# On strongly walk regular graphs, triple sum sets and their codes

Michael Kiermaier<sup>\*</sup>, Sascha Kurz<sup>\*</sup>, Patrick Solé<sup>†</sup>, Michael Stoll<sup>\*</sup>, and Alfred Wassermann<sup>\*</sup>

**Abstract:** Strongly walk-regular graphs can be constructed as coset graphs of the duals of projective three-weight codes whose weights satisfy a certain equation. We provide classifications of the feasible parameters in the binary and ternary case for medium size code lengths. Additionally some theoretical insights on the properties of the feasible parameters are presented.

Keywords: strongly walk-regular graphs, three-weight codes. MSC (2010): Primary 05E30, Secondary 94B05

# 1 Introduction

A strongly regular graph (SRG) is a regular graph such that the number of common neighbors of two distinct vertices depends only on whether these vertices are adjacent or not. They arise in a lot of applications, see e.g. [5]. As first observed in [10], there is a strong link to projective two-weight codes, see [8] for a survey. The notion of SRGs has been generalized to distance-regular graphs or association schemes. Noting that the number of common neighbors of two vertices equals the number of walks of length two between them, strongly walk-regular graphs (SWRG) were introduced in [23]. A graph is an s-SWRG if the number of walks of length s from a vertex to another vertex depends only on whether the two vertices are the same, adjacent, or not adjacent. Note that SRGs are s-SWRGs for all s > 1. In [23] is was shown that the adjacency matrix of a SWRG has at most four distinct

<sup>\*</sup>Department of Mathematics, University of Bayreuth, Bayreuth, Germany

 $<sup>^{\</sup>dagger}\mbox{I2M},$  CNRS, Aix-Marseille Univ, Centrale Marseille, Marseille, France

eigenvalues. If a *d*-regular graph  $\Gamma$  has four distinct eigenvalues  $k > \theta_1 > \theta_2 > \theta_3$ , then  $\Gamma$  is an *s*-SWRG for  $s \ge 3$  if and only if

$$(\theta_2 - \theta_3)\theta_1^s + (\theta_3 - \theta_1)\theta_2^s + (\theta_1 - \theta_2)\theta_3^s = 0.$$
 (1)

Moreover, it is known that s has to be odd. All known examples for s-SWRGs (with s > 3) satisfy  $\theta_2 = 0$  and  $\theta_3 = -\theta_1$ , where Equation (1) is automatically satisfied for all odd  $s \ge 3$ .

Mimicking the mentioned link between SRGs and projective two-weight codes, a construction of SRWGs as coset graphs of the duals of projective three-weight codes was given recently in [20]. In this situation the eigenvalues are integral and depend on the weights of the three-weight code, so that Equation 1 turns into a number theory question. Another bijection to triple sums sets (TSS) is given in [20].

Several research papers consider the feasible parameters of SRGs, see e.g. https: //www.win.tue.nl/~aeb/graphs/srg/srgtab.html for a large table summarizing the state of knowledge. We remark that the smallest cases, where the existence or non-existence of a SRG is unclear, consist of 65 or 69 nodes. The corresponding parameters cannot be attained by a two-weight code since these give graphs where the number of vertices is a power of the field size. Still, the existence of projective projective two-weight codes is an important source for the construction of SRGs, see e.g. [16], where several new examples have been found. An online database of known two-weight codes can be found at http://moodle.tec.hkr.se/~chen/research/ 2-weight-codes/search.php. Due to a result of Delsarte, see [10, Corollary 2], the possible parameters of two-weight code are quite restricted. More precisely, the weights of a projective two-weight code over a finite field with characteristic p can be written as  $w_1 = up^t$  and  $w_2 = (u + 1)p^t$  for suitable integers  $u \ge 1$  and  $t \ge 0$ .

Given the relation between the weights of a projective three-weight code and the eigenvalues of the coset graph its dual, corresponding solutions of Equation (1) can be easily enumerated. However, not all cases are feasible, i.e., attainable by a projective three-weight code. The aim of this paper is to study feasibility for the smallest cases. For binary codes we give results for lengths smaller than 72 and for ternary codes for lengths smaller or equal to 39. Within that range only a very few cases are left as open problems. This extends first enumeration results from [20]. Similar results for some special rings instead of finite fields are obtained in [15].

The remaining part of this paper is organized as follows. The necessary preliminaries are introduced in Section 2 followed by the enumeration results in Section 3. In Section 4 it is shown that for s = 5 and s = 7 the only rational solutions of Equation (1) are given by the parametric solution  $\theta_2 = 0$ ,  $\theta_3 = -\theta_1$ . For the binary case q = 2 we show that projective three-weight codes whose weights satisfy  $w_1 + w_2 + w_3 = 3n/2$  for the length *n* have a high divisibility of the weights and the length by powers of two, see Proposition 5 for the details. The remaining part of Section 5 studies divisibility properties of binary linear codes with few weights from a more general point of view and prepares some necessary auxiliary results. In Appendix A we collect generator matrices for the mentioned feasible parameters from Section 3.

## 2 Preliminaries

A linear q-ary code C of length n and dimension k is called an  $[n, k]_q$ . If the non-zero codewords of C only attain two different weights, we call C a *two-weight code* and a *three-weight code* if three different non-zero weights are attained. By  $A_i$ we denote the number of codewords of weight i and by  $B^i$  the number of codewords of weight i of the dual code  $C^{\perp}$ , with respect to the standard inner product. The numbers  $A_i$  and  $B_i$  are related via the so-called *MacWilliams identities*, see e.g. [18]:

$$\sum_{j=0}^{n-\nu} \binom{n-j}{\nu} A_j = q^{k-\nu} \cdot \sum_{j=0}^{\nu} \binom{n-j}{n-\nu} B_j \quad \text{for } 0 \le \nu \le n,$$
(2)

where, additionally,  $A_0 = B_0 = 1$ . The fact that the  $B_i$  are uniquely determined by the  $A_i$  can e.g. be seen by providing explicit equations for each  $B_i$  in dependence of the  $A_j$ . Those formulas involve the so-called *Krawtchouk polynomials* [17]. We call an  $[n, k]_q$  code *projective* if  $B_1 = 0$  and  $B_2 = 0$ . For a binary projective  $[n, k]_2$  code, the first four MacWilliams identities can be rewritten to:

$$\sum_{i>0} A_i = 2^k - 1, \tag{3}$$

$$\sum_{i>0} iA_i = 2^{k-1}n, \tag{4}$$

$$\sum_{i>0} i^2 A_i = 2^{k-2} \cdot n(n+1), \tag{5}$$

$$\sum_{i\geq 0} i^3 A_i = 2^{k-3} \cdot (n^2(n+3) - 6B_3).$$
(6)

In the special form of the left hand side, they are also called the first four (*Pless*) power moments, see [19]. Given the length n, the dimension k, and the weights  $w_1, w_2, w_3$ of a projective three-weight code, we can compute  $A_{w_i}$  and  $B_3$ :

$$A_{w_1} = \frac{2^{k-2} \cdot (n^2 - 2nw_2 - 2nw_3 + 4w_2w_3 + n) - w_2w_3}{(w_2 - w_1)(w_3 - w_1)}$$
(7)

$$A_{w_2} = \frac{2^{k-2} \cdot (n^2 - 2nw_1 - 2nw_3 + 4w_1w_3 + n) - w_1w_3}{(w_2 - w_3)(w_2 - w_1)}$$
(8)

$$A_{w_3} = \frac{2^{k-2} \cdot (n^2 - 2nw_1 - 2nw_2 + 4w_1w_2 + n) - w_1w_2}{(w_3 - w_1)(w_3 - w_2)}$$
(9)

$$3B_3 = \frac{n^2(n+3)}{2} - (w_1 + w_2 + w_3) n(n+1) + 2 (w_1w_2 + w_1w_3 + w_2w_3) n - 4w_1w_2w_3 + w_1w_2w_3 \cdot 2^{2-k}$$
(10)

Besides  $A_0 = 1$  all other  $A_i$  are equal to zero, so that the  $B_i$ , where  $i \ge i$ , can be uniquely determined using the remaining MacWilliams identities, i.e., those for  $\nu \ge 4$ . Note that the product  $w_1w_2w_3$  has to be divisible by  $2^{k-2}$ . We remark that we will obtain stronger divisibility conditions in Section 5. Of course, similar explicit expressions can also be determined for field sizes q > 2. However, we will mostly restrict our theoretical considerations to q = 2 in the remaining part of the paper.

