Short additive quaternary codes

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI (USA)

Yves Edel*
Department of Pure Mathematics and Computer Algebra
Ghent University
Ghent (Belgium)

Giorgio Faina,
Stefano Marcugini and Fernanda Pambianco
Dipartimento di Matematica
Università degli Studi di Perugia
Perugia (Italy)

Abstract

We use the geometric description to determine the best parameters of quaternary additive codes of small length. Only one open question remains for length ≤ 13. Among our results are the non-existence of $[12, 7, 5]$-codes and $[12, 4.5, 7]$-codes as well as the existence of a $[13, 7.5, 5]-$code.

*The research of the author is supported by the Interuniversitary Attraction Poles Programme-Belgian State-Belgian Science Policy: project P6/26-Bcrypt.

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 $[n,k]$-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 $[n,k]$-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 parameters are then also written $[n,k,d]$.*

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 $[n,k]$-code is also an additive $[n,k]$-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 $[n,k]$-code is based on lines in $PG(2k-1,2)$. In fact, consider a generator matrix G. For each quaternary coordinate $i \in \{1,2,\dots,n\}$ we are given 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 $\mathcal{C}$ as in Definition 2 is based on this multiset of lines (the **codelines**) $\{L_1, L_2, \dots, L_n\}$. 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 $[n,k]$-code $\mathcal{C}$ is an $[n,n-k]$-code, and $\mathcal{C}$ has strength t if and only if $\mathcal{C}^\perp$ has minimum distance $> t$.

As an example consider the following analogue of the Simplex codes:

Definition 3. *Let $\mathcal{S}_l$ be the additive quaternary code described by the set of all lines in $PG(l-1,2),\ l \geq 3$.*

As the number of lines in $PG(l-1,2)$ is $(2^l-1)(2^{l-1}-1)/3$ it follows that $\mathcal{S}_l$ is an additive $[(2^l-1)(2^{l-1}-1)/3, l/2, 2^{l-2}(2^{l-1}-1)]$-code. This code is optimal. In fact, concatenation yields a binary linear $[(2^l-1)(2^{l-1}-1), l, 2^{l-1}(2^{l-1}-1)]_2$-code, which meets the Griesmer bound with equality. The smallest codes of independent interest in this family are the $[7, 1.5, 6]$-code $\mathcal{S}_3$ (geometrically the 7 lines of the Fano plane) and the $[155, 2.5, 120]$-code $\mathcal{S}_5$.

Recall that the geometric description of linear codes is based on multisets of points, whereas the geometric description of additive quaternary codes uses lines. A codeline not contained in hyperplane H meets it in one point. This motivates to consider mixed quaternary-binary codes.

Definition 4. *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. We fill those gaps proving the following:

Theorem 1. *There is no additive $[12, 7, 5]$-code.*
There is no additive $[12, 4.5, 7]$-code.

On the constructive side we produce a $[13, 7.5, 5]$-code. The following is a check matrix, described by 13 lines in $PG(10,2)$, of strength 4 (the convention is $1 = 10, 2 = 01, 3 = 11$):

$$
\left(\begin{array}{c|c|c|c|c|c|c|c|c|c|c|c|c}
L_1 & L_2 & L_3 & L_4 & L_5 & L_6 & L_7 & L_8 & L_9 & L_{10} & L_{11} & L_{12} & L_{13} \\
1 & 0 & 0 & 0 & 0 & 2 & 0 & 3 & 3 & 1 & 2 & 3 & 1 \\
2 & 0 & 0 & 0 & 0 & 0 & 3 & 1 & 0 & 3 & 0 & 3 & 2 \\
0 & 1 & 0 & 0 & 0 & 2 & 2 & 0 & 1 & 1 & 2 & 2 & 0 \\
0 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 3 & 2 & 3 & 3 & 1 \\
0 & 0 & 1 & 0 & 0 & 2 & 2 & 1 & 2 & 2 & 0 & 0 & 0 \\
0 & 0 & 2 & 0 & 0 & 0 & 1 & 2 & 1 & 0 & 1 & 2 & 3 \\
0 & 0 & 0 & 1 & 0 & 2 & 1 & 2 & 0 & 0 & 0 & 3 & 1 \\
0 & 0 & 0 & 2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 3 & 3 \\
0 & 0 & 0 & 0 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 2 & 0 & 2 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 2 & 2 & 2
\end{array}\right).
$$

Here is a list of the largest minimum distance d for additive quaternary $[n, k, d]$-codes of length $n \leq 13$. The only question remaining open is the existence of a $[13, 6.5, 6]$-code.

