CLASSIFICATION OF INDECOMPOSABLE 2^r-DIVISIBLE CODES SPANNED BY BY CODEWORDS OF WEIGHT 2^r

SASCHA KURZ

ABSTRACT. We classify indecomposable binary linear codes whose weights of the codewords are divisible by 2^r for some integer r and that are spanned by the set of minimum weight codewords.
Keywords: linear codes, divisible codes, classification
MSC: 94B05.

1. INTRODUCTION

A binary $[n,k]_2$ code C is a k-dimensional subspace of the n-dimensional vector space $\mathbb{F}_2^n$, i.e., we consider linear codes only. Elements $c \in C$ are called codewords and n is called the length of the code. The support of a codeword c is the number of coordinates with a non-zero entry, i.e., $\operatorname{supp}(c) = \{i \in \{1,\dots,n\} \,:\, c_i \neq 0\}$. The (Hamming-) weight $\operatorname{wt}(c)$ of a codeword is the cardinality $|\operatorname{supp}(c)|$ of its support. A code C is called Δ-divisible if the weight of all codewords is divisible by some positive integer $\Delta \geq 1$, see e.g. [8] for a survey. A classification of all Δ-divisible codes seems out of reach unless the length is restricted to rather small values.

Given an $[n,k]_2$ code C, the $[n,n-k]_2$ code $C^\perp = \left\{x \in \mathbb{F}_2^n \,.\, x^T y = 0 \,\forall y \in C\right\}$ is called the orthogonal, or dual of C. A code is self-orthogonal if $C \subseteq C^\perp$ and self-dual if $C = C^\perp$. A self-orthogonal code is 2-divisible. In [6] self-orthogonal codes which are generated by codewords of weight 4, which then are 4-divisible, are completely characterized. Here we want to generalize that result, see [6, Theorem 6.5], and characterize 2^r-divisible codes that are generated by codewords of weight 2^r. Further related work includes the classical result of Bonisoli characterizing one-weight codes [1] and the generalization to two-weight codes where one of the weights is twice the other [3].

2. PRELIMINARIES

We call a code C non-trivial if its dimension $\dim(C) = k$ is at least 1. Using the abbreviation $\operatorname{supp}(C) = \cup_{c \in C} \operatorname{supp}(c)$, we call $|\operatorname{supp}(C)|$ the effective length n_{eff} of C. Here we assume that all codes are non-trivial and that the effective length n_{eff} equals the length n (or $n(C)$ to be more precise). We emphasize this by speaking of an $[\underline{n},k]_2$ code. A matrix G with the property that the linear span of its rows generate the code C, is a generator matrix of C. A generator matrix G is called systematic if it starts with a unit matrix. Each code admits a systematic generator matrix. The assumption that the effective length n_{eff} is equal to the length n is equivalent to the property that generator matrices do not contain a zero-column. By $A_i(C)$ we denote the number of codewords of weight i in C and by $B_i(C)$ the number of codewords of weight i in $C^\perp$. Mostly, we will just write A_i and B_i, whenever the code C is clear from the context. In our setting we have $A_0 = B_0 = 1$ and $B_1 = 0$. In general, the A_i and the B_i are related by the so-called MacWilliams identities, see e.g. [4]. The first four MacWilliams identities can be rewritten to:

$$\sum_{i>0} A_i = 2^k - 1, \tag{1}$$

$$\sum_{i\geq 0} iA_i = 2^{k-1}n, \tag{2}$$

$$\sum_{i\geq 0} i^2A_i = 2^{k-1}(B_2 + n(n+1)/2), \tag{3}$$

$$\sum_{i\geq 0} i^3A_i = 2^{k-2}(3(B_2n - B_3) + n^2(n+3)/2). \tag{4}$$

In this special form they are also called the first four *(Pless) power moments*, see [5]. The weight distribution of C is the sequence $A_0, \dots, A_n$ and the weight enumerator of C is the polynomial $w(C) = w(C;x) = \sum_{i=0}^{n} A_i x^i$.

Two codes C, C' are equivalent, notated as $C \simeq C'$, if there exists a permutation in $\mathcal{S}_n$ sending C into C'. The direct sum of an $[\underline{n}, k]_2$ code C and an $[\underline{n'}, k']_2$ code C' is the $[\underline{n+n'}, k+k']_2$ code $C \oplus C' = \{(c_1 + c'_1, \dots, c_n + c'_n) \,:\, (c_1, \dots, c_n) \in C, (c'_1, \dots, c'_n) \in C'\}$. If D can be written as $C \oplus C'$ it is called decomposable, otherwise indecomposable [7].

