

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

Michael Kiermaier<sup>1</sup>  $\odot$  · Sascha Kurz<sup>1</sup> · Patrick Solé<sup>2</sup> · Michael Stoll<sup>1</sup> · Alfred Wassermann<sup>1</sup>

Received: 26 April 2022 / Revised: 9 September 2022 / Accepted: 10 September 2022 / Published online: 15 November 2022 © The Author(s) 2022

# Abstract

Strongly walk regular graphs (SWRGs or *s*-SWRGs) form a natural generalization of strongly regular graphs (SRGs) where paths of length 2 are replaced by paths of length *s*. They 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 of these codes in the binary and ternary case for medium size code lengths. For the binary case, the divisibility of the weights of these codes is investigated and several general results are shown. It is known that an *s*-SWRG has at most 4 distinct eigenvalues  $k > \theta_1 > \theta_2 > \theta_3$ , and that the triple ( $\theta_1, \theta_2, \theta_3$ ) satisfies a certain homogeneous polynomial equation of degree s - 2 (Van Dam, Omidi, 2013). This equation defines a plane algebraic curve; we use methods from algorithmic arithmetic geometry to show that for s = 5 and s = 7, there are only the obvious solutions, and we conjecture this to remain true for all (odd)  $s \ge 9$ .

Keywords Strongly walk-regular graphs · Triple sum sets · Three-weight codes

Mathematics Subject Classification Primary 05E30 · Secondary 11D41 · 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. [8]. As first observed in [14], there is a strong link to projective two-weight codes, see [11] 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

Communicated by Y. Zhou.

Michael Kiermaier michael.kiermaier@uni-bayreuth.de

<sup>&</sup>lt;sup>1</sup> Department of Mathematics, University of Bayreuth, Bayreuth, Germany

<sup>&</sup>lt;sup>2</sup> I2M, CNRS, Aix-Marseille Univ, Centrale Marseille, Marseille, France

(SWRG) were introduced in [32]. 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 [32, Theorem 3.4] it is shown that the adjacency matrix of a SWRG has at most four distinct eigenvalues and the following characterization of SWRGs is given.

**Lemma 1.1** (van Dam, Omidi [32, Proposition 4.1]) Let  $\Gamma$  be a k-regular graph with 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 Eq. (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 [27]. The eigenvalues of such graphs are integral and depend on the weights of the three-weight code, so that Eq. (1) turns into a number theory question. In [27], a construction of SWRGs from triple sum sets (TSS) is given.

Several research papers consider the feasible parameters of SRGs, see e.g. [6] for a large table together with references 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 vertices. The corresponding parameters cannot be attained by two-weight codes since these always give graphs where the number of vertices is a power of the field size. Still, the existence of projective two-weight codes is an important source for the construction of SRGs, see e.g. [21], where several new examples have been found. An online database of known two-weight codes can be found at [12]. Due to a result of Delsarte [14, Corollary 2] the possible weights of two-weight codes are quite restricted, see Lemma 2.2.

Given the relation between the weights of a projective three-weight code and the eigenvalues of the coset graph of its dual, corresponding solutions of Eq. (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 up to 39. Within that range only very few cases are left as open problems. This extends and corrects first enumeration results from [27]. Similar results for some special rings instead of finite fields are obtained in [26].

The remaining part of this paper is organized as follows. The necessary preliminaries are introduced in Sect. 2 followed by the enumeration results in Sect. 3. In Sect. 4 it is shown that for s = 5 and s = 7 the only rational solutions of Eq. (1) are given by the parametric solution  $\theta_2 = 0$ ,  $\theta_3 = -\theta_1$ . For s = 5, this reduces to the determination of the set of rational points on an elliptic curve and for s = 7, it leads to a curve of genus 2.

The computational results from Sect. 3 for the case q = 2 suggest that projective threeweight codes of length *n* whose weights satisfy  $w_1 + w_2 + w_3 = 3n/2$  possess a high divisibility of the weights and the length by powers of two. In Sect. 5 this is shown, see Lemma 5.11 and the following theorems for the details. In Appendix A we collect generator matrices for the mentioned feasible parameters from Sect. 3.

### 2 Preliminaries

In this article,  $q \ge 2$  will always be the power of some prime p.

A linear *q*-ary code *C* of length *n* and dimension *k* is called an  $[n, k]_q$  code. The number of positions which are not all-zero is called the *effective length* of *C*. If the length equals the effective length, *C* is called *full-length*. Two positions  $i, j \in \{1, ..., n\}$  of *C* are called *projectively equivalent* if there is a  $\lambda \in \mathbb{F}_q^*$  with  $c_i = \lambda c_j$  for all codewords  $c \in C$ . The code *C* is called *projective* if it is full-length and there are no projectively equivalent positions. For a general full-length code, the *position multiplicity type* is the sequence  $(m_i)$  where  $m_i$ denotes the number of projective equivalence classes of size *i*.

### 2.1 Restrictions on the weights

If there is only a single non-zero weight, C is called a *constant weight code*. The linear constant weight codes are completely classified.

**Lemma 2.1** (Bonisoli [2]) Let C be a full-length  $[n, k]_q$  code of constant weight w of dimension  $k \ge 1$ . Then  $q^{k-1} \mid w$ , and C is isomorphic to the u-fold repetition of the q-ary simplex code  $\operatorname{Sim}_q(k)$  of dimension k with  $u = w/q^{k-1}$ . In particular,  $n = u \cdot \frac{q^k-1}{q-1}$ .

If C has exactly two different non-zero weights, C is called a two-weight code.

**Lemma 2.2** (Delsarte [14, Corollary 2]) Let *C* be a projective two-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  $w_2 = (u+1)p^t$ .

If C has exactly three different non-zero weights, C is called a *three-weight code*. Furthermore, C is called  $\Delta$ -*divisible* for some integer  $\Delta \ge 1$  if all weights of C are divisible by  $\Delta$ .

**Lemma 2.3** Let C be a linear projective  $[n, k]_q$  three-weight code. Then  $n \leq \frac{q^k - 1}{q - 1} - 2$ .

**Proof** Let G be a generator matrix of C. Since C is projective, G neither has a zero column, nor a pair of projectively equivalent columns. So each of the  $\frac{q^k-1}{q-1}$  projective equivalence classes of non-zero vectors in  $\mathbb{F}_q^k$  appears at most once as a column of G, showing that  $n \leq \frac{q^k-1}{q-1}$ . In the case  $n = \frac{q^k-1}{q-1}$ , C is the simplex code  $\operatorname{Sim}_q(k)$  of dimension k over  $\mathbb{F}_q$ , which is a code of constant weight  $q^{k-1}$ . In the case  $n = \frac{q^k-1}{q-1} - 1$ , C is the simplex code  $\operatorname{Sim}_q(k)$  punctured in a single position, so C has only the two weights  $q^{k-1}$  and  $q^{k-1} - 1$ . This contradicts the assumption that C is a three-weight code.

### 2.2 Weight enumerators and the MacWilliams identity

The weight distribution of *C* is the sequence of numbers  $(A_i)$  where  $A_i$  denotes the number of codewords of weight *i*. It can also be denoted as  $(0^{A_0}1^{A_1}2^{A_2}...)$ , where entries with  $A_i = 0$  may be omitted. The weight distribution is often given in polynomial form as the (univariate) weight enumerator  $W_C(x) = \sum_i A_i x^i$  or the homogeneous weight enumerator  $W_C(x, y) = \sum_i A_i x^{n-i} y^i$ .

The weight distribution of the dual code  $C^{\perp}$  will be denoted by  $(B_i)$ . We always have  $A_0 = B_0 = 1$ . Furthermore,  $B_0 = 0$  if and only if C is full-length and  $B_0 = B_1 = 0$  if and only C is projective. For the number  $B_2$  of general full-length codes, the following statement can be checked.

<sup>&</sup>lt;sup>1</sup> In fact, in this case C is a MacDonald code.

**Lemma 2.4** Let C be a full-length q-ary linear code of length n and  $(m_i)$  the position multiplicity type of C. Then

$$\sum_{i} im_{i} = n \quad and$$
$$\sum_{i} (q-1) \binom{i}{2} m_{i} = B_{2}$$

The weight distributions of C and  $C^{\perp}$  are related via the *MacWilliams identities* [24]

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

or in homogeneous polynomial form as

$$W_{C^{\perp}}(x, y) = \frac{1}{\#C} \cdot W_C(x + (q - 1)y, x - y).$$

In fact, the  $B_i$  are uniquely determined by the  $A_i$ , as can be seen by the following variant of the MacWilliams identities. Based on the *i*-th *q*-ary Krawtchouk polynomial

$$K_{i}(x) = \sum_{\nu=0}^{i} (-1)^{\nu} {\binom{x}{\nu}} {\binom{n-x}{i-\nu}} (q-1)^{i-\nu},$$

we have

$$B_i = \frac{1}{\#C} \cdot \sum_{j=0}^n K_i(j) A_j$$

For a binary projective  $[n, k]_2$  code, the system of the four equations with  $i \in \{0, 1, 2, 3\}$  can be rewritten to

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

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

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

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

In this special form of the left hand side, they are also called the first four (*Pless*) power moments, see [25]. 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  $B_3$ :

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

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

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

D Springer

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

All  $A_j$  except  $A_0 = 1$  and  $A_{w_1}$ ,  $A_{w_2}$ ,  $A_{w_3}$  are equal to zero, so that the  $B_i$  with  $i \ge 4$  are uniquely determined using the remaining MacWilliams identities, i.e., those for  $\nu \ge 4$ . Note that (10) implies 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 Sect. 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.

For a linear  $[n_1, k_1]_q$  code  $C_1$  and a linear  $[n_2, k_2]_q$  code  $C_2$ , the *direct sum* of  $C_1$  and  $C_2$  is defined as

$$C_1 \oplus C_2 = \{(c_1, c_2) \mid c_1 \in C_1, c_2 \in C_2\}.$$

It is a linear  $[n_1 + n_2, k_1 + k_2]_q$  code. Its weight enumerator is given by

$$W_{C_1 \oplus C_2}(x) = W_{C_1}(x) \cdot W_{C_2}(x).$$

#### 2.3 The coset graph triple sum sets

A *coset* of a linear code *C* is any translate of *C* by a constant vector. A *coset leader* of a fixed coset is any 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 [7, Theorem 1.11.1]:

**Theorem 2.5** Let C be a projective  $[n, k]_q$  code with distinct weights  $w_0 = 0, w_1, \ldots, w_r$ . Then, the coset graph  $\Gamma_{C^{\perp}}$  of its dual code  $C^{\perp}$  is n(q-1)-regular and the eigenvalues are given by  $n(q-1) - qw_i$  for  $i \in \{0, \ldots, r\}$ .

