Discrete Mathematics 309 (2009) 2202–2216

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

# Full rank perfect codes and $\alpha$-kernels

Olof Heden

*Department of Mathematics, KTH, S-100 44 Stockholm, Sweden*

ARTICLE INFO

*Article history:*
Received 8 December 2004
Received in revised form 18 April 2008
Accepted 25 April 2008
Available online 4 June 2008

*Keywords:*
Perfect codes

ABSTRACT

A perfect 1-error correcting binary code $C$, perfect code for short, of length $n = 2^m - 1$ has full rank if the linear span $\langle C\rangle$ of the words of $C$ has dimension $n$ as a vector space over the finite field $F_2$. There are just a few general constructions of full rank perfect codes, that are not given by recursive methods using perfect codes of length shorter than $n$. In this study we construct full rank perfect codes, the so-called *normal $\alpha$-codes*, by first finding the superdual of the perfect code.

The superdual of a perfect code consists of two matrices $G$ and $T$ in which simplex codes play an important role as subspaces of the row spaces of the matrices $G$ and $T$. The main idea in our construction is the use of $\alpha$-words. These words have the property that they can be added to certain rows of generator matrices of simplex codes such that the result will be (other) sets of generator matrices for simplex codes.

The kernel of these normal $\alpha$-codes will also be considered. It will be proved that any subspace, of the kernel of a normal $\alpha$-code, that satisfies a certain property will be the kernel of another perfect code, of the same length $n$. In this way, we will be able to relate some of the full rank perfect codes of length $n$ to other full rank perfect codes of the same length $n$.

## 1. Introduction

A *perfect 1-error correcting binary code*, or for short *perfect code*, of length $n$, is a subset $C$ of the direct product $Z_2^n$ satisfying the following property:

*To any element $x = (x_1, x_2, \ldots, x_n)$ of $Z_2^n$ there is a unique element $c = (c_1, c_2, \ldots, c_n)$ of $C$ such that $x$ and $c$ differ in at most one coordinate position.*

For basic facts about perfect codes see e.g. [23]. Let us only remark that, by counting the number of words, one can easily see that the length $n$ of a perfect code is always equal to $n = 2^t - 1$, for some integer $t$, and that the size of $C$ will be equal to $|C| = 2^{n-\log(n+1)}$. Further for any integer $t$ there is at least one perfect code of length $n = 2^t - 1$, as was proved by Hamming [8]. More precisely, a so-called *Hamming* code of length $n = 2^t - 1$ is the null space of a $t \times n$-matrix $H$, which as columns has all the nonzero binary words of length $t$. Hamming codes are linear perfect codes.

There are now very many, in fact more than 20, different constructions of nonlinear perfect codes, but not yet any classification or enumeration of them, not even for such a small length as $n = 15$. The first construction of a nonlinear perfect code was given by Vasil'ev [24]. Other researchers, who have contributed with nice constructions, are Zinov'ev [25], Mollard [16], Solov'eva [22], Phelps [19] and Avgustinovich and Solov'eva [2].

Here we will consider perfect codes that have full rank, a concept that we now define.

The *rank* of a perfect code $C$, $rank(C)$, is the dimension of the subspace spanned by the elements, or *words*, of $C$, where we consider $Z_2^n$ as a vector space over the finite field $Z_2$. A perfect code $C$ of length $n$, is said to be of *full rank* if $rank(C) = n$.

*E-mail address:* olohed@math.kth.se.

0012-365X/$ – see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.disc.2008.04.051

The study of full rank perfect codes is essential, as these codes are important and fundamental ingredients in the construction of perfect codes given by tilings, for details see [6].[1]

Our main result will be:

*A new construction of full rank perfect codes.*

These codes will be called *normal $\alpha$-codes* and their precise construction will be given in Section 3. Thereby we will use the superdual of a perfect code. That concept was introduced in [11] and will be summarized in the next section. The advantage with this construction is that these codes are formally easy to construct and it is easy to find many examples of full rank perfect codes by using this construction. The proof of the general theorem that says that all normal $\alpha$-codes are full rank perfect codes, is however a bit long, although not very complicated.