Lemma 2.1. *Let C be an indecomposable $[\underline{n}, k]_q$ code. If $k \geq 2$, then C contains an indecomposable $\left[\underline{\leq n-1}, k-1\right]_q$ code C' as a subcode.*

PROOF. Let G be a systematic generator matrix of C. We will construct C' by row-wise building up a generator matrix. To this end let $\mathcal{R}$ be the set of rows and set $\mathcal{C} = \emptyset$. For the start pick some row $r \in \mathcal{R}$ add it to $\mathcal{C}$ and remove it from $\mathcal{R}$. As long as $\# < k-1$ we choose some element $r \in \mathcal{R}$ with $\operatorname{supp}(r) \cap \operatorname{supp}(c) \neq \emptyset$ for at least one $c \in \mathcal{C}$. Since C is indecomposable such a row r must indeed exist. Again, add r to $\mathcal{C}$ and remove it from $\mathcal{R}$. □

In other words, indecomposable codes can always be obtained by extending indecomposable subcodes.

Corollary 2.2. *Each indecomposable $[\underline{n}, k]_q$ code C contains a chain $C_0 \subseteq C_1 \subseteq \cdots \subseteq C_k = C$ of indecomposable subcodes such that $\dim(C_i) = i$ and the effective length is strictly increasing.*

Given some $[\underline{n}, k]_2$ code C we can restrict the coordinates of the codewords to some subset $I \subseteq N := \{1, \dots, n\}$, i.e., $C_I = \{c_I \,:\, c \in C\}$, where c_I denotes the codeword c restricted to the positions in I. Special cases are the code $C_{\operatorname{supp}(c)}$ restricted to some codeword $c \in C$ and the corresponding residual code $C_{N \setminus \operatorname{supp}(c)}$. Note that the dimensions of both codes is at most $k-1$ but can be strictly less. If C is 2^r divisible for some positive integer r, then a residual code of C is 2^{r-1}-divisible, see e.g. [9, Lemma 13], so that also the corresponding restricted code is 2^{r-1}-divisible.

If all non-zero codewords of a binary linear code have the same weight, then the code is a replication of a simplex code, see [1]. For the reader's convenience we prove a specialization of that result.

Lemma 2.3. *Let C be an $[\underline{n}, k]_2$ code where all non-zero codewords have weight 2^a. Then, $k \leq a+1$ and $C \simeq S_{k-1}^{a+1-k}$.*

PROOF. By Lemma 3.1 there exists a code C' with $C = C'^{a+1-k}$. By construction all non-zero codewords of C' have weight 2^{k-1}. Using equations (1)-(3) we compute $n = 2^k - 1$ and $B_2 = 0$. Since there are only $2^k - 1$ different non-zero vectors in $\mathbb{F}_2^k$ we have $C' \simeq S_{k-1}^0$, so that $C \simeq S_{k-1}^{a+1-k}$. □

3. THE CHARACTERIZATION

We want to prove our main characterization result for indecomposable 2^r-divisible $[\underline{n}, k]_2$ codes that are generated by codewords of weight 2^r in Theorem 3.7. To this end, we describe some families of codes and then derive some auxiliary results. So, by S_l we denote the $(l+1)$-dimensional simplex code, i.e., $\dim(S_l) = l+1$ and $w_{S_l}(X) = 1 + (2^{l+1}-1)\cdot X^{2^l}$, where $l \ge 0$. So, S_l is 2^l-divisible and has effective length $n = 2^{l+1}-1$. By A_l we denote the $\left[2^{l+1}, l+2, 2^l\right]$ 1st-order Reed-Muller code, which geometrically corresponds to the affine $(l+1)$-flat, i.e., $S_{l+1} - S_l +$ in terms of point sets. So, $\dim(A_l) = l+2$ and $w_{A_l}(X) = 1 + \left(2^{l+2}-2\right)\cdot X^{2^l} + 1\cdot X^{2^{l+1}}$, i.e., it is 2^l-divisible and has effective length $n = 2^{l+1}$. By R_l we denote the l-dimensional code generate by the l codewords having a 1 at position 1 and a second one at position $i+1$ for $1 \le i \le l$. So, R_l has dimension $\dim(R_l) = l$, effective length $n = l+1$ and is 2^1-divisible. If C is a code then by C^m we denote the code that arises if we replace every 0 by a block of 2^m consecutive zeroes and every 1 by a block of 2^m consecutive ones. So, especially we have $C^0 = C$. In general the dimension does not change, the effective length is multiplied by 2^m and a 2^l-divisible code is turned into a 2^{l+m}-divisible code. For the weight enumerator we have $w(C^m; x) = w(C; x^m)$.