A coset of a linear code C is any translate of C by a constant vector. A coset leader is any coset element that minimizes the weight. The weight of a coset is the weight of any of its coset leaders. With this, the coset graph  $\Gamma_C$  of a linear code C is defined on the cosets of C as vertices, where two cosets are connected iff they differ by a coset of weight one. To ease notation, we speak of the eigenvalues of a graph  $\Gamma$ meaning the eigenvalues of the corresponding adjacency matrix. For a projective code C the eigenvalues of the coset graph  $\Gamma_{C^{\perp}}$  of its dual code are completely determined by the occurring non-zero weights  $w_i$  of C, see [4, Theorem 1.11.1]:

**Theorem 1.** Let C be a projective  $[n, k]_q$  code with occurring non-zero weights  $w_1, \ldots, w_r$ . Then, the coset graph  $\Gamma_{C^{\perp}}$  of its dual code  $C^{\perp}$  is d-regular for some integer d and the eigenvalues are given by  $n(q-1) - qw_i$  for  $1 \le i \le r$  and d.

Generalizing partial difference sets, triple sum sets (TSS) have been introduced in [9]. The set  $\Omega \subseteq \mathbb{F}_q^k$  is a TSS if it is closed under scalar multiplication and there are constants  $\sigma_0$  and  $\sigma_1$  such that a each non-zero  $h \in \mathbb{F}_q^k$  can be written as h = x + y + zwith  $x, y, z \in \Omega$  exactly  $\sigma_0$  times if  $h \in \Omega$  and  $\sigma_1$  times if  $h \in \mathbb{F}_q^k \setminus \Omega$ . If  $\Omega \subseteq \mathbb{F}_q^k$  and  $0 \notin \Omega$ , then we denote by  $C(\Omega)$  the projective code of length  $n = \#\Omega/(q-1)$  obtained as the kernel of the  $k \times n$  matrix H whose columns are the projectively non-equivalent elements of  $\Omega$ . Thus, H is the check matrix of the linear code  $C(\Omega)$ . In order to ease the notation, we abbreviate  $\Gamma_{C(\Omega)}$  as  $\Gamma(\Omega)$ . In [20, Theorem 2] it was shown that  $\Omega$  is a TSS if and only if  $\Gamma(\Omega)$  is a 3-SWRG. (Actually, [20, Theorem 2] states the equivalence of  $\Gamma(\Omega)$  being an *s*-SWRG and  $\Omega$  being an *s*-sum set, where the element *h* in the definition of a TSS is a sum of *s* elements from  $\Omega$ .)

A coding-theoretic characterization of triple sum sets is given as follows, see [9, Theorem 2.1] or [20, Theorem 5].

**Theorem 2.** If  $\Omega \subseteq \mathbb{F}_q^k$  so that  $C(\Omega)^{\perp}$  has length m and attains exactly three non-zero weights  $w_1$ ,  $w_2$ , and  $w_3$ , then  $\Omega$  is a TSS iff  $w_1 + w_2 + w_3 = \frac{3n(q-1)}{q}$ .

Using Theorem 1, Equation (1), and 3-SWRGs as intermediate steps, the link becomes obvious. To this end we remark that

$$(\theta_2 - \theta_3)\theta_1^s + (\theta_3 - \theta_1)\theta_2^s + (\theta_1 - \theta_2)\theta_3^s = (\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3) \cdot \sum_{h+i+h=s-2} \theta_1^h \theta_2^i \theta_3^j, \quad (11)$$

so that for s = 3 Equation (1) is satisfied iff  $\theta_1 + \theta_2 + \theta_3 = 0$ . Plugging in the formula for the eigenvalues from Theorem 1 gives the condition  $w_1 + w_2 + w_3 = \frac{3n(q-1)}{q}$ .

As mentioned in the introduction, all known examples for s-SWRGs satisfy  $\theta_2 = 0$ and  $\theta_3 = -\theta_1$ , i.e., they are s-SWRGs for all odd  $s \ge 3$ . So, starting from projective three-weight codes to construct SWRGs it is sufficient to study those that satisfy the weight constraint  $w_1 + w_2 + w_3 = \frac{3n(q-1)}{q}$ . We do so in Section 3. In Section 4 we show that for s = 5 or s = 7 all rational solutions of Equation (1) satisfy  $\theta_2 = 0$ and  $\theta_3 = -\theta_1$ . The computational results from Section 3 for the binary case q = 2suggest that the length n as well as the weights  $w_1, w_2, w_3$  have to be divisible by a large power of 2 if n increases. We proof a corresponding result in Section 5, see especially Proposition 5.

### 

As outlined in Section 2 we can construct 3-SWRGs from projective  $[n, k]_q$  three weight codes if the weights satisfy  $w_1 + w_2 + w_3 = \frac{3n(q-1)}{q}$ . So, here we study the

feasible sets of parameters  $n, k, w_1, w_2, w_3$  such that a corresponding projective threeweight code exists. In Subsection 3.1 we consider the possibilities for all length n < 72in the binary case and in Subsection 3.2 we consider the possibilities for all lengths  $n \leq 39$  in the ternary case.

In that range we can simply loop over all weight-triples  $1 \leq w_1 < w_2 < w_3 \leq n$ satisfying  $w_1 + w_2 + w_3 = 3n(q-1)/q$ . For q = 2 Equation (10) implies that the product  $w_1w_2w_3$  is divisible by  $2^{k-2}$ , which restricts the possible choices for the dimension k. For q = 3 we may use the trivial bounds  $1 \le k \le n$ . Then, the MacWilliams identities uniquely determine the  $A_i$  and  $B_i$ . As a first check we test if all of these values are non-negative integers. In [24, Theorem 1] it has been shown that if the weights of an  $[n,k]_q$  are divisible by some integer t > 1 that is coprime to the field size q, then the code is a t-fold repetition of an  $[n/t, k]_q$  code, i.e., the code is not projective. Thus, we can assume  $gcd(w_1, w_2, w_3, q) = 1$ . Examples where we can apply this criterion to exclude the existence of codes are given by n = 36,  $(w_1, w_2, w_3) = (12, 18, 24)$ , and  $k \in \{6,7,8\}$ . (The corresponding values of  $(A_{w_1}, A_{w_2}, A_{w_3})$  are given by (2,56,5), (10, 104, 13), and (26, 200, 29), respectively.) Other cases where this criterion can be applied for q = 3 are n = 24, k = 4 for weight vector w = [14, 16, 18] and n = 36,  $k \in \{5, 6\}$  for weight vector w = [18, 24, 30]. In order to find examples we have used the software package LinCode [3] to enumerate matching codes or tried to reduce the problem complexity by prescribing automorphisms and applying exact or heuristic solvers for the resulting integer linear programs.

# 3.1 Feasible parameters for projective binary three-weight codes with $w_1 + w_2 + w_3 = 3n/2$

In the subsequent tables we list the feasible parameters for projective binary threeweight codes with  $w_1 + w_2 + w_3 = 3n/2$ . For each length n < 72 we list the possible dimensions k and weight vectors  $w = [w_1, w_2, w_3]$ . If a certain length or dimension is not listed, then they are excluded with the criteria mentioned at the beginning of Section 3. As extra information we also state the weight distribution in the form e = $[A_{w_1}, A_{w_2}, A_{w_3}]$ . For some cases we can also state the number of isomorphism types of those codes. The 8-divisible  $[n, k]_2$  with length at most 48 are classified in [1] and the projective codes are extracted in [13]. If not mentioned otherwise, the remaining classification results are obtained with the software package LinCode [3]. We also list those non-existence results where more sophisticated methods are necessary. We mark those instances with the keyword "**None**" in the comment column of the subsequent tables and also give a reference to the used method. One of those, that is frequently used, is:

**Proposition 1.** ([11, Proposition 5], cf. [21]) Let C be an  $[n, k, d]_2$ -code with all weights divisible by  $\Delta := 2^a$  and let  $(A_i)_{i=0,1,\dots,n}$  be the weight distribution of C. Put

$$\alpha := \min\{k - a - 1, a + 1\},$$
  

$$\beta := \lfloor (k - a + 1)/2 \rfloor, and$$
  

$$\delta := \min\{2\Delta i \mid A_{2\Delta i} \neq 0 \land i > 0\}.$$

Then the integer

$$T := \sum_{i=0}^{\lfloor n/(2\Delta) \rfloor} A_{2\Delta i}$$

satisfies the following conditions.

