EA(q)-additive Steiner 2-designs

Marco Buratti * Mario Galici † Alessandro Montinaro ‡
Anamari Nakić§ Alfred Wassermann¶

Abstract

A design is G-additive with G an abelian group, if its points are in G and each block is zero-sum in G. All the few known "manageable" additive Steiner 2-designs are EA(q)-additive for a suitable q, where EA(q) is the elementary abelian group of order q. We present some general constructions for EA(q)-additive Steiner 2-designs which unify the known ones and allow to find a few new ones: an additive EA(2^8)-additive 2-$(52, 4, 1)$ design which is also resolvable, and three pairwise non-isomorphic EA(3^5)-additive 2-$(121, 4, 1)$ designs, none of which is the point-line design of PG$(4, 3)$. In the attempt to find also an EA(2^9)-additive 2-$(511, 7, 1)$ design, we prove that a putative 2-analog of a 2-$(9, 3, 1)$ design cannot be cyclic.

Keywords: additive design; Steiner 2-design; cyclic design; 1-rotational design; q-analog of a classic design; Segre variety.

*Sapienza Università di Roma, Dipartimento di Scienze di Base e Applicate per l'Ingegneria (SBAI), Via Antonio Scarpa 14, 00161 Roma, Italy, email: marco.buratti@uniroma1.it

†Dipartimento di Matematica e Fisica "Ennio de Giorgi", Università del Salento, Lecce, Italy, email: mario.galici@unisalento.it

‡Dipartimento di Matematica e Fisica "Ennio de Giorgi", Università del Salento, Lecce, Italy, email: alessandro.montinaro@unisalento.it

§University of Zagreb, Faculty of Electrical Engineering and Computing, Unska 3, 10000 Zagreb, Croatia, email: anamari.nakic@fer.unizg.hr

¶Department of Mathematics, University of Bayreuth, D-95440 Bayreuth, Germany, email: alfred.wassermann@uni-bayreuth.de

1 Introduction

A 2-(v,k,λ) *design* is a pair $(V,\mathcal{B})$ where V is a v-set whose elements are called *points* and $\mathcal{B}$ is a collection of k-subsets of V called *blocks* such that every pair of distinct points is contained in precisely λ blocks. To avoid trivial designs, it is assumed that $v > k > 2$. In the special case that λ is 1 the design is said to be a *Steiner* 2*-design*. Throughout the paper, we will write "(v,k,λ)-design" rather than "2-(v,k,λ) design". An *automorphism* of a design $(V,\mathcal{B})$ is a permutation on V leaving $\mathcal{B}$ invariant. A design is said to be *cyclic* if it admits an automorphism cyclically permuting all its points, whereas it is said to be 1*-rotational* if it admits an automorphism fixing one point and cyclically permuting all the others. Finally, a (v,k,λ)-design $(V,\mathcal{B})$ is said to be *resolvable* if there exists a partition of $\mathcal{B}$ (*resolution*) into classes (*parallel classes*) each of which is a partition of V.

The nice notion of an additive design has been introduced in [21]. A (v,k,λ)-design is said to be *additive* if, up to isomorphism, its points are elements of an abelian group G and its blocks are all zero-sum in G. As in [13], a design as above will be said G-additive.

The characteristics of additive designs make them highly elegant combinatorial objects. It is worth noting that the use of zero-sum blocks in the construction of combinatorial designs is a common occurrence (see, e.g., [6, 7, 16, 23, 26, 30, 37, 40]). In addition, the motivation to examine and construct additive designs comes from their significant connections with various areas of discrete mathematics, including coding theory and additive combinatorics.

Throughout the paper $\mathrm{EA}(q)$ will denote the elementary abelian group of order q which, of course, can be seen as the additive group of $\mathbb{F}_q$, the field of order q. We denote by $\mathrm{AG}(n,q)$ and $\mathrm{PG}(n,q)$ the n-dimensional affine and, respectively, projective geometry over $\mathbb{F}_q$. A *q-analog of a (v,k,λ)-design* is a $(\frac{q^v-1}{q-1},\frac{q^k-1}{q-1},\lambda)$-design with point-set $V = PG(v-1,q)$ whose blocks are $(k-1)$-dimensional subspaces of V. It has been proved in [14] that every such design is $\mathrm{EA}(q^v)$-additive.