Lemma 3.1. *Let $q = p^e$ be a prime power and C be a q-ary linear code (considered as a powerset of $\mathbb{F}_q^n$) that is q^r-divisible, where $re \in \mathbb{N}_{\ge 0}$. For each $\emptyset \subseteq M \subseteq S \subseteq C$ with $1 \le |S| \le r+1$ we have that $q^{r+1-|S|}$ divides $\#I_{M,S}(C)$, where*

$$I_{M,S}(C) = \{i \in \mathit{supp}(S) \,:\, i \in \operatorname{supp}(c)\,\forall c \in M \;\wedge\; i \notin \operatorname{supp}(c)\,\forall c \in S\backslash M\}\,.$$

PROOF. For $M = \emptyset$ we have $I_{M,S}(C) = \emptyset$, so that $\#I_{M,S}(C) = 0$ and the statement is trivially true. In the following we assume $M \neq \emptyset$ and prove by induction on $\#S$. For the induction start let $S = \{c\}$. Due to our assumption we have $M = \{c\}$, so that $I_{M,S}(C) = \#\operatorname{supp}(c) = \operatorname{wt}(c)$, which is divisible by $q^{r+1-|S|} = q^r$. Now let $|S| \ge 2$ and $\bar{c} \in M$ be arbitrary. With $I = \operatorname{supp}(\bar{c})$ we set $C' = C_I$, i.e., the restricted code. As noted in Section 2, C' is q^{r-1}-divisible (since $|S| \le r+1$ implies $r \ge 1$). We set $M' = \{c_I \,:\, c \in M\backslash\{\bar{c}\}\}$ and $S' = \{c_I \,:\, c \in S\backslash\{\bar{c}\}\}$, so that $\emptyset \subseteq M' \subseteq S' \subseteq C'$. Since $\#S' = \#S - 1$ and $I_{M,S}(C) = I_{M',S'}(C')$ the statement follows from the induction hypothesis. □

Corollary 3.2. *In the setting of Lemma 3.1 we have that $q^{r+1-|S|}$ divides the cardinality of* $\operatorname{supp}(S)$.

PROOF. Since

$$\operatorname{supp}(S) = \cup_{c\in S}\operatorname{supp}(c) = \sum_{\emptyset \subseteq M \subseteq S} I_{M,S}(C),$$

the statement follows directly from Lemma 3.1. □

Lemma 3.3. *Let $C = R_l^a$ for integers $l \ge 1$ and $a \ge 0$, c' be a further codeword with weight 2^{a+1} and $\emptyset \neq \operatorname{supp}(c') \cap \operatorname{supp}(C) \neq \operatorname{supp}(C)$. If $C' := \langle C, c'\rangle$ is 2^{a+1}-divisible, then either $C' \simeq R_{l+1}^a$ or $l = 2$, $a \ge 1$, and $C' \simeq S_2^{a-1}$.*

PROOF. As an abbreviation we set $\Delta := 2^{a+1}$ and note that C is Δ-divisible. If $l = 1$, then $C = \{0, c\}$, where $\operatorname{wt}(c) = \Delta$. From Lemma 3.1 we conclude that $\frac{\Delta}{2}$ divides $|\operatorname{supp}(C) \cap \operatorname{supp}(c')|$. Since $\operatorname{supp}(C) = \operatorname{supp}(c)$ and $\emptyset \neq \operatorname{supp}(C) \cap \operatorname{supp}(c') \neq \operatorname{supp}(C)$, we have $|\operatorname{supp}(C) \cap \operatorname{supp}(c')| = \frac{\Delta}{2}$. Thus, $C' \simeq R_2^a = R_{l+1}^a$.

Now we assume $l \ge 2$. For $1 \le i \le l+1$ we set $P_i := \left\{j \in \mathbb{N} \,:\, \frac{\Delta}{2}(i-1)+1 \le j \le \frac{\Delta}{2}i\right\}$ and $f_i(c) := |\operatorname{supp}(c) \cap P_i|$ for each codeword $c \in C'$. Note that $f_i(c) \in \left\{0, \frac{\Delta}{2}\right\}$ for all $c \in C$ and all $1 \le i \le l+1$. Moreover, for each $1 \le i < j \le l+1$ there exists a codeword $c^{i,j} \in C$ with $f_i(c^{i,j}) = f_j(c^{i,j}) = \frac{\Delta}{2}$ and $f_h(c^{i,j}) = 0$ otherwise. Now suppose that there is an index $1 \le i \le l+1$ with $0 < f_i(c') < \frac{\Delta}{2}$. For each index $1 \le j \le l+1$ with $i \neq j$ we have

$$\operatorname{wt}(c^{i,j} + c') = \operatorname{wt}(c^{i,j}) + \operatorname{wt}(c') - 2\cdot\operatorname{wt}(c^{i,j} \cap c') = 2\Delta - 2f_i(c') - 2f_j(c'),$$

so that $\operatorname{wt}(c^{i,j} + c') = \Delta$ and $f_i(c') + f_j(c') = \frac{\Delta}{2}$. Since $l \ge 2$ there exists at least another index in $\{1, \dots, l+1\} \cap \{i, j\}$, so that this implies $f_h(c') = \frac{\Delta}{4}$ for all $1 \le h \le l+1$. Thus, $\Delta = \operatorname{wt}(c') > \sum_{h=1}^{l+1} f_h(c')$ implies $l = 2$ and $C' \simeq S_2^{a-1}$. Otherwise we have $f_h(c') \in \left\{0, \frac{\Delta}{2}\right\}$ for all $1 \le h \le l+1$, i.e., there exists an index $1 \le i \le l+1$ with $f_i(c') = \frac{\Delta}{2}$ and $f_h(c') = 0$ otherwise. If $i \neq 1$ we consider $c' + c^{1,i}$ to conclude that $C' = R^a_{l+1}$. □