- (i) T is divisible by  $2^{\lfloor (k-1)/(a+1) \rfloor}$ .
- (ii) If  $T < 2^{k-a}$ , then

$$T = 2^{k-a} - 2^{k-a-t}$$

for some integer t satisfying  $1 \le t \le \max\{\alpha, \beta\}$ . Moreover, if  $t > \beta$ , then C has an  $[n, k - a - 2, \delta]_2$ -subcode and if  $t \le \beta$ , it has an  $[n, k - a - t, \delta]_2$ -subcode.

(iii) If  $T > 2^k - 2^{k-a}$ , then

 $T = 2^k - 2^{k-a} + 2^{k-a-t}$ 

for some integer t satisfying  $0 \le t \le \max\{\alpha, \beta\}$ . Moreover, if a = 1, then C has an  $[n, k - t, \delta]_2$ -subcode. If a > 1, then C has an  $[n, k - 1, \delta]_2$ -subcode unless  $t = a + 1 \le k - a - 1$ , in which case it has an  $[n, k - 2, \delta]_2$ -subcode.

A special and well-known subcase is that the number of even weight codewords in a  $[n, k]_2$  code is either  $2^{k-1}$  or  $2^k$ , see Lemma 3. For n = 32, k = 10, and weight vector w = [8, 16, 24] we obtain  $A_{w_1} = 61$ ,  $A_{w_2} = 899$ , and  $A_{w_3} = 63$ . Applying Proposition 1 gives  $\Delta = 8$ , a = 3,  $\alpha = 4$ ,  $\beta = 4$ ,  $\delta = 16$ , and T = 900. As required by Part (1), Tis divisible by 4. However, Part (1) gives t, which contradicts  $0 \le t \le \max\{\alpha, \beta\}$ , so that a code cannot exist.

Bounds for the largest possible minimum distance are well studied in the literature, see e.g. the online tables at http://www.codetables.de [12]. For length

n = 64 and dimension k = 11 the largest possible minimum distance is known to be either 26 or 27, which rules out the existence of a projective code with weight vector w = [28, 32, 36]. We use the comment "Codetables" in this case. For n = 64and w = [24, 32, 40] we use a classification result from [14], i.e., every 13-dimensional 8-divisible binary linear code with non-zero weights in  $\{24, 32, 40, 56, 64\}$  has to contain a codeword of weight 64. Anticipating the results from Section 5 we also apply Corollary 1, which shows that the length n has to be divisible by 4. The case n = 58is excluded by that criterion. For length n = 64 and weight vector w = [16, 32, 48]we analyze the subcodes spanned by codewords of weight 16 and show that the dimension can be at most 11, see Proposition 2. Just four cases remain undecided. The occur for length  $n \in \{40, 48, 56, 64\}$  and mark them with the keyword "**Open**". For each feasible case we give one corresponding generator matrix as an example in Appendix A.

n = 4	4	
k = 3	$3  w = [1, 2, 3], \ e = [1, 3, 3]  1$	isomorphism type
n = 8		
k = 4	w = [2, 4, 6], e = [1, 11, 3]	1 isomorphism type
k = 5	w = [2, 4, 6], e = [5, 19, 7]	1 isomorphism type
k = 6	w = [2, 4, 6], e = [13, 35, 15]	1 isomorphism type
		]
n = 12		
k=5	w = [4, 6, 8], e = [6, 16, 9]	4 isomorphism types
k = 6	w = [4, 6, 8], e = [18, 24, 21]	2 isomorphism types
n = 16		
k = 5	w = [6, 8, 10], e = [6, 15, 10]	5 isomorphism types
k = 6	w = [6, 8, 10], e = [22, 15, 26]	1 isomorphism type
k = 7	w = [6, 8, 10], e = [54, 15, 58]	None Proposition $1$
k = 5	w = [4, 8, 12], e = [1, 27, 3]	1 isomorphism type
k = 6	w = [4, 8, 12], e = [5, 51, 7]	1 isomorphism type
k = 7	w = [4, 8, 12], e = [13, 99, 15]	2 isomorphism types
n = 20		
k = 5	w = [8, 10, 12], e = [5, 16, 10]	3 isomorphism types
k = 6	w = [8, 10, 12], e = [25, 8, 30]	None Proposition 1

n = 24		
k = 5	w = [10, 12, 14], e = [3, 19, 9]	1 isomorphism type
k = 6	w = [10, 12, 14], e = [27, 3, 33]	None Proposition 1
k = 6	w = [8, 12, 16], e = [6, 48, 9]	8 isomorphism types
k = 7	w = [8, 12, 16], e = [18, 88, 21]	52 isomorphism types
k = 8	w = [8, 12, 16], e = [42, 168, 45]	66 isomorphism types
k = 9	w = [8, 12, 16], e = [90, 328, 93]	13 isomorphism types
k = 10	w = [8, 12, 16], e = [186, 648, 189]	2 isomorphism types
k = 11	w = [8, 12, 16], e = [378, 1288, 381]	1 isomorphism type

n = 32		
k = 6	w = [12, 16, 20], e = [6, 47, 10]	
k = 7	w = [12, 16, 20], e = [22, 79, 26]	
k = 8	w = [12, 16, 20], e = [54, 143, 58]	
k = 9	w = [12, 16, 20], e = [118, 271, 122]	
k = 10	w = [12, 16, 20], e = [246, 527, 250]	
k = 6	w = [8, 16, 24], e = [1, 59, 3]	1 isomorphism type
k = 7	w = [8, 16, 24], e = [5, 115, 7]	1 isomorphism type
k = 8	w = [8, 16, 24], e = [13, 227, 15]	2 isomorphism types
k = 9	w = [8, 16, 24], e = [29, 451, 31]	1 isomorphism type
k = 10	w = [8, 16, 24], e = [61, 899, 63]	<b>None</b> Proposition 1

n = 40		
k = 6	w = [18, 20, 22], e = [25, 3, 35]	None Proposition 1
k = 6	w = [16, 20, 24], e = [5, 48, 10]	
k = 7	w = [16, 20, 24], e = [25, 72, 30]	
k = 8	w = [16, 20, 24], e = [65, 120, 70]	
k = 9	w = [16, 20, 24], e = [145, 216, 150]	
k = 10	w = [16, 20, 24], e = [305, 408, 310]	Open

n = 48		
k = 6	w = [22, 24, 26], e = [18, 15, 30]	1 isomorphism type
k = 6	w = [20, 24, 28], e = [3, 51, 9]	1 isomorphism type
k = 7	w = [20, 24, 28], e = [27, 67, 33]	$\geq 209586$ isomorphism types
k = 8	w = [20, 24, 28], e = [75, 99, 81]	$\geq 86$ isomorphism types
k = 9	w = [20, 24, 28], e = [171, 163, 177]	Open
k = 7	w = [16, 24, 32], e = [6, 112, 9]	8 isomorphism types
k = 8	w = [16, 24, 32], e = [18, 216, 21]	66 isomorphism types
k = 9	w = [16, 24, 32], e = [42, 424, 45]	$\geq 7$ isomorphism types
k = 10	w = [16, 24, 32], e = [90, 840, 93]	$\geq$ isomorphism types
k = 11	w = [16, 24, 32], e = [186, 1672, 189]	$\geq 2$ isomorphism types
k = 12	w = [16, 24, 32], e = [378, 3336, 381]	