Additive designs with $\lambda > 1$ are not so rare (see, e.g., [12, 11, 20, 22, 36, 38, 39]). On the other hand, the additive $(v,k,1)$-designs appear to be "precious". Indeed, the few known results on additive Steiner 2-designs can be summarized as follows.

Theorem 1.1. *The following facts are known.*

(i) The point-line design associated with $\mathrm{AG}(n,q)$ *is* $\mathrm{EA}(q^n)$*-additive;*

(ii) the point-line design associated with $\mathrm{PG}(n,q)$ *is* $\mathrm{EA}(q^{n+1})$*-additive (see [21, 14]);*

(iii) the well celebrated 2*-analogs of a* $(13,3,1)$ *design [5] are* $\mathrm{EA}(2^{13})$*-additive* $(8191,7,1)$*-designs;*

(iv) there exists an $\mathrm{EA}(5^3)$*-additive* $(124, 4, 1)$*-design (see [11]).*

(v) if k *is neither singly even nor of the form* 2^n3*, then there exists a* $G \times EA(q)$*-additive* $(kq, k, 1)$*-design for a suitable zero-sum group* G *of order* k *and a suitable power* q *of a prime divisor of* k *(see [13]).*

Result (v) is important from a theoretical point of view since, for the time being, it is the only one assuring the existence of an additive $(v, k, 1)$-design for some values of v when k is not of the forbidden form and neither a prime power nor a prime power plus one. On the other hand, it is not practical at all since it leads to very cumbersome designs. Indeed, the mentioned "suitable" power q has to be really huge in comparison with k. Thus, the known "manageable" additive Steiner 2-designs are all $\mathrm{EA}(q)$-additive for a suitable prime power q. Inspired by this, here we want to investigate further the $\mathrm{EA}(q)$-additive $(v, k, 1)$-designs. In the next section, we first establish which are the admissible prime powers q and then we give two theoretical constructions for $\mathrm{EA}(q)$-additive $(v, k, 1)$-designs which are either cyclic with point-set the v-th roots of unity of $\mathbb{F}_q$ with $q \equiv 1 \pmod{v}$ admissible, or 1-rotational with point-set the $(v-1)$-th roots of unity of $\mathbb{F}_q$ and 0 with $q \equiv 1 \pmod{v-1}$ admissible. These constructions are put in practice in the subsequent two sections where we find a 1-rotational $\mathrm{EA}(2^8)$-additive $(52, 4, 1)$-design which is also resolvable, and three pairwise non-isomorphic cyclic $\mathrm{EA}(3^5)$-additive $(121, 4, 1)$-designs, none of which is the point-line design of $\mathrm{PG}(4, 3)$. In the last section, we discuss the possible existence of cyclic $\mathrm{EA}(2^n)$-additive $(2^n-1, k, 1)$-designs. At the moment they are known to exist only when $k = 3$ (they come from Theorem 1.1 (ii)) and when $(n, k) = (13, 7)$ in view of Theorem 1.1 (iii). The least possible unknown case is $(n, k) = (9, 7)$: does there exist a cyclic $\mathrm{EA}(2^9)$-additive $(511, 7, 1)$-design? Unfortunately, we are still not able to answer this question. If it exists, however, it cannot be the 2-analog of a $(9, 3, 1)$-design. We prove this by means of two different approaches: the Kramer-Mesner method and a geometrical method.

2 Some general results

Here we give some general results on the $\mathrm{EA}(q)$-additive $(v, k, 1)$-designs starting with a useful restrictive condition on the possible prime powers q.

Theorem 2.1. *If there exists an* $\mathrm{EA}(q)$*-additive* $(v, k, 1)$ *design, then* q *is a power of a prime divisor of* $\frac{v-k}{k-1}$.