Lemma 3.4. *Let C be a binary, non-trivial, indecomposable 2^1-divisible linear code that is spanned by codewords of weight 2. Then, $C \simeq R^0_l$ for some integer $l \ge 1$.*

PROOF. We will prove by induction on the dimension k of C. The induction start $k = 1$ is obvious. For the induction step let C' be an indecomposable subcode of C with dimension $k-1$, see Lemma 2.1. From the induction hypothesis we conclude $C' \simeq R^0_{k-1}$, so that Lemma 3.3 gives $C \simeq R^0_k$. □

Note that $S^1_0 \simeq R^0_1$, $S^0_1 \simeq R^0_2$, and $A^0_1 \simeq R^0_3$.

Lemma 3.5. *Let C be a binary, non-trivial, indecomposable Δ-divisible linear code that is spanned by codewords of weight Δ, where $\Delta = 2^a$ and $a \in \mathbb{N}_{>0}$. Let c' be a further codeword with weight Δ and $\emptyset \neq \operatorname{supp}(c') \cap \operatorname{supp}(C) \neq \operatorname{supp}(C)$ such that $C' := \langle C, c' \rangle$ is Δ-divisible.*
(1) If $C \simeq S^0_a$ then $C' \simeq A^0_a$.
(2) If $C \simeq S^1_{a-1}$ then $C' \simeq S^0_a$ or $C' \simeq A^1_{a-1}$.
(3) If $a \ge 1$ and $C \simeq A^0_a$ then $a = 1$ and $C' = R^0_4$.
(4) If $a \ge 2$ and $C \simeq A^1_{a-1}$ then $a = 2$ and $C' \simeq R^1_4$.
(5) If $a \ge 3$ and $C \simeq A^2_{a-2}$ then $a = 3$ and $C' \simeq R^2_4$.

PROOF. We note that $1 \le n(C') - n(C) \le \Delta - 1$. Since $n(C) \le 2\Delta$ in all cases the non-zero weights in C' are either Δ or 2Δ.

(1) From equations (1)-(2) we compute $A_{2\Delta} = 2n(C') - 4\Delta + 1$, i.e., $A_{2\Delta} \ge 1$. Let D be the residual code of a codeword of weight 2Δ in C' ($C' \backslash C$). By construction D is $\frac{\Delta}{2}$-divisible, projective, and has an effective length of at most $\Delta - 2 < 2 \cdot \frac{\Delta}{2} - 1$. Thus, Lemma 2.3 implies that D is a trivial code, i.e., $n(D) = 0$ and $n(C') = 2\Delta$. With this we have $A_{2\Delta} = 1$ and $C' \simeq A^0_a$.
(2) From equations (1)-(2) we compute $A_\Delta = 4\Delta - 2 - n(C')$ and $A_{2\Delta} = n(C') - 2\Delta + 1$, i.e., $n(C') \ge 2\Delta - 1$. If $n(C') = 2\Delta - 1$ then $A_{2\Delta} = 0$ and Lemma 2.3 gives $C' \simeq S^0_a$. If $n(C') = 2\Delta$ then $A_{2\Delta} = 1$ and adding the all-one word to C gives $C' \simeq A^1_{a-1}$. In the remaining cases we have $n(C') > 2\Delta$ and $A_{2\Delta} \ge 1$. Let D be the residual code of a codeword of weight 2Δ in C' ($C' \backslash C$). By construction D is $\frac{\Delta}{2}$-divisible, has column multiplicity at most 2, and has an effective length of at most $\Delta - 3 < 2 \cdot \frac{\Delta}{2} - 2$. Thus, Lemma 2.3 implies that D is a trivial code – contradiction. (The two possibilities with column multiplicity 1 or 2 would have an effective length of $\Delta - 1$ or $\Delta - 2$, respectively.)
(3) From equations (1)-(2) we compute $A_\Delta = 16\Delta - 2 - 4n(C')$ and $A_{2\Delta} = 4n(C') - 8\Delta + 1$. Let D be the residual code of a codeword of weight 2Δ in $C' \backslash C$. By construction D is $\frac{\Delta}{2}$-divisible, projective, contains the all-1 codeword, and has an effective length of at most $\Delta - 1$. Thus, Lemma 2.3 implies that $D \simeq S^{a-1}_0$, where $a = 1$. So, $C = R^0_3$ and Lemma 3.3 yields $C' = R^0_4$.
(4) From equations (1)-(2) we compute $A_\Delta = 8\Delta - 2 - 2n(C')$ and $A_{2\Delta} = 2n(C') - 4\Delta + 1$. Let D be the residual code of a codeword of weight 2Δ in $C' \backslash C$. By construction D is $\frac{\Delta}{2}$-divisible, has maximum column multiplicity at most 2, contains the all-1 codeword, and has an effective length of at most $\Delta - 1$. Thus, Lemma 2.3 implies that either $D \simeq S^0_0$ or $D \simeq S^1_0$. In the first case we have $\Delta = 2$ and $a = 1$, which is not possible. In the second case we have $\Delta = 4$, $a = 2$, and $C \simeq A^1_1 \simeq R^1_3$, so that Lemma 3.3 implies $C' \simeq R^1_4$.
(5) From equations (1)-(2) we compute $A_\Delta = 4\Delta - 2 - n(C')$ and $A_{2\Delta} = n(C') - 2\Delta + 1$. Let D be the residual code of a codeword of weight 2Δ in $C' \backslash C$. By construction D is $\frac{\Delta}{2}$-divisible, has maximum column multiplicity at most 4, contains the all-1 codeword, and has an effective length of at most $\Delta - 1$. Thus, Lemma 2.3 implies that either $D \simeq S^0_0$, $D \simeq S^1_0$, or $D \simeq S^2_0$. Since we assume $a \ge 3$, only $a = 3$ and $\Delta = 8$ is possible, where $C \simeq R^2_3$, so that Lemma 3.3 implies $C' \simeq R^2_4$.

