A nonexistence proof for 3-error-correcting codes

Citation for published version (APA):

Document status and date:
Published: 01/01/1974

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.
A NONEXISTENCE PROOF FOR 3-ERROR-CORRECTING CODES

by

H. Reuvers

Department of Mathematics
University of Technology
PO Box 513, Eindhoven,
The Netherlands.
A nonexistence proof for 3-error-correcting codes

H. Reuvers

1. Definitions

Let $S$ be a set of $q$ symbols and $V := S^m$. 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

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

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

2. Conditions

Necessary conditions for the existence of perfect codes are:

a) the sphere packing condition:

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

b) the polynomial condition (see [3], [4]):

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

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

In this paper we only use the polynomial condition.

3. Previous results

A. Tietavainen proved that there are no perfect codes with $e > 1$, $q = p^m$, $p$ prime, except for trivial codes and the two Golay codes (see [2]). We use a method employed by J.H. van Lint in [1] to prove that there are not perfect codes if $e = 3$, and $q$ is not a prime power. Therefore the binary Golay code is the only nontrivial 3-error-correcting perfect code over any alphabet. From now on we assume that $q$ is not a prime power.
4. Lemma 1. Let \( t := n(q - 1) \), \( \theta := qx - t \). By \( \theta \) and \( t \) the Lloyd polynomial \( P_3(x) \) is transformed into:

\[
P_3(x) = F(\theta) = \theta^3 + 3(q - 3)\theta^2 + (2q^2 - 9q + 18)\theta - 6 - t(3\theta + 2q - 7) .
\]

There must be a zero \( \theta_0 = qx_0 - t \) (with \( x_0 \in \mathbb{Z} \)) of \( F(\theta) \) if a perfect code with \( e = 3 \) exists, such that \( -(q - 3) < \theta_0 < 1 \).

Proof. \( F(3 - q) = (q - 1)(q - 2)(n - 3) > 0 \)

\( F(1) = 2(q - 1)(q - 2)(1 - n) < 0 \).

The lemma now follows from the polynomial condition.

5. Proposition 1. There is no perfect code with \( e = 3 \) if \( 3 \nmid q \).

Proof.

i) For the roots \( x_1, x_2, x_3 \) of the Lloyd polynomial \( P_3(x) \) we have (if a perfect code exists with \( e = 3, 3 \nmid q \))

\[
x_1 + x_2 + x_3 = \frac{3(n - 3)}{q} (q - 1) + 6
\]

so \( q \mid 3(n - 3) \), so if \( 3 \nmid q \) we have \( n = 3 + qv \).

ii) Since \( q > 2 \) we have:

\[ n - v - 1 < n - v - 2/q < n - v . \]

Hence there is no integer \( x_0 \) such that

\[ qn - qv - 3 + 3 - q < qx_0 < qn - qv - 2 , \]

i.e.

\[ t + 3 - q < qx_0 < t + 1 . \]

iii) Now remark that ii) contradicts lemma 1 if we assume the existence of a perfect code with \( e = 3, 3 \nmid q \).

6. Proposition 2. There is no perfect code with \( e = 3 \) if \( q = 3p \), where \( p \in \mathbb{N}, p \neq 2 \).
Proof.

i) For the roots $x_1, x_2, x_3$ of the Lloyd polynomial $P_3(x)$ we have (if a perfect code exists with $e = 3$, $q = 3p$)

$$x_1 + x_2 + x_3 = \frac{3(n - 3)}{q} (q - 1) + 6,$$

so $q | 3(n - 3)$, so $n = 3 + pv$.

ii) Since $p > 2$ we have:

$$n - v - 1 < n - v - 2/p < n - v.$$

Hence there is no integer $z_0$ such that

$$pn - pv - 3 + 3 - p < pz_0 < pn - pv - 2 ,$$

i.e.

$$pn - n + 3 - p < pz_0 < pn - n + 1 .$$

By the substitution $y_0 := z_0 + 2n$ we find that there is no integer $y_0$ such that

$$t + 3 - p < py_0 < t + 1 .$$

Now assume there is a $x_0 \in \mathcal{E}$ such that

$$t + 3 - q < qx_0 < t + 1 .$$

Then for $y_0 = 3x_0$ we have:

$$t + 3 - q < py_0 < t + 1 .$$

But since there is no integer $y_0$ such that

$$t + 3 - p < py_0 < t + 1$$

and hence no integer $y_0$ such that

$$t + 3 - 2p < py_0 < t + 1 - p$$

or

$$t + 3 - q < py_0 < t + 1 - 2p$$

We conclude that $py_0 = qx_0$ must have one of the values:
\[ t + 3p, t + 2p, t + 1p, t + 3 - 2p, t + 2 - 2p, t + 1 - p. \]

Now, since \( t \equiv n(q - 1) \equiv -n \equiv -3 \pmod{p} \) and \( p \neq 2 \), we can only have \( qx_0 - t = 3 - p \) or \( qx_0 - t = 3 - 2p \).

iii) According to lemma 1 we must have \( F(3 - p)F(3 - 2p) = 0 \) if a perfect code exists with \( e = 3 \), \( q = 3p \).

\[
F(3 - p) = -10p^3 + 27p^2 + 9p + 48 - t(3p + 2) < 0
\]
since \( t = n(q - 1) > 3p \) and \( p \geq 5 \),

\[
F(3 - 2p) = -8p^3 + 18p + 48 - 2t < 0
\]
since \( t = n(q - 1) > 3p \) and \( p \geq 5 \).

So we find a contradiction to lemma 1 and therefore we have proved proposition 2.

7. Proposition 3. There is no perfect code with \( e = 3 \) and \( q = 6 \).

Proof. Assume there is such a code. Then, according to lemma 1 we must have \( F(-2)F(-1)F(0) = 0 \).

But \( F(-2) = -50 + 5n \neq 0 \) unless \( n = 10 \),

\[
F(0) = -6 - 25n < 0, \\
F(-1) = -34 - 10n < 0,
\]
so we must have \( n = 10 \).

Then we have \( n = 10, q = 6, e = 3 \) and

\[
x_1 + x_2 + x_3 = \frac{5(10 - 3)}{2} + 6 = \frac{47}{2} \notin \mathbb{Z}
\]
a contradiction.

8. Theorem. There is no perfect code with \( e = 3 \), \( q \) not a power of a prime.

Proof. This is proved by combining propositions 1, 2 and 3.
9. References