*Triple sum sets* (TSS) have been introduced in [13] as generalization of partial difference sets. A set  $\Omega \subseteq \mathbb{F}_q^k$  is called a *triple sum set* if it is closed under scalar multiplication and there are constants  $\sigma_0$  and  $\sigma_1$  such that each non-zero  $h \in \mathbb{F}_q^k$  can be written as h = x + y + z with  $x, y, z \in \Omega$  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  $n = \frac{\#\Omega}{(q-1)}$  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 parity check matrix of the linear code  $C(\Omega)$ . In order to ease the notation, we abbreviate  $\Gamma_{C(\Omega)}$  as  $\Gamma(\Omega)$ . In [27, Theorem 2] it was shown that  $\Omega$  is a TSS if and only if  $\Gamma(\Omega)$  is a 3-SWRG. (Actually, [27, 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  $\Omega$ .)

**Lemma 2.6** Let  $s \ge 2$  be an integer. The following equation holds for all  $\theta_1$ ,  $\theta_2$ ,  $\theta_3$  over any commutative ring:

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

A coding-theoretic characterization of triple sum sets is given as follows, see [13, Theorem 2.1] or [27, Theorem 5].

**Theorem 2.7** If  $\Omega \subseteq \mathbb{F}_q^k$  so that  $C(\Omega)^{\perp}$  has length n and attains exactly three non-zero weights  $w_1$ ,  $w_2$ , and  $w_3$ , then  $\Omega$  is a TSS iff  $w_1 + w_2 + w_3 = \frac{3n(q-1)}{q}$ .

**Proof** Using Eq. (11) from Lemma 2.6 for s = 3, (1) becomes

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

Theorem 2.5 shows that the eigenvalues are pairwise different and we conclude that (1) is satisfied iff  $\theta_1 + \theta_2 + \theta_3 = 0$ . Plugging in the formula for the eigenvalues from Theorem 2.5 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  $w_1 + w_2 + w_3 = 3n(q-1)/q$ . We do so in Sect. 3. We would like to point out that there are (many) binary projective three-weight codes with  $w_1 + w_2 + w_3 \neq 3n(q-1)/q$ . As an example, consider the binary [6, 5]<sub>2</sub> parity check code. It is a projective three-weight-code with weight distribution is  $(0^12^{15}4^{15}6^1)$ . The sum of its weights is 12, but  $\frac{3}{2}n = 9$ .

#### 2.4 The geometric point of view to linear codes

For a vector space V, let  $\begin{bmatrix} V \\ k \end{bmatrix}_q$  be the set of all subspaces of dimension k. If V is of finite dimension v,  $\#\begin{bmatrix} V \\ k \end{bmatrix}_q$  equals the Gaussian binomial coefficient  $\begin{bmatrix} v \\ k \end{bmatrix}_q$ . Conveniently, we will identify a vector space V with the set  $\begin{bmatrix} V \\ 1 \end{bmatrix}_q$  of *points* contained in V.

A *multiset* on a base set *S* is a mapping  $M : S \to \mathbb{Z}_{\geq 0}$ , assigning a multiplicity to each element in *S*. For  $T \subseteq S$ , we set  $M(T) = \sum_{s \in T} M(s)$ . The *cardinality* of *M* is #M = M(S), which is the sum of the multiplicities of all elements. In enumerative form, a multiset may be written by statements of the form  $M = \{\{s_1, s_2, \ldots, s_n\}\}$ , with the obvious interpretation. If *N* is a multiset on a base set *T* and  $\phi$  is a predicate on *T*, we may also use multiset-builder notations like  $M = \{\{t \in N \mid \phi(t)\}\}$ .

We will make use of the geometric description of linear codes as in [16]. There is a bijective correspondence of (semi-)linear equivalence classes of linear full-length  $[n, k]_q$ -codes C and (semi-)linear equivalence classes of spanning multisets C of n points in PG(V)  $\cong$  PG(k - 1, q), where V is a  $\mathbb{F}_q$ -vector space of dimension k. For a concrete assignment, let G be a generator matrix of C and  $v_1, \ldots, v_n$  the columns of G and consider the multiset  $C = \{\{v_1\}, \ldots, \langle v_n\}\}$  of points in  $V = \mathbb{F}_q^k$ . In this way, a codeword c = xG is represented by the hyperplane  $H = x^{\perp}$  (in fact, H represents all the q - 1 codewords which are projectively equivalent to c). The weight of c has a natural geometric description, namely w(c) = n - C(H), where the hyperplane H is identified with the set of points contained in H. In other words, w(c) is the number of points in C, counted with multiplicity, which are not contained in H. The code C is projective if and only if C is a proper set.

The following codes have an easy geometric description:

- (i) The *q*-ary simplex code  $\text{Sim}_q(k)$  of dimension  $k \ge 1$  corresponds to the set of all points contained in a vector space of (algebraic) dimension *k*. It is a projective linear  $[(q^k 1)/(q 1), k]_q$  constant code weight code with weight enumerator  $W_{\text{Sim}_q(k)}(x) = 1 + (q^k 1)x^{q^{k-1}}$ .
- (ii) The *q*-ary first order Reed-Muller code  $\operatorname{RM}_q(k)$  of dimension  $k \ge 2$  corresponds to an affine subspace of dimension k 1, that is the set of points contained in  $A = V \setminus W$ , where *V* is an  $\mathbb{F}_q$ -vector space of dimension *k* and *W* is a subspace of codimension 1. It is a projective linear  $[q^{k-1}, k]_q$  two-weight code with weight enumerator  $W_{\operatorname{RM}_q(k)}(x) = 1 + (q^k q)x^{(q-1)q^{k-2}} + (q 1)x^{q^{k-1}}$ . In the geometric description, the space *W* is known as the *hyperplane at infinity* of *A*. It corresponds to the q 1 codewords of weight  $q^{k-1}$ .

For a fixed point P in V, we consider the standard projection  $\pi_P : V \to V/P, x \mapsto x+P$ . It is extended to the multiset C of points as

$$\pi_P(\mathcal{C}) = \{\!\!\{\pi_P(Q) \mid Q \in \mathcal{C} \text{ with } Q \neq P\}\!\!\}.$$

We have  $\#\pi_P(\mathcal{C}) = \#\mathcal{C} - \mathcal{C}(P)$ .

The projections  $\pi_P(\mathcal{C})$  with  $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}_q$  correspond to the subcodes C' of C of codimension one. A codeword  $c \in C$  with corresponding hyperplane H < V is contained in C' if and only if  $P \in H$ .

Let *C* be a projective  $[n, k]_q$ -code with weight enumerator  $W_C(x) = \sum_i A_i x^i$  and *C* a corresponding point set. If the complement  $C^{\complement} = \begin{bmatrix} \mathbb{F}_q^k \\ 1 \end{bmatrix}_q \setminus C$  is spanning (or equivalently,  $A_{q^{k-1}} = 0$ ), we call its corresponding  $\begin{bmatrix} \frac{q^k-1}{q-1} - n, k \end{bmatrix}_q$ -code  $C^{\complement}$  the *anticode* of *C*. In this way, the anticode of *C* is defined up to isomorphism. Its weight enumerator is  $W_{C^{\complement}}(x) = 1 + \sum_{i>0} A_{q^{k-1}-i} x^i$ .

# 3 Feasible parameters of projective three-weight codes satisfying $w_1 + w_2 + w_3 = 3n(q - 1)/q$

As outlined in Sect. 2 we can construct 3-SWRGs from projective  $[n, k]_q$  three-weight codes if the weights satisfy  $w_1 + w_2 + w_3 = 3n(q-1)/q$ . So, here we study the feasible sets of parameters  $n, k, w_1, w_2, w_3$  such that a corresponding projective three-weight code exists. In Sect. 3.1 we consider the admissible parameters for all lengths n < 72 in the binary case and in Sect. 3.2 we consider the admissible parameters for all lengths  $n \le 39$  in the ternary case.

In that range we can simply loop over all weight-triples  $(w_1, w_2, w_3)$  with  $1 \le w_1 < w_2 < w_3 \le n$  satisfying  $w_1 + w_2 + w_3 = 3n(q-1)/q$ . For q = 2, (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 values of all  $A_i$ s and  $B_i$ s. As a first check we test if all of these values are non-negative integers. As a consequence of [33, Theorem 1], any full-length  $\Delta$ -divisible  $[n, k]_q$  code is the  $\Delta/\gcd(\Delta, q^{k-1})$ -fold repetition of some code. As projectivity forbids proper repetitions, we can restrict ourselves to the cases where  $\gcd(\Delta, q^{k-1}) = \gcd(w_1, w_2, w_3, q)$  is a power of p. Examples where we can apply this criterion to exclude the existence of codes are  $q = 2, n = 36, (w_1, w_2, w_3) = (12, 18, 24)$ , and  $k \in \{6, 7, 8\}$ . The corresponding values of  $(A_{w_1}, A_{w_2}, A_{w_3})$  are (2, 56, 5), (10, 104, 13), and (26, 200, 29). For q = 3, this criterion

can be applied to the parameters n = 24, k = 4 and weight triple w = (14, 16, 18) as well as n = 36,  $k \in \{5, 6\}$  and weight triple w = (18, 24, 30). In order to find examples, we have used the software package LinCode [4] 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.