□

Note that if we drop the condition $\operatorname{supp}(C') \neq \operatorname{supp}(C)$, then A^1_{a-1} can be extended to A^0_a and A^2_{a-2} can be extended to A^1_{a-1}.

Lemma 3.6. *Let C be a binary, non-trivial, indecomposable 2^2-divisible linear code that is spanned by codewords of weight 4. Then, $C \simeq R^1_l$ for some integer $l \geq 1$ or either $C \simeq S^l_{2-l}$ or $C \simeq A^l_{2-l}$ for some $l \in \{0, 1\}$.*

PROOF. First note that the mentioned families of codes satisfy all assumptions. If $\dim(C) \leq 2$ then Lemma 3.1 implies that there is some code C' with $C = C'^1$, i.e., we can apply Lemma 3.4. If $\dim(C) \geq 3$ we apply Corollary 2.2 and consider the corresponding chain $C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_k = C$, where $k = \dim(C)$. Lemma 3.1 gives the existence of a binary, non-trivial, indecomposable 2^1-divisible linear code C' with $C_2 = C'^2$ that is spanned by codewords of weight 2. Thus, Lemma 3.4 gives $C' \simeq R^0_2$ and $C_2 \simeq R^1_2$. Lemma 3.3 then gives $C_3 \simeq R^1_3$ or $C_3 \simeq S^0_2$. If $C_3 \simeq R^1_3$ then recursively applying Lemma 3.3 yields $C_l \simeq D^1_l$ for all $3 \leq l \leq k$. If $C_3 \simeq S^0_2$ and $k \geq 4$, then Lemma 3.5 gives $C_4 \simeq A^0_2$ and $k = 4$ (since A^0_2 cannot be extended). □

Note that $S^1_1 \simeq R^1_2$ and $A^1_1 \simeq R^1_3$.

Theorem 3.7. *For a positive integer a let C be a binary, non-trivial, indecomposable 2^a-divisible linear code that is spanned by codewords of weight 2^a. Then, $C \simeq R^{a-1}_l$ for some integer $l \geq 1$ or either $C \simeq S^l_{a-l}$ or $C \simeq A^l_{a-l}$ for some $l \in \{0, 1, \ldots, a-1\}$.*

PROOF. We prove by induction on a. Lemma 3.4 and Lemma 3.6 give the induction start, so that we can assume $a \geq 3$ in the following. First note that the mentioned families of codes satisfy all assumptions. If $\dim(C) \leq a$ then Lemma 3.1 implies that there is some code C' with $C = C'^1$, i.e., we can apply the induction hypothesis. If $\dim(C) \geq a + 1$ we apply Corollary 2.2 and consider the corresponding chain $C_0 \subsetneq C_1 \subsetneq \cdots \subsetneq C_k = C$, where $k = \dim(C)$. Lemma 3.1 gives the existence of a binary, non-trivial, indecomposable 2^{a-1}-divisible linear code C' with $C_a = C'^2$ that is spanned by codewords of weight 2^{a-1}. Then the induction hypothesis gives that either $C_a \simeq R^{a-1}_a$, $C_a \simeq S^1_{a-1}$, or $C_a \simeq A^2_{a-2}$. In the first case recursively applying Lemma 3.3 yields $C_l \simeq R^{a-1}_l$ for all $a \leq l \leq k$. If either $C_a \simeq S^1_{a-1}$ or $C_a \simeq A^2_{a-2}$ we can apply Lemma 3.5 to conclude $C_{a+1} \simeq S^0_a$, $C_{a+1} \simeq A^1_{a-1}$, or $a = 3$ and $C_4 \simeq R^2_4$. In the latter case we have $C_l \simeq R^2_l$ for all $4 \leq l \leq k$ due to Lemma 3.3. Otherwise either $k = a + 1$ or $C_{a+2} \simeq A^0_a$ and $k = a + 2$ due to Lemma 3.5. □

