Additive quaternary codes of small length

Jürgen Bierbrauer jbierbra@mtu.edu
Department of Mathematical Sciences Michigan Technological University Houghton, Michigan 49931 (USA)

Giorgio Faina faina@dipmat.unipg.it

Stefano Marcugini gino@dipmat.unipg.it

Fernanda Pambianco fernanda@dipmat.unipg.it
Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli 1, Perugia, 06123, ITALY

Abstract. In this paper the non-existence of an additive $[12, 7, 5]_4$-code is proved. This is part of an ongoing work about the existence of the additive quaternary codes of length ≤ 12.

1 Introduction

Additive codes are generalizations of linear codes, see for example Chapter 17 of [2] for a general introduction and a theory of cyclic additive codes. Here we concentrate on the quaternary case.

Definition 1. *Let k be such that $2k$ is a positive integer. An additive quaternary $[n, k]_4$-code $\mathcal{C}$ (length n, dimension k) is a $2k$-dimensional subspace of $\mathbb{F}_2^{2n}$, where the coordinates come in pairs of two. We view the codewords as n-tuples where the coordinate entries are elements of $\mathbb{F}_2^2$.*

A **generator matrix** *G of $\mathcal{C}$ is a binary $(2k, 2n)$-matrix whose rows form a basis of the binary vector space $\mathcal{C}$.*

Definition 2. *Let $\mathcal{C}$ be an additive quaternary $[n, k]_4$-code. The* **weight** *of a codeword is the number of its n coordinates where the entry is different from 00. The minimum weight (equal to* **minimum distance***) d of $\mathcal{C}$ is the smallest weight of its nonzero codewords.*

The strength of $\mathcal{C}$ is the largest number t such that all $(2k, 2t)$-submatrices of a generator matrix whose columns correspond to some t quaternary coordinates have full rank $2t$.

Notation for length and dimension has been chosen to facilitate comparison with quaternary **linear** codes. In fact it is clear that each linear $[n, k]_4$-code is also an additive $[n, k]_4$-code (where k of course is an integer) and the notations of minimum distance and strength of the linear code coincide with the additive notions introduced above.

The geometric description of an additive $[n, k]_4$-code is based on lines in the projective space $PG(2k-1, 2)$. In fact, consider a generator matrix G. For each quaternary coordinate $i \in \{1, 2, \ldots, n\}$ we have two points $P_i, Q_i \in PG(2k-1, 2)$. Let L_i be the line determined by P_i, Q_i. The geometric description of code $\mathcal{C}$ is based on this multiset of lines (the **codelines**) $\{L_1, L_2, \ldots, L_n\}$. Code $\mathcal{C}$ has minimum distance $\geq d$ if and only if for each hyperplane H of $PG(2k-1, 2)$ we find at least d codelines (in the multiset sense), which are not contained in H. Strength t means that any set of t codelines is in general position. Duality is based on the Euclidean bilinear form, the dot product for binary spaces. The dual of an additive $[n, k]_4$-code $\mathcal{C}$ is an $[n, n-k]_4$-code, and $\mathcal{C}$ has strength t if and only if $\mathcal{C}^\perp$ has minimum distance $> t$.

Recall that the geometric description of linear codes is based on multisets of points, whereas the geometric description of additive quaternary codes uses lines. There are two ways for a line L not to be contained in hyperplane H. Either L is skew to H meaning $L \cap H = \emptyset$ or L meets H in a point. The latter situation suggests to consider mixed quaternary-binary codes.

Definition 3. *An $[(l, r), k]_{(4,2)}$-code is a $2k$-dimensional vector space of binary $(2l + r)$-tuples, where the coordinates are divided into l pairs (written on the left) and r single coordinates. We view each codeword as an $(l + r)$-tuple, where the left coordinates are quaternary, the right ones are binary.*

A code $[(l, r), k]_{(4,2)}$ is described geometrically by a multiset of l lines and r points (codelines and codepoints) in $PG(2k-1, 2)$. The code has strength $\geq t$ if any set of t objects (codepoints or codelines) are in general position. The definition of minimum distance (equal to the minimum weight) is obvious. A generator matrix is a binary $(2k, 2l+r)$-matrix whose rows form a binary basis of the code. The dual of an additive $[(l, r), k]_{(4,2)}$-code of strength t is an additive $[(l, r), l + r/2 - k, t + 1]_{(4,2)}$-code.

Blokhuis-Brouwer [1] determine the optimal code parameters for additive quaternary codes of length ≤ 12, with two exceptions. Our main result is the following:

Theorem 1. *There is no additive $[12, 7, 5]_4$-code.*

The only remaining existence problem for additive quaternary codes in length less than or equal to twelve concerns the parameters $[12, 4.5, 7]_4$. Our work on this problem is near completion. We are convinced that such a code cannot exist.

In Section 2 we start with a synthetic construction of a self-dual $[7, 3.5, 4]_4$-code. The proof of Theorem 1 is in Section 3.

2 A self-dual $[7, 3.5, 4]_4$-code

A computer construction of a cyclic additive $[7, 3.5, 4]_4$-code was given in [1]. We start with a synthetic construction of this code.

