All binary, (n,e,r)-uniformly packed codes are known

Citation for published version (APA):
Tilborg, van, H. C. A. (1975). *All binary, (n,e,r)-uniformly packed codes are known*. (Eindhoven University of Technology : Dept of Mathematics : memorandum; Vol. 7508). Technische Hogeschool Eindhoven.

Document status and date:
Published: 01/01/1975

Document Version:
Publisher’s PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

• A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
• The final author version and the galley proof are versions of the publication after peer review.
• The final published version features the final layout of the paper including the volume, issue and page numbers.

Link to publication

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the “Taverne” license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy
If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.

Download date: 08. Feb. 2024

TECHNISCHE HOGESCHOOL EINDHOVEN

Onderafdeling der Wiskunde

Memorandum 1975-08

juni 1975

All binary, (n,e,r)-uniformly packed codes are known

door

H.C.A. van Tilborg

Technische Hogeschool
Onderafdeling der Wiskunde
PO Box 513, Eindhoven
Nederland

§ 1. Introduction

Let V be a n-dimensional vectorspace over GF(2). For $\underline{u} \in V$, the weight $w(\underline{u})$ is the number of its nonzero components. The Hamming distance $d(\underline{u},\underline{v})$ for any two vectors $\underline{u}$ and $\underline{v}$ im V is the weight of their difference, i.e. $d(\underline{u},\underline{v}) = w(\underline{u} - \underline{v})$.

A code C of length n is any subset of V, with $|C| \geq 2$; its minimum distance $d(C)$ is the minimum value of the distance between any two distinct elements of C. A code C is called e-error-correcting iff $e = [\frac{d(C) - 1}{2}]$. The weight-enumerator of a code C is the polynomial $W_c(z)$ defined by

$$(1) \qquad W_c(z) := \sum_{i=0}^{n} A(i)z^i := \sum_{\underline{u} \in C} z^{w(\underline{u})} .$$

Clearly A(i) is the number of codewords of weight i. We need some more definitions:

$$(2) \qquad B(\underline{x},k) := |\{\underline{c} \in C \mid d(\underline{x},\underline{c}) = k\}|, \quad \underline{x} \in V,\ 0 \leq k \leq n ,$$

$$(3) \qquad p(\underline{x}) := \min\{k \mid B(\underline{x},k) \neq 0\}, \quad \underline{x} \in V ,$$

$$(4) \qquad C_e := \{\underline{x} \in V \mid p(\underline{x}) \geq e\} ,$$

$$(5) \qquad r(\underline{x}) := B(\underline{x},e) + B(\underline{x},e + 1) .$$

In words: $r(\underline{x})$ is the number of code words at distance e or e + 1 from $\underline{x}$.
Let $\underline{x} \in C_e$ be fixed. By a suitable translation of the code, we may assume that $\underline{x} = \underline{0} = (0,0,\ldots,0)$.
Now $r(\underline{0})$ equals the number of codewords of weight e or e + 1. Since the mutual distance of these code words is at least 2e + 1, we have $r(\underline{0}) \leq [\frac{n + 1}{e + 1}]$, i.e.

$$(6) \qquad r(\underline{x}) \leq [\frac{n + 1}{e + 1}], \quad (\forall_{\underline{x} \in C_e}) .$$

Let r(C) be the average value of $r(\underline{x})$ for $\underline{x} \in C_e$. Since

$$(7) \qquad |C_e| = 2^n - |C| \sum_{i=0}^{e-1} \binom{n}{i}$$

and

$$(8) \qquad \sum_{\underline{x} \in C_e} r(\underline{x}) = |C|\{\binom{n}{e}+\binom{n}{e+1}\}$$

it follows that

$$(9) \qquad \frac{|C|.\{\binom{n}{e} + \binom{n}{e+1}\}}{2^n - |C| . \sum_{i=0}^{e-1} \binom{n}{i}} = r(C) \le [\frac{n+1}{e+1}] .$$

The inequality in (2) was originally derived in [2].

A code C is called a (n,e,r)-uniformly packed code if for all $\underline{x} \in C_e$, $r(\underline{x}) = r = r(C)$.

Clearly $r \ge 2$, since $r = 1$ implies that the code is $(e+1)$-error-correcting. We remark that this in the original definition of uniformly packed codes (see [5]).

Later this definition was generalized to other fields and the condition for r was replaced by

$$\underline{x} \in V,\ p(\underline{x}) = e \Rightarrow B(\underline{x}, e+1) = \lambda ,$$

$$\underline{x} \in V,\ p(x) > e \Rightarrow B(x, e+1) = \mu .$$

So our case reduces to $\lambda + 1 = \mu = r$ (see [1]). If $r = \frac{n+1}{e+1}$, where $e+1$ divides $n+1$, then C is called perfect. This is the case where the spheres of radius e around the codewords form a partition of V.

If $r = [\frac{n+1}{e+1}]$, where $e+1$ does not divide $n+1$, then C is called nearly perfect.

It was shown by van Lint and Tietävainen that there are no unknown perfect codes (see [4] and [6]). Recently K. Lindström proved that there are no unknown binary, nearly perfect codes (see [3]).

It is the aim of this paper to prove:

Theorem. There are no unknown, uniformly packed binary codes.