Summarizing the above, we call parameters  $(q, n, k, w_1, w_2, w_3)$  admissible if

(i)  $1 \le w_1 < w_2 < w_3 \le n$  and  $w_1 + w_2 + w_3 = 3n(q-1)/q$  and

- (ii)  $gcd(w_1, w_2, w_3, q)$  is a power of p and
- (iii)  $w_1w_2w_3$  is divisible by  $2^{k-2}$  (if q = 2) or  $1 \le k \le n$  (if q = 3) and
- (iv) all  $A_i$  and  $B_i$  with  $i \in \{0, ..., n\}$  are non-negative integers and
- (v)  $B_1 = B_2 = 0.$

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

In Table 1 we list the admissible parameters for projective binary three-weight codes with  $w_1 + w_2 + w_3 = 3n/2$ . For each length  $4 \le n < 72$  we list the admissible dimensions k, weight triples  $w = (w_1, w_2, w_3)$ , and the weight distribution in the form  $(A_{w_1}, A_{w_2}, A_{w_3})$ . The last column contains known results about the existence of codes with these parameters. For some cases we can state the number of isomorphism types of those codes. The 8-divisible  $[n, k]_2$  codes with length at most 48 are classified in [1] and the projective codes are extracted in [18]. If not mentioned otherwise, the remaining complete classification results are obtained with the software package LinCode [4]. For the parameters marked with  $\ge 1$  we constructed at least one code by prescribing an automorphism group, see [5].

We mark the non-existence results with the keyword "**None**" in the comment column of Table 1 and give a reference to the used method. One frequently showing up is the following.

**Lemma 3.1** ([15, Proposition 5], cf. [28]) 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

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

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

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

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

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

Deringer

n	k	$(w_1, w_2, w_3)$	$(A_{w_1}, A_{w_2}, A_{w_3})$	isom. types
4	3	(1, 2, 3)	(1, 3, 3)	1
8	4	(2, 4, 6)	(1, 11, 3)	1
8	5	(2, 4, 6)	(5, 19, 7)	1
8	6	(2, 4, 6)	(13, 35, 15)	1
12	5	(4, 6, 8)	(6, 16, 9)	4
12	6	(4, 6, 8)	(18, 24, 21)	2
16	5	(6, 8, 10)	(6, 15, 10)	5
16	6	(6, 8, 10)	(22, 15, 26)	1
16	7	(6, 8, 10)	(54, 15, 58)	None Lem. 3.1
16	5	(4, 8, 12)	(1, 27, 3)	1
16	6	(4, 8, 12)	(5, 51, 7)	1
16	7	(4, 8, 12)	(13, 99, 15)	2
20	5	(8, 10, 12)	(5, 16, 10)	3
20	6	(8, 10, 12)	(25, 8, 30)	None Lem. 3.1
24	5	(10, 12, 14)	(3, 19, 9)	1
24	6	(10, 12, 14)	(27, 3, 33)	None Lem. 3.1
24	6	(8, 12, 16)	(6, 48, 9)	8
24	7	(8, 12, 16)	(18, 88, 21)	52
24	8	(8, 12, 16)	(42, 168, 45)	66
24	9	(8, 12, 16)	(90, 328, 93)	13
24	10	(8, 12, 16)	(186, 648, 189)	2
24	11	(8, 12, 16)	(378, 1288, 381)	1
32	6	(12, 16, 20)	(6, 47, 10)	$\geq 1$
32	7	(12, 16, 20)	(22, 79, 26)	$\geq 1$
32	8	(12, 16, 20)	(54, 143, 58)	$\geq 1$
32	9	(12, 16, 20)	(118, 271, 122)	$\geq 1$
32	10	(12, 16, 20)	(246, 527, 250)	$\geq 1$
32	6	(8, 16, 24)	(1, 59, 3)	1
32	7	(8, 16, 24)	(5, 115, 7)	1
32	8	(8, 16, 24)	(13, 227, 15)	2
32	9	(8, 16, 24)	(29, 451, 31)	1
32	10	(8, 16, 24)	(61, 899, 63)	None Lem. 3.1
40	6	(18, 20, 22)	(25, 3, 35)	None Lem. 3.1
40	6	(16, 20, 24)	(5, 48, 10)	$\geq 1$
40	7	(16, 20, 24)	(25, 72, 30)	$\geq 1$
40	8	(16, 20, 24)	(65, 120, 70)	$\geq 1$
40	9	(16, 20, 24)	(145, 216, 150)	$\geq 1$
40	10	(16, 20, 24)	(305, 408, 310)	Open
48	6	(22, 24, 26)	(18, 15, 30)	1
48	6	(20, 24, 28)	(3, 51, 9)	1
48	7	(20, 24, 28)	(27, 67, 33)	$\geq 209586$
48	8	(20, 24, 28)	(75, 99, 81)	$\geq 86$

Table 1 Admissible and realizable parameters of binary projective three-weight codes

Table 1 continued

n	k	$(w_1, w_2, w_3)$	$(A_{w_1}, A_{w_2}, A_{w_3})$	isom. types	
48	9	(20, 24, 28)	(171, 163, 177)	Open	
48	7	(16, 24, 32)	(6, 112, 9)	8	
48	8	(16, 24, 32)	(18, 216, 21)	66	
48	9	(16, 24, 32)	(42, 424, 45)	$\geq 7$	
48	10	(16, 24, 32)	(90, 840, 93)	$\geq 2$	
48	11	(16, 24, 32)	(186, 1672, 189)	$\geq 2$	
48	12	(16, 24, 32)	(378, 3336, 381)	$\geq 1$	
52	6	(24, 26, 28)	(13, 24, 26)	1	
56	6	(26, 28, 30)	(7, 35, 21)	1	
56	7	(24, 28, 32)	(28, 64, 35)	$\geq 1$	
56	8	(24, 28, 32)	(84, 80, 91)	$\geq 1$	
56	9	(24, 28, 32)	(196, 112, 203)	$\geq 1$	
56	10	(24, 28, 32)	(420, 176, 427)	Open	
58	8	(24, 31, 32)	(76, 128, 51)	None Cor. 5.7	
64	7	(28, 32, 36)	(28, 63, 36)	$\geq 1$	
64	8	(28, 32, 36)	(92, 63, 100)	$\geq 1$	
64	9	(28, 32, 36)	(220, 63, 228)	$\geq 1$	
64	10	(28, 32, 36)	(476, 63, 484)	Open	
64	11	(28, 32, 36)	(988, 63, 996)	None codetables	
64	7	(24, 32, 40)	(6, 111, 10)	$\geq 1$	
64	8	(24, 32, 40)	(22, 207, 26)	$\geq 1$	
64	9	(24, 32, 40)	(54, 399, 58)	$\geq 1$	
64	10	(24, 32, 40)	(118, 783, 122)	$\geq 1$	
64	11	(24, 32, 40)	(246, 1551, 250)	42	
64	12	(24, 32, 40)	(502, 3087, 506)	1	
64	13	(24, 32, 40)	(1014, 6159, 1018)	None [19]	
64	7	(16, 32, 48)	(1, 123, 3)	$\geq 1$	
64	8	(16, 32, 48)	(5, 243, 7)	$\geq 1$	
64	9	(16, 32, 48)	(13, 483, 15)	$\geq 1$	
64	10	(16, 32, 48)	(29, 963, 31)	$\geq 1$	
64	11	(16, 32, 48)	(61, 1923, 63)	1 [22]	
64	12	(16, 32, 48)	(125, 3843, 127)	None Theorem 3.2	
64	13	(16, 32, 48)	(253, 7683, 255)	None Theorem 3.2	
64	14	(16, 32, 48)	(509, 15363, 511)	None Theorem 3.2	
64	15	(16, 32, 48)	(1021, 30723, 1023)	None Theorem 3.2	
68	9	(30, 32, 40)	(64, 299, 148)	None Theorem 3.2	

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 of Lemma 3.1 is that the number of even weight codewords in a  $[n, k]_2$  code is either  $2^{k-1}$  or  $2^k$ , see Lemma 5.1. As an example, for n = 32, k = 10, and weight triple w = (8, 16, 24) we obtain  $(A_{w_1}, A_{w_2}, A_{w_3}) = (61, 899, 63)$ . Applying Lemma 3.1 gives  $\Delta = 8$ , a = 3,  $\alpha = 4$ ,  $\beta = 4$ ,  $\delta = 16$ , and T = 900. As required by Part (i), T is divisible by 4. However, Part (iii) gives t = 5, which contradicts  $0 \le t \le \max{\alpha, \beta}$ , so that a code cannot exist.

Bounds for the largest possible minimum distance for given length and dimension are well studied in the literature, see e.g. the online tables [17]. 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 triple w = (28, 32, 36). We use the comment "codetables" in this case. For n = 64 and w = (24, 32, 40) we use a classification result from [19], 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 Sect. 5 we also apply Corollary 5.7, which shows that the length n has to be divisible by 4. The case n = 58 is excluded by that criterion. For length n = 64 and weight triple w = (16, 32, 48), the dimension can be at most 11 by Theorem 3.2. Just four cases remain undecided. They occur for length  $n \in \{40, 48, 56, 64\}$  and are marked by "**Open**". For each feasible case we give a suitable generator matrix as an example in Appendix A.

Based on [23, Thm. 4] (for the projective case an alternative proof is found in [20, Sec. 4]), we derive the following classification result on three-weight codes.

**Theorem 3.2** Let  $\Delta = 2^a$  with  $a \ge 3$  an integer and let *C* be a full-length  $[n, k]_2$  three-weight code with the non-zero weights  $\Delta$ ,  $2\Delta$  and  $3\Delta$  and length  $3\Delta \le n \le 4\Delta$ . Then  $k \le 2a + 3$ . In the case of equality, we have that  $n \in \{4\Delta - 1, 4\Delta\}$ , *C* is projective and falls into one of the following two cases.

