# Designs in Additive Codes over $GF(4)$

Jon-Lark Kim and Vera Pless
Department of Mathematics, Statistics, and Computer Science,
University of Illinois–Chicago,
Chicago, IL 60607-7045, USA,
e-mail: jlkim@math.uic.edu, pless@math.uic.edu

September 30, 2001

Key Words :
Additive code, Assmus-Mattson Theorem, generalized $t$-design.

## Corresponding author :

Vera Pless
Department of Mathematics, Statistics, and Computer Science
322 SEO(M/C 249),
University of Illinois–Chicago
851 S. Morgan, Chicago, IL 60607-7045, USA
e-mail: pless@math.uic.edu
Tel : 1-312-413-2177
Fax : 1-312-996-1491

**Abstract**

The purpose of this paper is to study designs in additive codes over $GF(4)$. There are two types of designs. One is a classical $t$-design with repeated blocks. In this case we have an analogue of the Assmus-Mattson Theorem for additive codes over $GF(4)$. The other is a generalized $t$-design first introduced by Delsarte [4]. As an example, we consider the dodecacode, which is the unique additive even self-dual $(12, 2^{12}, 6)$ code. We show that there exists a 5-$(12, 6, 3)$ design in the dodecacode with either 3 distinct blocks or 3 repeated blocks covering a 5-set. We also find a new simple 3-$(11, 5, 4)$ design in the shortened dodecacode by a computer search. Additionally we show that any extremal additive even self-dual code over $GF(4)$ is homogeneous.

# 1 Introduction

Recently additive codes over $GF(4)$ have gained in popularity because of their connection to quantum codes [3]. Several papers [2, 5, 6, 7] were devoted to classifing additive self-dual codes over $GF(4)$. It was shown in [7] that certain vectors in some additive self-dual codes over $GF(4)$ hold generalized $t$-designs. We study further generalized $t$-designs in additive codes over $GF(4)$ as well as classical $t$-designs with repeated blocks. We give some basic definitions.

An *additive code* $\mathcal{C}$ *over* $GF(4)$ *of length* $n$ is an additive subgroup of $GF(4)^n$. As $\mathcal{C}$ is a free $GF(2)$-module, it has size $2^k$ for some $0 \le k \le 2n$. We call $\mathcal{C}$ an $(n, 2^k)$ code. It has a basis, as a $GF(2)$-module, consisting of $k$ basis vectors; a *generator matrix* of $\mathcal{C}$ will be a $k \times n$ matrix with entries in $GF(4)$ whose rows are a basis of $\mathcal{C}$. Interest in additive codes over $GF(4)$ has arisen because of their correspondence to quantum codes as described in [3]. There is a natural inner product arising from the trace map. If we let $GF(4) = \{0, 1, \omega, \overline{\omega}\}$ where $\overline{\omega} = \omega^2 = 1 + \omega$, the *trace* map $\mathrm{Tr} : GF(4) \to GF(2)$ is given by

$$\mathrm{Tr}(x) = x + x^2.$$

In particular $\mathrm{Tr}(0) = \mathrm{Tr}(1) = 0$ and $\mathrm{Tr}(\omega) = \mathrm{Tr}(\overline{\omega}) = 1$. The *conjugate* of $x \in GF(4)$, denoted $\overline{x}$, is the image of $x$ under the Frobenius automorphism; in other words, $\overline{0} = 0$ $\overline{1} = 1$, and $\overline{\overline{\omega}} = \omega$. We now define the *trace inner product* of two vectors $\mathbf{x} = x_1 x_2 \cdots x_n$ and $\mathbf{y} = y_1 y_2 \cdots y_n$ in $GF(4)^n$ to be

$$\mathbf{x} \star \mathbf{y} = \sum_{i=1}^{n} \mathrm{Tr}(x_i \overline{y_i}).$$

**Example 1.1.** Let $\mathcal{G}_6$ be the $[6, 3, 4]$ *hexacode* whose generator matrix as a linear $GF(4)$-code is

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & 0 & 1 & \omega & \omega & 1 \end{bmatrix}.$$

This is also an additive code; thinking of $\mathcal{G}_6$ as an additive code, it has the following generator matrix

$$\begin{bmatrix} 1 & 0 & 0 & 1 & \omega & \omega \\ \omega & 0 & 0 & \omega & \overline{\omega} & \overline{\omega} \\ 0 & 1 & 0 & \omega & 1 & \omega \\ 0 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} \\ 0 & 0 & 1 & \omega & \omega & 1 \\ 0 & 0 & \omega & \overline{\omega} & \overline{\omega} & \omega \end{bmatrix}.$$

If $\mathcal{C}$ is an additive code, its *dual*, denoted $\mathcal{C}^\perp$, is the additive code $\{\mathbf{x} \in GF(4)^n \mid \mathbf{x}\star\mathbf{c} = 0 \text{ for all } \mathbf{c} \in \mathcal{C}\}$. If $\mathcal{C}$ is an $(n, 2^k)$ code, then $\mathcal{C}^\perp$ is an $(n, 2^{2n-k})$ code. As usual, $\mathcal{C}$ is *self-orthogonal* if $\mathcal{C} \subseteq \mathcal{C}^\perp$ and *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. In particular, if $\mathcal{C}$ is self-dual, $\mathcal{C}$ is an $(n, 2^n)$ code. The code $\mathcal{G}_6$ in Example 1.1 is self-dual as an additive code. (Any $GF(4)$-linear code that is self-orthogonal under the Hermitian inner product is a self-orthogonal additive code under the trace inner product.)