§ 2. Lemmas

In [1] the following result is proved:

Lemma 1. If C is a (n,e,r)-uniformly packed code, e = 1 or 2, then either C is (nearly) perfect or we are in one of the following cases:

a) $\qquad e = 1,\ n = (2^{m-1} + 1)(2^m - 1),\ r = \binom{2^{m-1}+1}{2},\ m \ge 2;$

b) $\qquad e = 1,\ n = (2^{m-1} - 1)(2^m + 1),\ r = \binom{2^{m-1}}{2},\ m \ge 3;$

c) $e = 1,\ n = 2^m - 2,\ r = 2^{m-1} - 1, \qquad m \geq 3;$

d) $e = 2,\ n = 2^{2m} - 1,\ r = (2^{2m} - 1)/3, \qquad m \geq 2;$

e) $e = 2,\ n = 2^{2m+1} - 1,\ r = (2^{2m} - 1)/3, \qquad m \geq 2;$

f) $e = 2,\ n = 11,\ r = 3\ .$

For a description of these codes see [1].

Definition. $C(n,e,r)$ denotes the set of (n,e,r)-uniformly packed codes C, where C is not perfect.

Lemma 2. If $C \in C(n,e,r)$, then $d(C) = 2e + 1$.

Proof. Assume that $d(C) = 2e + 2$. W.l.o.g. $\underline{0} \in C$ and $\underline{c} := (1,1,\ldots,1,0,0,\ldots,0)$, where $w(\underline{c}) = 2e + 2$, is in the code. Take $\underline{x} = (1,1,\ldots,1,0,\ldots,0)$, $w(\underline{x}) = e$. Then $r = r(\underline{x}) = 1$. However for $\underline{y} = (1,1,\ldots,1,0,\ldots,0)$, $w(\underline{y}) = e + 1$, we find $r = r(\underline{y}) \geq 2$. □

Lemma 3. If $C \in C(n,e,r)$, then

$$|C|\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}(\binom{n}{e} + \binom{n}{e+1})\} = 2^n\ . \tag{10}$$

Proof. This is a reformulation of (9). □

Lemma 4. If $C(n,e,r)$ is nonempty, then the polynomial

$$Q(x) := \sum_{i=0}^{e-1} P_i^{(n)}(x) + \frac{1}{r} P_e^{(n)}(x) + \frac{1}{r} P_{e+1}^{(n)}(x) = \tag{11}$$

$$= \frac{1}{r}\{(r-1)P_{e-1}^{(n-1)}(x-1) + P_{e+1}^{(n-1)}(x-1)\} \tag{12}$$

has $e+1$ distinct integer roots $x_1, x_2, \ldots, x_{e+1}$ in $[1,n]$. Here

$$P_k^{(n)}(x) := \sum_{i=0}^{k} (-2)^i \binom{n-i}{k-i}\binom{x}{i} = \sum_{i=0}^{k} (-1)^i \binom{n-x}{k-i}\binom{x}{i}\ . \tag{13}$$

Proof. See [1]. □

Lemma 5. If $x_1 < x_2 < \dots < x_{e+1}$ are the zeros of $Q(x)$, $e \geq 3$, then

$$\text{(14) i)} \quad \sum_{i=1}^{e+1} x_i = \frac{(n+1)(e+1)}{2} ,$$

$$\text{(15) ii)} \quad x_i + x_{e+1-i} = n+1, \quad 1 \leq i \leq e+1 ,$$

$$\text{(16) iii)} \quad \prod_{i=1}^{e+1} x_i = \frac{r(e+1)!2^{n-e-1}}{|C|} \geq \frac{(e+1)!\binom{n}{e+1}}{2^{e+1}} ,$$

$$\text{(17) iv)} \quad 2^{e+1} \prod_{i=1}^{e+1} (x_i - 1) = (n-1)(n-2)\dots(n-e+1)\{n^2 - (2e+1)n + re(e+1)\},$$

$$\text{(18) v)} \quad 2^{e+1} \prod_{i=1}^{e+1} (x_i - 2) = (n-2)(n-3)\dots(n-e+1)\{(r-1)(e+1)e(n-2e+1) + \\ + (n-e)(n-e-1)(n-2e-3)\} .$$

Proof. Let $C_k(p(x))$ denote the coefficients of x^k in the polynomial $p(x)$. Since

$$C_{e+1}(Q(x)) = C_{e+1}(\tfrac{1}{r} P_{e+1}^{(n)}(x)) = (-2)^{e+1} \frac{1}{r(e+1)!} ,$$

it follows that

$$\text{(19)} \qquad Q(x) = \frac{(-2)^{e+1}}{r(e+1)!} \prod_{i=1}^{e+1} (x - x_i) .$$

Now i) follows from (11) and the observation

$$\sum_{i=1}^{e+1} x_i = -C_e(Q(x))/C_{e+1}(Q(x)) .$$

The equality in iii) follows similarly from (11) and

$$\prod_{i=1}^{e+1} x_i = (-1)^{e+1} C_0(Q(x))/C_{e+1}(Q(x)) .$$

The inequality in iii) follows from (10) and

$$\frac{r(e+1)!2^{n-e-1}}{|C|} = \frac{(e+1)!\{\sum_{i=0}^{e-1} \binom{n}{i} + \frac{1}{r}\binom{n}{e} + \frac{1}{r}\binom{n}{e+1}\}}{2^{e+1} \frac{1}{r}} \geq \frac{(e+1)!\binom{n}{e+1}}{2^{e+1}} .$$

