Optimal additive quaternary codes of low dimension

Jürgen Bierbrauer
Department of Mathematical Sciences
Michigan Technological University
Houghton, Michigan 49931 (USA)

S. Marcugini* and F. Pambianco*
Dipartimento di Matematica e Informatica
Università degli Studi di Perugia
Perugia (Italy)

July 13, 2020

Abstract

An additive quaternary \([n, k, d]\)-code (length \(n\), quaternary dimension \(k\), minimum distance \(d\)) is a \(2k\)-dimensional \(\mathbb{F}_2\)-vector space of \(n\)-tuples with entries in \(\mathbb{Z}_2 \times \mathbb{Z}_2\) (the 2-dimensional vector space over \(\mathbb{F}_2\)) with minimum Hamming distance \(d\). We determine the optimal parameters of additive quaternary codes of dimension \(k \leq 3\). The most challenging case is dimension \(k = 2.5\). We prove that an additive quaternary \([n, 2.5, d]\)-code where \(d < n - 1\) exists if and only if \(3(n - d) \geq \lceil d/2 \rceil + \lceil d/4 \rceil + \lceil d/8 \rceil\). In particular we construct new optimal 2.5-dimensional additive quaternary codes. As a by-product we give a direct proof for the fact that a binary linear

---

*The research of S. Marcugini and F. Pambianco was supported in part by the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA - INDAM) and by University of Perugia (Project: Curve, codici e configurazioni di punti, Base Research Fund 2018).
The concept of additive codes is a far-reaching and natural generalization of linear codes, see [2], Chapter 18. Here we restrict to the quaternary case.

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

We write the parameters of the code as \([n, k, d]\) where \( d \) is the minimum Hamming distance. Here \( k \) is the quaternary dimension. As an example, in case \( k = 2.5 \) the code is a 5-dimensional vector space over \( \mathbb{F}_2 \). Additive codes are particularly interesting because of a link to quantum stabilizer codes, see [4, 5, 9]. We will also use the geometric construction of additive quaternary codes. In fact, a quaternary \([n, k, d]\)-code is equivalent to a multiset of \( n \) lines in \( PG(2k-1, 2) \) such that each hyperplane of \( PG(2k-1, 2) \) contains at most \( s = n - d \) of those lines, in the multiset sense. Blokhuis and Brouwer [8] first suggested the problem of determining the optimum parameters of additive quaternary codes. In earlier work we determined all such optimal parameters when \( n \leq 13 \), see [2], Chapter 18 and [6]. For further results concerning larger lengths see [1, 7]. In the present work we determine all optimal parameters when the quaternary dimension is \( k \leq 3 \). Dimensions \( k \leq 2 \) are degenerate cases, see Section 2. Dimension 3 is easily dealt with as well, see Section 3. Our main result is Theorem 2 in Section 4 where the optimal parameters of 2.5-dimensional additive quaternary codes are determined. For \( k > 1 \) we prefer to work with the species \( s = n - d \) instead of the minimum distance \( d \). Define \( n_k(s) \) to be the maximal length \( n \) such that an additive \([n, k, n - s]\)-code exists. For integer \( k \), let \( n_{k,lin}(s) \) be the maximal \( n \) such that a linear quaternary \([n, k, n - s]\)-4-code exists. In the present paper we determine \( n_k(s) \) for \( k \leq 3 \) and all \( s \). The following obvious lemma will be used to prove nonexistence results:

\[ [3m, 5, 2e]_2 \text{-code for } e < m - 1 \text{ exists if and only if the Griesmer bound } \]
\[ 3(m - e) \geq \lceil e/2 \rceil + \lceil e/4 \rceil + \lceil e/8 \rceil \text{ is satisfied.} \]

Keywords: Quaternary additive codes, projective spaces, optimal codes, binary linear codes.

