TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY

On perfect ternary constant weight codes

Citation for published version (APA):
van Lint, J. H., & Tolhuizen, L. M. G. M. (1999). On perfect ternary constant weight codes. *Designs, Codes and Cryptography*, *18*(1-3), 231-234. https://doi.org/10.1023/A:1008314009092

DOI:
10.1023/A:1008314009092

Document status and date:
Published: 01/01/1999

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: 19. Jan. 2021


Designs, Codes and Cryptography, 18, 231–234 (1999)
© 1999 Kluwer Academic Publishers, Boston. Manufactured in The Netherlands.

On Perfect Ternary Constant Weight Codes

JACK VAN LINT* wsdwjhvl@urc.tue.nl
Stan Ackermans Institute, Eindhoven University of Technology, Eindhoven, the Netherlands

LUDO TOLHUIZEN
Philips Research Laboratories, Eindhoven, the Netherlands

Accepted November 22, 1998

Dedicated to the memory of E. F. Assmus

Abstract. We consider the space of ternary words of length n and fixed weight w with the usual Hamming distance. A sequence of perfect single error correcting codes in this space is constructed. We prove the nonexistence of such codes with other parameters than those of the sequence.

Keywords: constant weight code, perfect code.

1. Introduction

We use the usual terminology of coding theory. In this note we shall consider as space R the subset of all words of fixed weight w in $\mathbb{F}_3^n$ for given w and n. Hamming distance $d(\mathbf{a}, \mathbf{b})$ of two words $\mathbf{a}, \mathbf{b}$ is defined in the usual way. Clearly, the total number of words in R is $\binom{n}{w}2^w$.

A subset C of R will be called a *perfect single error correcting code* if every word in R has Hamming distance 0 or 1 to *exactly* one word in C. Since the number of words in a Hamming ball of radius 1 in R is $w+1$, one can prove that C is indeed such a perfect code by showing that C has minimum distance 3 and that $|C| = \binom{n}{w}2w/(w+1)$.

An easy example of such a code is obtained from the ternary Hamming code of length 4 by deleting the all-0 word. Here $n = 4$, $w = 3$, and $|C| = 8$. Recently T. Ericson showed the first author a construction of such a code of length 8 due to M. Svanström. This triggered our interest in these codes. In this note we shall show that the code of length 8 is an element of an infinite sequence of perfect ternary constant weight codes with parameters $n = 2^l$, $w = n - 1$. In our construction, the code size is obviously 2^{n-1}, so we only have to show that the minimum distance is 3. We also show that these parameters are the only ones for which perfect single error correcting ternary codes exist. In fact, the proof of the nonexistence theorem shows that the construction that we give is more or less forced.

2. A Lemma

Let C be a ternary constant weight code of length n with $d = 3$. Clearly

$$|C| \le \frac{\binom{n}{w}2^w}{w+1}. \tag{2.1}$$

* This paper was solicited by the Editors-in-Chief

If equality holds in (2.1), then C is perfect.

Now, let C be perfect (i.e. we have equality in (2.1)). Define the subcode C_i of C by

$$C_i := \{\mathbf{c} \in C | c_i = 0\}, \qquad (i = 1, \ldots, n). \tag{2.2}$$

Each word in C is in exactly $n - w$ of these subcodes. Hence we have

$$\frac{1}{n}\sum_{i=1}^{n} |C_i| = \frac{n-w}{n}|C| = \frac{\binom{n-1}{w}2^w}{w+1}. \tag{2.3}$$

Since deleting the i-th symbol in C_i yields a ternary constant weight code of length $n-1$, it follows from (2.1) and (2.3) that each of these shortened codes is again perfect. We state this as a lemma.

LEMMA 1 *If C is a perfect single error correcting ternary constant weight code with parameters n and w, then the shortened codes, defined by deleting the i-th coordinate in the codes C_i of (2.2), are also perfect* (*with parameters $n-1$ and w*).

COROLLARY 1 *If the code of Lemma 1 exists, then $w+1$ must be a power of 2.*

Proof. Apply Lemma 1 $n - w$ times to find a code with $2^w/(w+1)$ words. ∎

Remark 1. The result of applying the lemma $n - w$ times is essentially a binary code which is perfect (with the Hamming parameters).