4. AN APPLICATION TO PROJECTIVE 3-WEIGHT CODES

When deciding the question whether a code with certain parameters exist one often checks whether the MacWilliams identities admit a non-negative integer solution. If so, then sometimes more combinatorial are necessary. In the proof of e.g. [2, Lemma 24] the existence of an $[\underline{51}, 9]_2$ code with weight enumerator $w(C) = 1 + 2x^8 + 406x^{24} + 103x^{32}$ had to be excluded in a subcase. Since the sum of two codewords of weight 8 would have a weight between 8 and 16 this is impossible. Using the classification result of Theorem 3.7 this can easily be generalized.

Proposition 4.1. *Let C be a Δ-divisible $[\underline{n}, k]_2$ code, where $\Delta = 2^r$ for some positive integer r. If C does not contain a codeword of weight 2Δ, then $A_\Delta \in \left\{2^i - 1 \,:\, 0 \leq i \leq r + 1\right\}$.*

PROOF. Let C' be the subcode of C spanned by the codewords of weight Δ and $C' = C_1 \oplus \cdots \oplus C_l$ the up to permutation unique decomposition into indecomposable codes. Since C' does not contain a codeword of weight 2Δ we have $l \leq 1$. For $l = 0$ we obviously have $A_\Delta = 0$. If $l = 1$, then Theorem 3.7 gives $C_1 \simeq S^{r-i}_i$, where $0 \leq i \leq r$, and $A_\Delta = 2^{i+1} - 1$. □

In general, if we know that an $[n, k]_2$ code is $\Delta := 2^r$-divisible and contains some codewords of weight Δ one can consider the decomposition $C' = C_1 \oplus \cdots \oplus C_l$ of the subcode C' spanned by codewords of weight Δ. Obviously, we have

(1) $w(C')=\prod_{i=1}^{l} w(C_i)$, i.e., especially $A_\Delta(C')=\sum_{i=1}^{l} A_\Delta(C_i)$;
(2) $\dim(C)\ge\dim(C')=\sum_{i=1}^{l}\dim(C_i)$;
(3) $n(C)\ge n(C')=\sum_{i=1}^{l} n(C_i)$;
(4) $\omega(C)\ge\omega(C')=\sum_{i=1}^{l}\omega(C_i)$, where $\omega(D)$ denotes the maximum weight of a codeword in D.

With respect to Theorem 3.7 we remark
(1) $A_\Delta(S_{r-l}^{l})=2^{r+1-l}-1$, $\dim(S_{r-l}^{l})=r+1-l$, $n(S_{r-l}^{l})=2^{r+1}-2^{l}$, and $\omega(S_{r-l}^{l})=\Delta$ for $0\le l\le r$;
(2) $A_\Delta(A_{r-l}^{l})=2^{r+2-l}-2$, $\dim(A_{r-l}^{l})=r+2-l$, $n(A_{r-l}^{l})=2\Delta=2^{r+1}$, and $\omega(A_{r-l}^{l})=2\Delta$ for $0\le l\le r-1$;
(3) $A_\Delta(R_l^{r-1})=\binom{l+1}{2}$, $\dim(R_l^{r-1})=l$, $n(R_l^{r-1})=\frac{\Delta}{2}\cdot(l+1)$, and $\omega(R_l^{r-1})=\lceil l/2\rceil\cdot\Delta$ for $l\ge 1$.

A more sophisticated example, compared to Proposition 4.1, occurs in the area of binary projective 3-weight codes. Projective codes, i.e., those with $B_2=0$, having few weights have a lot of applications and have been studied widely in the literature. Here we consider $[\underline{n},k]_2$ codes with weights in $\{0,\Delta,2\Delta,3\Delta\}$ and length $n=4\Delta$, where $\Delta=2^r$ for some positive integer r.