As usual, the *weight* $\mathrm{wt}(\mathbf{c})$ of $\mathbf{c} \in \mathcal{C}$ is the number of nonzero components of $\mathbf{c}$. The minimum weight $d$ of $\mathcal{C}$ is the smallest weight of any nonzero codeword in $\mathcal{C}$. If $\mathcal{C}$ is an $(n, 2^k)$ additive code of minimum weight $d$, $\mathcal{C}$ is called an $(n, 2^k, d)$ code. $\mathcal{C}$ is *Type II* if $\mathcal{C}$ is self-dual and all codewords have even weight; Type II codes of length $n$ exist only if $n$ is even [6]. If $\mathcal{C}$ is self-dual but some codeword has odd weight (in which case the code cannot be $GF(4)$-linear), the code is *Type I* (see [12, section 4.2]). There is a bound on the minimum weight of an additive self-dual code [12, Theorem 33]. If $d_I$, $d_{II}$ is the minimum distance of an additive self-dual Type I, Type II code, respectively, of length $n > 1$, then

$$d_I \leq \begin{cases} 2\left\lfloor \frac{n}{6} \right\rfloor + 1 & \text{if } n \equiv 0 \pmod 6 \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 3 & \text{if } n \equiv 5 \pmod 6 \\ 2\left\lfloor \frac{n}{6} \right\rfloor + 2 & \text{otherwise} \end{cases} \tag{1}$$

$$d_{II} \leq 2\left\lfloor \frac{n}{6} \right\rfloor + 2. \tag{2}$$

A code that meets the appropriate bound is called *extremal*. Note that (2) is the same as saying that $d = 2m + 2$ if $n = 6m + 2(i - 1)$, with $i = 1, 2$, or 3. Type II codes meeting the bound $d_{II}$ have a unique weight enumerator. This property is not true for Type I codes. A self-dual (with respect to Hermitian inner product) linear code over $GF(4)$ also satisfies bound (2) and an extremal code is a $[6m, 3m, 2m + 2]$ code.

We say that two additive codes $\mathcal{C}_1$ and $\mathcal{C}_2$ are *equivalent* provided there is a map sending the codewords of $\mathcal{C}_1$ onto the codewords of $\mathcal{C}_2$ where the map consists of a permutation of coordinates followed by a scaling of coordinates by elements of $GF(4)$ followed by conjugation of some of the coordinates. Notice that permuting coordinates, scaling coordinates, and conjugating some coordinates of a self-orthogonal (or self-dual) code does not change self-orthogonality (or self-duality). The *automorphism group* of $\mathcal{C}$, denoted $\mathrm{Aut}(\mathcal{C})$, consists of all maps which permute coordinates, scale coordinates, and conjugate coordinates that send codewords of $\mathcal{C}$ to codewords of $\mathcal{C}$.

The purpose of this paper is to study designs in additive codes over $GF(4)$. There are two types of designs. One is a classical $t$-design with repeated blocks. For these we have an analogue of the Assmus-Mattson Theorem for additive codes over $GF(4)$. The other is a generalized $t$-design first introduced by Delsarte [4]. As an example, we consider the dodecacode, which is the unique additive even self-dual $(12, 2^{12}, 6)$ code. We show that there exists a 5-$(12, 6, 3)$ design in the dodecacode with either 3 distinct blocks or 3 repeated blocks covering a 5-set. We also find a new simple 3-$(11, 5, 4)$ design in the shortened dodecacode. Additionally we show that any extremal additive even self-dual code over $GF(4)$ is homogeneous.

## 2 Assmus-Mattson Theorem

We recall the Assmus-Mattson Theorem which guarantees simple $t$-designs in some linear codes and their duals over $GF(q)$.

**Theorem 2.1 ([1, 11]).** *Let $\mathcal{C}$ be an $[n,k,d]$ linear code over $GF(q)$ with dual code $\mathcal{C}^\perp$. Suppose $\mathcal{C}^\perp$ has minimum weight $d^\perp$. If $q = 2$, let $w = n$; if $q > 2$, let $w$ be the largest integer so that*

$$w - \lfloor \frac{w+q-2}{q-1} \rfloor < d.$$

*Define $w^\perp$ analogously using $d^\perp$. Suppose that $\{A_i : 0 \le i \le n\}$ and $\{B_i : 0 \le i \le n\}$ are the weight distributions of $\mathcal{C}$ and $\mathcal{C}^\perp$, respectively. Let $s$ be the number of $i$ with $B_i \neq 0$ for $0 < i \le n-t$. Suppose $t < d$ and $s \le d - t$. Then the following hold.*
*(i) The vectors of weight $i$ in $\mathcal{C}$ hold a $t$-design provided $A_i \neq 0$ and $d \le i \le w$.*
*(ii) The vectors of weight $i$ in $\mathcal{C}^\perp$ hold a $t$-design provided $B_i \neq 0$ and $d^\perp \le i \le \min\{n-t, w^\perp\}$.*

**Remark 2.2.** The condition on $w$ and $w^\perp$ in Theorem 2.1 ensures that there cannot be repeated blocks. This arises from the linearity of the code. Since we consider additive codes over $GF(4)$, there is no restriction on $w$ and $w^\perp$ as in Theorem 2.7.