The equalities iv) and v) can easily be verified by substitution of $x = 1$ resp. $x = 2$ in (11) and (19). The definition of $P_k^{(n)}(x)$ in (13) leads to the obvious observation $P_k^{(n)}(x) = (-1)^k P_k^{(n)}(n - x)$. Using (12), one finds $Q(x) = (-1)^{e+1} Q(n + 1 - x)$. This implies ii). $\square$

Lemma 6. Let $C \in \mathcal{C}(n,e,r)$, $\underline{0} \in C$. Then the words of weight k in C form an $e - (n,k,\lambda(k))$ design, where $\lambda(k)$ depends on k, $\lambda(2e + 1) = r - 1$. Moreover, the words of weight k in the extended code form an $(e + 1) - (n + 1,k,\mu(k))$ design, where $\mu(k)$ depends on k, $\mu(2e + 2) = r - 1$.

Proof. See [5]. $\square$

Lemma 7. Let $\sum_{i=0}^{n} A(i)z^i$ be the weight enumerator of a code $C \in \mathcal{C}(n,e,r)$. Then for all $0 \le k \le n$

$$(20) \qquad \binom{n}{k} = \sum_{\delta=0}^{e+1} \alpha_\delta \sum_{i=0}^{\delta} A(k + \delta - 2i) \binom{k + \delta - 2i}{\delta - i} \binom{n - k - \delta + 2i}{i},$$

where $\alpha_0 = \alpha_1 = \ldots = \alpha_{e-1} = 1$, $\alpha_e = \alpha_{e+1} = \frac{1}{r}$.

Proof. See [5]. $\square$

Lemma 8. If $\mathcal{C}(n,e,r)$, $e \ge 3$, is nonempty, then $e \ge 17$ or

$e = 3,\ n \ge 90,$
$e = 4,\ n \ge 135,$
$e = 5,\ n \ge 189,$
$e = 6,\ n \ge 430,$
$e = 7,\ n \ge 324,$
$e = 8,\ n \ge 405,$
$e = 9,\ n \ge 262,$
$e = 10,\ n \ge 314,$
$e = 11,\ n \ge 371,$
$e = 12,\ n \ge 242,$
$e = 13,\ n \ge 279,$
$e = 14,\ n \ge 319,$
$e = 15,\ n \ge 361,$
$e = 16,\ n \ge 407$.

Proof. This is done by a computer analysis. For each of the admissable parameters, we first checked whether they satisfy the necessary conditions for the existence of an $(e + 1) - (n + 1, 2e + 2, r - 1)$ design (lemma 6). If so, then we applied lemma 3. This excluded all the remaining cases. The total computer time was 16 seconds on a Burroughs B6700. $\square$

Lemma 9. If $\mathcal{C}(n,e,r)$, $e \ge 3$, is nonempty then

i) $\qquad n \ge \dfrac{(r - 1)e^2 + (3r - 2)e + (2r - 2)}{r} \quad$ for $r \ge 4$,

ii) $$n \geq \frac{2e^2 + 8e + 4}{3} \quad \text{for } r = 3 ,$$

iii) $$n \geq \frac{e^2 + 4e + 3}{2} \quad \text{for } r = 2 .$$

Proof. With the aid of lemma 7, it is easy to verify that

$$A(2e + 2) = A(2e + 1)\frac{n - 2e - 1}{2(e + 1)}$$

and

$$A(2e + 3) = \frac{A(2e + 1).g(n)}{(2e + 3)(2e + 2)(r - 1)} ,$$

where $g(n) := r(n - e)(n - e - 1) - r(r - 1)e(e + 1) - (r - 1)(e + 1)(e + 3)(n - 2e - 1)$. At this point we must remark that the cases $n = 2e + 1$ and $n = 2e + 2$ never occur in $C(n,e,r)$.
Since $g(2e + 1) = r(2 - r)e(e + 1) \leq 0$, it follows that n must be greater than or equal to the largest zero of $g(x)$. Using $e^4(r - 1)^2$ as a lower bound for the discriminant of $g(n)$ for $r \geq 4$, one easily obtains i). Direct calculations for $r = 2$ and 3 lead to ii) and iii). □

Lemma 10. If $C(n,e,r)$, $e \geq 3$, is nonempty, then

$$(r - 1)(n - e + 1) \geq (e + 2)(e + 3) .$$

Proof. Since the words of weight $2e + 1$ form an e-design with $\lambda = r - 1$, one can apply the generalisation of Fisher's inequality to the parameters (see [8]). This leads to the lemma. □

Lemma 11. If $C(n,e,r)$, $e \geq 3$, is nonempty, then

(21) $$n \geq \frac{2}{3}(e + 1)(e + 2) .$$

Proof. Apply lemma 9 for $r \geq 3$ and lemma 10 for $r = 2$. □

Definition. For any $m \in \mathbb{N}$, $A(m)$ is defined as the largest odd divisor of m. We define an equivalence relation on $\mathbb{N}$ by

$$m \sim n :\Leftrightarrow A(m) = A(n) .$$

Let $s(C)$, for any $C \in C(n,e,r)$, be the number of equivalence classes X_i containing at least one zero of $Q(x)$. Moreover let n_i be the number of equivalence classes containing exactly i zeros of $Q(x)$. Clearly