1 Introduction

The concept of additive codes is a far-reaching and natural generalization of linear codes, see [2], Chapter 18. Here we restrict to the quaternary case.
Lemma 1. The concatenation of a quaternary additive $[n, k, d]$-code and the binary linear $[3, 2, 2]_2$-code is a binary linear $[3n, 2k, 2d]_2$-code.

2 Dimensions $k \leq 2$.

Clearly dimension $k = 1$ is a trivial case, the optimal parameters being $[n, 1, n]$. Dimension $k = 1.5$ is degenerate as well. The ambient space is the Fano plane and the optimal choice is to use each of its seven lines with multiplicity $s$. This shows $n_{1.5}(s) = 7s$. The corresponding codes have parameters $[7s, 1.5, 6s]$. Dimension $k = 2$ still is degenerate. In the linear case we have $n_{2,lin}(s) = 5s$. In fact we work in the projective line $PG(1, 4)$ and the optimal choice is to use each of its points with multiplicity $s$.

Proposition 1. We have $n_2(s) = n_{2,lin}(s) = 5s$ for all $s$.

Proof. Assume $n_2(s) > 5s$. We would have a $[5s + 1, 2, 4s + 1]$-code. Lemma 1 would yield a binary linear $[15s + 3, 4, 8s + 2]_2$-code. This contradicts the Griesmer bound.

3 The case of dimension $k = 3$.

The optimal parameters of linear quaternary 3-dimensional codes are of course known:

Proposition 2. We have $n_{3,lin}(2) = 6, n_{3,lin}(3) = 9, n_{3,lin}(4) = 16, n_{3,lin}(5i) = 21i, n_{3,lin}(5i + 1) = 21i + 1$ and $n_{3,lin}(5i + \sigma) = 21i + 1 + 5(\sigma - 1)$ for $i \geq 1, \sigma \in \{2, 3, 4\}$.

Proof. For $d < 9$ this is easy to check. For larger $d$ we can invoke a result by Hamada-Tamari [10] stating that linear $[n, 3, d]_q$-codes for $d \geq (q - 1)^2$ exist if and only if the parameters satisfy the Griesmer bound (see [2], Theorem 17.7). This coincides with the statement of our proposition.

Theorem 1. We have $n_3(s) = n_{3,lin}(s)$ for all $s$.

Proof. Assume there is an additive 3-dimensional code with larger $n$ and the same species. We illustrate with case $s = 5i$. We would have a $[21i + 1, 3, 16i + 1]$-code. Lemma 1 yields a linear $[63i + 3, 6, 32i + 2]_2$-code, which contradicts the Griesmer bound. The other cases are analogous.
4 The case of dimension 2.5.

Our main result is the following:

**Theorem 2.** An additive quaternary \([n, 2.5, d]\)-code where \(d < n - 1\) exists if and only if \(3(n - d) \geq \lceil d/2 \rceil + \lfloor d/4 \rfloor + \lfloor d/8 \rfloor\).

In the present section we prove Theorem \(2\). In the sequel use the abbreviation \(d_i = \lceil d/l \rceil\). The necessity is obvious. In fact, Lemma \(1\) applied to an additive quaternary \([n, 2.5, d]\)-code yields a binary linear \([3n, 5, 2d]_2\)-code. The condition of Theorem \(2\) is the Griesmer bound as applied to this binary code. It remains to prove sufficiency: given \(d, n\) satisfying the condition of the theorem we need to construct an additive quaternary \([n, 2.5, d]\)-code. As before, let \(s = n - d\). For each \(s\) consider the pair \(D_s = (s, m_s)\) where \(m_s\) is the maximal \(n\) such that \(n, d = n - s\) satisfy the condition in Theorem \(2\). We need to prove the existence of an \([m_s, 2.5, m_s - s]\)-code, for all \(s \geq 2\). When such a code exists we say that we represented \(D_s\). Here are some examples:

\[
D_2 = (2, 8), D_3 = (3, 11), D_4 = (4, 16), D_5 = (5, 21), D_6 = (6, 26), D_7 = (7, 31).
\]