The *kernel* of a perfect code $C$, $\ker(C)$, is the set of *periods* $p$ of $C$, i.e.

$$\ker(C) = \{p \in Z_2^n \mid p + C = C\} \quad \text{where } p + C = \{p + c \mid c \in C\}.$$

The kernel of a perfect code is always a subspace of $Z_2^n$. If the all zero word $(0, 0, \ldots, 0)$ belongs to $C$ then the kernel is a subset of $C$. It was proved by Shapiro and Slotnik [21], that the kernel of any perfect code, besides the all zero word $(0, 0, \ldots, 0)$, always contains the all one word $(1, 1, \ldots, 1)$.

An example of a normal $\alpha$-code was already given in [14]. There we gave an example of a full rank perfect code of length 31 and with a kernel of dimension 21. That example finalized the *rank–kernel problem* of Etzion and Vardy [7], which was to find all possible triples $(n, r, k)$ for which there exists a perfect code of length $n$, rank $r$, containing the all zero word and with a kernel of dimension $k$. For given $n$ and given $r$ respectively $k$, the following upper and lower bounds were given by Phelps and Villanueva [20] and independently by Avgustinovich, Heden and Solov'eva [3]:

$$k \geq \begin{cases} 2^{n-r} & \text{if } n - \log(n+1) + 1 < r \leq n, \\ 2^{n-r} - 1 & \text{if } r = n - \log(n+1) + 1, \end{cases} \tag{1}$$

and

$$r \leq k + 2^{n-\log(n+1)-k} - 1. \tag{2}$$

It is worth mentioning that, an asymptotically complete solution to the problem of existence was already given by Avgustinovich, Heden and Solov'eva [5], and that it is now clear, see [14] for details, that the only cases for which there does not exist any perfect code with parameters $(n, r, k)$, where $n = 2^t - 1$ and $t \geq 4$, satisfying the inequalities in the above Eqs. (1) and (2), are when

$$(n, r, k) \in \{(15, 15, 6), (15, 15, 7), (15, 15, 8), (31, 31, 22)\}.$$

As a consequence of the construction of normal $\alpha$-codes, we will prove in Section 6 the following result, that we found both useful and not quite out of interest.

*Let $C$ be any normal $\alpha$-code of length $n$. For any $\alpha$-subspace $F$ of $Z_2^n$ satisfying*

$$\{0\} \neq F \subseteq \ker(C),$$

*the subspace $F$ will be the kernel of some full rank perfect code of length $n$.*

(The concept $\alpha$-subspace will be described in the next section.) These $\alpha$-subspaces are easy to find, and there will be many of them. Hence, by using this result one may obtain, as we will see in Section 6, many distinct full rank perfect codes. It should perhaps also be remarked that the kernel structure of full rank perfect codes has not yet been studied very much, but that in this paper we at least obtained some information at least for the kernel of normal $\alpha$-codes. We will also observe that the kernel of any normal $\alpha$-code is contained in some Hamming code and that all normal $\alpha$-codes are systematic.

Another motivation for this study was to have a look at the superdual of a full rank perfect code. In any case, the construction below has not yet been described before, and particularly, we have found full rank perfect codes of length 15 with a kernel of dimensions 4 and 5, without any computer search.[2]

## 2. Preliminaries

The *weight* of a word $c$, $w(c)$, is the number of nonzero coordinates of $c$. The *support* of a word $c = (c_1, c_2, \ldots, c_n)$ is the following set:

$$\text{supp}(c) = \{i \mid c_i \neq 0\}.$$

[1] In the paper *The partial order of perfect codes associated to a perfect code*, submitted, by the author, it is shown that to every perfect code one may associate a partial order of perfect codes. The atoms in this partial order are either full rank perfect codes or linear perfect codes.

[2] As pointed out by the referee, perfect codes with these parameters and found without a computer search, were already presented by S.A. Malyugin in the journal Discrete Analysis and Operation Research, 13 (1) (2006) 77–98, Novosibirsk (Russia).