(i) For  $n = 4\Delta - 1$ , C is isomorphic to the direct sum of the binary simplex code of dimension a + 1 and the binary first order Reed-Muller code of dimension a + 2. The weight enumerator of C is

$$W_C(x) = 1 + (6\Delta - 3)x^{\Delta} + (8\Delta^2 - 8\Delta + 3)x^{2\Delta} + (2\Delta - 1)x^{3\Delta}.$$

(ii) For  $n = 4\Delta$ , C is isomorphic to the code with the generator matrix

$$\begin{pmatrix} \begin{matrix} R_{a+2} \\ 1 & \cdots & 1 \\ \hline \\ R_{a+2} \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{F}_2^{(2a+3)\times 4\Delta},$$

where

$$\begin{pmatrix} R_{a+2} \\ 1 & \cdots & 1 \end{pmatrix} \in \mathbb{F}_2^{(a+2) \times 2\Delta}$$

denotes a generator matrix of the binary first order Reed-Muller code of dimension a + 2, such that the all-one word is the last row of the generator matrix. The weight enumerator of *C* is

$$W_C(x) = 1 + (4\Delta - 3)x^{\Delta} + (8\Delta^2 - 8\Delta + 3)x^{2\Delta} + (4\Delta - 1)x^{3\Delta}.$$

**Proof** After appending zero positions, we may consider *C* as a code of length  $4\Delta$ . Let **1** be the all-one word of length  $4\Delta$ . The code  $\overline{C} = C + \langle \mathbf{1} \rangle$  is a  $\Delta$ -divisible binary linear code of effective length  $4\Delta$  containing the all-one word **1**. By [23, Thm. 4], dim $(\overline{C}) \leq 2a + 4$ , and in the case of equality we may assume  $\overline{C} = \text{RM}_2(a+2) \oplus \text{RM}_2(a+2)$ , up to isomorphism. So  $k = \dim(C) \leq 2a + 3$ , and in the case of equality, *C* is a codimension 1 subcode of  $\overline{C}$  not containing **1**.

We switch to the geometric description of linear codes. The corresponding point set of  $\overline{C} = \operatorname{RM}_2(a+2) \oplus \operatorname{RM}_2(a+2)$  has the form  $\overline{C} = A_1 \cup A_2$  with  $A_1 = V_1 \setminus W_1$  and  $A_2 = V_2 \setminus W_2$ , where  $V_1$  and  $V_2$  are vector spaces over  $\mathbb{F}_2$  of dimension a+2 having trivial intersection, and  $W_1 < V_1$ ,  $W_2 < V_2$  are codimension 1 subspaces.<sup>2</sup> The ambient vector space is  $V = V_1 \oplus V_2$ . The codeword  $\mathbf{1} \in \overline{C}$  corresponds to a hyperplane  $H_0$  of V not containing any point of  $\overline{C}$ . By the dimension formula, dim $(H_0 \cap V_1) \ge a+1$ , which forces  $H_0 \cap V_1 = W_1$ . In the same way,  $H_0 \cap V_2 = W_2$  and therefore,  $W_1 + W_2 < H_0$ . Since  $W_1 + W_2$  has codimension 2 in V, there are only  $\begin{bmatrix} 2\\1\\2 \end{bmatrix}_2 = 3$  hyperplanes of  $\overline{C}$ , so  $H_0$  is the third one.

As *C* is a subcode of  $\overline{C}$  of codimension 1, a corresponding point set *C* of *C* is given by the multiset image  $\pi_P(\overline{C})$  of the projection  $\pi_P : V \to V/P, x \mapsto x + P$  with respect to a suitable point  $P \in \begin{bmatrix} V \\ 1 \end{bmatrix}_q$ . Since  $\mathbf{1} \notin C$ , we have that  $P \notin H_0$ , so *P* must be contained in one of the other two hyperplanes containing  $W_1 + W_2$ . Without restriction, we may assume  $P \in V_1 + W_2$ . Together with  $P \notin H_0$ , this implies  $P \in (V_1 + W_2) \setminus (W_1 + W_2)$ .

Case 1:  $P \in \overline{C}$ , so  $P \in V_1 \setminus W_1$ . We get that  $\pi_P(A_1)$  is the set of all points in a subspace of algebraic dimension a + 1,  $\pi_P(A_2)$  is again an affine subspace of dimension a + 2, and  $\langle \pi_P(A_1) \rangle \cap \langle \pi_P(A_2) \rangle = \{0\}$ . Therefore,  $C \cong \text{Sim}_2(a + 1) \oplus \text{RM}_2(a + 2)$ . The weight enumerator is computed as  $W_C(x) = W_{\text{Sim}_2(a+1)}(x) \cdot W_{\text{RM}_2(a+2)}(x)$ .

Case 2:  $P \notin \overline{C}$ , so  $P \in (V_1 + W_2) \setminus ((W_1 + W_2) \cup V_1)$ . A moment's reflection shows that all these choices for *P* lead to equivalent point sets  $\overline{C}$ . As *P* is not collinear with two different points of  $\overline{C}$ , the projection *C* with respect to *P* is a proper set and therefore, *C* is projective. So *C* is the disjoint union of the two affine subspaces  $\pi_P(A_1)$  and  $\pi_P(A_2)$  of dimension a + 1.

The dimension formula leads to  $\dim(\pi_P(V_1) \cap \pi_P(V_2)) = 1$ . There are unique points  $Q_1 \in V_1 \setminus W_1$  and  $Q_2 \in W_2$  such that P is the third point on the line  $L = Q_1 + Q_2$ . The affine space  $\pi_P(A_2)$  has the hyperplane at infinity  $(W_2 + P)/P$ , which contains the single point  $(Q_1 + P)/P = (Q_2 + P)/P = L/P$  of the affine space  $\pi_P(A_1)$ . So the point  $\pi_P(V_1) \cap \pi_P(V_2) = L/P$  is contained in  $\pi_P(A_1)$  and in the hyperplane at infinity of  $\pi_P(A_2)$ . This leads to the generator matrix stated in the theorem.

By construction, the code corresponding to the point set C is a projective  $[2^{a+1}, 2a+3]_2$ code with (at most) the weights  $\Delta$ ,  $2\Delta$  and  $3\Delta$ . Equations (7), (8) and (9) evaluate to the
stated weight enumerator of C.

Looking at the feasible cases in Table 1, 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 Eq. (1). While we conjecture that all integral solutions of Eq. (1) satisfy this extra constraint for all  $s \ge 5$ , see Sect. 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 research into this direction we propose:

<sup>&</sup>lt;sup>2</sup> Remember that  $V_1 \setminus W_1$  is a lazy way for writing  $\begin{bmatrix} V_1 \\ 1 \end{bmatrix}_q \setminus \begin{bmatrix} W_1 \\ 1 \end{bmatrix}_q$ .

<b>Table 2</b> Parameters of potentialcounterexamples to	n	$w_1$	$w_2$	$w_3$	$y = 2^{k-2}$	$A_1$	$A_2$	$A_3$	<i>B</i> <sub>3</sub>
Conjecture 3.3	112	50	54	64	128	48	336	127	322
	116	54	56	64	128	256	56	199	440
	120	54	62	64	64	72	120	63	1180
	124	56	64	66	64	72	119	64	1296
	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
	212	96	110	112	512	649	896	502	1090
	240	110	122	128	256	288	480	255	2450

**Conjecture 3.3** Let C be a projective  $[n, k]_2$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . Then  $w_2 = \frac{n}{2}$ .

We remark that the MacWilliams identities, using the non-negativity and integrality constraints, are not sufficient to prove Conjecture 3.3. As an example, the values  $(n, w_1, w_2, w_3) \in \{(58, 24, 31, 32), (68, 30, 32, 40)\}$  go in line with these conditions for q = 2 but are excluded with more sophisticated methods, see the details stated above. Given the results obtained so far we can state that Conjecture 3.3 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 Lemma 3.1 to conclude the non-existence of a binary linear code with these parameters. More precisely, Lemma 3.1.(iii), 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 Table 2 we list all parameters  $(n, w_1, w_2, w_3, y = 2^{k-2}, A_1, A_2, A_3, B_3)$  up to n = 256, where all  $B_i$  are integral and non-negative and also Lemma 3.1 does not yield a contradiction, i.e., the parameters of potential counterexamples to Conjecture 3.3.

# 3.2 Feasible parameters for projective ternary three-weight codes with w<sub>1</sub> + w<sub>2</sub> + w<sub>3</sub> = 2n

In Table 3 we list the admissible parameters for projective ternary three-weight codes with  $w_1 + w_2 + w_3 = 2n$ . For each length  $3 \le n \le 39$  we list the admissible dimensions k and weight triples  $(w_1, w_2, w_3)$ , and the weight distribution in the form  $(A_{w_1}, A_{w_2}, A_{w_3})$ . The last column contains known results about the existence of codes with these parameters. For some cases we can also state the number of isomorphism types of those codes. If not mentioned otherwise, the classification results are obtained with the software package LinCode [4]. For the parameters marked with  $\ge 1$  we constructed at least one code by prescribing an automorphism group, see [5].

We also list those non-existence results where more sophisticated methods are necessary. We mark the non-existence results with the keyword "**None**" in the comment column of Table 3 and give a reference to the used method.

For n = 27, k = 6, and weight triple (9, 18, 27) we have used exhaustive enumeration using LinCode to exclude the existence of the corresponding code. It would be nice to also have a theoretical argument. For  $36 \le n \le 39$  four cases remain undecided, which we

n	k	$(w_1,w_2,w_3)$	$\left(A_{w_1},A_{w_2},A_{w_3}\right)$	isomorphism types
3	3	(1, 2, 3)	(6, 12, 8)	1
6	3	(3, 4, 5)	(8, 6, 12)	1
9	3	(5, 6, 7)	(6, 8, 12)	1
9	4	(3, 6, 9)	(6, 66, 8)	1
18	4	(9, 12, 15)	(8, 60, 12)	4
18	5	(9, 12, 15)	(44, 150, 48)	213
18	6	(9, 12, 15)	(152, 420, 156)	52
27	4	(15, 18, 21)	(6, 62, 12)	2
27	5	(15, 18, 21)	(60, 116, 66)	$\geq 2695546$
27	6	(15, 18, 21)	(222, 278, 228)	6
27	5	(9, 18, 27)	(6, 228, 8)	1
27	6	(9, 18, 27)	(24, 678, 26)	None exhaustive enumeration
36	5	(21, 24, 27)	(72, 90, 80)	$\geq 1$
36	6	(21, 24, 27)	(288, 144, 296)	$\geq 1$
36	7	(21, 24, 27)	(936, 306, 944)	Open
39	5	(21, 27, 30)	(42, 188, 12)	Open
39	6	(21, 27, 30)	(156, 494, 78)	Open
39	7	(21, 27, 30)	(498, 1412, 276)	Open

Table 3 Admissible and realizable parameters of ternary projective three-weight codes

mark with the keyword "**Open**". For each feasible case we give a suitable generator matrix in Appendix A.

Similar to Conjecture 3.3, the numerical data suggests the conjecture  $w_2 = \frac{2}{3}n$ . Based on our computational data, we dare to state the following *q*-ary version of Conjecture 3.3.