(22) $$\sum_{i=1}^{e+1} n_i = s(C) \ ,$$

(23) $$\sum_{i=1}^{e+1} in_i = e + 1 \ .$$

<u>Lemma 12</u>. If $C(n,e,r)$, $e \geq 3$, is nonempty and $Q(x)$ has k zeros on $[0,\alpha(n+1)]$, $\alpha < \frac{1}{2}$, then

(24) $$\prod_{i=1}^{e+1} x_i \leq (4\alpha(1-\alpha))^k \left(\frac{n+1}{2}\right)^{e+1} \ .$$

<u>Proof</u>. Since $x_1 < x_2 < \ldots < x_k \leq \alpha(n+1)$ it follows from (15) that

$$x_i \ x_{e+1-i} \leq \alpha(1-\alpha)(n+1)^2 = 4\alpha(1-\alpha)\left(\frac{n+1}{2}\right)^2, \quad 1 \leq i \leq k \ ,$$

$$x_i \ x_{e+1-i} \leq \left(\frac{n+1}{2}\right)^2, \quad \text{for the other values of } i \ .$$

Together these inequalities imply the lemma. □

<u>Lemma 13</u>. Let $C \in C(n,e,r)$, $e \geq 3$. Then

(25) $$n + 1 \geq (e+1)^{\frac{e+1}{\log(e+1)}\frac{5\log 2}{4} - (e+1-s(C))} \prod_{\substack{i \leq e+1-s(C) \\ i \text{ odd}}} i^2 \ .$$

<u>Proof</u>. Since

$$2^{2e} = \sum_{i=0}^{e} \binom{2e+1}{i} \leq A(|C|) \ . \sum_{i=0}^{e} \binom{n}{i} \leq 2^{n-k} \ ,$$

one has $n - k - e - 1 > 0$ (here $|C| = A(|C|).2^k$). Therefore by lemma 5, iii) and by the inequality in (9)

(26) $$A\left(\prod_{i=1}^{e+1} x_i\right) = A\left(\frac{r(e+1)!2^{n-k-e-1}}{A(|C|)}\right) = \frac{A(r)A((e+1)!)}{A(|C|)} \leq$$

$$\leq rA((e+1)!) \leq \frac{n+1}{e+1} A((e+1)!) \ .$$

Tietäväinen has proved in [6] that for all $e \geq 7$

$$(27) \qquad A((e+1)!) < p(e+1)(e+1)^{[\frac{e+1}{2}] + 1 - \frac{e+1}{\log(e+1)} \frac{5 \log 2}{4}} ,$$

where $p(e+1) = \prod_{\substack{i \leq e+1 \\ i \text{ odd}}} i$.

Suppose that the smallest zero x and the largest zero y in one equivalence class, satisfy $16x \leq y$. Clearly $x \leq \frac{n+1}{16}$. However (24) now implies

$$\prod_{i=1}^{e+1} x_i \leq \frac{15}{64}\left(\frac{n+1}{2}\right)^{e+1} .$$

Comparing this with the inequality in (16) results in

$$\frac{15}{64} \geq \prod_{i=1}^{e+1} \left(1 - \frac{i}{n+1}\right) .$$

Since the right hand side is at least $1 - \frac{(e+1)(e+2)}{2(n+1)}$, we obtain a contradiction with lemma 11.

Therefore $n_\ell = 0$ for $\ell \geq 5$ and $n_4 \neq 0$ implies that the elements of a class X_i with four zeros look like a, $2a$, $4a$ and $8a$. Moreover, clearly $a \leq \frac{1}{8}(n+1)$. Suppose that the sum of any 2 zeros in this class is never $n+1$. Let $Y := \{n+1-a,\ n+1-2a,\ n+1-4a,\ n+1-8a\}$. Now, using the arithmeticmean-geometricmean inequality, we obtain

$$\prod_{j=1}^{e+1} x_j = \prod_{x \in X_i \cup Y} x \prod_{\substack{j=1 \\ x_j \notin X_i \cup Y}}^{e+1} x \leq \frac{1}{8} \cdot \frac{7}{8} , (n+1)^2 \, \frac{1}{4} \, \frac{3}{4} (n+1)^2 \left(\frac{n+1}{2}\right)^4 .$$

$$\prod_{\substack{j=1 \\ x_j \notin X_i \cup Y}}^{e+1} x = \frac{21}{64}\left(\sum_{x \in X_i \cup Y} \frac{x}{8}\right)^8 \left(\prod_{\substack{j=1 \\ x_j \notin X_i \cup Y}}^{e+1} x_j\right) \leq \frac{21}{64}\left(\sum_{x \in X_i \cup Y} \frac{x}{8}\right)^8 \left(\sum_{\substack{j=1 \\ x_j \notin X_i \cup Y}}^{e+1} \frac{x_j}{e-7}\right)^{e-7}$$

$$\leq \frac{21}{64}\left(\sum_{j=1}^{e+1} \frac{x_j}{e+1}\right)^{e+1} \leq \frac{21}{64}\left(\frac{n+1}{2}\right)^{e+1} .$$

This leads, as above, to a contradiction with (16) and lemma 11.