n = 52		
k = 6	w = [24, 26, 28], e = [13, 24, 26]	1 isomorphism type

n = 56		
k = 6	w = [26, 28, 30], e = [7, 35, 21]	1 isomorphism type
k = 7	w = [24, 28, 32], e = [28, 64, 35]	
k = 8	w = [24, 28, 32], e = [84, 80, 91]	
k = 9	w = [24, 28, 32], e = [196, 112, 203]	
k = 10	w = [24, 28, 32], e = [420, 176, 427]	Open

n = 58		
k = 8	w = [24, 31, 32], e = [76, 128, 51]	None Corollary 1

n = 64		
k = 7	w = [28, 32, 36], e = [28, 63, 36]	
k = 8	w = [28, 32, 36], e = [92, 63, 100]	
k = 9	w = [28, 32, 36], e = [220, 63, 228]	
k = 10	w = [28, 32, 36], e = [476, 63, 484]	Open
k = 11	w = [28, 32, 36], e = [988, 63, 996]	None Codetables
k = 7	w = [24, 32, 40], e = [6, 111, 10]	
k = 8	w = [24, 32, 40], e = [22, 207, 26]	
k = 9	w = [24, 32, 40], e = [54, 399, 58]	
k = 10	w = [24, 32, 40], e = [118, 783, 122]	
k = 11	w = [24, 32, 40], e = [246, 1551, 250]	42 isomorphism types
k = 12	w = [24, 32, 40], e = [502, 3087, 506]	1 isomorphism type
k = 13	w = [24, 32, 40], e = [1014, 6159, 1018]	<b>None</b> [14]
k = 7	w = [16, 32, 48], e = [1, 123, 3]	
k = 8	w = [16, 32, 48], e = [5, 243, 7]	
k = 9	w = [16, 32, 48], e = [13, 483, 15]	
k = 10	w = [16, 32, 48], e = [29, 963, 31]	
k = 11	w = [16, 32, 48], e = [61, 1923, 63]	
k = 12	w = [16, 32, 48], e = [125, 3843, 127]	<b>None</b> Proposition 2
k = 13	w = [16, 32, 48], e = [253, 7683, 255]	<b>None</b> Proposition 2
k = 14	w = [16, 32, 48], e = [509, 15363, 511]	<b>None</b> Proposition 2
k = 15	w = [16, 32, 48], e = [1021, 30723, 1023]	<b>None</b> Proposition 2
<u>.</u>		

n = 68		
k = 9	w = [30, 32, 40], e = [64, 299, 148]	None Proposition 1

**Proposition 2.** If C is a projective  $[64, k]_2$  code with non-zero weights in  $\{16, 32, 48\}$ , then  $k \leq 11$ .

*Proof.* We consider the subcode  $C_{16}$  of C that is generated by the codewords of weight 16 in C. W.l.o.g. we can assume that the rows of a generator matrix of  $C_{16}$  all have weight 16. If a linear code C' can be written as the direct sum of two non-trivial smaller codes, then we call C' decomposable and indecomposable otherwise. Using the software package LinCode [3] we have enumerate all indecomposable  $[n, k]_2$  codes with non-zero weights in  $\{16, 32, 48\}$  and  $n \leq 64$ . The parameters n, k and the corresponding counts of the non-zero weights of the occurring cases are given by

 $[16, 1]_2$ :  $16^1$ ,  $[24, 2]_2$ :  $16^3$ ,  $[28, 3]_2$ :  $16^7$ ,  $[30, 4]_2$ :  $16^{15}$ ,  $[31, 5]_2$ :  $16^{31}$ ,  $[32, 6]_2$ :  $16^{62}32^1$ ,  $[32, 5]_2$ :  $16^{30}32^1$ ,  $[32, 4]_2$ :  $16^{14}32^1$ ,  $[32, 3]_2$ :  $16^{6}32^1$ ,  $[32, 2]_2$ :  $16^{2}32^1$ ,  $[40, 4]_2$ :  $16^{10}32^5$ , and  $[48, 5]_2$ :  $16^{15}32^{14}48^1$ . We remark that the parameters are that small, that these codes can also be classified *by hand*, but since such an analysis is rather boring and extensive, we refrain from giving the details.

Note that if C' is an  $[n', k']_2$  code with maximum weight w' and C'' is an  $[n'', k'']_2$ code with maximum weight w'', than the direct sum of C' and C'' is an  $[n' + n'', k' + k'']_2$ code with maximum weight w' + w''. Thus, not many combinations are possible. So, let us write  $C_{16}$  as a direct sum of subcodes  $C_1, \ldots, C_r$  from the above list. Due to the maximum weight of 48 we have  $r \leq 3$ .

First we show that C satisfies  $A_{16} \leq 93$ . If one  $C_i$  equals the  $[32, 6]_2$  code with weight distribution  $0^{1}16^{62}32^{1}$ , then we have  $r \leq 2$  (due to the maximum weight) and the possible other component can only consist of non-zero codewords of weight 16. Thus, we have  $A_{16} \leq 62 + 31 = 93$ . If the  $[32, 6]_2$  code with weight distribution  $0^{1}16^{62}32^{1}$  is not equal to one of the  $C_i$ , then we not that every other possibility for the  $C_i$  contains at most 31 codewords of weight 16 so that we can also conclude  $A_{16} \leq 93$ .

From the MacWilliams identities we conclude that  $A_{16} \ge 125$  for  $k \ge 12$ , see also the explicit cases listed above, which is a contradiction.

We remark that it is also possible to classify the unique projective  $[64, 11]_2$  code with non-zero weights in  $\{16, 32, 48\}$  extending the approach of the proof of Proposition 2.

Looking at the feasible cases listed above, we notice that all of them satisfy  $w_2 = n/2$ , which corresponds to  $\theta_2 = 0$ ,  $\theta_3 = -\theta_1$  for the eigenvalues of s-SWRGs, see Equation (1). While we conjecture that all integral solutions of Equation (1) satisfy this extra constraint for all  $s \ge 5$ , see Section 4, the condition  $\theta_1 + \theta_2 + \theta_3 = 0$ , i.e.,  $w_1 + w_2 + w_3 = 3n(q-1)/q$ , is sufficient for s = 3. So, it is an interesting open question, if 3-SWRGs obtained from the coset graph of the dual code of a projective three-weight code also have to satisfy this extra condition. To stimulate some research in this directions we propose:

**Conjecture 1.** Let C be a projective  $[n, k]_2$  3-weight code with weights satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_1 < w_2 < w_3$ . Then,  $w_2 = n$ .

We remark that the MacWilliams identities, using the non-negativity and integrality constraints, are not sufficient to prove Conjecture 1. For the examples  $(n, w_1, w_2, w_3) = (58, 24, 31, 32)$  and (68, 30, 32, 40) go in line with these conditions but are excluded with more sophisticated methods, see the details stated above. Given the results obtained so far we can state that Conjecture 1 is true for all n < 72. The next case, where all non-negativity and integrality constraints for the  $B_i$  are satisfied, is given by  $(n, w_1, w_2, w_3) = (100, 46, 48, 56)$ . Here we have k = 7,  $A_{w_1} = 32$ ,  $A_{w_2} = 145$ ,  $A_{w_3} = 78$ , and  $B_3 = 580$ . However, we can apply Proposition 1 to conclude the non-existence of a binary linear code with these parameters. More precisely, Proposition 1.1, applied with a = 1 and T = 224, yields a contradiction since  $T - 2^k + 2^{k-a} = 96$  is not a power of two. In the following we list all tuples  $(n, w_1, w_2, w_3, y = 2^{k-2}, A_1, A_2, A_3, B_3)$  up to n = 256, where all  $B_i$  are integral and non-negative and also Proposition 1 does not yield a contradiction, i.e., the parameters of possible counter examples to Conjecture 1:

- (112, 50, 54, 64, 128, 48, 336, 127, 322)
- (116, 54, 56, 64, 128, 256, 56, 199, 440)
- $\bullet (120, 54, 62, 64, 64, 72, 120, 63, 1180)$
- (124, 56, 64, 66, 64, 72, 119, 64, 1296)
- $\bullet \ (140, 64, 72, 74, 64, 71, 120, 64, 1840)$
- (202, 96, 103, 104, 64, 67, 128, 60, 5396)
- (212, 96, 110, 112, 256, 297, 640, 86, 1860)
- $\bullet \ (212, 96, 110, 112, 512, 649, 896, 502, 1090)$
- $\bullet \ (240, 110, 122, 128, 256, 288, 480, 255, 2450)$