Proof. Recall that the number of blocks through any point of a $(v, k, 1)$-design is the constant $r := \frac{v-1}{k-1}$ known as the *replication number*. Let x be any point and let $B_1, \ldots, B_r$ be the blocks through x. Obviously, the singleton $\{x\}$ and the r sets $B_1 \setminus \{x\}, \ldots, B_r \setminus \{x\}$ form a partition of the point set. Considering that each B_i is zero-sum, the sum of all elements of $B_i \setminus \{x\}$ is equal to $-x$ for every i. Then the sum σ of all the points is equal to $x + r(-x) = (1-r)x$. Thus we have $\sigma = (1-r)x$ for every point x. It follows that $(1-r)(x-y) = 0$ for any pair of points x and y, hence the order of any difference of two points is a divisor of $r - 1 = \frac{v-k}{k-1}$. The assertion follows considering that the order of any non-zero element of $\mathbb{F}_q$ is the characteristic of $\mathbb{F}_q$. $\square$

The prime powers satisfying the condition of Theorem 2.1 for a given pair (v,k) will be said *admissible*.

It is known that a cyclic $(v,k,1)$-design has necessarily $v \equiv 1$ or $k \pmod{k(k-1)}$, whereas a 1-rotational $(v,k,1)$ design has necessarily $v \equiv k-1 \pmod{k(k-1)}$. In order to explain how to construct cyclic and 1-rotational Steiner 2-designs we need to recall the notion of a difference family.

Given a set $\mathcal{F} = \{B_1, \ldots, B_n\}$ of subsets of a group G, the *list of differences* of $\mathcal{F}$ is the multiset $\Delta\mathcal{F}$ consisting of all possible differences $x - y$ (if G is additive) or all possible ratios xy^{-1} (if G is multiplicative), with (x,y) an ordered pair of distinct elements from the same B_i.

Given a subgroup H of a group G, a (G,H,k,λ) *difference family* is a set of k-subsets (called *base blocks*) of G whose list of differences is precisely λ times the set $G \setminus H$ (see [8]).

Speaking of a *cyclic* $(G,k,1)$ *difference family* we will mean a $(G,H,k,1)$ difference family where G is a cyclic group of order $v \equiv 1$ or $k \pmod{k(k-1)}$ and H is the subgroup of G of order 1 or k, respectively.

Speaking of a 1-*rotational* $(G,k,1)$ *difference family* we will mean a $(G,H,k,1)$ difference family where G is a cyclic group of order $v \equiv k-1 \pmod{k(k-1)}$ and H is the subgroup of G of order $k-1$.

The above terminology is justified by the following well-known result.

Theorem 2.2. *The following facts hold.*

(i) Up to isomorphism, the cyclic $(v,k,1)$-designs with $v \equiv 1 \pmod{k(k-1)}$ are precisely those of the form $(G,\mathcal{B})$, where G is a cyclic group of order v and $\mathcal{B}$ is the set of all possible translates (under G) of the base blocks of a cyclic $(G,k,1)$ difference family.

(ii) Up to isomorphism, the cyclic $(v,k,1)$-designs with $v \equiv k \pmod{k(k-1)}$ are precisely those of the form $(G,\mathcal{B})$, where G is a cyclic group of order v and $\mathcal{B}$ is the set of all possible translates (under G) of the base blocks of a cyclic $(G,k,1)$ difference family and all possible cosets of the subgroup of G of order k.

(iii) Up to isomorphism, the 1-rotational $(v,k,1)$-designs are precisely those of the form $(G \cup \{\infty\},\mathcal{B})$, where G is a cyclic group of order $v-1$, ∞ is a symbol not in G, and $\mathcal{B}$ is the set of all possible translates (under G) of the

base blocks of a 1*-rotational* $(G, k, 1)$ *difference family and all possible sets of the form* $C \cup \{\infty\}$*, with* C *a coset of the subgroup of* G *of order* $k-1$.