If the sum of two zero's in X_i equals $n+1$, we get in the same way, but easier, a contradiction. Hence $n_4 = 0$. Now clearly

$$A(\prod_{i=1}^{e+1} x_i) \geq \{1.3.5\ldots(2s(C)-1)\}.1^2.3^2\ldots(2n_3-1)^2(2n_3+1)\ldots(2n_2+2n_3-1) =$$

$$\begin{aligned}
(28) \qquad & = p(2s(C)).p(2n_3).p(2(n_2+n_3)) = \\
& = p(2s(C)).p(2n_3).p(2(e+1-s(C)-n_3)) \geq \\
& \geq p(2s(C)).\{p(e+1-s(C))\}^2 \geq \\
& \geq p(e+1)(e+1)^{s(C)-(e+1-[\frac{e+1}{2}])}.\{p(e+1-s(C))\}^2 .
\end{aligned}$$

Comparing (26) and (28) leads, with the use of (27), to the assertion of the lemmas for $e \geq 7$. For $e = 3,4,5$ and 6 the lemma follows from lemma 8. □

At this moment we have enough lower bounds on possible values of n. The next 2 lemmas will provide us with upper bounds on n.

Lemma 14. If $y_1, y_2, \ldots, y_s$ and p are positive integers such that $\frac{y_{i+1}}{y_i} \geq p$, for all $1 \leq i \leq s-1$, then

$$\prod_{i=1}^{s} y_i \leq R^{s-1}\Big(\sum_{i=1}^{s} \frac{y_i}{s}\Big)^s, \quad \text{where } R = \frac{4p}{(1+p)^2} .$$

Proof. See [7]. □

Lemma 15. If $C \in \mathcal{C}(n,e,r)$, $e \geq 3$, then

$$(29) \qquad (\tfrac{8}{9})^{e+1-s(C)} \geq 1 - \frac{(e+1)(e+2)}{2(n+1)} .$$

Proof. Let

$$Y_i := X_i \cap \{x_1, x_2, \ldots, x_{e+1}\}, \ t(i) := |Y_i|$$

$$R_i := (\prod_{x \in Y_i} x)/(\sum_{x \in Y_i} \frac{x}{t(i)})^{t(i)} \quad \text{for } Y_i \neq \emptyset .$$

Since $x \in Y_i$, $y \in Y_i$, $y > x$ implies $y \geq 2x$, we get by lemma 14 that $R_i \leq (\frac{8}{9})^{t(i)-1}$. Therefore, using the arithmetic-mean-geometric-mean inequality

$$\prod_{i=1}^{e+1} x_i = \prod_{i=1}^{s(C)} (\prod_{x \in Y_i} x) \leq \prod_{i=1}^{s(C)} (\tfrac{8}{9})^{t(i)-1}(\sum_{x \in Y_i} \frac{x}{t(i)})^{t(i)} \leq$$

$$(\frac{8}{9})^{\sum_{i=1}^{s(C)} (t(i)-1)} (\sum_{i=1}^{e+1} \frac{x_i}{e+1})^{e+1} = (\frac{8}{9})^{e+1-s(C)} (\frac{n+1}{2})^{e+1} .$$

Here we also used (22), (23) and (14).

Comparing this inequality with the inequality in (16) one obtains

$$(\frac{8}{9})^{e+1-s(C)} \geq \prod_{i=1}^{e+1} (1 - \frac{i}{n+1}) .$$

The right hand side in turn is at least $1 - \frac{(e+1)(e+2)}{2(n+1)}$. ☐

<u>Lemma 16</u>. If $C(n,e,r)$, $e \geq 3$, is nonempty, then

$$(30) \qquad (n+1)^{1-2/e} \leq (\frac{A((e+1)!)}{e+1})^{2/e} (1 + \frac{\delta_n}{2})^2 . 2(e+1)(e+2)$$

where $\delta_n := (\frac{e+1}{(n+1)A((e+1)!)})^{1/e}$.

<u>Proof</u>. Let us reorder the roots of $Q(x)$ in such a way that $x_i = A(x_i)2^{\alpha_i}$, $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{e+1}$.

$$(31) \qquad \prod_{i=1}^{e} \text{g.c.d.}(x_i, x_{i+1}) = \prod_{i=1}^{e} \text{g.c.d.}(A(x_i), A(x_{i+1})) . 2^{\alpha_i} \geq \prod_{i=1}^{e} 2^{\alpha_i} =$$

$$= \frac{x_1 \, x_2 \ldots x_e}{A(x_1 . x_2 \ldots x_e)} .$$

As in the proof of lemma 13 we remark that $n-k-e-1 > 0$ if $|C| = A(|C|).2^k$.
Using (31) and (16) we obtain

$$(32) \qquad \prod_{i=1}^{e} \frac{|x_i - x_{i+1}|}{x_i} \geq \prod_{i=1}^{e} \frac{\text{g.c.d.}(x_i, x_{i+1})}{x_i} \geq \frac{1}{A(x_1 . x_2 \ldots x_e)} \geq \frac{1}{A(x_1 \ldots x_{e+1})}$$

$$= \frac{A(|C|)}{A(r)A((e+1)!)} \geq \frac{1}{A(r)A((e+1)!)} \geq \frac{1}{rA((e+1)!)} \geq \frac{e+1}{(n+1)A((e+1)!)} .$$

