A nonexistence proof for 4-error-correcting codes

Citation for published version (APA):

Document status and date:
Published: 01/01/1976

Publisher’s Version:
Published: 01/01/1976

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.
A Nonexistence Proof for 4-Error-Correcting Codes

by

H. Reuvers
A nonexistence proof for 4-error-correcting codes

by

H. Reuvers

1. Definitions

Let $S$ be a set of $q$ symbols and $V := S^n$. For $x \in V$, $y \in V$ define the Hamming distance $d(x, y)$ to be the number of coordinates in which $x$ and $y$ differ.

Let

$$S_e(x) := \{z \in V | d(z, x) \leq e\}.$$

A perfect $e$-error-correcting code is a subset $C \subseteq V$ such that the $S_e(x) (x \in C)$ form a partition of $V$.

2. Conditions

Necessary conditions for the existence of perfect codes are:

a) the sphere packing condition:

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

b) the polynomial condition (see [1], [2]):

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

has $e$ different integral zeros among $1, 2, 3, \ldots, n$.

3. Previous results

It was proved by A. Tietävainen (see [5], [6]) that if a perfect $e$-code on $q$ symbols exists and $e \geq 3$, then $q$ is divisible by at least three distinct primes.

In this paper we reduce $P_4(X)$ to a cubic polynomial which can be treated in a way like Van Lint did in [3] and I did in [4] to prove that there is no unknown perfect 3-code.
4. The case $e = 4$

In the following we shall prove that there does not exist a perfect four-error-correcting code, except maybe if $(n,q)$ belongs to a certain set of pairs, with cardinality 100 or so, some of whose elements $(n,q)$ maybe satisfy the sphere packing condition. In Lemma 3 we suppose that this is not true.

**Lemma 1.** Let $P(Z) := z^4 + pz^2 + rZ + s$ be a polynomial in $\mathbb{C}[Z]$ with four integral zeros. Then $Q(Z)$ has three integral zeros, where

$$Q(Z) := Z^3 - pz^2 - 4sz + 4ps - r^2.$$

**Proof.** Let $P(Z)$ have integral zeros $z_1, z_2, z_3, z_4$. Then we can write $p, r$ and $s$ as the symmetric expressions:

$$\begin{align*}
+ p &= z_1z_2 + z_1z_3 + z_1z_4 + z_2z_3 + z_2z_4 + z_3z_4 \\
- r &= z_1z_2z_3 + z_1z_2z_4 + z_1z_3z_4 + z_2z_3z_4 \\
+ s &= z_1z_2z_3z_4
\end{align*}$$

Now define

$$Q(Z) := (Z - y_1)(Z - y_2)(Z - y_3),$$

where

$$\begin{align*}
y_1 &= z_1^2 + z_3z_4 \\
y_2 &= z_1z_3 + z_2z_4 \\
y_3 &= z_2^2 + z_1z_4
\end{align*}$$

Then it is straightforward to show that

$$\begin{align*}
y_1 + y_2 + y_3 &= p \\
y_1y_2 + y_1y_3 + y_2y_3 &= -4s \\
y_1y_2y_3 &= r^2 - 4ps.
\end{align*}$$

Moreover, $y_1, y_2$ and $y_3$ are integers.
**Theorem.** A perfect four-error-correcting code does not exist.

**Proof.** Assume that there exists such a code, with parameters \( n, c, q \).

Then by \( \theta := qx - n(q - 1) \) and \( z := 2\theta + 3q - 8 \) the Lloyd polynomial \( P_4(x) \)
is transformed into \( T_4(z) := z^4 + pz^2 + rz + s \), where \( p, r \) and \( s \) shall
not be mentioned.

Following Lemma 1, we find that \( Q_3(z) \) must have three integral zeros, where

\[
Q_3(z) := z^3 - pz^2 - 4sz + 4ps - r^2.
\]

Since the coefficient of \((n - 4)^3\) in \( Q_3(z) \) is independent of \( z \) we substitute

\[
2y := z + 24(q - 1)(n - 4)
\]

and find that \( F(Y) \) must have three integral zeros, where

\[
F(Y) := a_2(Y)(n - 4)^2 + a_1(Y)(n - 4) + a_0(Y),
\]

and

\[
a_2(Y) := 3Y + 11q^2 + 16q - 16
\]

\[
a_1(Y) = -24(q - 1)(Y + 5q^2)(Y + q^2 + 4q - 4)
\]

\[
a_0(Y) = (Y - 3q^2)(Y + 3q^2)(Y + 5q^2).
\]

Now if \( Y_0 = -\frac{1}{3}(11q^2 + 16q - 16) \), we have: \( a_2(Y_0) = 0 \) and

\[
a_2(Y_0) - \frac{1}{3} = -32(q - 1)^2,
\]

and

\[
72q^4(q - 1) < a_1(Y) < 88q^4(q - 1)
\]

for \( Y = Y_0 \) and \( Y = Y_0 - \frac{1}{3} \), and

\[
0 < q_0(Y) < 8q^6 \text{ for } Y = Y_0 \text{ and } Y = Y_0 - \frac{1}{3}.
\]