If $\mathcal{C}$ is a self-dual additive $(n, 2^n, d)$ code, we can obtain a self-dual code of length $n-1$ by a process we call *shortening*. We use this term even though it differs from the usual meaning as our notion can be regarded as a generalization. Let $G$ be a generator matrix of $\mathcal{C}$. As $\mathcal{C}$ is self-dual, no column of $G$ is all 0's. Choose any column of $G$, say the $i^{\text{th}}$ one. The entries in column $i$ can be any of 0, 1, $\omega$, or $\overline{\omega}$. By row reducing $G$ (to obtain another generator matrix we call $G$ again), we can make all the entries in column $i$ equal to 0 except for one or two entries; if two they would be two of the three values 1, $\omega$, or $\overline{\omega}$. The *shortened code of $\mathcal{C}$ on coordinate $i$*, denoted $\mathcal{C}'$ is the code with generator matrix $G'$ obtained from $G$ by eliminating one row of $G$ with a nonzero entry in column $i$ and then eliminating column

$i$. [If there is only one nonzero entry in column $i$ of $G$, then $\mathcal{C}'$ is $\mathcal{C}$ shortened in the usual sense.] Clearly $\mathcal{C}'$ is a self-dual additive $(n-1, 2^{n-1}, d')$ code with $d' \geq d-1$ [5, 6].

Let $\mathcal{C}$ be an additive $(n, 2^k, d)$ code over $GF(4)$. Let $T$ be a set of $t$ coordinate positions and $I$ the remaining $n-t$ coordinate positions. Let $C(I)$ be the code obtained from $\mathcal{C}$ by removing these $t$ coordinate positions. Consider now the subcode $D$ of $\mathcal{C}^\perp$, which is 0 on all the positions in $T$. Let $D(I)$ be the code of length $n-t$ gotten by removing the $t$ coordinate positions from $D$.

**Remark 2.3.** If $T = \{i\}$, then $D(I)$ is a shortened code of $\mathcal{C}^\perp$ on coordinate $i$ if $\mathcal{C}^\perp$ has a generator matrix $G^\perp$ with only one nonzero element on its $i^{\text{th}}$ position. Otherwise, $D(I)$ is obtained by deleting the two rows of $G^\perp$ which have distinct nonzero elements on its $i^{\text{th}}$ position and eliminating the $i^{\text{th}}$ column of $G^\perp$.

The following lemmas will be used to prove Theorem 2.7. These are well-known for linear codes over finite fields. As we consider additive codes, we need to prove the results.

**Lemma 2.4.** *Let $\mathcal{C}$ be an additive $(n, 2^k, d)$ code over $GF(4)$. Then the following hold.*
*(i) $C(I)^\perp = D(I)$ ; moreover*
*(ii) if $t < d$, then dim$(C(I)) = k$ and dim$(D(I)) = 2n - 2t - k$.*

*Proof.* Clearly $D(I) \subset C(I)^\perp$. Take any vector $x'$ in $C(I)^\perp$. It is of length $n-t$ and if we extend it to a length $n$ vector $x$ by adjoining $t$ zeros, then $x$ certainly is in $D$. Hence $x'$ should be in $D(I)$. This proves (i).

To prove (ii), suppose that we remove $t(< d)$ coordinate positions of $\mathcal{C}$. If the dimension of $C(I)$ changes, this means that there exist $k'(< k)$ rows of $C(I)$ whose linear combination is a zero vector. Since these $k'$ rows of $C(I)$ come from $k'$ rows of $\mathcal{C}$, we would have a vector in $\mathcal{C}$ of weight $t$ less than $d$, which is absurd. Thus $\dim(C(I)) = k$ and hence $\dim(D(I)) = 2n - 2t - k$. □

The following MacWilliams identities are known for additive codes over $GF(4)$ (see [7, 12]).

**Lemma 2.5.** *Let $\mathcal{C}$ be an additive $(n, 2^k)$ code over $GF(4)$ and $\mathcal{C}^\perp$ be the dual $(n, 2^{2n-k})$ code. Then their weight enumerators are related as follows.*

$$W_{\mathcal{C}}(x, y) = \frac{1}{|\mathcal{C}^\perp|} W_{\mathcal{C}^\perp}(x + 3y, x - y).$$

We give a uniqueness theorem which can be derived from Lemma 2.5.