Let \(C\) be an \([n, 2.5, d]\)-code and \(C'\) the code obtained by increasing each line multiplicity of \(C\) by 1. As \(PG(4, 2)\) has 155 lines and \(PG(3, 2)\) has 35 lines we see that \(C'\) is an \([n + 155, 2.5, d + 120]\)-code. Concerning the bound of the theorem we observe that \(3(n - d) - d_2 - d_4 - d_8\) is invariant under the substitution \(n \mapsto n + 155, d \mapsto d + 120\). This shows that we need prove the existence of an \([n, 2.5, d]\)-code only for \(n < 155\). This means that it suffices to construct \(D_2, D_3, \ldots, D_{35} = (35, 155)\). Observe that there is an obvious sum construction which shows that the existence of codes \([m_1, 2.5, l_1]\) and \([m_2, 2.5, l_2]\) implies the existence of an \([m_1 + m_2, 2.5, l_1 + l_2]\)-code. This shows that if \(D_{s_1}\) and \(D_{s_2}\) can be constructed then also \(D_{s_1} + D_{s_2}\) can be constructed. We see now that it suffices to construct \(D_2, \ldots, D_7\) as the remaining \(D_s, s \leq 35\) follow from the sum construction. Here are some examples:

\[
D_8 = D_6 + D_2, D_9 = D_7 + D_2, D_{10} = D_5 + D_5, D_{11} = D_9 + D_2, D_{12} = D_6 + D_6.
\]

It remains to construct \(D_2, \ldots, D_7\). Now \(D_2\) implies \(D_4\) as \(D_2 + D_2 = D_4\) and \(D_5 = (5, 21)\) is constructed as there is even a linear \([21, 3, 16]_4\)-code (corresponding to the points of \(PG(2, 4)\)). We are reduced to construct \(D_2, D_3, D_6, D_7\). Now \(D_2 = (2, 8)\) corresponds to a \([8, 2.5, 6]\)-code. This is
the Blokhuis-Brouwer construction \[8, 3\]. In the same context an \([11, 2.5, 8]\)-code was constructed. This is a representation of \(D_3 = (3, 11)\). We are finally reduced to construct \(D_6\) and \(D_7\).

**A construction**

Consider a chain

\[ l_0 \subset E_0 \subset H_0 \subset PG(4, 2) \]

where \(l_0\) is a line, \(E_0\) a plane and \(H_0\) a solid (hyperplane) in \(PG(4, 2)\). Let \(\mathcal{V}\) be a set of 8 lines such that each point in \(E_0 \setminus l_0\) is on precisely two lines of \(\mathcal{V}\), each point outside \(H_0\) is on precisely one line of \(\mathcal{V}\). Also, let \(\mathcal{E}\) be a set of 8 lines partitioning the points outside \(E_0\) (Blokhuis-Brouwer construction).

**Definition 2.** Let \(C(g, h, v, e)\) be the additive 2.5-dimensional quaternary code described by the following multiset of lines: line \(l_0\) with multiplicity \(g\), the remaining lines of \(E_0\) each with multiplicity \(h\), the lines of \(\mathcal{V}\) with multiplicity \(v\) and the lines of \(\mathcal{E}\) with multiplicity \(e\).

Clearly \(C(g, h, v, e)\) has length \(n = g + 6h + 8v + 8e\). Let \(m(P)\) be the number of codelines (including multiplicities) that contain point \(P\). If \(P \in l_0\), then \(m(P) = g + 2h\), if \(P \in E_0 \setminus l_0\) then \(m(P) = 3h + 2v\). If \(P \in H_0 \setminus E_0\) then \(m(P) = e\) whereas points \(P\) outside \(H_0\) have \(m(P) = v + e\). For each hyperplane \(H\) let \(m(H) = \sum_{P \in H} m(P)\). By double counting we obtain

\[ s(H) = (m(H) - n)/2 \]

where \(s(H)\) (the species of \(H\)) is the number of codelines contained in \(H\). It follows that the numbers \(n - s(H)\) are the nonzero weights of our code. The numbers \(m(H)\) and \(s(H)\) are easy to determine:

**Lemma 2.** If \(l_0 \not\subset H\) then \(m(H) = g + 8h + 12v + 12e\).

If \(l_0 \subset H\) but \(E_0 \not\subset H\) then \(m(H) = 3g + 6h + 8v + 12e\).