Theorem 4.2. *For an integer $r\ge 2$ let $\Delta=2^r$ and C be a projective Δ-divisible $[\underline{4\Delta},k]_2$ code with non-zero weights in $\{\Delta,2\Delta,3\Delta\}$. Then $k\le 2r+3$. If $k=2r+3$ and $r\ge 3$ then C is isomorphic to a code with generator matrix*

$$\begin{pmatrix} A_{r-1}^0 & A_{r-1}^0 & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & S_r^0 & \mathbf{0}\\ \mathbf{1} & \mathbf{0} & \mathbf{1} & 1\end{pmatrix},$$

where $\mathbf{0}$ and $\mathbf{1}$ are matrices of approbriate sizes that entirely consist of 0's or 1's, respectively

PROOF. Using equations (1)-(3) and $B_2=0$ we compute $A_\Delta=2^{k-r-1}-3\ge 1$. Consider the decomposition $C'=C_1\oplus\cdots\oplus C_l$ of the subcode C' spanned by codewords of weight Δ. Since $\omega(C)=3\Delta$, we have $1\le l\le 3$. If $\omega(C_i)=\Delta$ for all $1\le i\le l$, i.e., $C_i=S_{r-j_i}^{j_i}$ for some $0\le j_i\le r-1$, then $A_\Delta(C')=\sum_{i=1}^{l}A_\Delta(C_i)\le l\cdot(2\Delta-1)\le 3\cdot\left(2^{r+1}-1\right)$, so that $k<2r+4$. If $\omega(C_1)=2\Delta$, then due to Theorem 3.7 we have either $C_1\simeq R_3^{r-1}$, $C_1\simeq R_4^{r-1}$, or $C_1\simeq A_{r-j}^{j}$ for some $0\le j\le r-1$, so that $A_\Delta(C_1)\le 2^{r+2}-2$. Since then $l\le 2$, $\omega(C_2)\le\Delta$, and $A_\Delta(C_2)\le 2^{r+1}-1$, we have $A_\Delta(C')=\sum_{i=1}^{l}A_\Delta(C_i)\le 3\cdot\left(2^{r+1}-1\right)$, so that $k<2r+4$. If $\omega(C_1)\ge 3\Delta$, then $l=1$ and $\omega(C_1)=3\Delta$, so that Theorem 3.7 gives $C_1\simeq R_5^{r-1}$ or $C_1\simeq R_6^{r-1}$, i.e., $A_\Delta(C')\le 21\le 3\cdot\left(2^{r+1}-1\right)$, so that $k<2r+4$. Thus, we have $k\le 2r+3$ in all cases.

For $k=2r+3$ we need a more detailed analysis of the possible decompositions $C'=C_1\oplus\cdots\oplus C_l$. First we note $\omega(C_i)\in\{\Delta,2\Delta,3\Delta\}$, $A_\Delta=2^{r+2}-3\ge 1$, so that $C_i\not\simeq A_r^0$, and $1\le l\le 3$. Let us start to consider the case $\omega(C_i)=\Delta$ for all i, i.e., $A_\Delta=2^{r+1-j_i}-1$ for some $0\le j_i\le r$ ($C_i=S_{r-j_i}^{j_i}$ for some $0\le j_i\le r$). If $j_i\ge 1$ for all i, then $A_\Delta(C')\le 3\cdot(2^r-1)<2^{r+2}-3$, so that we assume $j_1=0$. Since $2^{r+2}-3=2^{r+1}-1$ is equivalent to $r=0$, we have $l\ge 2$. If $l=2$ and $j_2=0$, then $A_\Delta(C')\ge 2^{r+2}-2>2^{r+2}-3$. If $l=2$ and $j_2\le 1$, then $A_\Delta(C')\le 2^{r+1}-1+2^r-1<2^{r+2}-3$ for $r\ge 1$. Thus, we have $l=3$. If $j_2=0$ or $j_3=0$, then $A_\Delta(C')\ge 2\cdot\left(2^{r+1}-1\right)>2^{r+2}-3$. If $j_2\ge 1$, $j_3\ge 1$, and $j_2+j_3\ge 3$, then $A_\Delta(C')\le 2^{r+1}-1+2^r-1+2^{r-1}-1<2^{r+2}-3$. The only possibility with $A_\Delta(C')=2^{r+2}-3$ is $j_1=0$, $j_2=j_3=1$. However, in this case we have $n(C')=\left(2^{r+1}-1\right)+\left(2^{r+1}-2\right)+\left(2^{r+1}-2\right)=2^{r+2}+\left(2^{r+1}-5\right)>2^{r+2}=n$ for $r\ge 2$.

If $\omega(C_i)=3$ for some i, then $l=3$ and Theorem 3.7 gives $C_1\simeq R_5^{r-1}$ or $C_1\simeq R_6^{r-1}$, so that $A_\Delta(C')=\binom{6}{2}=15$ or $A_\Delta(C')=\binom{7}{2}=21$. Since $2^{r+2}-3<15$ for $r\le 2$ and $2^{r+2}-3>21$ for $r\le 3$, this is not possible. Thus, there exists an index i with $\omega(C_i)=2$. W.l.o.g. we assume $\omega(C_1)=2$. From Theorem 3.7 we conclude $C_1\simeq R_4^{r-1}$ or $C_1\simeq A_{r-j}^{j}$ for some integer $0\le j\le r-1$. If $l=2$, then $\omega(C_2)=\Delta$, so that in any case we have $A_\Delta(C')=A_\Delta(C_1)+2^x-1$ for some integer $0\le x\le r+1$. If $C_1\simeq R_4^{r-1}$, then the equation $A_\Delta(C')=2^{r+2}-3=10+2^x-1$ has the unique integer solution