**Lemma 2.6.** *If $A_i$'s are the number of vectors of weight $i$ in $\mathcal{C}$ and $B_i$'s the number of vectors of weight $i$ in $\mathcal{C}^\perp$, then there exists a unique solution of $A_i$'s and $B_i$'s if there are at most $s$ unknown values of $A_i$'s and $B_1, \cdots, B_{s-1}$ are known.*

We now give an analogue of the Assmus-Mattson Theorem for additive codes over $GF(4)$ which gives designs with possibly repeated blocks. The original Assmus-Mattson Theorem gives simple designs.

**Theorem 2.7.** *Let $\mathcal{C}$ be an additive $(n, 2^k)$ code over $GF(4)$ with minimum weight $d$. Let $\mathcal{C}^\perp$ be its dual $(n, 2^{n-k})$ code with minimum weight $d'$. Let $0 < t < d$. Let $s$ be the number of weights $B_i \neq 0$ in $\mathcal{C}^\perp$ where $0 < i \leq n - t$. Suppose that $s \leq d - t$. Then the following hold.*
*(i) For each weight $u$ ($d \leq u \leq n$), the set of supports of codewords of weight $u$ in $\mathcal{C}$ holds a $t$-design with possibly repeated blocks.*
*(ii) The set of supports of vectors of weight $w$ in $\mathcal{C}^\perp$ where $B_w \neq 0$ and $d' \leq w \leq n - t$ hold a $t$-design with possibly repeated blocks.*
*(iii) The supports of minimum weight vectors are either simple blocks or have repetition number 3.*

*Proof.* Let $T$ be a set of $t$ coordinate positions and $I$ the remaining $n-t$ coordinate positions. Then it follows from Lemma 2.4 that $C(I)^\perp = D(I)$ with $D(I)$ an $(n-t, 2^{2n-2t-k})$ code.

$(*)$ Let $B'_i$ be the number of vectors of weight $i$ in $D(I)$. Then $B'_i \leq B_i$, and if $s'$ is the number of $i$ so that $B'_i \neq 0$, then $s' \leq s$. Since we know by hypothesis $s \leq d - t$, we see $s' \leq d - t$; hence $s'$ is less than or equal to the minimum weight of $C(I)$. Now we can apply Lemma 2.5 to the codes $C(I)$ and $D(I)$ and we obtain a unique solution to their weight distributions. This solution just depends on the dimensions, $k$ and $2n - 2k - t$ of the two codes. Thus it is the same for any set of $t$-coordinates chosen.

Suppose $u = d$. Let $E_1$ be the family of supports of codewords of $\mathcal{C}$ of weight $d$. These supports may be repeated. The number of blocks(=supports) in $E_1$ containing a given $t$-subset $T$ is the number of vectors in $C(I)$ of weight $d-t$. By $(*)$, this number is independent of the choice of $T$. Hence the set of supports of codewords of $\mathcal{C}$ of weight $d$ holds a $t$-design.

The rest of the proof of (i) is the same as that of the Assmus-Mattson theorem([11]) except that blocks can be repeated. So we omit the details.

$(**)$ We prove (ii). Let $d' \leq w \leq n - t$. Let $F$ be the family of supports of codewords of weight $w$ in $\mathcal{C}^\perp$. Again supports can be repeated. Consider the family $F'$ consisting of the complements of the sets in $F$. For any $t$-subset $T$ of $n$ coordinate positions, it follows that the number of blocks of $F'$ containing $T$ is equal to the number of vectors of weight $w$ in $D(I)$. By the previous argument $(*)$ this number does not depend on the choice of $T$. Therefore, $F'$ is a $t$-design and hence $F$ is also a $t$-design since the complements of $t$-design with possibly repeated blocks give another $t$-design with the same number of repeated blocks.

For (iii), we first show that there is no block with multiplicity 2. Suppose that there are two codewords $\mathbf{u}$ and $\mathbf{v}$ of weight $d$ with the same supports. Each nonzero component of $\mathbf{u}$ must be different from the corresponding component of $\mathbf{v}$ (otherwise we will have a codeword $\mathbf{u} + \mathbf{v}$ whose weight is less than $d$). Hence the sum $\mathbf{u} + \mathbf{v}$ is of weight $d$ with the same support as **u** and **v**. If there are 3 vectors of weight $d$ with the same support, there cannot be more as in any given position all three of the non-zero values occur. $\square$

**Remark 2.8.** The $\lambda$ for these designs is computed by the usual formula from the weight distribution.

**Corollary 2.9.** *Let $n_i := 6m + 2(i-1)$ with $m \geq 1$ any integer and $i = 1, 2,$ or $3$. Let $\mathcal{C}$ be an extremal additive even self-dual $(n_i, 2^{n_i})$ code over $GF(4)$ with minimum weight $d = 2m+2 \geq 6$. Then the vectors of each weight $w$ in $\mathcal{C}$ where $A_w \neq 0$ and $d \leq w \leq n_i$ hold a $(7-2i)$-design with possibly repeated blocks.*

*Proof.* We only consider the case $n = 6m$. The other cases are similar. By (2) $2m+2$ is the minimum weight of an extremal even code of length $6m$. We note that the value $s$ in Theorem 2.7 is $\{(6m-4)-(2m+2)\}/2 = 2m-3$, which equals $d-t = 2m+2-5 = 2m-3$. Hence this corollary follows immediately. $\square$

We remark that this is the analogue of an extremal binary doubly-even $[24m+8(i-1), 12m+4(i-1), 4m+4]$ self-dual code ($m \geq 1, i = 1, 2,$ or $3$). It is well-known that the vectors of each nonzero weight in such a code hold a simple $(7-2i)$-design.