**Conjecture 3.4** Let C be a projective  $[n, k]_q$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = 3(1 - \frac{1}{q})n$ . Then  $w_2 = (1 - \frac{1}{q})n$ . Moreover,  $w_1 = w_2 - t$  and  $w_3 = w_2 + t$ , where t is a power of the characteristic p of  $\mathbb{F}_q$ .

For q = 2, Conjecture 3.4 follows from Conjecture 3.3 by Lemma 5.10. We further remark that the precondition  $w_1 + w_2 + w_3 = 3(1 - \frac{1}{q})n$  cannot be dropped, as seen by the binary [7, 4]<sub>2</sub> Hamming code, which is a three-weight code with weight distribution  $(0^{1}3^{3}4^{3}7^{1})$ .

### 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) by Lemma 2.6. 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 [3]) 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 (http://www.lmfdb.org/EllipticCurve/Q/50/a/350.*a*3 in the LMFDB [30]). In Cremona's tables or under the link above, one can check that this curve has exactly three rational points. This proves the following.

#### Lemma 4.1

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

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

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

A procedure implemented in Magma [3] then produces the hyperelliptic equation

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

for  $C'_5$ . A 2-descent as described in [29] (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 [10]), 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.

### Lemma 4.2

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

The combination of Lemmas 4.1 and 4.2 with Lemma 1.1 leads to the following theorem.

**Theorem 4.3** Let  $\Gamma$  be a k-regular graph with four distinct eigenvalues  $k > \theta_1 > \theta_2 > \theta_3$ and let  $s \in \{5, 7\}$ . Then  $\Gamma$  is an s-SWRG if and only if  $\theta_2 = 0$  and  $\theta_3 = -\theta_1$ .

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 (http://www.lmfdb.org/EllipticCurve/Q/10368/j/110368.j1 in the LMFDB [31]). 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

$$x^{4} + 2x^{3}y + x^{2}y^{2} - xy^{3} - y^{4} + 2x^{3}z - 4x^{2}yz - 3xy^{2}z + 2y^{3}z + 4x^{2}z^{2} - 3xyz^{2} + 3y^{2}z^{2} + 3xz^{3} - 4yz^{3} + z^{4} = 0$$

Deringer

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 [9] 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 Lemmas 4.1 and 4.2.

**Conjecture 4.4** *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. In Eqs. (3)–(6), the code has been assumed to be projective, i.e.  $B_2 = 0$ . For the more general situation, we prepare

$$\sum_{k=0}^{k} A_{k} = q^{k} - 1, \tag{13}$$

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

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

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

for an  $[n, k]_q$  code C with  $B_1 = 0$ .

**Lemma 5.1** (Folklore) Let C be an  $[n, k]_2$  code and  $C_2$  the subset of all codewords of even weight. Then  $C_2$  is a linear subcode of C of dimension k or k - 1.

**Proof** Consider the  $\mathbb{F}_2$ -linear map  $f : C \to \mathbb{F}_2$ ,  $c \mapsto \sum_{i=0}^n c_i$ . Then  $C_2 = \ker f$  is a linear subspace of C. By the rank-nullity theorem, the codimension of  $C_2$  in C equals dim ker  $f \in \{0, 1\}$ .

We call  $C_2$  the *even-weight subcode* of C. A direct consequence of Lemma 5.1 is the following.

**Lemma 5.2** Let C be an  $[n, k]_2$  code of dimension  $k \ge 2$ . Then C has a non-zero even weight.

**Lemma 5.3** Let C be a linear binary  $[n, k]_2$  three-weight code. Then  $k \ge 2$ . If C is projective, then  $k \ge 3$ .

**Proof** if  $k \leq 1$ , then C consists of at most a single non-zero codeword, so C cannot have three different weights.

Assume that *C* is projective of dimension k = 2 and let *G* be a generator matrix of *C*. Then *G* neither has a zero column, nor a repeated column. Therefore, each of the  $2^k - 1 = 3$  possible column vectors in  $\mathbb{F}_2^2 \setminus \{0\}$  appears at most once as a column of *G*, implying that  $n \leq 3$ . As *C* has three different non-zero weights,  $n \geq 3$ , so together we get n = 3 and each of the 3 non-zero vectors appears exactly once as a column of *G*. Therefore, *C* is isomorphic to the simplex code Sim<sub>2</sub>(2), which is a constant weight code. This is a contradiction.

**Remark 5.4** There are indeed (many) non-projective binary three-weight codes of dimension 2. An example for the smallest possible length n = 3 is given by the generator matrix  $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$ , which spans a code with the weight distribution  $(0^1 1^1 2^1 3^1)$ .

**Lemma 5.5** Let C be a projective full-length  $[n, k]_2$  three-weight code with non-zero weights  $w_1$ ,  $w_2$  and  $w_3$ , such that n is even and exactly one weight is odd. W.l.o.g. let  $w_2$  be the odd weight.

Then  $w_2 = \frac{n}{2}$  and the even-weight subcode  $C_2$  of C has effective length n and is a 2-fold replication of a projective  $\left[\frac{n}{2}, k-1\right]_2$  two-weight code with non-zero weights  $\frac{w_1}{2}$  and  $\frac{w_3}{2}$ .

**Proof** Let  $A_{w_i}$  be the number of codewords of weight  $w_i$  in *C*. Furthermore, let  $(B_i)$  be the dual weight distribution of *C* and  $(B'_i)$  the dual weight distribution of  $C_2$ . Since *C* is projective, we have  $B_1 = B_2 = 0$ . We set  $y = 2^{k-2} = \frac{1}{4} \# C$ . By Lemma 5.3,  $y \in \mathbb{Z}$ . Since  $w_2$  is the only odd weight, Lemma 5.1 gives  $A_{w_2} = 2y$ . Now Eq. (4) applied to *C* yields

$$w_1 A_{w_1} + w_3 A_{w_3} = 2y(n - w_2).$$

From Lemma 5.1 we conclude that  $C_2$  is a two-weight code of dimension k - 1 and effective length  $n' \le n$  with non-zero weights  $w_1$  and  $w_3$ . Since C is projective, we have  $n' \in \{n-1, n\}$ . Noting that  $A_{w_1}$  and  $A_{w_3}$  are also the numbers of codewords of weights  $w_1$  and  $w_3$  in  $C_2$ , the application of Eq. (14) to the full-length code arising from  $C_2$  after (possibly) removing the zero position yields

$$w_1 A_{w_1} + w_3 A_{w_3} = n' y. (17)$$

Hence  $n'y = 2y(n - w_2)$  and thus  $n' = 2(n - w_2)$  is even. By the assumption that *n* is even, n' = n - 1 is not possible. Therefore n' = n and  $w_2 = \frac{n}{2}$ . So  $C_2$  is full-length and hence  $B'_1 = 0$ . Now the difference of Eq. (15) for *C* and  $C_2$  with  $w_2 = \frac{n}{2}$ ,  $A_{w_2} = 2y$  and  $B_2 = 0$ gives

$$\frac{n^2}{4} \cdot 2y = 2y \cdot \frac{n(n+1)}{2} - y\left(B'_2 + \frac{n(n+1)}{2}\right),$$

which simplifies to  $\frac{n^2}{2} = \frac{n(n+1)}{2} - B'_2$  and further to  $B'_2 = \frac{n}{2}$ . As *C* is projective, the position multiplicities of the codimension 1 subcode  $C_2$  are at most 2. Denoting the number of position pairs of multiplicity 2 by *m*, Lemma 2.4 yields  $m = B'_2 = \frac{n}{2}$ . Therefore, all positions of  $C_2$  appear with multiplicity 2 and thus,  $C_2$  is the two-fold repetition of a projective two-weight code with non-zero weights  $\frac{w_1}{2}$  and  $\frac{w_3}{2}$ .

**Remark 5.6** As seen in the above proof, in the situation of Lemma 5.5 we have  $A_{w_2} = 2y$ . Moreover, we can use Eqs. (13) and (14) to compute the frequencies

$$A_{w_1} = \frac{(2y-1)w_3 - yn}{w_3 - w_1}$$
 and  $A_{w_3} = \frac{yn - (2y-1)w_1}{w_3 - w_1}$ 

depending on the weights  $w_1$  and  $w_3$ .

From now on, we add the extra constraint  $w_1 + w_2 + w_3 = \frac{3n}{2}$ .

**Corollary 5.7** Let C be a projective  $[n, k]_2$  three-weight code with non-zero weights  $w_1$ ,  $w_2$  and  $w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . Then n is a multiple of 4.

**Proof** Since  $\frac{3n}{2} = w_1 + w_2 + w_3$  is an integer, *n* has to be even, so that we assume  $n \equiv 2 \pmod{4}$ . Then  $\frac{3n}{2} = w_1 + w_2 + w_3$  is odd. By Lemma 5.2, *C* has an even weight, so exactly one weight of *C* is odd. Without restriction, let  $w_2$  be the odd weight. Lemma 5.5 yields  $w_2 = \frac{n}{2}$ . From  $w_1 + w_2 + w_3 = \frac{3}{2}n$  we may further assume  $w_1 < w_2 < w_3$ , so  $w_1 = \frac{n}{2} - t$  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 5.5 says that  $\frac{w_1}{2}$  and  $\frac{w_3}{2}$  are the weights of a projective binary two-weight code. By Lemma 2.2 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 that t = 1, so

$$w_1 = \frac{n}{2} - 1$$
,  $w_2 = \frac{n}{2}$  and  $w_3 = \frac{n}{2} + 1$ .

Writing  $y = 2^{k-2}$ , the frequencies from Remark 5.6 evaluate to

$$A_{w_1} = y - \frac{n}{4} - \frac{1}{2}, \quad A_{w_2} = 2y \text{ and } A_{w_3} = y + \frac{n}{4} - \frac{1}{2}.$$
 (18)

Plugging these expressions into Eq. (5) leads to

$$n^2y + 2y + \frac{n^2}{4} - 1 = n(n+1)y$$

and further to the quadratic equation

$$n^2 - 4ny + (8y - 4) = 0$$

with the two solutions  $n \in \{2, 4y - 2\}$ . Since the length of a three-weight code is at least 3, necessarily n = 4y - 2. Now Eq. (18) yields  $A_{w_1} = 0$  – a contradiction.