# 3.2 Feasible parameters for projective ternary three-weight codes with $w_1 + w_2 + w_3 = 2n$

In the subsequent tables we list the feasible parameters for projective ternary three-weight codes with  $w_1+w_2+w_3 = 2n$ . For each length  $n \leq 39$  we list the possible dimensions k and weight vectors  $w = [w_1, w_2, w_3]$ . If a certain length or dimension is not listed, then they are excluded with the criteria mentioned at the beginning of Section 3. As extra information we also state the weight distribution in the form  $e = [A_{w_1}, A_{w_2}, A_{w_3}]$ . For some cases we can also state the number of isomorphism types of those codes. If not mentioned otherwise, the remaining classification results are obtained with the software package LinCode [3]. We also list those non-existence results where more sophisticated methods are necessary. We mark those instances with the keyword "None" in the comment column of the subsequent tables and also give a reference to the used method. For n = 27, k = 6, and weight weight vector w = [9, 18, 27] we have used an exhaustive enumeration using LinCode to exclude the existence of the corresponding code. It would be nice to also have a theoretical argument. For  $n \ge 36$  four cases remain undecided, which we mark with the keyword "**Open**". For each feasible case we give one corresponding generator matrix as an example in Appendix A.

n = 3		
k = 3	w = [1, 2, 3], e = [6, 12, 8]	1 isomorphism type

n = 6k = 3 w = [3, 4, 5], e = [8, 6, 12] 1 isomorphism type

n = 9		
k = 3	w = [5, 6, 7], e = [6, 8, 12]	1 isomorphism type
k = 4	w = [3, 6, 9], e = [6, 66, 8]	1 isomorphism type

n = 18		
k = 4	w = [9, 12, 15], e = [8, 60, 12]	4 isomorphism types
k = 5	w = [9, 12, 15], e = [44, 150, 48]	213 isomorphism types
k = 6	w = [9, 12, 15], e = [152, 420, 156]	52 isomorphism types

n = 27		
k = 4	w = [15, 18, 21], e = [6, 62, 12]	2 isomorphism types
k = 5	w = [15, 18, 21], e = [60, 116, 66]	$\geq 2695546$ isomorphism types
k = 6	w = [15, 18, 21], e = [222, 278, 228]	6 isomorphism types
k = 5	w = [9, 18, 27], e = [6, 228, 8]	1 isomorphism type
k = 6	w = [9, 18, 27], e = [24, 678, 26]	<b>None</b> exhaustive enumeration

n = 36		
k = 5	w = [21, 24, 27], e = [72, 90, 80]	
k = 6	w = [21, 24, 27], e = [288, 144, 296]	
k = 7	w = [21, 24, 27], e = [936, 306, 944]	Open

n = 39		
k = 5	w = [21, 27, 30], e = [42, 188, 12]	Open
k = 6	w = [21, 27, 30], e = [156, 494, 78]	Open
k = 7	w = [21, 27, 30], e = [498, 1412, 276]	Open

# 4 Plane curves given by the sum of all monomials of given degree

In this section, we present some results on rational (or integral) solutions of the equation

$$\sum_{h+i+j=s-2} \theta_1^h \theta_2^i \theta_3^j = 0, \qquad (12)$$

which for pairwise distinct  $\theta_1, \theta_2, \theta_3$  is equivalent to (1), compare (11). We restrict to the case that s is odd. (When s is even, then there are no nontrivial real solutions, so a *fortiori* no rational solutions.)

We denote by  $C_{s-2}$  the plane projective curve defined by (12), and we will rename the variables  $\theta_1, \theta_2, \theta_3$  in this section as x, y, z. As already mentioned,  $C_1$  is the line x + y + z = 0, and there are many rational points on this curve. In general, it is not hard to see that  $C_d$  is smooth over  $\mathbb{Q}$ , so the curve is in particular geometrically irreducible and has genus  $g(C_d) = (d-1)(d-2)/2$ .

For d = 3 (corresponding to s = 5),  $C_3$  is a curve of genus 1 with some rational points, so it is an elliptic curve. A standard procedure (implemented, for example, in Magma [2]) produces an isomorphic curve in Weierstrass form. It turns out that  $C_3$  is isomorphic to the curve with label 50*a*1 in the Cremona database (50.*a*3 in the LMFDB). In Cremona's tables or under the link above, one can check that this curve has exactly three rational points. This proves the following.

#### Proposition 3.

$$C_3(\mathbb{Q}) = \{ (1:-1:0), (-1:0:1), (0:1:-1) \}.$$

The curve  $C_5$  is a plane quintic of genus 6. Note that there is an action of the symmetric group  $S_3$  on three letters on every curve  $C_d$  by permuting the coordinates. We can restrict this action to an action of the subgroup  $A_3$  generated by a cyclic permutation. The quotient  $C'_5$  of  $C_5$  by this action of  $A_3$  is a curve of genus 2. We

can compute a singular plane model of  $C'_5$  by taking the image of  $C_5$  under the map

$$\mathbb{P}^2 \to \mathbb{P}^2 \,, \quad (x:y:z) \mapsto \left( xyz: (xy+yz+zx)(x+y+z): (x-y)(y-z)(z-y) \right) \,.$$

A procedure implemented in Magma [2] then produces the hyperelliptic equation

$$H_5: y^2 = -3x^6 + 8x^5 - 28x^4 - 30x^3 + 40x^2 + 16x - 15$$

for  $C'_5$ . A 2-descent as described in [22] (and implemented in Magma) shows that the Mordell-Weil rank of the Jacobian J of  $H_5$  is at most 1. Since one finds a point on J of infinite order (with Mumford representation  $(x^2 - x + 2, 7x + 7)$ ), the rank is indeed 1. Using the Magma implementation of Chabauty's method combined with the Mordell-Weil sieve (see [7]), one quickly finds that the only rational point on this hyperelliptic curve is (-1, 0). This point must be the image of the three obvious rational points on  $C_5$ . Since any other rational point would have to map to a different point on  $H_5$ , this proves the following.

#### Proposition 4.

$$C_5(\mathbb{Q}) = \{(1:-1:0), (-1:0:1), (0:1:-1)\}.$$

Considering larger odd d, we can say the following. The quotient  $C''_7$  of  $C_7$  by the full  $S_3$ -action is an elliptic curve, which is isomorphic to the curve with label 10368w1 in the Cremona database (10368.j1 in the LMFDB). Unfortunately, this curve has rank 2 and therefore has infinitely many rational points. So we cannot use this approach to determine the set of rational points on  $C_7$ .

The quotient  $C_9''$  of  $C_9$  by the  $S_3$ -action is a smooth plane quartic curve, isomorphic to the curve with equation

$$\begin{aligned} x^4 + 2x^3y + x^2y^2 - xy^3 - y^4 + 2x^3z - 4x^2yz - 3xy^2z \\ &+ 2y^3z + 4x^2z^2 - 3xyz^2 + 3y^2z^2 + 3xz^3 - 4yz^3 + z^4 = 0 \,. \end{aligned}$$

A point search finds the two rational points (-5:1:4) and (-1:1:0). The first is the image of the three obvious rational points on  $C_9$ , whereas the second point does not lift to a rational point on  $C_9$ . Let J be the Jacobian of the curve. Then  $\#J(\mathbb{F}_3) = 3^3$  and  $\#J(\mathbb{F}_7) = 11 \cdot 31$ , so  $J(\mathbb{Q})$  has trivial torsion subgroup. Therefore, the point in  $J(\mathbb{Q})$  given by the difference of the two rational points has infinite order. It might be possible to use the methods of [6] to determine the rank of  $J(\mathbb{Q})$ . If the rank turns out to be  $\leq 2$ , then an application of Chabauty's method might show that the two known rational points are the only ones.

In any case, searching for rational points does not exhibit any other points than the obvious ones when  $d \ge 3$  is odd. This leads to the following conjecture, which generalizes the results of Propositions 3 and 4.