Let t be defined by

$$\frac{|x_t - x_{t+1}|}{x_t} = \max_{1 \leq i \leq e} |\frac{x_i - x_{i+1}}{x_i}| .$$

Then (32) implies

$$\frac{|x_t - x_{t+1}|}{x_t} \geq \left(\frac{e+1}{(n+1)A((e+1)!)}\right)^{1/e} = \delta_n \ .$$

Since the function $\frac{x}{(1+x)^2}$ is monotonically increasing on $[0,1]$ and decreasing on $[1,\infty)$, it follows that for $x_t < x_{t+1}$, i.e. $\frac{x_{t+1}}{x_t} > 1 + \delta_n$ we have

$$(33) \qquad \frac{x_t\, x_{t+1}}{\left(\frac{x_t + x_{t+1}}{2}\right)^2} = \frac{\frac{x_{t+1}}{x_t}}{\left(\frac{1 + \frac{x_{t+1}}{x_t}}{2}\right)^2} < \frac{1+\delta_n}{\left(\frac{2+\delta_n}{2}\right)^2} = 1 - \frac{\delta_n^2}{4}\left(\frac{2}{2+\delta_n}\right)^2 =: 1 - \gamma \ ,$$

and similarly, for $x_t > x_{t+1}$,

$$(34) \qquad \frac{x_t\, x_{t+1}}{\left(\frac{x_t + x_{t+1}}{2}\right)^2} < \frac{1-\delta_n}{\left(\frac{2-\delta_n}{2}\right)^2} = 1 - \frac{\frac{\delta_n^2}{4}}{1 - \delta_n + \frac{\delta_n^2}{4}} < 1 - \frac{\delta_n^2}{4} < 1 - \gamma \ ,$$

where (33) defines γ.

Using (33), (34), the arithmetic-mean geometric-mean inequality and (14), we obtain

$$\prod_{i=1}^{e+1} x_i = x_t x_{t+1} \prod_{\substack{i=1 \\ i \neq t,t+1}}^{e+1} x_i \leq (1-\gamma)\left(\frac{x_t + x_{t+1}}{2}\right)^2 \left(\sum_{\substack{i=1 \\ i \neq t,t+1}}^{e+1} \frac{x_i}{e-1}\right)^{e-1} \leq$$

$$\leq (1-\gamma)\left(\sum_{i=1}^{e+1} \frac{x_i}{e+1}\right)^{e+1} = (1-\gamma)\left(\frac{n+1}{2}\right)^{e+1} \ .$$

Comparing this inequality with the one in (16), yields, using again that

$$\prod_{i=1}^{e+1} \left(1 - \frac{i}{n+1}\right) \geq 1 - \frac{(e+1)(e+2)}{2(n+1)} \ ,$$

$$1 - \frac{\delta_n^2}{4}\left(\frac{2}{2+\delta_n}\right)^2 = 1 - \gamma > 1 - \frac{(e+1)(e+2)}{2(n+1)} \ , \text{ i.e.}$$

$$(n+1)\delta_n^2 < 2\left(1 + \frac{\delta_n}{2}\right)^2 (e+1)(e+2) \ .$$

Substitution of δ_n in the left hand side yields the lemma. □

§ 3. Proof of the theorem

Let $C \in \mathcal{C}(n,e,r)$, $e \geq 3$. Suppose $e+1-s(C) \geq 12$. Then lemma 15 implies

$$n+1 \leq \frac{(e+1)(e+2)}{2(1-(\frac{8}{9})^{e+1-s(C)})} \leq \frac{(e+1)(e+2)}{2(1-(\frac{8}{9})^{12})} \leq \frac{2(e+1)(e+2)}{3},$$

thus violating lemma 11.

For $e+1-s(C) = 1,2,\ldots,11$, we compare lemma 13 with lemma 15. In each case we are left with a gap of admissible parameters. However all these gaps are covered by lemma 8. For instance for $e+1-s(C) = 1$, lemma 13 reads:

$$(n+1) \geq (e+1)^{\frac{e+1}{\log(e+1)} \frac{5\log 2}{4} - 1},$$

and lemma 15 reads:

$$(n+1) \leq \frac{9}{2}(e+1)(e+2).$$

We derive a contradiction for $e \geq 9$. For $e = 3,4,5,6,7$ and 8

$$(n+1) \leq \frac{9}{2}(e+1)(e+2)$$

implies that these cases are covered by lemma 8.

So from now on we may assume $e+1-s(C) = 0$. Let $m(e)$ be the right hand side of (25) after substitution of $e+1-s(C) = 0$.

Since $\delta_n \leq \delta_{m(e)}$ we may replace δ_n by $\delta_{m(e)}$ in (30). Then (30) yields an upperbound for $n+1$ which contradicts (25) for $e \geq 11$. Hence $3 \leq e \leq 10$. At this moment we are left with a finite (but still large) set of admissible parameters. We could let the computer do the rest for us.

The rest of this article is devoted to avoiding the use of a computer for this part of the proof.

Since $e+1-s(C) = 0$, it follows from (26) that

$$(35) \qquad \prod_{i=1}^{e+1} (2i-1) \leq A(\prod_{i=1}^{e+1} x_i) \leq \frac{n+1}{e+1} A((e+1)!).$$

This gives a lower bound $a(e)$ for $n+1$.