Using the abbreviation  $y = 2^{k-2}$ , we prepare Eqs. (7)–(10) in the special case  $w_1 = \frac{n}{2} - t$ ,  $w_2 = \frac{n}{2}$  and  $w_3 = \frac{n}{2} + t$ .

$$A_{w_1} = \frac{n(4y - n - 2t)}{8t^2} \tag{19}$$

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

$$A_{w_3} = \frac{n(4y - n + 2t)}{8t^2} \tag{21}$$

$$3B_3 = \frac{n(n-2t)(n+2t)}{8y}$$
(22)

**Lemma 5.8** Let C be a projective  $[n, 3]_2$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . Then C has length n = 4, weight distribution  $(0^1 1^1 2^3 3^3)$  and is isomorphic to the code spanned by the generator matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

🖉 Springer

**Proof** By Lemma 2.3,  $n \le 5$ , and by Corollary 5.7,  $4 \mid n$ . Therefore n = 4. The code *C* is isomorphic to a systematic code, which has a generator matrix of the form  $(I_3 \mid v)$ , where  $I_3$  denotes the  $3 \times 3$  unit matrix and v is a vector in  $\mathbb{F}_2^3$ . As *C* is projective,  $w(v) \ge 2$ . Furthermore, w(v) = 3 is not possible, as *C* would have only the two weights 2 and 4. So w(v) = 2. We note that the three possibilities for v lead to equivalent codes, and that the resulting code has the stated weight distribution.

We remark that geometrically, the above  $[4, 3]_2$  code corresponds to the complement of a triangle in the projective plane PG(2, 2).

**Theorem 5.9** Let C be a projective  $[n, k]_2$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$ . Then n is a multiple of 4, and one of the following cases occurs.

- (i)  $k \ge 4$ ,  $n \ge 8$  and all weights of C are even.
- (ii) The code C has the parameters  $[4, 3]_2$  and is isomorphic to the code in Lemma 5.8.

**Proof** By Corollary 5.7, *n* is a multiple of 4.

In the case that *n* has only even weights, the largest weight is at least 6, so  $n \ge 8$ . Moreover,  $k \ge 4$  by Lemma 5.8.

Now we assume that *C* has an odd weight. As  $\frac{n}{2}$  is even, *C* has at least two odd weights by Lemma 5.5. Since  $w_1 + w_2 + w_3 = n$  is even, we get that *C* has exactly two odd weights, say  $w_1$  and  $w_3$ . Let  $C_2$  be the even-weight subcode of *C*. The code *C* is projective and by Lemma 5.1, the codimension of  $C_2$  in *C* is 1. Therefore, the maximum position multiplicity of  $C_2$  is at most 2, and the effective length n' of  $C_2$  is either n - 1 or n. Since  $w_2$  is the only even weight of *C*, the subcode  $C_2$  is a code of constant weight  $w_2$  and frequency  $A_{w_2} = \#C_2 - 1 = 2^{k-1} - 1$ . From Lemma 2.1 we conclude that  $w_2 = u \cdot 2^{k-2}$  and  $n' = u \cdot (2^{k-1} - 1)$  with an integer  $u \in \{1, 2\}$ , where  $u \leq 2$  follows from the maximum position multiplicity.

Let us first investigate the case u = 2. Here,  $n' = 2^k - 2$  and  $n \in \{2^k - 2, 2^k - 1\}$ . Let G be a generator matrix of C. Since C is projective, G neither has a zero column, nor a repeated column. So each of the  $2^k - 1$  non-zero vectors in  $\mathbb{F}_2^k$  occurs exactly once as a column in G, possibly with the excection that a single vector might not occur at all. In the case  $n = 2^k - 1$ , all vectors occur as a column in G, so  $C = \text{Sim}_2(k)$ , which is a code of constant weight  $2^{k-1}$ . In the case  $n = 2^k - 2$ , C is the simplex code  $\text{Sim}_2(k)$  punctured in a single position, so C has the two weights  $2^{k-1}$  and  $2^{k-1} - 1$ .<sup>3</sup> This contradicts the assumption that C is a three-weight code.

It remains to consider u = 1. Here,  $w_2 = 2^{k-2}$  and  $n' = 2^{k-1} - 1$ , which is odd. Since *n* is even, necessarily n' = n - 1, so  $n = 2^{k-1}$  and  $w_2 = \frac{n}{2}$ . Combined with  $w_1 + w_2 + w_3 = \frac{3n}{2}$  we can write  $w_1 = \frac{n}{2} - t$  and  $w_3 = \frac{n}{2} + t$  for some positive integer *t*. Together with the abbreviation  $y = 2^{k-2}$ , Eqs. (19)–(21) can be simplified to

$$A_{w_1} = \frac{y(y-t)}{2t^2}$$
$$A_{w_2} = 4y - 1 - \frac{y^2}{t^2}$$
$$A_{w_3} = \frac{y(y+t)}{2t^2}.$$

<sup>&</sup>lt;sup>3</sup> In fact, in this case C is a MacDonald code.

Now we use  $A_{w_2} = 2^{k-1} - 1 = 2y - 1$  to conclude  $y = 2t^2$  (or y = 0, which is impossible). As y is a power of 2, so is t. From  $w_1 = t(2t - 1)$  odd we get that t is so dd. Together, this forces t = 1, which gives y = 2 and therefore k = 3. Therefore, C is isomorphic to the code in Lemma 5.8.

**Lemma 5.10** Let C be a projective  $[n, k]_2$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_2 = \frac{n}{2}$ . Then  $w_1 = w_2 - t$  and  $w_3 = w_2 + t$  where t is a power of 2. Moreover,  $2t \mid n$ , and t is the largest integer  $\Delta$  such that C is  $\Delta$ -divisible.

**Proof** Equations (19) and (21) give  $A_{w_3} - A_{w_1} = \frac{n}{2t}$ , so  $2t \mid n$ . Therefore  $t \mid w_2 = \frac{n}{2}$ , implying that t is the greatest common divisor of  $w_1 = w_2 - t$ ,  $w_2$  and  $w_3 = w_2 + t$ , so  $\Delta = t$ . Since C is projective, C cannot be the proper repetition of some code. Now as a consequence of [33, Theorem 1], the number  $\Delta = t$  must be a power of 2.

**Lemma 5.11** Let C be a projective  $[n, k]_2$  three-weight code with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_2 = \frac{n}{2}$ . Let  $a \ge 0$  be the largest integer such that C is  $2^a$ -divisible. Then  $k \le 8a + 9$ .

**Proof** As before, we will use the abbreviation  $y = 2^{k-2}$  and write  $w_1 = \frac{n}{2} - t$  and  $w_3 = \frac{n}{2} + t$  with an integer  $t \ge 1$ . By Lemma 5.3,  $y \in \mathbb{Z}$ . By Lemma 5.10,  $t = 2^a$  is the largest integer  $\Delta$  such that *C* is  $\Delta$ -divisible. There is an odd integer *z* and a non-negative integer *x* with  $n = 2^x \cdot z$ . Since *C* is projective,  $n \le 2^k - 1$ . Together with  $2t \mid n$ , we get  $a + 1 \le x \le k - 1$ . Plugging  $t = 2^a$ ,  $n = 2^{x_z}$  and  $y = 2^{k-2}$  into Eqs. (19)–(22) we get

$$A_{w_1} = \frac{z \cdot (2^{k-a-1} - 2^{x-a-1}z - 1)}{2^{a+2-x}},$$
(23)

$$A_{w_2} = 2^{2(x-a-1)}z^2 + 2^k - 2^{x+k-2a-2}z - 1,$$
(24)

$$A_{w_3} = \frac{z \cdot (2^{k-a-1} - 2^{x-a-1}z + 1)}{2^{a+2-x}},$$
(25)

$$3B_3 = \frac{z \cdot (2^{x-a-1}z - 1) \cdot (2^{x-a-1}z + 1)}{2^{k-x-2a-1}}.$$
(26)

First case:  $k \ge x + 2a + 2$ . Equivalently,  $k - x - 2a - 1 \ge 1$ , so the denominator of the right hand side of Eq. (26) is even. By  $B_3 \in \mathbb{Z}$ , the numerator is even, too. Since *z* is odd, this implies a = x - 1. Now  $0 < w_1 = \frac{n}{2} - t = 2^{x-1}z - 2^a = 2^a(z-1)$  yields z > 1. Equation (26) with a = x - 1 yields

$$3B_3 = \frac{z \cdot (z-1) \cdot (z+1)}{2^{k-3x+1}}.$$

From our precondition  $k \ge x + 2a + 2 = 3x$  we have  $k - 3x \ge 0$ , so  $2^{k-3x}$  is an integer. Since gcd(z - 1, z + 1) = 2, we have that  $2^{k-3x}$  either divides z - 1 or z + 1. Therefore,  $z = s \cdot 2^{k-3x} + \alpha$  for some integer s and  $\alpha \in \{-1, 1\}$ . By z > 1,  $s \ge 1$ . Now Eq. (23) yields

$$0 < \frac{2^{a+2-x}}{z} \cdot A_{w_1} = 2^{k-x} - \left(s \cdot 2^{k-3x} + \alpha + 1\right) \le 2^{k-x} - s \cdot 2^{k-3x},$$

so that  $s < 2^{2x}$  and hence  $s \le 2^{2x} - 1$ .