From now on, $\mathbb{F}_q^*$ will denote the multiplicative group of $\mathbb{F}_q$. Also, if $q \equiv 1 \pmod{n}$, we denote by $R_{q,n}$ the subgroup of $\mathbb{F}_q^*$ of order n, that is the group of n-th roots of unity in $\mathbb{F}_q$.

The following theorems may be useful to find new additive Steiner 2-designs which are cyclic or 1-rotational.

Theorem 2.3. *Let* $q = nv+1$ *be a prime power and assume that there exists a cyclic* $(R_{q,v}, k, 1)$ *difference family whose base blocks are all zero-sum in* $\mathbb{F}_q$*. Then there exists an* $\mathrm{EA}(q)$*-additive* $(v, k, 1)$ *design.*

Proof. Let $\mathcal{F}$ be a difference family as in the assumption. Given that $R_{q,v}$ has order v, by the definition of a cyclic difference family we necessarily have $v \equiv 1$ or $k \pmod{k(k-1)}$.

Consider first the case $v \equiv 1 \pmod{k(k-1)}$. By Theorem 2.2(i), any block of the cyclic $(v, k, 1)$-design generated by $\mathcal{F}$ is of the form Bg with $B \in \mathcal{F}$ and $g \in R_{q,v}$. Then, considering that B is zero-sum in $\mathbb{F}_q$ by assumption, this block Bg is zero-sum as well.

Now consider the case $v \equiv k \pmod{k(k-1)}$. By Theorem 2.2(ii), any block of the cyclic $(v, k, 1)$-design generated by $\mathcal{F}$ is either of the form Bg with $B \in \mathcal{F}$ and $g \in R_{q,v}$, or of the form Hg with $H = R_{q,k}$ the subgroup of $R_{q,v}$ of order k and $g \in R_{q,v}$. Both Bg and Hg are zero-sum in $\mathbb{F}_q$ since B is zero-sum in $\mathbb{F}_q$ by assumption, and H is also zero-sum since it is known that any non-trivial subgroup of $\mathbb{F}_q^*$ is zero-sum.

Thus, in any case, all the blocks of the design generated by $\mathcal{F}$ are zero-sum and the assertion follows. □

Similarly, we have the following.

Theorem 2.4. *Let* $q = n(v-1)+1$ *be a prime power and assume that there exists a* 1*-rotational* $(R_{q,v-1}, k, 1)$ *difference family whose base blocks are all zero-sum in* $\mathbb{F}_q$*. Then there exists an* $\mathrm{EA}(q)$*-additive* $(v, k, 1)$*-design.*

Proof. Let $\mathcal{F}$ be a difference family as in the assumption. Given that $R_{q,v-1}$ has order $v-1$, by the definition of a 1-rotational difference family we necessarily have $v \equiv k-1 \pmod{k(k-1)}$.

Let us use $\mathcal{F}$ to construct a 1-rotational $(v, k, 1)$-design as indicated in Theorem 2.2(iii) by taking as extra point ∞ the zero of $\mathbb{F}_q$. Thus any block of this design is of the form Bg with $B \in \mathcal{F}$ and $g \in R_{q,v-1}$, or of the form $Hg \cup \{0\}$ with $H = R_{q,k-1}$ the subgroup of $R_{q,v-1}$ of order $k-1$ and $g \in R_{q,v-1}$. Reasoning as in Theorem 2.3, we see that this block is zero-sum in $\mathbb{F}_q$ and the assertion follows. □

It is obvious that Theorem 2.3 (resp. Theorem 2.4) may be useful only if we already know that a cyclic (resp. 1-rotational) $(v, k, 1)$-design exists.

In the affirmative case we have to take the prime powers $q \equiv 1 \pmod{v}$ or $\pmod{v-1}$, respectively, which are admissible according to Theorem 2.1. Anyway it may happen that no admissible prime power satisfies the required congruence. In this case we can exclude that the theorem leads to an additive $(v, k, 1)$ design. Here are two examples.