Using Corollary 2.9 and the fact that a $t$-design with repeated blocks implies a $(t-1)$-design with repeated blocks, we see the following.

**Corollary 2.10.** *All codes $\mathcal{C}^p$ punctured on some coordinate of an extremal additive even self-dual code $\mathcal{C}$ over $GF(4)$ have the same weight distribution. More precisely, if we let $A_i$ ($a_i$, resp.) be the weight distribution of $\mathcal{C}$ ($\mathcal{C}^p$, resp.), then*

$$a_{2i+1} = \lambda_1^{2i+2} \text{ and } a_{2i+2} = A_{2i+2} - \lambda_1^{2i+2},$$

*where $\lambda_1^{2i+2}$ is the number of (possibly repeated) supports of the codewords in $\mathcal{C}$ of weight $2i+2$ having nonzeros on coordinate $j$.*

Let $M_i$ be the matrix whose rows consist of all codewords of nonzero weight $i$ in an additive code $\mathcal{C}$ over $GF(4)$. Suppose that each column of $M_i$ has a constant weight, depending only on $i$. Then $\mathcal{C}$ is called *homogeneous*.

It is known [10] that any extremal linear Hermitian self-dual code over $GF(4)$ is homogeneous. This can be reproved by the following corollary.

**Corollary 2.11.** *Any extremal additive even self-dual code over $GF(4)$ is homogeneous.*

*Proof.* Use Corollary 2.10. $\square$

**Example 2.12.** There exists a unique extremal additive even self-dual $(12, 2^{12}, 6)$ code up to equivalence [5, 6]. It is called the *dodecacode* (see Table 1). The automorphism group of the dodecacode is a semidirect product of $Z(3)^3$ with $S(4)$, where $Z(n)$ denotes a cyclic group of order $n$, and has order 648 [12, pp. 193]. This code is homogeneous by Corollary 2.11. By Corollary 2.9, the set of supports of vectors of weight 6 hold a 5-design with possibly repeated blocks. There are two kinds of blocks. One is a simple block and the other has multiplicity 3. We remark that there are 18 codewords of weight 6 whose supports form blocks repeated 3 times. Among them, exactly 12 codewords are such that their scalar multiples are also codewords. In the dodecacode, $A_6 = 396$. So there are 396-18=378 codewords of weight 6 whose supports are simple blocks. Note that $396 = \lambda_5 \binom{12}{5} / \binom{6}{5}$, whence $\lambda_5 = 3$. Allowing repeated blocks we obtain a 5-$(12, 6, \lambda_5 = 3)$ design in the dodecacode. Each 5 set is either contained in one block repeated 3 times or in 3 distinct blocks. It seems like that this is the first example of a design of these parameters with multiplicity 1 or 3. Furthermore we see that vectors of other weights 8, 10, and 12 hold 5-designs with possibly repeated blocks with $\lambda = 105, 630$, and 234, respectively. See Table 2 for the weight distribution of the dodecacode.

**Example 2.13.** It was shown [5, 6] that there exists a unique additive $(11, 2^{11}, 5)$ self-dual code up to equivalence. This is the shortened dodecacode. See Table 1 for one such obtained by eliminating the last coordinate of the generator matrix $QC\_12$ and its last row. It can be seen in Theorem 3.4 that the minimum weight vectors are always simple blocks. We have shown by computer that the vectors of weight 5 in the shortened dodecacode hold a simple 3-$(11, 5, 4)$ design. This design looks interesting by itself and seems to be new. We also get simple 2-$(11, 5, 12)$ and 1-$(11, 5, 30)$ designs. Also, the vectors of weight 6 hold a 4-(11,6,9) design with repeated blocks. See Table 2 for the weight distribution of the shortened dodecacode.

When we consider a punctured dodecacode on the last column of $QC\_12$, we have 3-$(11, 5, 12)$, 2-$(11, 5, 36)$ and 1-$(11, 5, 90)$ designs with repeated blocks from weight 5 vectors. We also have the same 4-$(11, 6, 9)$ design with repeated blocks from weight 6 vectors as we got from the shortened dodecacode.

These examples lead to the following theorem.

**Theorem 2.14.** *There exists a 5-*$(12, 6, 3)$ *design with multiplicity 1 or 3 in the dodecacode. There exists a simple 3-*$(11, 5, 4)$ *design in the shortened dodecacode which is not equivalent to the 3-design obtained from the ternary Golay* $[11, 6, 5]$ *code with the same parameters.*

*Proof.* For the second claim, we note that both designs have 66 blocks and are 3-$(11, 5, 4)$ designs. So we compare automorphims of both designs. It is well known that the ternary Golay $[11, 6, 5]$ code has an automorphism which is a cycle of length 11 while the dodecacode does not have such a cycle. The automorphism group of the shortened dodecacode has order 18 (see Table 2). □

**Example 2.15.** The existence of an extremal additive even self-dual $(24, 2^{24}, 10)$ code over $GF(4)$ is a long standing open question. If there exists such a code, it contains 5-designs for each even weight 10 to 24. There is no $GF(4)$ linear $[24, 12, 10]$ code [9].