**Conjecture 2.** If  $d \ge 3$  is odd, then

$$C_d(\mathbb{Q}) = \{(1:-1:0), (-1:0:1), (0:1:-1)\}.$$

Equivalently, all solutions  $(\theta_1, \theta_2, \theta_3)$  in integers of (1) with  $s \ge 5$  odd and  $\theta_1 > \theta_2 > \theta_3$  satisfy  $\theta_2 = 0$  and  $\theta_3 = -\theta_1$ .

## 5 Divisibility for binary linear codes with few weights

In this section we want to study the divisibility properties of the weights and the length of the binary linear codes with few weights. A first but very powerful tool are the MacWilliams identities. Since we do not want to assume that the codes are binary or projective, i.e.,  $B_2 \neq 0$  is possible, we replace Equations (3)-(6) by

$$\sum_{i>0} A_i = q^k - 1, (13)$$

$$\sum_{i>0} iA_i = q^{k-1}n, \tag{14}$$

$$\sum_{i\geq 0} i^2 A_i = q^{k-1} (B_2 + n(n+1)/2), \tag{15}$$

$$\sum_{i\geq 0} i^3 A_i = q^{k-2} (3(B_2 n - B_3) + n^2(n+3)/2),$$
(16)

for an  $[n, k]_q$  code with  $B_1 = 0$ . Given a codeword c of an  $[n, k]_q$  code C we denote by  $\operatorname{supp}(c)$  the support of c, i.e., the set of coordinates  $1 \leq i \leq n$  with non-zero entries  $c_i \neq 0$ .

We start with a few auxiliary results for codes with just one or two non-zero weights.

#### Lemma 1. (folklore)

If C is an  $[n,k]_q$  code, where all non-zero weights are equal to  $w_1$ , i.e., a 1-weight code, then there exists an integer  $u \ge 1$  such that  $n = u \cdot \frac{q^k - 1}{q - 1}$  and  $w_1 = u \cdot q^{k-1}$ . Moreover, C is a u-fold replication of the k-dimensional simplex code over  $\mathbb{F}_q$ . *Proof.* The first statement is a direct implication of the first two MacWilliams identities.  $\Box$ 

#### Lemma 2. ([10, Corollary 2])

Let C be a projective 2-weight code over  $\mathbb{F}_q$ , where  $q = p^e$  for some prime p. Then there exist suitable integers u and t with  $u \ge 1$ ,  $t \ge 0$  such that the weights are given by  $w_1 = up^t$  and  $w_2 = (u+1)p^t$ .

This structural result e.g. implies that not both weights of a binary projective 2-weight code can be odd, which is also true for non-projective 2-weight codes.

#### Lemma 3. (folklore)

Let C be an  $[n, k]_2$  code. By  $C_2$  we denote the subcode of C spanned be the codewords of even weight. The dimension of  $C_2$  is either k-1 or k and all codewords of  $C_2$  have an even weight.

We also call  $C_2$  the even-weight subcode of C.

**Lemma 4.** Let C be an  $[n, k]_2$  s-weight code, where  $s \ge 2$ . Then, at most s - 1 of the s non-zero weights of C can be odd.

*Proof.* It suffices to observe that the sum of two different codewords of odd weight is a non-zero codeword of even weight.  $\Box$ 

**Lemma 5.** Let C be a projective  $[n, k]_2$  3-weight code with weights  $w_1$ ,  $w_2$ , and  $w_3$ . If n is even,  $w_2$  is odd and  $w_1, w_3$  are even, then  $w_2 = n/2$  and the even-weight subcode  $C_2$  of C has effective length n and is a 2-fold replication of a projective  $\left[\frac{n}{2}, k-1\right]_2$  2-weight code with weights  $w_1/2$  and  $w_3/2$ .

*Proof.* We consider the even-weight subcode  $C_2$  of C. From Lemma 3 we conclude that  $C_2$  is an  $[n', k - 1]_2$  2-weight code with non-zero weights  $w_1$  and  $w_3$ . Since C is projective we have  $n' \in \{n - 1, n\}$ . Using the equations (13)-(14) gives

$$A_{w_1} + A_{w_3} = 2y - 1 \tag{17}$$

$$w_1 A_{w_1} + w_3 A_{w_3} = n' y, (18)$$

where  $y = 2^{k-2}$ . Note that  $A_{w_1}$  and  $A_{w_3}$  are also the counts for codewords of weights  $w_1$  and  $w_3$  in C, respectively. Thus, we can plug in the equations (7) and (9) for  $A_{w_1}$  and  $A_{w_3}$ , respectively. These give  $w_1A_{w_1}+w_3A_{w_3}=2y(n-w_2)$ , so that  $n'=2(n-w_2)$ .

If n' = n - 1, then  $n - 1 = 2w_2$ , which contradicts the assumption that n is even. So, we have n' = n and  $w_2 = n/2$ . Solving Equation (15) gives  $B_2 = n/2$  for  $C_2$ . Since C is projective,  $C_2$  has a maximum column multiplicity of 2. So, effective length n and  $B_2 = n/2$  implies that all columns of a generator matrix of  $C_2$  have multiplicity exactly 2.

**Corollary 1.** Let C be a projective  $[n, k]_2$  3-weight code with weights  $w_1, w_2$ , and  $w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . Then,  $n \equiv 0 \pmod{4}$ .

Proof. Since  $w_1 + w_2 + w_3$  is an integer, n has to be even, so that we assume  $n \equiv 2 \pmod{4}$ . Since then  $\frac{3n}{2} = w_1 + w_2 + w_3$  is odd we can apply Lemma 4 to deduce that exactly one weight is odd. Assuming w.l.o.g. that  $w_2$  is odd, we can apply Lemma 5 to deduce  $w_2 = n/2$ , which is odd. As an abbreviation we set  $w_1 = \frac{n}{2} - t$  and  $w_3 = \frac{n}{2} + t$  for some positive integer t. Since  $w_1$  and  $w_3$  are even t has to be odd. Moreover, Lemma 5 says that  $w_3/2$  and  $w_1/2$  are the weights of a projective binary 2-weight code. By Lemma 2 the weight difference  $\frac{w_3}{2} - \frac{w_1}{2} = t$  has to be a power of 2. Since t is odd, we conclude t = 1. With this Equation (18) reads

$$\frac{n(4yn+4-n^2)}{8} = ny$$

Solving for n gives the three possibilities n = 0, n = 2, and n = 4y - 2. Since each binary projective 3-weight code has a length of at least 3, we have n = 4y - 2. Plugging in into Equation (7) for  $A_{w_1}$  gives  $A_{w_1} = 0$  – a contradiction.

After Lemma 4 we have seen that a projective 3-weight code can have two odd weights. What happens if we add the extra constraint  $w_1 + w_2 + w_3 = \frac{3n}{2}$ ?

**Lemma 6.** Let C be a projective  $[n, k]_2$  3-weight code with weights satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . If n > 4, then all weights are even. If  $n \le 4$ , then C is isomorphic to the unique  $[n, 3]_2$  code 3-weight code with weight enumerator  $0^{1}1^{1}2^{3}3^{3}$  and a generator matrix of C is given by

$$\left(\begin{array}{rrrr} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{array}\right) \,.$$

*Proof.* By Lemma 4 at most two of the weights  $w_1$ ,  $w_2$ , and  $w_3$  are odd. If just one weight is odd, say  $w_2$ , then Lemma 5 gives  $w_2 = \frac{n}{2}$ , which contradicts Corollary 1. This leaves the case that exactly two weights, say  $w_1$  and  $w_3$ , are odd. Let  $A_1$ ,  $A_2$ , and  $A_3$  denote the number of codewords in C of weights  $w_1$ ,  $w_2$ , and  $w_3$ , respectively. Let  $C_2$  be the even-weight subcode of C. Since C is projective, the columns of a

generator matrix of  $C_2$  have multiplicity at most 2. Moreover,  $C_2$  is an  $[n', k - 1]_2$  code, where  $n' \in \{n - 1, n\}$ , and the only occurring non-zero weight is  $w_2$ , i.e.,  $C_2$  is a 1-weight code. Thus,  $w_2 = 2^{k-2}$  and  $A_2 = 2^{k-1} - 1$ . From Lemma 1 we conclude  $n' = u \cdot (2^{k-1} - 1)$  for some integer  $1 \le u \le 2$ . (The upper bound for u follows from the maximum column multiplicity.)