If \(E_0 \subset H \neq H_0\) then \(m(H) = 3g + 18h + 16v + 8e\).

Finally \(m(H_0) = 3g + 18h + 8v + 8e\).

**Proof.** This is a trivial calculation. In the first case above \(H\) has one point of \(l_0\), two further points in \(E_0\), four further points in \(H_0\) and finally 8 affine points for a grand total \(m(H) = g + 8h + 4v + 4e + 8(v + e)\). In the second case \(H\) contains three points on \(l_0\), no further point on \(E_0\), four further points on \(H_0\) and eight affine points: \(m(H) = 3g + 6h + 4e + 8(v + e)\). The remaining two cases are analogous.  

\[ \square \]
Our basic formula yields:

**Corollary 1.** The nonzero weights of the codewords of $C(g, h, v, e)$ are

$$g + 5h + 6(v + e), 6h + 8v + 6e, 4v + 8e, 8(v + e).$$

$C(g, h, v, e)$ is an $[g + 6h + 8(v + e), 2.5, d]_4$-code where

$$d = \text{Min}(w_1 = g + 5h + 6(v + e), w_2 = 6h + 8v + 6e, w_3 = 4v + 8e).$$

We see that $C(2, 0, 1, 2)$ is a $[26, 2.5, 20]$-code and $C(1, 1, 0, 3)$ is a $[31, 2.5, 24]$-code. This completes the proof of Theorem 2. Lemma 1 yields

**Corollary 2.** A binary linear $[3m, 5, 2e]_2$-code for $e < m - 1$ exists if and only if the Griesmer bound $3(m - e) \geq e_2 + e_4 + e_8$ is satisfied.

**References**

[1] D. Bartoli, J. Bierbrauer, G. Faina, S. Marcugini, and F. Pambianco: *The nonexistence of an additive quaternary $[15, 5, 9]$-code*, Finite Fields and Their Applications 36 (2015), 29-40.

[2] J. Bierbrauer: *Introduction to Coding Theory, Second Edition*, Chapman and Hall/CRC Press, Fall 2016.

[3] J. Bierbrauer, Y. Edel, G. Faina, S. Marcugini, F. Pambianco: *Short additive quaternary codes*, IEEE IT Transactions 55 (2009), 952-954.

[4] J. Bierbrauer, G. Faina, M. Giulietti, S. Marcugini, and F. Pambianco: *The geometry of quantum codes*, Innovations in Incidence Geometry 6-7 (2009), 53-71.

[5] J. Bierbrauer, R.D. Fears, S. Marcugini, and F. Pambianco: *The nonexistence of a $[[13, 5, 4]]$ quantum stabilizer code*, [arXiv:0908.1348](http://arxiv.org/abs/0908.1348) IEEE IT Transactions 57 (2011), 4788-4793.

[6] J. Bierbrauer, S. Marcugini, and F. Pambianco: A geometric nonexistence proof of an extremal additive code, *Journal of Combinatorial Theory, Series A*, 117 (2010), 128-137.
[7] J. Bierbrauer, S. Marcugini, and F. Pambianco: *Additive quaternary
codes related to exceptional linear quaternary codes,*
*IEEE IT Transactions* **66** (2020), 273-277.

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

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

[10] N. Hamada and F. Tamari: *Construction of optimal codes and optimal
fractional factorial designs using linear programming,*
*Annals of Discrete Mathematics* **6** (1980), 175-188.