$k \backslash n$	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	2	3	4	5	6	7	8	9	10	11	12	13
1.5		1	2	3	4	5	6	6	7	8	9	10	11
2		1	2	3	4	4	5	6	7	8	8	9	10
2.5			1	2	3	4	5	6	6	7	8	8	9
3			1	2	3	4	4	5	6	6	7	8	9
3.5				1	2	3	4	4	5	6	7	8	8
4				1	2	2	3	4	5	6	6	7	8
4.5					1	2	3	3	4	5	6	6	7
5					1	2	2	3	4	5	6	6	7
5.5						1	2	3	3	4	5	6	6
6						1	2	2	3	4	5	6	6
6.5							1	2	3	3	4	5	$5-6$
7							1	2	2	3	4	4	5
7.5								1	2	2	3	4	5
8								1	2	2	3	4	4
8.5, 9									1	2	2	3	4
9.5, 10										1	2	2	3
10.5, 11											1	2	2

The geometric work happens in binary projective spaces. As we find it often more convenient to work with vector space dimensions we denote i-dimensional vector subspaces by V_i $(= PG(i-1,2))$. The following obvious observation is often useful:

Proposition 1. *Let C be an additive $[n,k,d]$-code. Assume some i codelines generate a subspace V_{2i-j}. Then the subcode of C consisting of the codewords with vanishing entry in those i coordinates is an $[n-i, k-i+j/2, d]$-code.*

The non-existence of a $[12,7,5]$-code is proved in Section 3. In Section 2 the non-existence proof for $[12,4.5,7]$ is outlined. A preliminary version of parts of the present paper appeared in [3].

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

It is easier to consider the dual, a $[12,5]$-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 $[12,5,7]$-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 $[8,3.5,5]$-code. Such a code does not exist.

Lemma 1. *The maximum number of lines of a $[12,5]$-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 $[6,4.5]$-code. Its dual, a $[6,1.5,5]$-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 $[6,4.5]$-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 $[(7,5),4.5]_{(4,2)}$-code of strength 4. A computer search showed that not even a single point can be appended:

Proposition 2. *There is no* $[(7,1),4.5]_{(4,2)}4$*-code of strength* 4.

We conclude that the maximum number of codelines on a hyperplane is 6. Choose $L_1,\ldots,L_6$ as above. The intersection with the remaining codelines shows that this can be extended to a $[(6,6),4.5]_{(4,2)}$-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 $[(6,6),4.5]_{(4,2)}$-mixed codes of strength 4 and their duals, $[(6,6),4.5,5]_{(4,2)}$-codes do exist.

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

3 Nonexistence of an additive $[12,4.5,7]$-code

The proof is geometric in nature and much more involved than in the case of $[12,7,5]$. We work in $PG(8,2)$. Geometric reasoning shows the following:

Lemma 2. *There are no repeated codelines. Each* V_6 *contains at most* 3 *codelines and any three codelines generate* V_5 *or* V_6*. Any two codelines are mutually skew.*

Let M be the union of the points on the codelines. Then M is a set of 36 points, at most 22 on each hyperplane. This describes a binary code $[36,9,14]_2$, obtained from the hypothetical $[12,4.5,7]$ by concatenation. We study the distribution of the points of M (**codepoints**) on subspaces as well as the structure induced on corresponding factor spaces. The proof that any three codelines must be in general position already involves a computer search. It can then be shown that any two codelines are contained in a subspace $PG(4,2)$ which contains 8 codepoints. The final computer search shows that this configuration cannot be extended to a $[12,4.5,7]$-code.

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, G. Faina, S. Marcugini, F. Pambianco: Additive quaternary codes of small length, *Proceedings ACCT, Zvenigorod (Russia) September 2006*, 15-18.