Let us consider the case u = 2 first. Here  $n' = 2^k - 2$  and the  $C_2$  is the 2-fold replication of the binary (k-1)-dimensional simplex codes, where all non-zero vectors in  $\mathbb{F}_2^{k-1}$  occur exactly once (twice in the replication). Now consider the generator matrix extended by one extra row, which is a generator matrix of C. Since C is projective every column occurs exactly once. Let  $e_k$  denote the k-th unit vector in  $\mathbb{F}_2^k$ , i.e., the vector with k - 1 zeroes and a single one on the last coordinate. Thus, the columns of a generator matrix of C would consist either of all non-zero vectors of  $\mathbb{F}_2^k$  or of all non-zero vectors of  $\mathbb{F}_2^k$  except  $e_k$ . In both cases C would be a 2-weight code (with weights  $2^{k-2}$ ,  $2^{k-1} - 1$  or  $2^{k-2}$ ,  $2^{k-1}$ , respectively).

Since the case u = 2 is excluded above, we have  $n' = 2^{k-1} - 1$  and  $C_2$  is binary (k-1)-dimensional simplex code, which is projective. Since  $w_1 + w_2 + w_3 = \frac{3n}{2}$  implies that n is even we have n' = n - 1, i.e.,  $n = 2^{k-1}$ . Since  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_2 = \frac{n}{2}$ , we can write  $w_1 = \frac{n}{2} - t$  and  $w_3 = \frac{n}{2} + t$  for some positive integer t. Using this and the abbreviation  $y = 2^{k-2}$  we can rewrite equations (7)-(9) to

$$A_{w_1} = \frac{y(y-t)}{2t^2}$$
(19)

$$A_{w_2} = \frac{(4y-1)t^2 - y^2}{t^2} \tag{20}$$

$$A_{w_3} = \frac{y(y+t)}{2t^2}.$$
 (21)

Now we use  $A_{w_2} = 2^{k-1} - 1 = 2y - 1$  to conclude  $y = 2t^2$  (or y = 0, which is impossible). This gives  $A_{w_1} = 2t^2 - t$ ,  $A_{w_2} = 4t^2 - 1$ ,  $A_{w_3} = 2t^2 + t$ ,  $B_3 = 4t^4 - t^2$ ,  $n = 4t^2$ ,  $w_1 = 2t^2 - t$ ,  $w_2 = 2t^2$ , and  $w_3 = 2t^2 + t$ . Since we have assumed  $w_1$  and  $w_3$ to be odd, only t = 1 is possible, which gives  $A_{w_1} = 1$ ,  $A_{w_2} = 3$ ,  $A_{w_3} = 3$ ,  $B_3 = 1$ , n = 4,  $w_1 = 1$ ,  $w_2 = 2$ ,  $w_3 = 3$ , y = 2, and k = 3. With respect of the classification of the corresponding codes up to isomorphism, we can choose a systematic generator matrix, i.e., the first three columns are the three unit vectors of  $\mathbb{F}_2^3$  and due to  $A_{w_1} = 1$ the fourth column has to consist of two 1s and a zero.

**Proposition 5.** Let C be a projective  $[n, k]_2$  3-weight code with weights satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_2 = \frac{n}{2}$ . For each positive integer r there exists an integer

N(r) such that  $n \ge N(r)$  implies that  $2^r$  divides n and that all three weights are divisible by  $2^{r-1}$ .

*Proof.* Let t be a positive integer with  $w_1 = \frac{n}{2} - t$  and  $w_3 = \frac{n}{2} + t$ . With this (and  $y = 2^{k-2}$ ) the equations (7)-(10) are equivalent to

$$A_{w_1} = \frac{n(4y - n - 2t)}{8t^2} \tag{22}$$

$$A_{w_2} = \frac{4t^2(4y-1) - n(4y-n)}{4t^2}$$
(23)

$$A_{w_3} = \frac{n(4y - n + 2t)}{8t^2} \tag{24}$$

and

$$3B_3 = \frac{n(n-2t)(n+2t)}{8y}, \tag{25}$$

where we set  $y = 2^{k-2}$ . Since  $A_{w_3} - A_{w_1} = \frac{n}{2t}$  the effective length n has to be divisible by 2t. From  $A_2 \in \mathbb{N}$  we conclude that  $t^2$  divides n(4y - n). So, if  $p^l$  divides t for some odd prime p, then  $p^{2l}$  has to divide n since y is a power of 2. Now let us try to parameterize  $t = 2^u \cdot v$  and  $n = 2^x \cdot v^2 \cdot z$  for odd positive integers v, z and non-negative integers u, x. Plugging in and simplifying gives

$$A_{w_1} = \frac{z \cdot (2^{k-u-1} - 2^{x-u-1}v^2 z - v)}{2^{u+2-x}}$$
(26)

$$A_{w_2} = 2^{2(x-u-1)}v^2z^2 + 2^k - 2^{x+k-2u-2}z - 1$$
(27)

$$A_{w_3} = \frac{z \cdot (2^{k-u-1} - 2^{x-u-1}v^2 z + v)}{2^{u+2-x}}$$
(28)

$$3B_3 = \frac{v^4 z \cdot (2^{x-u-1}vz - 1) \cdot (2^{x-u-1}vz + 1)}{2^{k-x-2u-1}},$$
(29)

where  $u \leq x - 1$  (t divides  $\frac{n}{2}$ ) and  $x \leq k - 1$  ( $n \leq 2^k - 1$  since C is projective).

If  $k - x - 2u - 1 \ge 1$  then  $B_3 \in \mathbb{N}$  and  $v, z \equiv 1 \pmod{2}$  imply u = x - 1. Since gcd(vz - 1, vz + 1) = 2, we have that  $2^{k-3u-3}$  either divides vz - 1 or vz + 1. So, we use the parameterization  $vz = s \cdot (2^{k-3u-3}) + \alpha$  for some positive integer s and  $\alpha \in \{-1, 1\}$ . With this  $A_{w_1} > 0$  gives

$$2^{k-u-1} - v\left(s \cdot \left(2^{k-3u-3}\right) + \alpha + 1\right) > 0,$$

so that  $vs < 2^{2u+2}$ , i.e.,  $sv \le 2^{2u+2} - 1$ . Now  $A_{w_2} > 0$  gives  $v^2 z^2 + 2^k > 2^{k-u-1} z$ , which is equivalent to

$$sv(vz)^{2} + 2^{k}sv > s2^{k-u-1}vz = s^{2}2^{2k-4u-4} + \alpha s2^{k-u-1} > s^{2}2^{2k-4u-4} - s2^{k+2u+2}.$$
 (30)

Since  $sv \leq 2^{2u+2} - 1$  the left hand side is at most

$$s^{2}2^{2k-4u-4} - s^{2}2^{2k-6u-6} + s\alpha 2^{k-u} - s\alpha 2^{k-3u-2} + \alpha^{2}2^{2u+2} - \alpha^{2} + 2^{k+2u+2} - 2^{k} \leq s^{2}2^{2k-4u-4} - s^{2}2^{2k-6u-6} + 2s2^{k-u} + 2^{2u+2} + 2^{k+2u+2} \leq s^{2}2^{2k-4u-4} - s^{2}2^{2k-6u-6} + 3s2^{k+2u+2}.$$

Thus

$$4s \cdot 2^{k+2u+2} > s^2 2^{2k-6u-6} \tag{31}$$

has to be satisfied, so that  $k \leq 8u + 9$  and

$$x \ge u \ge \frac{k-9}{8}.\tag{32}$$

Otherwise we have  $k \leq x + 2u + 1$ . From  $A_1 > 0$  we conclude 4y - n > 0. Since 4y - n is an integer and both 4y and n are divisible by  $2^x$  we have  $4y - n \geq 2^x$ . Now  $A_{w_2} > 0$  and Equation (23) imply

$$4v^2 2^{2u} \cdot 2^k - 2^x v^2 z \cdot 2^x > 0,$$

so that k + 2u + 2 > 2x, i.e.,

$$k \ge 2x - 2u + 1. \tag{33}$$

Combined with  $k \le x + 2u + 1$  we obtain  $x \le 4u$  and  $k \le 6u + 1$ , i.e.,

$$x \ge u \ge \frac{k-1}{6}.\tag{34}$$

In both cases we can conclude  $x \ge u \ge \frac{k-9}{8}$ , so that the result follows from  $n < 2^k$ .