Using Eq. (24) we get

$$\begin{aligned} 0 &< s(A_{w_2} + 1) \\ &= s(z^2 + 2^k) + s \cdot z \cdot 2^{k-x} \\ &\leq (2^{2x} - 1)((s2^{k-3x} + \alpha)^2 + 2^k) - s(s2^{k-3x} + \alpha)2^{k-x} \\ &= (2^{2x} - 1)(s^2 2^{2k-6x} + 2\alpha s2^{k-3x} + 1 + 2^k) - s(s2^{k-3x} + \alpha)2^{k-x} \\ &= s^2 2^{2k-4x} + 2\alpha s2^{k-x} + 2^{2x} + 2^{k+2x} - s^2 2^{2k-6x} - \alpha s2^{k-3x+1} - 1 - 2^k \\ &- s^2 2^{2k-4x} - \alpha s2^{k-x} \\ &= \alpha s(2^{k-x} - 2^{k-3x+1}) + (2^{2x} + 2^{k+2x}) - s^2 2^{2k-6x} - (1 + 2^k) \\ &\leq 2s \cdot 2^{k+2x} + 2s \cdot 2^{k+2x} - s2^{2k-6x} \\ &= s(2^{k+2x+2} - s^{2k-6x}), \end{aligned}$$

where in the second last step  $s \ge 1$  has been used. Therefore k + 2x + 2 > 2k - 6x and hence

$$k \le 8x + 1 = 8(a + 1) + 1 = 8a + 9.$$

Second case:  $k \le x + 2a + 1$ . Equation (19) implies

$$0 < \frac{8t^2}{n}A_{w_1} = 4y - n - 2t < 4y - n.$$

We have  $2^x \mid n$  and from  $x \le k - 1$  also  $2^x \mid 2^k = 4y$ . Therefore  $2^x \mid 4y - n > 0$  and thus  $4y - n \ge 2^x$ .

By Eq. (20),

$$0 < 4t^{2}A_{w_{2}}$$
  
=  $4t^{2}(4y - 1) - n(4y - n)$   
 $\leq 4t^{2} \cdot 4y - n \cdot 2^{x}$   
=  $2^{k+2a+2} - 2^{2x}z$   
 $\leq (2^{k+2a+2} - 2^{2x})$ 

and thus k + 2a + 2 > 2x and  $k \ge 2x - 2a - 1$ . Combined with  $k \le x + 2a + 1$ , finally

$$k = 2k - k \le 2(x + 2a + 1) - (2x - 2a - 1) = 6a + 3 < 8a + 9.$$

By Lemmas 5.11 and 2.3, the following numbers K(r) and N(r) are well-defined.

**Definition 5.12** Let  $a \ge 1$  be an integer. We define K(a) (resp. N(a)) as the largest dimension (resp. length) of a projective  $[n, k]_2$  three-weight code C with non-zero weights  $w_1 < w_2 < w_3$  satisfying  $w_1 + w_2 + w_3 = \frac{3n}{2}$  and  $w_2 = \frac{n}{2}$  such that C is not  $2^a$ -divisible.

**Theorem 5.13** *Let*  $a \ge 1$  *be an integer. Then* 

$$2a + 1 \le K(a) \le 8a + 1$$
 and  $2^{2a+1} - 2^{a+1} \le N(a) \le 2^{K(a)} - 3$ 

**Proof**  $K(a) \le 8(a-1) + 9 = 8a + 1$  by Lemma 5.11 and  $N(a) \le 2^{K(a)} - 3$  by Lemma 2.3.

For the lower bounds, let  $C = \text{Sim}_2(a) \oplus \text{RM}_2(a+1)$ . It is a projective three-weight code of length  $n = (2^a - 1) + 2^a = 2^{a+1} - 1$ , dimension k = a + (a + 1) = 2a + 1 and weights  $w_1 = 2^{a-1}$ ,  $w_2 = 2^a$  and  $w_3 = 3 \cdot 2^{a-1}$ .<sup>4</sup> Since C does not have the weight  $2^{k-1} = 2^{2a}$ , the anticode  $C^{\complement}$  is defined. It is a projective three-weight code of the same dimension k, length  $n^{\complement} = (2^k - 1) - n = 2^{2a+1} - 2^{a+1}$  and the three non-zero weights

$$w_1^{\mathsf{C}} = 2^{k-1} - w_3 = 2^{2a} - 3 \cdot 2^{a-1} = 2^{a-1}(2^{a+1} - 3),$$
  

$$w_2^{\mathsf{C}} = 2^{k-1} - w_2 = 2^{2a} - 2^a = 2^{a-1}(2^{a+1} - 2) \text{ and }$$
  

$$w_3^{\mathsf{C}} = 2^{k-1} - w_1 = 2^{2a} - 2^{a-1} = 2^{a-1}(2^{a+1} - 1),$$

so  $C^{\complement}$  is  $2^{a-1}$ -divisible, but not  $2^a$ -divisible. Furthermore

$$w_1^{\complement} + w_2^{\complement} + w_3^{\complement} = 3 \cdot 2^{2a} - 3 \cdot 2^a = \frac{3}{2}n^{\complement}$$
 and  $w_2^{\complement} = \frac{n^{\circlearrowright}}{2}$ .

Therefore,  $K(a) \ge k = 2a + 1$  and  $N(a) \ge n^{\complement} = 2^{2a+1} - 2^{a+1}$ .

For small values of a, we can determine the exact values of N(a) and K(a).

**Theorem 5.14** (*a*) K(1) = 3 and N(1) = 4. (*b*) K(2) = 6 and N(2) = 56. (*c*) K(3) = 11 and N(3) = 2024.

**Proof** The case a = 1: The values K(1) = 3 and N(1) = 4 are a direct consequence of Theorem 5.9.<sup>5</sup>

The case a = 2: Using  $K(2) \le 17$  from Theorem 5.13 and  $t = 2^a = 4$  from Lemma 5.10, we determined all feasible parameters computationally. The ones with  $k \ge 7$  are listed below.

п	k	$w_1$	$w_2$	$w_3$
244	8	120	122	124
116	7	56	58	60
112	7	54	56	58
16	7	6	8	10

The last code has already been excluded in Sect. 3 via Lemma 3.1. Of the first three codes, the anticodes would have the parameters [11, 8, 4], [11, 7, 4] and [15, 7, 6]. The application of the Hamming bound to the punctured parameters [10, 7, 3], [10, 6, 3] and [14, 7, 5] shows that these codes do not exist.

Among all feasible parameters with  $k \le 6$ , the ones with the largest possible length are n = 56, k = 6,  $w_1 = 26$ ,  $w_2 = 28$  and  $w_3 = 30$ . These parameters are realized by the anticode of the binary [7, 6]<sub>2</sub> parity check code.

The case a = 3: Similar as before, based on  $K(3) \le 25$  and t = 8 we were able to determine all feasible parameters computationally. There is only a single feasible parameter set with  $k \ge 12$ , which is n = 4040, k = 12,  $w_1 = 2016$ ,  $w_2 = 2020$  and  $w_3 = 2024$ . The anticode would have the parameters [55, 12, 24], which does not exist according to the online tables [17].

<sup>&</sup>lt;sup>4</sup> We have already seen the code C in Theorem 3.2 Case (i), with a - 1 in instead of a.

<sup>&</sup>lt;sup>5</sup> Theorem 5.9 refers to the code in Lemma 5.8. It is isomorphic to the code  $C^{\complement}$  considered in the proof of Theorem 5.13 in the smallest case a = 1.

Among all parameters with  $k \le 11$ , the ones with the largest possible length are n = 2024, k = 11,  $w_1 = 1008$ ,  $w_2 = 1012$  and  $w_3 = 1016$ . These parameters are realized by the code  $(C^{\perp})^{\complement}$ , where *C* is the binary [23, 12]<sub>2</sub> Golay code. The code  $C^{\perp}$  has the weight enumerator  $1 + 506x^8 + 1288x^{12} + 253x^{16}$ .

Theorem 5.14 indicates that in general, neither the lower nor the upper bound of Theorem 5.13 are sharp. We leave it as a research problem to improve the bounds and further investigate the asymptotic growth.

Funding Open Access funding enabled and organized by Projekt DEAL.

**Data Availability** The datasets generated during and/or analysed during the current study are available from the corresponding author on reasonable request.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

# 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 Sect. 3.

•	<i>q</i> =	= 2	2, n	=	16,	k =	6, ı	<i>v</i> =	[6,	8, 1	0]:	$ \begin{pmatrix} 0\\0\\0\\1\\0\\0\\0 \end{pmatrix} $	00010 01011 00001 00101 00100 10110	0110 0001 1011 0000 1100 0001	)010 1101 1001 )110 )100 1010	011 000 001 100 101 010	)		
•	<i>q</i> :	= 2	2, n	=	16,	k =	5, ι	<i>v</i> =	[4,	8, 1	2]:	$\begin{pmatrix} 1\\1\\1\\1\\0 \end{pmatrix}$	10001 10011 01010 10110 10110 11111	1101 0001 1001 0001 1011	100 001 110 101 100	100 011 010 001 111	)		
•	<i>q</i> =	= 2	2, n	=	16,	k =	6, ι	<i>v</i> =	[4,	8, 1	2]:	$\begin{pmatrix} 1\\1\\1\\1\\1\\1\\1 \end{pmatrix}$	10100 11000 10100 00101 10011 11001	1010 1000 0101 1111 1011 1100	)010 )011 1001 1100 1111 )011	101 101 011 000 011 000	)		
•	<i>q</i> :	=2	2, n	=	16,	k =	7, ι	v =	[4,	8, 1	2]:	$\left(\begin{smallmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{smallmatrix}\right)$	00000 10000 01000 00100 00010 00001 00000	011 010 000 000 000 011	1011 100 1110 101 100 1011 1011	110 000 000 100 101 111			
•	<i>q</i> =	= 2	2, n	=	20,	k =	5, ι	<i>v</i> =	[8,	10,	12]:	(	11101 00101 10100 11101 11010	110 0010 1010 000 1010	1000 0111 0001 1001 0100	100 000 110 101 010	1010 00110 1100 0001 0000	$\begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$	
•	<i>q</i> :	= 2	2, n	=	24,	k =	5, ι	<i>v</i> =	[10	), 12	, 14	]: (	$\left(\begin{array}{c}1110\\0110\\0000\\0101\\1000\end{array}\right)$	)111 )101 )110 (100 )001	0001 1011 1111 1110 0111	1010 1000 1000 110 111	0000 0111 1101 1000 0110	01011 10101 01011 00110 01000	$\begin{pmatrix} 1 \\ 1 \\ 0 \\ 01 \\ 01 \end{pmatrix}$
•	<i>q</i> :	= 2	2, n	=	24,	k =	6, ı	<i>v</i> =	[8,	12,	16]:	(	10000 01000 00100 00010 00001 00000	)001 )101 )000 )101 )101 (100 )010	0111 0011 1011 1101 0100 1000	100 011 011 010 010 0101	1000 1110 0101 0011 0001 0000	11111 01100 10111 11010 10001 01111	
•	q :	=2	2, n	=	24,	k =	7, ι	v =	[8,	12,	16]:		00111 01011 01011 10011 00111 10010 00000	1111 1111 1011 1110 1101 0111 0000	1011 0111 1111 1110 1101 1111 0011	101 011 111 0111 111 111 110	1101 1011 0101 1100 1011 1010 1111	10001 01010 01001 11001 10010 11010 11100	
•	q :	= 2	2, n	=	24,	k =	8, ι	v =	[8,	12,	16]:		10001 01110 00110 00101 01110 11011 01001 00111	101 0011 0110 010 0111 010 0111 101 101	1110 1001 0110 1101 0001 1011 0110 1111	010 100 110 010 000 101 101 0010	0111 0100 0000 1011 1110 1001 1110 1001	11111 01101 10111 00101 10001 01110 10001 11001	
•	q :	= 2	2, n	=	24,	k =	9, ι	v =	[8,	12,	16]:		01111 11110 00101 11111 00110 01010 00110 11000 00111	1001 111 110 1010 0011 0100 0101 0101	1110 1000 1100 0101 0000 0001 0110 1110	)001 )010 )101 0000 )101 110 )000 )101	1110 1111 0000 0001 0111 1001 1101 110	01111 10101 11011 01101 10101 11011 01011 00001 10111	
•	q :	= 2	2, n	=	24,	k =	10,	<i>w</i> =	= [8	, 12	, 16	]:	$\left(\begin{array}{c} 100\\ 010\\ 001\\ 000\\ 000\\ 000\\ 000\\ 000$	0000 0000 1000 0100 0010 0001 0000 0000 0000	0000 0010 0000 0000 0000 0000 0000 000	0110 0101 0111 0001 0100 0100 0100 010	)1010 1001 1000 1100 )1100 )1001 )1010 )0100 00111 )0110	00010 0001 01010 011110 01010 11100 01101 011010 00100 01110	$\begin{pmatrix} 11\\ 11\\ 01\\ 00\\ 10\\ 01\\ 10\\ 01\\ 01\\ 11 \end{pmatrix}$