Let $\Omega = \{1, 2, 3, 4, 5, 6, 7\}$. There are exactly 30 Fano planes that can be constructed on the point set Ω. Any two different Fano planes on Ω have either $0, 1$ or 3 lines in common. In particular there exist pairs of Fano planes that do not have lines in common. For these facts see for example [3]. The fact that there exist 2 but not 3 linewise disjoint Fano planes on a given 7-element ground set is attributed to Cayley [5]. Let F_1, F_2 be a pair of linewise disjoint Fano planes and D_1, D_2 codes $[7, 3, 4]_2$, that is binary codes geometrically described by F_1 and F_2, respectively. For D_1 use as alphabet $00, 01$, for D_2 the alphabet $00, 10$ and consider both as embedded in Q^7, where $Q = \mathbb{F}_2^2$. Let D be the (direct) sum of D_1 and D_2. Then D is a $[7, 3, 4]_4$-code. Because of the linewise disjointness of F_1, F_2 we have that $(11)^7$ has distance 4 from D and together with D generates an additive $[7, 3.5, 4]_4$-code. This code is self-orthogonal with respect to the dot-product.

Observe that additive codes which are self-dual or self-orthogonal with respect to the symplectic form correspond to quantum codes. A length 7 distance 4 quantum code cannot exist, see [4].

A computer program showed that 7 points can be appended to our code. This leads to a mixed $[(7, 7), 3.5]_{(4,2)}$-code of strength 3.

3 Nonexistence of an additive $[12, 7, 5]_4$-code

It is easier to use the dual, a $[12, 5]_4$-code of strength 4. What is the maximum hyperplane intersection of this code $\mathcal{C}$? It is impossible that there are at most 5 lines on each hyperplane as this would produce an additive $[12, 5, 7]_4$-code, which does not exist. It follows that there must be a hyperplane with at least 6 codelines. There can be no 8 codelines on any hyperplane as this would yield a $[8, 4.5]$ code of strength 4 whose dual would be a $[8, 3.5, 5]_4$-code. Such a code does not exist.

Lemma 1. *The maximum number of lines of a* $[12, 5]_4$*-code of strength* 4 *on a hyperplane is either* 6 *or* 7.

In particular we find a hyperplane that contains 6 codelines. This defines an additive $[6, 4.5]_4$-code. Its dual, a $[6, 1.5, 5]_4$-code, corresponds to using all lines but one of the Fano plane and is therefore uniquely determined. The following codelines can be used to describe our $[6, 4.5]_4$-code of strength 4 :

$$L_1 = \langle v_1, v_2 \rangle,\ L_2 = \langle v_3, v_4 \rangle,\ L_3 = \langle v_5, v_6 \rangle,\ L_4 = \langle v_7, v_8 \rangle,$$

$$L_5 = \langle v_1 + v_3 + v_5 + v_7, v_9 \rangle, L_6 = \langle v_2 + v_4 + v_6 + v_8, v_9 + v_1 + v_4 + v_5 + v_6 \rangle$$

We ran a computer program that determined the points completing those lines to a $(6, 1)$-code of strength 4. There are 45 such points. Exactly 24 of those points are distributed on lines that complete the $[6, 4.5]$-code to a $[7, 4.5]$-code of strength 4. There are thus 8 such lines.

Assume at first there is a hyperplane H containing 7 codelines of $\mathcal{C}$. We can choose $L_1, \ldots, L_6$ above and L_7 is one of the 8 lines that our computer search produced. The intersection with the codelines shows that this code must be embeddable in a mixed $[(7, 5), 4.5]_4$-code of strength 4. A computer search showed that not even a single point can be appended:

Proposition 1. *There is no* $[(7, 1), 4.5]_4$*-code of strength* 4.

We conclude that the maximum number of codelines on a hyperplane is 6. We can choose $L_1, \ldots, L_6$ as above. The intersection with the remaining codelines shows that this can be extended to a $[(6, 6), 4.5]_4$-mixed code of strength 4. The points forming the sextuple must be from the set of 45 extension points mentioned above. A computer search showed that there are exactly six such sextuples. In particular $[(6, 6), 4.5]_4$-mixed codes of strength 4 and their duals, $[(6, 6), 4.5, 5]_4$-codes do exist.

Another computer program showed that none of those six codes can be embedded in a $[12, 5]_4$-code of strength 4.

References

[1] A. Blokhuis and A. E. Brouwer, *Small additive quaternary codes European Journal of Combinatorics* **25** (2004), 161-167.

[2] J. Bierbrauer: *Introduction to Coding Theory,*
Chapman and Hall/ CRC Press 2004.

[3] J. Bierbrauer: *Nordstrom-Robinson code and A_7-geometry, Finite Fields and Their Applications*, to appear.

[4] A. R. Calderbank, E. M. Rains, P. M. Shor, N. J. A. Sloane:
Quantum error-correction via codes over $GF(4)$,
IEEE Transactions on Information Theory **44** (1998), 1369-1387.

[5] A. Cayley: *On the triadic arrangements of seven and fifteen things, London, Edinburgh and Dublin Philos. Mag and J.Sci* **37** (1850), 50-53.