these), with an odd factor $2^k + 1$ or $2^k - 1$; further possibilities are $2^{2k+1} \pm 2^k$, $2^{2k+1} \pm 3.2^k$, with odd factor $2^{k+1} \pm 1$, resp. $2^{k+1} \pm 3$, etc.

Clearly $A(y_1)A(y_2)$ is at least $(2^k - 1)(2^{k+1} - 3)$. However by (6.15) and the inequality on n above

$$3A(\mu) \le \frac{3}{8}(2^{2k+2} + 2^{k+1} + 1) \ ,$$

i.e. we have established a contradiction with (5.16). The case $y_3 = 2^{2k}$ does not yield a contradiction, if we treat it the same way, but two possibilities

$$\text{(6.17)} \quad \begin{array}{l} \text{a) } y_1 = 2^{2k} + 2^k,\ y_2 = 2^{2k} + 2^{k+1},\ \mu = \dfrac{2(2^k + 1)(2^{k-1} + 1)}{3},\ A(|C|) = 1, \\ \text{b) } y_1 = 2^{2k} - 2^k,\ y_2 = 2^{2k} - 2^{k+1},\ \mu = \dfrac{2(2^k - 1)(2^{k-1} - 1)}{3},\ A(|C|) = 1. \end{array}$$

Since $|y_3 - \frac{n+1}{2}| \le \frac{1}{2}\sqrt{n(3 + \sqrt{3})}$, one has in both cases

$$n - 2\sqrt{n} \le 2^{2k+1} \le n + 2\sqrt{n}$$

$$\frac{1}{6}(n - 4\sqrt{n}) \le \mu \le \frac{1}{6}(n + 4\sqrt{n}) \ .$$

Since $0 \le \lambda < \frac{n}{4}$, (3.5), one has by (5.2)

$$\frac{11}{6} n - \frac{4}{3}\sqrt{n} \le y_1 + y_2 + y_3 + y_4 \le \frac{7}{3} n + \frac{4}{3}\sqrt{n} \ .$$

Consequently,

$$\frac{11}{6} n - \frac{4}{3}\sqrt{n} - 3(\frac{n}{2} + 2\sqrt{n}) \le y_4 \le \frac{7}{3} n + \frac{4}{3}\sqrt{n} - 3(\frac{n}{2} - 2\sqrt{n}) \ ,$$

i.e.

$$\frac{1}{3} n - \frac{22}{3}\sqrt{n} \le y_4 \le \frac{5}{6} n + \frac{22}{3}\sqrt{n} \ .$$

On the other hand by (6.16) $A(y_4) = 1$, and the only power of two between these two bounds is y_3 for $n \ge 19.000$.

For $2300 \le n \le 19.000$, this leaves us with one possibility $y_3 = 4096$, $7840 \le n \le 8560$. In this case one can compute the two possibilities for y_1, y_2 and μ from (6.17). With these more precise figures one now also obtains a contradiction, after reasoning as above.

We conclude that μ has to be odd. So $\mu = A(\mu) \le \frac{n+1}{4}$.
Since $n \ge 2300$ we deduce from (6.14)

(6.18) $\quad A(y_3)A(y_4) \le 5$,

(6.19) $\quad \mu \ge \frac{n}{26} A(y_3)A(y_4)$.

Let us assume that $y_4 = x_1$. Then by (5.5)

$$x_1 = \frac{3\mu}{4}\frac{2^n}{|C|}(x_2x_3x_4)^{-1} \ge \frac{3\mu}{4}\binom{n}{3}(x_2x_3x_4)^{-1} \ge \frac{3}{4}\,\frac{nA(x_1)}{26}\binom{n}{3}\left(\frac{n+1+2\sqrt{n}}{2}\right)^{-3}.$$

Hence $\frac{x_1}{A(x_1)} \ge \frac{n}{30}$ and therefore x_1 is divisible by 8. If one of the zeros y_i, $i \le 3$, is not divisible by 8, then $A(y_i) \ge \frac{1}{4}\left(\frac{n+1-2\sqrt{n}}{2}\right)$. Since at least one other zero x has $A(x) \ge \left(\frac{n+1-2\sqrt{n}}{2.2\sqrt{n}}\right)$, we do get a contradiction with (5.17).
Since this later argument also applies if $y_4 = x_4$, we conclude

(6.20) $\quad$ all x_i are divisible by 8 .

By (5.2), (5.4) and (5.6) we have

(6.21) $\quad n + \mu - \lambda \equiv 0 \pmod 4$

(6.22) $\quad 3n + 3(\mu - \lambda)^2 - 6\mu - 4 \equiv 0 \pmod{16}$

(6.23) $\quad (n-1)(n-2)\{(n-8)(n-3-4\lambda) + 4\mu(n-3) - 8\lambda\} \equiv 16 \pmod{32}$.

As in theorem (5.2) one can easily derive

(6.24) $\quad \sum\limits_{i<j<k} x_ix_jx_k = \frac{1}{2}p_3(n) = \frac{1}{2}\{n^3 + 3(\mu-\lambda-1)n^2 + (3\mu+3\lambda+4)n + 8\mu - 2\lambda\}$.

By (6.20)

(6.25) $\quad p_3(n) \equiv 0 \pmod{2^{10}}$.

Substitution of (6.21) in (6.22) yields

(6.26) $\quad 3n(n+1) - 6\mu - 4 \equiv 0 \pmod 8$.

Since μ is odd, we deduce from (6.26) $n(n+1) \equiv 2 \pmod 4$. Suppose $n \equiv 2 \pmod 4$. Then by (6.21) λ is odd. However this contradicts (6.25), since $p_3(n) \equiv -2\lambda \equiv 2 \pmod 4$. Hence $n \equiv 1 \pmod 4$. Since the expression between braces in (6.23) is congruent to $n(n-3) \equiv n^2 + n \equiv 2 \pmod 4$, it follows that

$n - 1 \equiv 8 \pmod{16}$. Substitution of this result in (6.26) yields $\mu \equiv 3 \pmod 4$. By (6.21) $\lambda \equiv 0 \pmod 4$. If one reduces $p_3(n) \pmod 8$, one obtains $p_3(n) \equiv 2 + 6\mu \equiv 4 \pmod 8$, contradicting (6.25). □

Acknowledgement

The author wishes to thank J.H. van Lint for his helpfull suggestions and F.C. Bussemaker for his excellent programming.

References

[1] P. Delsarte, An algebraic approach to the association schemes of coding theory, Philips Res. Repts. Suppl. No. 10, 1973.

[2] J.M. Goethals and H.C.A. van Tilborg, Uniformly packed codes, MBLE Research Laboratory, Rept. R272, 1974.

[3] J.H. van Lint, Coding Theory, Springer-Verlag, Lecture Notes in Mathematics, 201, 1971.

[4] G. Szegö, Orthogonal polynomials, Amer. Math. Soc. Colloquium Publications, Vol. XXIII, 1959.