3. An Infinite Sequence of Perfect Ternary Constant Weight Codes

If C is a perfect ternary constant weight code of length 2^l and weight $w = 2^l - 1$, then by Remark 1, the code obtained by considering the words with a zero in position i and then deleting this zero is a binary perfect single error correcting code (on the alphabet $\{1, 2\}$). If we replace each zero coordinate in C by a 1 or a 2 in such a way that the new words have an even number of 1's and 2's, then the fact that these words are all different implies that we have obtained the even weight binary code of length 2^l. We exploit this by considering the even weight binary code as a union of cosets of the extended binary Hamming code.

We first need a lemma. Let $n = 2^l - 1$ and let α be a primitive element in $\mathbb{F}_{2^l}$ ($l \geq 3$). Let $\mathcal{H}$ be the binary Hamming code of length n, i.e. the cyclic code generated by the irreducible polynomial with α as a zero. Codewords are written as $\mathbf{c} = (c_0, c_1, \ldots, c_{n-1})$ and also as $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$.

LEMMA 2 *$\mathcal{H}$ does not contain a word of weight 4 with 1's in the positions i, $i+1$, j, $j+1$.*

Proof. If there were such a word, then $\alpha^i + \alpha^{i+1} + \alpha^j + \alpha^{j+1} = 0$, i.e. we would have $(1+\alpha)(1+\alpha^{j-i}) = 0$, contradicting the fact that α is primitive. ∎

Denote the $[2^l, 2^l - l - 1, 4]$ extended code by $\overline{\mathcal{H}}$ and denote the overall parity check symbol by c_∞.

We decompose the even-weight code of length $n+1$ into cosets of $\overline{\mathcal{H}}$. Each proper coset contains $(n+1)/2$ words of weight 2 of which the supports form a partition of $\{0, 1, \ldots, n-1, \infty\}$. We denote the coset that contains the word of weight 2 with 1's in position i and position ∞ by $\overline{\mathcal{H}_i}$, $(i = 0, 1, \ldots, n-1)$.

The Construction

We define $n+1$ ternary codes $\mathcal{T}, \mathcal{T}_0, \mathcal{T}_1, \ldots, \mathcal{T}_{n-1}$ as follows. The code $\mathcal{T}$ is obtained from $\overline{\mathcal{H}}$ by replacing the symbol in position ∞ by a 2. The code $\mathcal{T}_i$ is obtained from $\overline{\mathcal{H}_i}$ by replacing the symbol in position $i+1$ by a 2, where we interpret the indices mod n.

PROPOSITION 1 *Each of the codes $\mathcal{T}_i$ and $\mathcal{T}$ have minimum distance 3.*

Proof. Trivial. ■

We now consider two codes $\mathcal{T}_i$ and $\mathcal{T}_j$ $(0 \le i < j \le n-1)$. We distinguish between $j = i+1$ and $j > i+1$.

First, let $j = i+1$. Consider two words $\mathbf{a}' \in \mathcal{T}_i$, $\mathbf{b}' \in \mathcal{T}_j$. These have the form

$$\mathbf{a}' = (a_0, \ldots, a_i + 1, 2, a_{i+2}, a_{i+3}, \ldots, a_{n-1}, a_\infty + 1)$$

and

$$\mathbf{b}' = (b_0, \ldots, b_i, b_{i+1} + 1, 2, b_{i+3}, \ldots, b_{n-1}, b_\infty + 1),$$

where $\mathbf{a}$ and $\mathbf{b}$ are in $\overline{\mathcal{H}}$; (here addition is still mod 2).

If $\mathbf{a} = \mathbf{b}$, then $\mathbf{a}'$ and $\mathbf{b}'$ differ in positions i, $i+1$, and $i+2$. If $\mathbf{a} \neq \mathbf{b}$, then $\mathbf{a}'$ and $\mathbf{b}'$ differ in positions $i+1$ and $i+2$ and in at least one position $\neq i$ because $\mathbf{a}$ and $\mathbf{b}$ have distance ≥ 4. Hence $d(\mathbf{a}', \mathbf{b}') \ge 3$.