Note that Lemma 6 and Corollary 1 show that we can take N(2) = 5. (Trivially, we have N(1) = 1.) N(2) = 5. The unique  $[48, 6]_2$  code with weight distribution  $0^1 22^{18} 24^{15} 26^{30}$  given by the generator matrix

shows  $N(3) \ge 49$ .

## References

- K. Betsumiya and A. Munemasa, On triply even binary codes, Journal of the London Mathematical Society 86 (2012), no. 1, 1–16.
- [2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, vol. 24, 1997, Computational algebra and number theory (London, 1993), pp. 235–265. MR 1484478
- [3] I. Bouyukliev, S. Bouyuklieva, and S. Kurz, *Computer classification of linear codes*, arXiv preprint 2002.07826 (2020).
- [4] A.E. Brouwer, A.M. Cohen, and A. Neumaier, *Distance-regular graphs*, Springer-Verlag, Berlin, 1989.
- [5] A.E. Brouwer and W.H. Haemers, Spectra of graphs, Springer Science & Business Media, 2012.
- [6] N. Bruin, B. Poonen, and M. Stoll, Generalized explicit descent and its application to curves of genus 3, Forum of Mathematics. Sigma 4 (2016), e6, 80. MR 3482281
- [7] N. Bruin and M. Stoll, The Mordell-Weil sieve: proving non-existence of rational points on curves, LMS Journal of Computation and Mathematics 13 (2010), 272– 306. MR 2685127
- [8] R. Calderbank and W.M. Kantor, The geometry of two-weight codes, Bulletin of the London Mathematical Society 18 (1986), no. 2, 97–122.
- B. Courteau and J. Wolfmann, On triple-sum-sets and two or three weights codes, Discrete Mathematics 50 (1984), 179–191.
- [10] Ph. Delsarte, Weights of linear codes and strongly regular normed spaces, Discrete Mathematics 3 (1972), no. 1-3, 47–64.
- [11] S. Dodunekov, S. Guritman, and J. Simonis, Some new results on the minimum length of binary linear codes of dimension nine, IEEE Transactions on Information Theory 45 (1999), no. 7, 2543–2546.
- [12] M. Grassl, Bounds on the minimum distance of linear codes and quantum codes, 2007, online available at http://www.codetables.de.

- [13] D. Heinlein, T. Honold, M. Kiermaier, S. Kurz, and A. Wassermann, *Projective divisible binary codes*, The Tenth International Workshop on Coding and Cryptography 2017 : WCC Proceedings, Saint-Petersburg, September 2017.
- [14] D.B. Jaffe and D. Ruberman, A sextic surface cannot have 66 nodes, Journal of Algebraic Geometry 6 (1997), no. 1, 151–168.
- [15] M. Kiermaier, S. Kurz, M. Shi, and P. Solé, *Three-weight codes over rings and strongly walk regular graphs*, arXiv preprint 1912.03892 (2019).
- [16] A. Kohnert, Constructing two-weight codes with prescribed groups of automorphisms, Discrete Applied Mathematics 155 (2007), no. 11, 1451–1457.
- [17] M. Krawtchouk, Sur une généralisation des polynomes d'Hermite, Comptes Rendus 189 (1929), no. 620-622, 5–3.
- [18] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes, Elsevier, 1977.
- [19] V. Pless, Power moment identities on weight distributions in error correcting codes, Information and Control 6 (1963), no. 2, 147–152.
- [20] M. Shi and P. Solé, Three-weight codes, triple sum sets, and strongly walk regular graphs, Designs, Codes and Cryptography 87 (2019), 2395–2404.
- [21] J. Simonis, Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed-Muller codes, IEEE Transactions on Information Theory 40 (1994), no. 1, 194–196.
- [22] M. Stoll, Implementing 2-descent for Jacobians of hyperelliptic curves, Acta Arithmetica 98 (2001), no. 3, 245–277. MR 1829626
- [23] E.R. van Dam and G.R. Omidi, Strongly walk-regular graphs, Journal of Combinatorial Theory, Series A 120 (2013), no. 4, 803–810.
- [24] H.N. Ward, *Divisible codes*, Archiv der Mathematik **36** (1981), no. 1, 485–494.

# A Generator matrix of projective three-weights codes satisfying $w_1+w_2+w_3=3(q-1)n/q$

In this appendix we list examples of generator matrices corresponding to the feasible cases listed in Section 3.

• $q = 2, n = 4, k = 3, w = [1, 2, 3]: \begin{pmatrix} 1000\\ 0101\\ 0011 \end{pmatrix}$
• $q = 2, n = 8, k = 4, w = [2, 4, 6]: \begin{pmatrix} 01111011\\0110100\\10101100\\10110010 \end{pmatrix}$
• $q = 2, n = 8, k = 5, w = [2, 4, 6]: \begin{pmatrix} 11101110\\01010000\\00111010\\10001000\\11000011 \end{pmatrix}$
• $q = 2, n = 8, k = 6, w = [2, 4, 6]: \begin{pmatrix} 00110110\\00010001\\01010011\\10010110\\011011$
• $q = 2, n = 12, k = 5, w = [4, 6, 8]: \begin{pmatrix} 100100111001\\010100111100\\001000111101\\000010110010\\000001101010 \end{pmatrix}$
• $q = 2, n = 12, k = 6, w = [4, 6, 8]: \begin{pmatrix} 100000000111\\01000011010\\00100011010\\0001001$
• $q = 2, n = 16, k = 5, w = [6, 8, 10]$ : $\begin{pmatrix} 101111000110000\\1111011001011001\\0111111$
• $q = 2, n = 16, k = 6, w = [6, 8, 10]$ : $\begin{pmatrix} 0000100110010011\\ 0010110001101000\\ 0000011011001001\\ 10010100011001\\ 00010011001$
• $q = 2, n = 16, k = 5, w = [4, 8, 12]$ : $\begin{pmatrix} 1100011101100100\\ 1100110001001011\\ 10101000110010\\ 110110000110100\\ 011111001100$
• $q = 2, n = 16, k = 6, w = [4, 8, 12]$ : $\begin{pmatrix} 110100101010101101\\ 1110001000011101\\ 1101001010101$
• $q = 2, n = 16, k = 7, w = [4, 8, 12]$ : $\begin{pmatrix} 1000000111011110\\ 01000001110000\\ 001000001110000\\ 0001000001101000\\ 0000100001101100\\ 0000010011011111\\ 0000001101101111\\ 00000011011111 \end{pmatrix}$







• q = 2, n = 56, k = 8, w = [24, 28, 32]:



• q = 2, n = 64, k = 9, w = [24, 32, 40]:

 q = 2, n = 64, k = 10, w = [24, 32, 40]: 

q = 2, n = 64, k = 12, w = [24, 32, 40]:•

q = 2, n = 64, k = 7, w = [16, 32, 48]:

- q = 2, n = 64, k = 8, w = [16, 32, 48]:
- q = 2, n = 64, k = 9, w = [16, 32, 48]:

q = 2, n = 64, k = 10, w = [16, 32, 48]:



• 
$$q = 3, n = 36, k = 6, w = [21, 24, 27]:$$
   
 $\begin{pmatrix} 1101020211\\211020021\\0211012002\\1021202100\\01002212110 \end{pmatrix}$ 

$$\left(\begin{smallmatrix} 101011111100001011001101001011101101\\ 110102021110100101100110100102210210\\ 211020002111110020010011010010121021\\ 021101200211012002001001101102012202\\ 102120210021202200100100110210101120\\ 010221211002020210010010011122010012 \end{smallmatrix}\right)$$