$r = 2$ and $x = 2$, which corresponds to $C' \simeq R_4^1 \oplus S_1^1 \simeq R_4^1 \oplus R_2^1$. (The equation is equivalent to $2^{r+2} = 12 + 2^x$, so that $r \ge 2$. For $r \ge 2$ we have $x \ge 5$, so that the left hand side is divisible by 8 while the right hand side is not.) In the remaining cases we have $C_1 \simeq A_{r-j}^j$, so that $A_\Delta(C_1) = 2^{r+2-j} - 2$. Thus, we have to consider the Diophantine equation $A_\Delta(C') = 2^{r+2} - 3 = 2^y - 2 + 2^x - 1$, where $y = r + 2 - j$. The only integral solution is $y = x = r + 1$, i.e., $j = 1$, $C_1 \simeq A_{r-1}^1$, and $C_2 = S_r^0$.

To sum up, for $k = 2r+3$ and $r \ge 2$, up to permutations, the only possibility is $l = 2$, $C_1 \simeq A_{r-1}^1$, and $C_2 = S_r^0$ with $\dim(C') = 2r + 2$ and $n(C') = 2^{r+2} - 1 = 4\Delta - 1$. Having fixed $k = 2r + 3$ we can use equations (1)-(3) to compute $A_\Delta(C) = 2^{r+2} - 3$ and $A_{3\Delta}(C) = 2^{r+2} - 1$. Since $\dim(C) - \dim(C') = 1$ and $A_{3\Delta}(C') = 2^{r+1} - 1 < 2^{r+2} - 1$, we can assume that $C = \langle C', c' \rangle$ with $\operatorname{wt}(c') = 3\Delta$. Since C is projective from the 2Δ coordinates of the $C_1 \simeq A_{r-1}^1$-part exactly the half have to be ones (and the other half have to be zeroes) in c'. Thus, c' has a one in each of the remaining 2Δ coordinates, so that C is isomorphic to a code with generator matrix

$$G = \begin{pmatrix} A_{r-1}^0 & A_{r-1}^0 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & S_r^0 & \mathbf{0} \\ \mathbf{1} & \mathbf{0} & \mathbf{1} & 1 \end{pmatrix},$$

□

We remark that for $r = 1$ there exists a corresponding code of dimension $2r + 4$, i.e., there is a unique projective $[\underline{8}, 6]_2$ code with weight enumerator $1 + 13x^2 + 35^4 + 15x^6$. For $r = 2$ there exist more than one isomorphism types of codes of dimension $2r + 3$, i.e., there exist exactly two isomorphism types of projective $[\underline{16}, 7]_2$ codes with weight enumerator $1 + 13x^4 + 99x^8 + 14x^{12}$. (For the additional code we have $C' = R_4^1 \oplus R_2^1$, $\dim(C') = 6$, and $n(C') = 16$. Since $n(C) = n(C')$, $\dim(C) - \dim(C') = 1$, and C is projective, we have $C = C'^2$.) For $r = 3$ the non-existence of a projective $[\underline{32}, 10]_2$ code with weight enumerator $1 + 61x^8 + 899x^{16} + 63x^{24}$ can not be concluded directly from the MacWilliam identities.

REFERENCES

[1] A. Bonisoli, *Every equidistant linear code is a sequence of dual hamming codes*, Ars Combinatoria **18** (1983), 181–186.

[2] T. Honold, M. Kiermaier, and S. Kurz, *Partial spreads and vector space partitions*, Network Coding and Subspace Designs, Springer, 2018, pp. 131–170.

[3] D. Jungnickel and V.D. Tonchev, *The classification of antipodal two-weight linear codes*, Finite Fields and Their Applications **50** (2018), 372–381.

[4] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, Elsevier, 1977.

[5] V. Pless, *Power moment identities on weight distributions in error correcting codes*, Information and Control **6** (1963), no. 2, 147–152.

[6] V. Pless and N.J.A. Sloane, *On the classification and enumeration of self-dual codes*, Journal of Combinatorial Theory, Series A **18** (1975), no. 3, 313–335.

[7] D. Slepian, *Some further theory of group codes*, Bell System Technical Journal **39** (1960), no. 5, 1219–1252.

[8] H. Ward, *Divisible codes -a survey*, Serdica Mathematical Journal **27** (2001), no. 4, 263–278.

[9] H.N. Ward, *Divisibility of codes meeting the Griesmer bound*, Journal of Combinatorial Theory, Series A **83** (1998), no. 1, 79–93.

SASCHA KURZ, UNIVERSITY OF BAYREUTH, 95440 BAYREUTH, GERMANY
Email address: sascha.kurz@uni-bayreuth.de