Designs in a linear code and its shortened code are related as the following theorem states. We omit its proof.

**Theorem 2.16.** *The odd minimum weight vectors in a code shortened from a linear extremal even self-dual code $\mathcal{C}$ hold a simple design derived from the design held by the even minimum weight vectors in $\mathcal{C}$.*

**Example 2.17.** We note that the vectors of weight 7 in the $(17, 2^{17}, 7)$ code shortened from the unique linear $[18, 9, 8]$ code $S_{18}$ [8] contains simple 4,3, and 2 designs by Theorem 2.16 and the fact that $S_{18}$ is linear. The 4-design is a 4-$(17, 7, 6)$ design. This is a derived design from the 5-design held by the minimum weight vectors in $S_{18}$.

# 3 Generalized $t$-designs

We give some definitions about generalized $t$-designs from [4]. Let $F$ be a finite alphabet of size $q$ (we are interested in $F = GF(4)$ with $q = 4$). Let $G = F^n$, the set of $n$-tuples of $F$.

An element $a$ of $G$ is said to be *covered* by an element $b$ of $G$ if each nonzero component $a_i$ of $a$ is equal to the corresponding component $b_i$ of $b$; we denote this by $a \le b$. For example, if $F = GF(4) = \{0, 1, \omega, \overline{\omega}\}$, then $a = (1, 1, \omega, 0)$ is covered by $b = (1, 1, \omega, \overline{\omega})$.

A subset $S$ of $G$ is called a *generalized $t$-design of type $q-1$*, with parameters $t$-$(n, k, \mu_t), 0 \le t \le k \le n, \mu_t \ge 1$, if the following two conditions are satisfied;
(i) all elements of $S$ have the same weight $k$,
(ii) each element of weight $t$ in $G$ is covered by a constant number $\mu_t$ of elements of $S$.
If a subset $S$ of $G$ holds a generalized $t$-design of type $q-1$, then it holds a generalized $t-1$-design of type $q-1$ [4].

In the binary case($q = 2$), this is the same as a classical $t$-design without repeated blocks.

For a given code $\mathcal{C}$ of length $n$ and for an element $e$ of $G = F^n$, we denote by $\mu(i, e)$ the number of codewords of weight $i$ that cover $e$. Trivially, if $i < wt(e)$, then $\mu(i, e) = 0$.

Delsarte's theorem for any finite alphabet is as follows.

**Theorem 3.1 ([4]).** *Let $\mathcal{C}$ be a $q$-ary code of dual distance $d'$. Let $t$ be an integer, $1 \le t \le d'$, such that the number of weights of $\mathcal{C}$ that are at least equal to $t$ is at most equal to $d' - t$. Then each set of codewords of a given weight $\ge t$, is a generalized $t$-design of type $q-1$.*

Now we obtain generalized $t$-designs from additive codes over $GF(4)$.

**Corollary 3.2 ([7]).** *Let $\mathcal{C}$ be an extremal even additive self-dual code over $GF(4)$ of length $n = 6m$ ($n = 6m + 2$, resp.). Then the set of codewords of weight $w$ in $\mathcal{C}$ with $A_w \ne 0$ forms a generalized 2-design (1-design, resp.) of type 3.*

*Proof.* We observe that since $\mathcal{C}$ is extremal and even, its minimum weight is $2m+2$ which is also $d'$. As there are at most $2m(2m+1)$ non-zero weights in $\mathcal{C}$, the corollary follows. $\square$

From now on, we study designs in a shortened code and their relations to the code's weight distribution.

The following theorem is similar to Corollary 2.10 but its proof uses the property of a generalized 1-design in an extremal additive even self-dual code over $GF(4)$ of length $n = 6m$ or $6m+2$.

**Theorem 3.3.** *Let $\mathcal{C}$ be any extremal, even, additive self-dual code over $GF(4)$ of length $n = 6m$ ($n = 6m+2$, resp.) with $A_i$ its weight distribution. Let $\mathcal{C}'$ be a code shortened on some coordinate $j$ with $a_i$ its weight distribution. Let e1 be any vector of weight 1 in $GF(4)^n$. Then*

$$a_{2i+1} = \mu(2i+2, e1) = \frac{\lambda_1^{2i+2}}{3} \textit{ for } i = m, m+1, \cdots, 3m-1, (3m, resp.),$$

*where $\lambda_1^{2i+2}$ is the number of (possibly repeated) supports of the codewords in $\mathcal{C}$ of weight $2i+2$ having nonzeros on coordinate $j$. Moreover*

$$a_{2i+2} = A_{2i+2} - \lambda_1^{2i+2} \textit{ for } i = m, m+1, \cdots, 3m-1, (3m, resp.).$$

*In particular, this implies that the weight distribution of any code shortened from a given extremal code of length $6m$ ($6m+2$, resp.) is the same.*