Then we find:

\[
F(Y_0) > 72q^4(q - 1)(n - 4) > 0
\]

\[
F(Y_0 - \frac{1}{3}) < -32(q - 1)^2(n - 4)^2 + 88(q - 1)q^4(n - 4) + 8q^6,
\]
So

\[ F(Y_0 - \frac{1}{3}) < 0 \text{ if } n - 4 \geq \frac{14}{5} \frac{q^4}{q-1}. \]

Therefore, 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 \((Y_0 - \frac{1}{3}, Y_0)\).

Since this interval does not contain an integer we find that \( n - 4 < \frac{14}{5} \frac{q^4}{q-1} \).

Now we shall see in the following Lemmas 2 and 3 that this is impossible too. Hence we proved the theorem.

Lemma 2. Suppose that there exists a perfect four-error-correcting code with word length \( n - 4 < \frac{14}{5} \frac{q^4}{q-1} \), and let \( q = 2^{k_3} q' \), and \( \gcd(q', 6) = 1 \).

Then we have the following diagram of possibilities:

\[
\begin{array}{c|ccc}
  \ell & k = 0 & k = 1 & k = 2 & k \geq 3 \\
\hline
  \ell = 0 & q < 4 & q < 46 & q < 718 & q < 7 \\
  \ell \geq 1 & q < 10 & q < 136 & q < 2152 & q < 18
\end{array}
\]

Proof. Let \( x_1, x_2, x_3, x_4 \) be the zeros of the Lloyd polynomial \( P_4(x) \).

Then the following expressions must be integers:

\[
\begin{align*}
(i) & \quad x_1 + x_2 + x_3 + x_4 = \frac{4(n-4)(q-1)}{q} + 10 \\
(ii) & \quad x_1^2 + x_2^2 + x_3^2 + x_4^2 = 4(n-4)^2 + 20(n-4) + 30 - \frac{4(n-4)}{q^2}((2q-1)(n-3) + 4) \\
(iii) & \quad x_1^3 + x_2^3 + x_3^3 + x_4^3 = 4(n-4)^3 + 30(n-4)^2 + 90(n-4) + 100 - \frac{n-4}{q^3}((n-4)^2(12q^2 - 12q + 4) + (n-4)(24q^2 + 42q - 36) + (12q^2 + 54q + 24)) \\
(iv) & \quad P_4(1) = (n-1)(n-2)(n-3)(n-4)\frac{(q-1)^4}{q^4}
\end{align*}
\]

Then if \( 3 \mid q \) we see from (i) 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 (iii) that \(9 \mid n - 4\).

Furthermore, if \(8 \mid q\), we see from (i) that \(2 \mid n - 4\).
So \((2q - 1)(n - 3) + 4\) is odd.
Then, since \(64 \mid q^2\), we see from (ii) that \(4 \mid n - 4\).

Hence, since from (i) and (iv)
\(q \mid 4(n - 4)\) and
\(q^4 \mid (n - 1)(n - 2)(n - 3)(n - 4)\),
we can make the following diagram of possibilities, with A chosen in such a way that \(q^4 \mid A(n - 4)\):

\[
\begin{array}{cccc}
\lambda \backslash k & k = 0 & k = 1 & k = 2 & k \geq 3 \\
\lambda = 0 & A = 1 & A = 16 & A = 256 & A = 2 \\
\lambda \geq 1 & A = 3 & A = 48 & A = 768 & A = 6 \\
\end{array}
\]

Now is each of the cases listed in this diagram we have the condition

\[
\frac{q^4}{A} \leq n - 4 < \frac{14}{5} \frac{q^4}{q - 1} , \text{ so } q < \frac{14}{5} A + 1.
\]
So we have the diagram of possibilities listed in the lemmas statement.

**Lemma 3.** The several values of \(q\) listed in the statement of Lemma 2 are impossible too.

**Proof.** This can be checked by computer.

First of all, the \(q\) with only one or two prime divisors are excluded (since these are impossible following the results of Tietavainen).
Second, with each \(q\) is associated the (often unique) \(n\) such that

\[
q^4 \mid A(n - 4) \text{ and } n - 4 < \frac{14q^4}{5(q - 1)}.
\]
Finally for the remaining pairs \((n, q)\) it has to be verified that \(n\) and \(q\) do not satisfy the sphere packing condition.
Acknowledgements

Thanks to prof. Van Lint for some valuable suggestions, and for checking the calculations.

References


[6] A. Tietävainen; Nonexistence of nontrivial perfect codes in case $q = p_1^{r_1} p_2^{s_1}, e \geq 3$. Submitted to Discrete Mathematics.