• $q = 2, n = 24, k = 11, w = [8, 12, 16]$ :	$ \begin{pmatrix} 10000000000011011011010\\ 010000000000$
• $q = 2, n = 32, k = 6, w = [12, 16, 20]:$	$\left(\begin{smallmatrix} 100100001101011011001110001\\ 10011001111000101100001000011\\ 111101110$
• $q = 2, n = 32, k = 7, w = [12, 16, 20]:$	$ \begin{pmatrix} 01111000000111110000111111111110\\ 1110011011001000011111000110000\\ 1001111100100010$
• $q = 2, n = 32, k = 8, w = [12, 16, 20]:$	$ \begin{pmatrix} 11101100110111010010100111110011\\ 100110001000$
• $q = 2, n = 32, k = 9, w = [12, 16, 20]:$	$\left(\begin{array}{c} 100000000101101100111100001010\\ 0100000010000011011000001101100\\ 00100000000$
• $q = 2, n = 32, k = 10, w = [12, 16, 20]$	$\left(\begin{array}{c} 1111100000111111000000100000000\\ 000011111111$
• $q = 2, n = 32, k = 6, w = [8, 16, 24]:$	$ \begin{pmatrix} 0111101110010101111111101101111\\ 010010000111101100110$
• $q = 2, n = 32, k = 7, w = [8, 16, 24]:$	$ \left(\begin{smallmatrix} 11010100001101001100010111100101\\ 01010011101100100110001010101$
• $q = 2, n = 32, k = 8, w = [8, 16, 24]:$	$\left(\begin{smallmatrix} 1000000101111110000000101111110\\01000010100000101000000$
• $q = 2, n = 32, k = 9, w = [8, 16, 24]:$	$ \begin{pmatrix} 10101110000101001100011100001111\\ 010101001011110001101001010101$

- q = 2, n = 56, k = 7, w = [24, 28, 32]:

• q = 2, n = 56, k = 8, w = [24, 28, 32]: q = 2, n = 56, k = 9, w = [24, 28, 32]: = 2, n = 64, k = 9, w = [28, 32, 36]:• a q = 2, n = 64, k = 7, w = [24, 32, 40]:  $\frac{1}{100}$ • q = 2, n = 64, k = 8, w = [24, 32, 40]: • q = 2, n = 64, k = 9, w = [24, 32, 40]:  $\begin{array}{c} -2, n = 0, n = 0, n = 0, n = 0, 0 = 1, 0 = 0$ • q = 2, n = 64, k = 10, w = [24, 32, 40]: 

• 
$$q = 3, n = 3, k = 3, w = [1, 2, 3]: \begin{pmatrix} 001\\112\\210\end{pmatrix}$$

•  $q = 3, n = 6, k = 3, w = [3, 4, 5]: \begin{pmatrix} 111101\\121011\\100122 \end{pmatrix}$ 

• 
$$q = 3, n = 9, k = 3, w = [5, 6, 7]: \begin{pmatrix} 011011001\\110002111\\100121202 \end{pmatrix}$$



# References

- 1. Betsumiya K., Munemasa A.: On triply even binary codes. J. Lond. Math. Soc. 86(1), 1-16 (2012).
- Bonisoli A.: Every equidistant linear code is a sequence of dual Hamming codes. Ars Comb. 18, 181–186 (1984).
- Bosma W., Cannon J., Playoust C.: The Magma algebra system. I. The user language. J. Symbolic Comput. 24(3–4), 235–265 (1997).
- Bouyukliev Iliya, Bouyuklieva Stefka, Kurz Sascha: Computer classification of linear codes. IEEE Trans. Inf. Theory 67(12), 7807–7814 (2021).
- Braun M., Kohnert A., Wassermann A.: Optimal linear codes from matrix groups. IEEE Trans. Inf. Theory 51(12), 4247–4251 (2005).
- Brouwer A.E.: Parameters of strongly regular graphs. https://www.win.tue.nl/~aeb/graphs/srg/srgtab. html.
- 7. Brouwer A.E., Cohen A.M., Neumaier A.: Distance-Regular Graphs. Springer-Verlag, Berlin (1989).
- 8. Brouwer A.E., Haemers W.H.: Spectra of Graphs. Springer Science & Business Media, Berlin (2012).
- 9. Bruin N., Poonen B., Stoll M.: Generalized explicit descent and its application to curves of genus 3. Forum of mathematics. Sigma 4, e6 (2016).
- Bruin N., Stoll M.: The Mordell-Weil sieve: proving non-existence of rational points on curves. LMS J. Comput. Math. 13, 272–306 (2010).
- Calderbank R., Kantor W.M.: The geometry of two-weight codes. Bull. Lond. Math. Soc. 18(2), 97–122 (1986).

- 12. Chen E .: Two-weight codes. http://moodle.tec.hkr.se/~chen/research/2-weight-codes.
- Courteau B., Wolfmann J.: On triple-sum-sets and two or three weights codes. Discrete Math. 50(2–3), 179–191 (1984).
- Delsarte Ph.: Weights of linear codes and strongly regular normed spaces. Discrete Math. 3(1–3), 47–64 (1972).
- Dodunekov S., Guritman S., Simonis J.: Some new results on the minimum length of binary linear codes of dimension nine. IEEE Trans. Inf. Theory 45(7), 2543–2546 (1999).
- 16. Dodunekov S., Simonis J.: Codes and projective multisets. Electron. J. Comb. 5, #R37 (1998).
- 17. Grassl M.: Bounds on the minimum distance of linear codes and quantum codes (2007). http://www.codetables.de.
- Heinlein D., Honold T., Kiermaier M., Kurz S., Wassermann A.: Projective divisible binary codes. The Tenth International Workshop on Coding and Cryptography 2017 : WCC Proceedings, Saint-Petersburg (2017).
- Jaffe D.B., Ruberman D.: A sextic surface cannot have 66 nodes. J. Algebraic Geom. 6(1), 151–168 (1997).
- Kiermaier M., Kurz S.: Classification of Δ-divisible linear codes spanned by codewords of weight Δ, arXiv preprint arXiv:2011.05872 (2021).
- Kohnert A.: Constructing two-weight codes with prescribed groups of automorphisms. Discrete Appl. Math. 155(11), 1451–1457 (2007).
- Kurz S.: Classification of 8-divisible binary linear codes with minimum distance 24, arXiv preprint arXiv:2012.06163 (2020).
- 23. Liu X.: Binary divisible codes of maximum dimension. Int. J. Inf. Coding Theory 1(4), 355–370 (2010).
- MacWilliams J.: A theorem on the distribution of weights in a systematic code. Bell Syst. Tech. J. 42(1), 79–94 (1963).
- Pless V.: Power moment identities on weight distributions in error correcting codes. Inf. Control 6(2), 147–152 (1963).
- Shi M., Kiermaier M., Kurz, S., Solé, P.: Three-weight codes over rings and strongly walk regular graphs. Graphs Combin. 38(3), 23 (2022)
- Shi M., Solé P.: Three-weight codes, triple sum sets, and strongly walk regular graphs. Des. Codes Cryptogr. 87(10), 2395–2404 (2019).
- Simonis J.: Restrictions on the weight distribution of binary linear codes imposed by the structure of Reed–Muller codes. IEEE Trans. Inf. Theory 40(1), 194–196 (1994).
- 29. Stoll M.: Implementing 2-descent for Jacobians of hyperelliptic curves. Acta Arith. 98(3), 245–277 (2001).
- The LMFDB Collaboration: The L-functions and modular forms database, home page of the l-function *l*(*s*, *e*) for elliptic curve with lmfdb label 50.a3. https://www.lmfdb.org/EllipticCurve/Q/50/a/3, [Online; accessed 26 April 2022].
- The LMFDB Collaboration: The L-functions and modular forms database, home page of the l-function *l(s, e)* for elliptic curve with lmfdb label 10368.j1. https://www.lmfdb.org/EllipticCurve/Q/10368/j/ 1, [Online; accessed 26 April 2022].
- 32. van Dam E.R., Omidi G.R.: Strongly walk-regular graphs. J. Comb. Theory A 120(4), 803-810 (2013).
- 33. Ward H.N.: Divisible codes. Arch. Math. (Basel) 36(1), 485-494 (1981).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.