*Proof.* We only consider length $n = 6m$ as length $n = 6m+2$ is similar. Since codewords of weight $w = 2i+2$ in $\mathcal{C}$ with $A_w \neq 0$ hold a generalized 2-design of type 3 by Corollary 3.2, these vectors also hold a generalized 1-design of type 3. Thus for any given coordinate $j$ there are exactly two non-zero elements in $GF(4)$, say 1 and $\omega$, in the generator matrix $G$ before we shorten $\mathcal{C}$ on the coordinate $j$. The shortened code $\mathcal{C}'$ obtained by eliminating one row of $G$ with a nonzero entry, say $\omega$, in column $j$ and then eliminating column $j$ has odd weight vectors of weight $2i+1$ such that $a_{2i+1} = \mu(2i+2, e1)$. It follows from its definition that $\mu(2i+2, e1) = \lambda_1^{2i+2}/3$ for $i = m, m+1, \cdots, 3m-1$. This proves the first claim.

For the second claim we observe that the vectors of weight $2i+2$ in $\mathcal{C}'$ come from vectors of weight $2i+2$ in $\mathcal{C}$ having a zero on position $j$. As there are $\lambda_1^{2i+2}$ vectors in $\mathcal{C}$ which are nonzero on position $j$, the second claim follows.

As $\lambda_1^{2i+2}$ is independent of $j$, the third claim is obvious. $\square$

**Theorem 3.4.** *For any even additive code over $GF(4)$, vectors of odd minimum weight in the shortened code $\mathcal{C}'$ are the only vectors with their support.*

*Proof.* We may assume that the shortened code $\mathcal{C}'$ on some position $j$ is

$$\{(v_1, \cdots, v_{j-1}, v_{j+1}, \cdots, v_n) | \mathbf{v} = (v_1, \cdots, v_j, \cdots, v_n) \in \mathcal{C}, v_j = 0 \text{ or } 1\}.$$

Hence if there are two odd minimum weight vectors in $\mathcal{C}'$ with the same support, then we can add a 1 to these vectors on position $j$, getting two minimum weight vectors in $\mathcal{C}$. We see that the sum of these vectors in $\mathcal{C}$ has weight less than the minimum weight of $\mathcal{C}$. This is a contradiction. $\square$

**Theorem 3.5.** *Let $\mathcal{C}$ be an even additive code over $GF(4)$. Suppose that the set of codewords of weight $w$ in $\mathcal{C}$ with $A_w \neq 0$ forms a generalized 2-design of type 3. Then the set of codewords of odd weight $w-1$ or even weight $w$, respectively in a shortened code $\mathcal{C}'$ on any coordinate forms a generalized 1-design of type 3.*

*Proof.* Using a similar argument as in the proof of Theorem 3.4, we easily see that the set of codewords of odd weight $w-1$ in $\mathcal{C}'$ forms a generalized 1-design of type 3. From now on, we want to show that the set of codewords of even weight $w$ in $\mathcal{C}'$ forms a generalized 1-design of type 3. Suppose that $\mathcal{C}'$ is shortened on position $j$. As the weight $w$ vectors in $\mathcal{C}'$ come from the weight $w$ vectors in $\mathcal{C}$ with $j$th coordinate 0, it suffices to show that there is a constant number of vectors in $\mathcal{C}$ covering $01, 0\omega, 0\overline{\omega}$ [likewise $10, \omega 0, \overline{\omega}0$] respectively, where 0 is in the $j$th coordinate. To do this, we note that vectors of weight $w$ in $\mathcal{C}$ hold a generalized 1-design. So there are $\mu_1$ vectors covering any fixed non-zero element $a$ in $GF(4)$. These vectors have one of $0, 1, \omega, \overline{\omega}$ on their $j$th coordinate. Since there are $\mu_2$ vectors of weight $w$ in $\mathcal{C}$ covering $1a, \omega a, \overline{\omega}a$ [$a1, a\omega, a\overline{\omega}$] respectively, we see that there are $\mu_1 - 3\mu_2$ vectors of weight $w$ in $\mathcal{C}$ covering $0a$ [$a0$]. This completes the proof. $\square$

**Remark 3.6.** Under the same hypothesis as Theorem 3.5, the set of codewords of odd weight $w-1$ or even weight $w$ in a punctured code forms a generalized 1-design of type 3.

**Example 3.7.** Here we compute $\mu(i, e2)$ for the dodecacode, where $e2$ is any vector of weight 2 in $G = (GF(4)^{12})$. Since codewords of nonzero weight $i$ hold a generalized 2-design by Corollary 3.2, $\mu(i, e2)$ is independent of the choice of $e2$. We have $\mu(6, e2) = 10, \mu(8, e2) = 70, \mu(10, e2) = 150$, and $\mu(12, e2) = 26$. These numbers are obtained by dividing the $\lambda$ for the 2-design held by these vectors by 9.

# References


[1] E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory*, Vol. 6 (1969) pp. 122-151.

[2] C. Bachoc and P. Gaborit, On extremal additive $GF(4)$-codes of lengths 10 to 18, *J. Théorie Nombres Bordeaux*, Vol. 12 (2000) pp. 225-271.