Since $\delta_n \leq \delta_{a(e)}$, we find, after replacing δ_n by $\delta_{a(e)}$ in (30), that lemma 16 contradicts (35) for $e \geq 7$. For instance: $e = 7$;

(35) implies $n+1 \geq 51480 = a(7)$. Replacing δ_n by $\delta_{a(7)}$ in (30) yields $n+1 \leq 5418$ a clear contradiction.

The cases $e = 3,4,5,6$ will now be treated separately.

<u>$e = 6$</u>. (35) yields $n+1 \geq 3003 = a(6)$.
After replacement of δ_n by $\delta_{a(6)}$ in (35), it follows that $n+1 \leq 9735$. Suppose that $Q(x)$ has a zero on $[0,0.45(n+1)]$. Then it is not difficult to verify that lemma 12 contradicts the inequality in (16) for $n+1 \geq 3003$. Hence the roots x_i of $Q(x)$ are all in $[0.45(n+1),0.55(n+1)]$. Hence by the two bounds on $(n+1)$, we know that

(36) $\qquad 1352 \leq x_i \leq 5354, \quad i = 1,\ldots,7$.

Suppose that all zeros of $Q(x)$ have an odd part ≥ 3, then the left inequality in (35) can be sharpened by

$$3.5.7.9.11.13.15 \leq A(\prod_{i=1}^{7} x_i) .$$

Now (35) contradicts $n+1 \leq 9735$. So one zero, let us say x_1, has odd part 1. In the same way one zero, let us say x_2, has odd part 3. The only possibilities for x_1 by (36) are 2^{11} and 2^{12}, and for x_2 3.2^9 and 3.2^{10}.
However $x_i \in [0.45(n+1),0.55(n+1)]$ implies for x_1

$$n+1 \in [3723,4551] \text{ or } n+1 \in [7447,9102]$$

and for x_2

$$n+1 \in [2792,3413] \text{ or } n+1 \in [5585,6826] .$$

A contradiction.

<u>$e = 5$</u>. We repeat the argument of the case $e = 6$ and get $1386 \leq n+1 \leq 7944$. Each zero of $Q(x)$ is in $[0.42(n+1),0.58(n+1)]$. So each zero is in $[582,4607]$. Again we find that one zero x_1 has odd part 1. So $x_1 = 2^{10}, 2^{11}$ or 2^{12} and we find

$$n+1 \in [1765,2438], [3531,4876] \text{ or } [7062,9752] .$$

The assumption that some zero x_i of $Q(x)$ has odd part 5 leads to $x_i = 5.2^7$, 5.2^8 or 5.2^9.
The corresponding admissable intervals of $n+1$ have an empty intersection with the ones before. So we have a contradiction. Now (35) can be sharpened to

$$1.3.7.9.11.13 \leq \frac{n+1}{6} A(6!), \text{ i.e. } \quad n+1 \geq 3603 .$$

Now we start all over again. However we can now deduce that all zeros of $Q(x)$ are in $[0.45(n + 1), 0.58(n + 1)]$. Knowing that $Q(x)$ has no zero with odd part 5, implies that it has a zero, let us say x_2, with $A(x_2) = 3$. Now $x_1 = 2^{11}$ or 2^{12} implies

$$n + 1 \in [3723, 4551] \text{ or } n + 1 \in [7447, 9102] ,$$

and $x_2 = 3.2^{10}$ (the only possibility) implies $n + 1 \in [5585, 6826]$. A contradiction.

<u>e = 4</u>. Repeating the initial arguments of the case $e = 6$ yields

$$n + 1 \in [315, 15255] ,$$

and each zero is at least $0.35(n + 1)$, so at least 111.
Let $x_1 < x_2 < x_3 < x_4 < x_5$ be the zeros of $Q(x)$. Lemma 5, ii) implies $x_3 = \frac{n+1}{2}$.
Let $n + 1 = A(n + 1).2^a$. Then (35) reads

$$1 \,.\, 3 \,.\, \frac{n+1}{2^{a+1}} \,.\, 5 \,.\, 7 = 1.3.A(x_3).5.7 \leq \frac{n + 1}{5} A(5!) \text{ i.e. } 5.7 \leq 2^{a+1} .$$

Hence $n + 1 = A(n + 1).2^a$, $a \geq 5$. Let us now suppose that one zero x_i is odd. Clearly $i \neq 3$. Since also $n + 1 - x_i$ is odd in this case. Hence

$$A(x_i \cdot (n + 1 - x_i)) = x_i(n + 1 - x_i) \geq 111.(315 - 111) .$$

Substitution of this in (35) leads to an immediate contradiction. Hence all zeros are even. Let us now write down (17).

$$2^5 . \prod_{i=1}^{5} (x_i - 1) = (n - 1)(n - 2)(n - 3)(n^2 - 9n + 20r), \text{ i.e.}$$

$$2^5 . \prod_{i=1}^{5} (x_i - 1) = ((n + 1) - 2)((n + 1) - 3)((n + 1) - 4)((n + 1)^2 -$$
$$+ 11(n + 1) + 10 + 20r) .$$

Since all zeros x_i are even, it follows that the left hand side is divisible by 2^5. The right hand side has as highest power of two $2^1.2^0.2^2.2^1 = 2^4$, since $2^5 | (n + 1)$. This is a contradiction.