Now suppose $j \ge i+2$. We find

$$\mathbf{a}' = (a_0, \ldots, a_i + 1, 2, \ldots, a_j, a_{j+1}, \ldots, a_{n-1}, a_\infty + 1)$$

and

$$\mathbf{b}' = (b_0, \ldots, b_i, b_{i+1}, \ldots, b_j + 1, 2, \ldots, b_{n-1}, b_\infty + 1).$$

If $\mathbf{a} = \mathbf{b}$, then clearly $d(\mathbf{a}', \mathbf{b}') = 4$. If $\mathbf{a} \neq \mathbf{b}$, then $d(\mathbf{a}', \mathbf{b}') = 2$ would imply that there is a codeword of weight 4 in C with its 1's in the positions i, $i+1$, j, and $j+1$, contradicting Lemma 2. Hence, again a word in $\mathcal{T}_i$ and a word in $\mathcal{T}_j$ have distance at least 3. A similar argument applies to a word in $\mathcal{T}_i$ and one in $\mathcal{T}$.

We have proved the following proposition.

PROPOSITION 2 *The ternary code $\mathcal{T} \cup \mathcal{T}_0 \cup \cdots \cup \mathcal{T}_{n-1}$ has minimum distance 3.*

Each word of this code has exactly one coordinate equal to 2. So, by adding $(1, 1, \ldots, 1)$ to all the codewords we find a new ternary code of length $n+1$ of the same size and minimum distance 3 with all its words of weight n. Since this code has 2^n codewords, our construction is complete.

THEOREM 1 *There exists a sequence of ternary constant weight perfect single error correcting codes with length $n + l = 2^l$ and weight n ($l \geq 3$).*

Note that for $l = 1$ there is a trivial example and for $l = 2$ an example was given in the introduction.

4. A Nonexistence Theorem

Suppose C is a ternary constant weight code with weight $w = 2^l - 1$, length $n = w + 2$, and $d = 3$. Define

$$S := \{(\mathbf{c}, \mathbf{x}) | \mathbf{c} \in C, \mathbf{x} \in \{1, 2\}^n, (c_i \neq 0) \Rightarrow (c_i = x_i), (i = 1, \ldots, n)\} \tag{4.1}$$

Clearly

$$|S| = 4|C|. \tag{4.2}$$

Let $\mathbf{c}$ and $\mathbf{d}$ be in C, $\mathbf{x} \in \{1, 2\}^n$ and $(\mathbf{c}, \mathbf{x})$ and $(\mathbf{d}, \mathbf{x})$ both in S. Note that $c_i = x_i = d_i$ for all i for which $c_i \neq 0$ and $d_i \neq 0$. The fact that C has distance 3 implies that either $\mathbf{c} = \mathbf{d}$ or there is no position where $c_i = d_i = 0$. Therefore, for each $\mathbf{x}$ there are at most $\frac{n-1}{2}$ codewords $\mathbf{c}$ such that $(\mathbf{c}, \mathbf{x}) \in S$, i.e.

$$|S| \leq 2^n \left(\frac{n-1}{2} \right). \tag{4.3}$$

Hence

$$|C| \leq 2^{n-3}(n-1) = 2^{w-1}(w+1) < \frac{2^w \binom{w+2}{w}}{w+1}$$

and therefore it follows from (2.1) that C is *not* perfect.

We have proved the following theorem.

THEOREM 2 *A perfect single error correcting constant weight code with parameters $w = 2^l - 1$ and $n = w + 2$ does not exist.*

If we combine Theorem 1 with Lemma 1, we find our main result.

THEOREM 3 *If C is a perfect single error correcting ternary constant weight code, then either C is essentially a binary perfect code of length $2^l - 1$ (so $n = w = 2^l - 1$), or we have $w = 2^l - 1$ and $n = w + 1$ for some l.*

We cannot show that the codes constructed in Section 3 are unique and in fact we doubt that this is the case. Since there are many codes with the parameters of Hamming codes, these can conceivably be combined in a similar way to form ternary perfect codes.