[3] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory*, Vol. 44 (1998) pp. 1369–1387.

[4] Delsarte, Four fundamental parameters of a code and their combinatorial significance, *Inform. and Control*, Vol. 23 (1973) pp. 407–438.

[5] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, On the classification of extremal additive codes over $GF(4)$, *Proceedings of the 37th Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign (1999) pp. 535–544.

[6] P. Gaborit, W. C. Huffman, J.-L. Kim, and V. Pless, On additive $GF(4)$ codes, *DIMACS Workshop on Codes and Association Schemes,* DIMACS Series in Discrete Math. and Theoret. Computer Science, Amer. Math. Soc., Providence, RI, Vol. 56 (2001) pp. 135-149.

[7] G. Höhn, Self-dual codes over the Kleinian four group, preprint, 1996. An updated version in http://xxx.lanl.gov/(math.CO/0005266).

[8] W. C. Huffman, Characterization of quaternary extremal codes of lengths 18 and 20, *IEEE Trans. Inform. Theory* Vol. 43 (1997) pp. 1613–1616.

[9] C. W. H. Lam and V. Pless, There is no (24,12,10) self-dual quaternary code, *IEEE Trans. Inform. Theory* Vol. 36 (1990) pp. 1153–1156.

[10] V. Pless, Extremal codes are homogeneous, *IEEE Trans. Inform. Theory* Vol. 35 (1989) pp. 1329–1330.

[11] V. S. Pless, W. C. Huffman and R. A. Brualdi, An introduction to algebraic codes, *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, (1998) pp. 3–139.

[12] E. M. Rains and N. J. A. Sloane, Self-dual codes, *Handbook of Coding Theory*, ed. V. S. Pless and W. C. Huffman. Amsterdam: Elsevier, (1998) pp. 177–294.

Table 1: Generator Matrices of Dodecacode and Shortened Dodecacode

$$G(QC\_12) = \begin{bmatrix} 0&0&0&0&0&0&1&1&1&1&1&1 \\ 0&0&0&0&0&0&\omega&\omega&\omega&\omega&\omega&\omega \\ 1&1&1&1&1&1&0&0&0&0&0&0 \\ \omega&\omega&\omega&\omega&\omega&\omega&0&0&0&0&0&0 \\ 0&0&0&1&\omega&\overline{\omega}&0&0&0&1&\omega&\overline{\omega} \\ 0&0&0&\omega&\overline{\omega}&1&0&0&0&\omega&\overline{\omega}&1 \\ 1&\overline{\omega}&\omega&0&0&0&1&\overline{\omega}&\omega&0&0&0 \\ \omega&1&\overline{\omega}&0&0&0&\omega&1&\overline{\omega}&0&0&0 \\ 0&0&0&1&\overline{\omega}&\omega&\omega&\overline{\omega}&1&0&0&0 \\ 0&0&0&\omega&1&\overline{\omega}&1&\omega&\overline{\omega}&0&0&0 \\ 1&\omega&\overline{\omega}&0&0&0&0&0&0&\overline{\omega}&\omega&1 \\ \overline{\omega}&1&\omega&0&0&0&0&0&0&1&\overline{\omega}&\omega \end{bmatrix}, G((QC\_12)') = \begin{bmatrix} 0&0&0&0&0&0&1&1&1&1&1 \\ \overline{\omega}&1&\omega&0&0&0&\omega&\omega&\omega&\overline{\omega}&1 \\ 1&1&1&1&1&1&0&0&0&0&0 \\ \omega&\omega&\omega&\omega&\omega&\omega&0&0&0&0&0 \\ \overline{\omega}&1&\omega&1&\omega&\overline{\omega}&1&1&1&1&0 \\ 0&0&0&\omega&\overline{\omega}&1&1&1&1&\overline{\omega}&\omega \\ 1&\overline{\omega}&\omega&0&0&0&1&\overline{\omega}&\omega&0&0 \\ \omega&1&\overline{\omega}&0&0&0&\omega&1&\overline{\omega}&0&0 \\ 0&0&0&1&\overline{\omega}&\omega&\omega&\overline{\omega}&1&0&0 \\ 0&0&0&\omega&1&\overline{\omega}&1&\omega&\overline{\omega}&0&0 \\ 1&\omega&\overline{\omega}&0&0&0&1&1&1&\omega&\overline{\omega} \end{bmatrix}.$$

Table 2: Weight Distribution and Group Order of $QC\_12$ and $(QC\_12)'$

| Code | n | d | $\lvert\mathrm{Aut}(C)\rvert$ | $A_0$ | $A_4$ | $A_5$ | $A_6$ | $A_7$ | $A_8$ | $A_9$ | $A_{10}$ | $A_{11}$ | $A_{12}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $QC\_12$ | 12 | 6 | 648 | 1 | 0 | 0 | 396 | 0 | 1485 | 0 | 1980 | 0 | 234 |
| $(QC\_12)'$ | 11 | 5 | 18 | 1 | 0 | 66 | 198 | 330 | 495 | 550 | 330 | 78 | |