<u>e = 3</u>. The hardest case. Using (35) and subsequently lemma 16 yields

$$140 \leq n + 1 \leq 65.886 .$$

Using lemma 12 as before we observe that all zeros of $Q(x)$ are at least $\frac{1}{15}(n + 1)$. Suppose that some zero x_i of $Q(x)$ is odd. Then (35) implies

$$1 \,.\, 3 \,.\, 5 \,.\, \frac{n+1}{15} \le 1.3.5.x_i = 1.3.5.A(x_i) \le \frac{n+1}{4} A(4!) = \frac{3}{4}(n+1).$$

i.e. $n + 1 \le \frac{3}{4}(n + 1)$. A clear contradiction.
Let $x_1 < x_2 < x_3 < x_4$ be the zeros of $Q(x)$. Let $x_i = A(x_i)2^{\alpha_i}$. Since

$$x_3 \ge \frac{n+1}{2}\,,\; A(x_3) = \frac{x_3}{2^{\alpha_3}} \ge \frac{n+1}{2^{\alpha_e+1}}\,.$$

Substitution of this in (35) learns that $\alpha_3 \ge 4$. Similarly $\alpha_4 \ge 4$. Using lemma 12 as before, it follows that $x_2 \ge 0.403\ (n + 1)$, hence

$$A(x_2) = \frac{x_2}{2^{\alpha_2}} \ge \frac{0.403(n+1)}{2^{\alpha_2}}\,.$$

Substitution of this in (35) also learns that $\alpha_2 \ge 4$. Hence $n+1 = x_2 + x_3$ by (15) is divisible by $2^4 = 16$. We again write down (17)

$$2^4 \prod_{i=1}^{4} (x_i - 1) = (n-1)(n-2)\{n^2 - 7n + 12r\} =$$

$$= ((n+1)-2)((n+1)-3)\{(n+1)^2 - 9(n+1) + 8 + 12r\}\,.$$

Since all x_i's are even and $n+1$ is divisible by 16, it follows that $r \equiv 0 \pmod 4$.

For $e = 3$ it is not difficult to find the zeros of $Q(x)$. They are

$$x_{1234} = \frac{n + 1 \pm \sqrt{3n - 6r - 1 \pm \sqrt{6n^2 - 6n - 24rn + 36r^2 + 4}}}{2}\,.$$

Let us define s, ℓ and m by

(37) $$6n^2 - 6n - 24rn + 36r^2 + 4 = s^2$$

(38) $$3n - 6r - 1 + s = \ell^2$$

(39) $$3n - 6r - 1 - s = m^2\,.$$

Let us denote $n + 1 = A(n + 1)2^a$, $\ell = A(\ell)2^b$, $m = A(m)2^c$, $s = A(s)2^u$, $r = A(r).2^z$ and $|C| = A(|C|)2^k$.

Then (37), (38), and (39) can be rewritten

(40) $$3A^2(n+1)2^{2a+1} - 9A(n+1)2^{a+1} - 3A(r)A(n+1)2^{z+a+3} + 9A^2(r)2^{2z+2} +$$
$$+ 3A(r)2^{z+3} + 2^4 = A^2(s)2^{2u}\,.$$

$$(41) \qquad 3A(n+1)2^a - 3A(r)2^{z+1} - 2^2 + A(s)2^u = A^2(\ell)2^{2b}$$

$$(42) \qquad 3A(n+1)2^a - 3A(r)2^{z+1} - 2^2 - A(s)2^u = A^2(m)2^{2c}\ .$$

Considering the powers of 2 in each term we deduce from (40) that, since $a \geq 4$ and $z \geq 2$, u equals 2. Now (41) implies $b \geq 2$ and (42) implies $c \geq 2$. However since exactly one of $A(s) + 1$ and $A(s) - 1$ is congruent to 2 mod 4 and the other congruent to 0 mod 4, one of these equations will imply that $z = 2$ and the other $z \geq 3$. A contradiction. ☐

Acknowledgement

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

References

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

[2] S.M. Johnson, A new upper bound for error-correcting codes. IEEE Trans. Inform. Theory, IT-8 (1962), 203-207.

[3] K. Lindström, The nonexistence of unknown nearly perfect binary codes, Sarja, Series A, Turun Yliopisto, Turku, 1975.

[4] J.H. van Lint, Recent results on perfect codes and related topics, in Combinatorics, Part 1, M. Hall, Jr. and J.H. van Lint (Eds.), Mathematical Center Tracts, No. 55, Math. Centrum, Amsterdam (1974), 158-178.

[5] N.V, Semakov, V.A. Zinovjev and G.V. Zaitzev, Uniformly packed codes, Problemy Peredachi Informatsii, 7 (1971), 38-50.

[6] A. Tietävainen, and A. Perko, There are no unknown perfect binary codes, Ann. Univ. Turku, Ser. AI 148 (1971), 3-10.

[7] A. Tietävainen, On the nonexistence of perfect codes over finite fields, SIAM J. Appl. Math. 24 (1973), 88-96.

[8] R.M. Wilson, Lecture Notes, Ohio State University, Columbus, Ohio.