Example 2.5. It has been recently proved in [41] that there exists a cyclic $(v, 4, 1)$-design for any admissible v except 25 and 28. Thus, in particular, there exists a cyclic $(100, 4, 1)$-design. Assume that there exists an EA(q)-additive $(100, 4, 1)$-design for some prime power $q \equiv 1 \pmod{100}$. In this case, by Theorem 2.1, q must be a power of a prime divisor of $\frac{100-4}{4-1} = 2^5$, hence $q = 2^m$ for some m. On the other hand, it is obvious that there is no value of m for which the congruence $2^m \equiv 1 \pmod{100}$ holds.

We conclude that Theorem 2.3 cannot lead to any additive $(100, 4, 1)$-design.

Example 2.6. It is known that a cyclic $(105, 5, 1)$-design exists [1]. Assume that there exists an EA(q)-additive $(105, 5, 1)$-design for some prime power $q \equiv 1 \pmod{105}$. In this case, by Theorem 2.1, q must be a power of a prime divisor of $\frac{105-5}{5-1} = 5^2$, hence $q = 5^m$ for some m. On the other hand, it is obvious that there is no value of m for which the congruence $5^m \equiv 1 \pmod{105}$ holds.

Also here, Theorem 2.3 cannot be useful to find an additive $(105, 5, 1)$-design.

If, on the contrary, we have an admissible prime power $q = nv + 1$ (resp. $q = n(v-1) + 1$), we should make a computer search to establish whether a cyclic (resp. 1-rotational) $(R_{q,v}, k, 1)$ (resp. $(R_{q,v-1}, k, 1)$) difference family exists. Our experimental results seem to indicate that this search is usually heavy and that it succeeds very rarely. This is expected especially when q is much greater than v. Indeed, the larger is q with respect to v, the lesser is the number of candidates for the base blocks of the required difference family (recall indeed that they have to be zero-sum!).

Assume for instance that we want to construct an additive $(88, 4, 1)$-design using Theorem 2.4. It makes sense since it is known that there exists a 1-rotational $(v, 4, 1)$-design for any $v \equiv 4 \pmod{12}$ except $v = 28$ (see [42]). Here we have $\frac{v-k}{k-1} = \frac{88-4}{3} = 28$ so that, by Theorem 2.1, the admissible q must be powers of 2 or 7. Hence $q = 2^m$ or $q = 7^m$ some m. Recall, also, that Theorem 2.4 requires that $q \equiv 1 \pmod{87}$. The least m for which $2^m \equiv 1 \pmod{87}$ is 28, whereas the least m for which $7^m \equiv 1 \pmod{87}$ is 7. So, at this point, we should find a 1-rotational $(R_{87,q}, 4, 1)$ difference family whose base blocks are all zero-sum in $\mathbb{F}_q$ with either $q = 2^{28}$ or $q = 7^7$ which are both very large. In both cases, we have checked that $R_{87,q}$ does not even have one zero-sum subset of size 4.

3 An $\mathrm{EA}(2^8)$-additive 1-rotational and resolvable $(52,4,1)$-design

Assume that we want to construct an additive $(52,4,1)$-design. Given that 1-rotational $(52,4,1)$-designs exist, it makes sense trying to use Theorem 2.4. Here we have $v=52$ and $k=4$ so that $\frac{v-k}{k-1}=\frac{48}{3}=16$. Hence the admissible values of q must be powers of 2. The least power of 2 of the form $(v-1)n+1$ is $q=2^8$ which, fortunately, is not so large. We have to find a 1-rotational $(R_{q,51},4,1)$ difference family whose base blocks are all zero-sum in $\mathbb{F}_q$.

One can check that $p(x)=x^8+x^4+x^3+x^2+1$ is a primitive polynomial over $\mathbb{Z}_2$ so that we have $\mathbb{F}_q=\mathbb{Z}_2[x]/(p(x))$ and x is a primitive element of $\mathbb{F}_q$. Given that $2^8=51\cdot 5+1$, the group $R_{q,51}$ can be viewed as the group of non-zero 5th powers of $\mathbb{F}_q$. Hence $g:=x^5$ is a generator of $R_{q,51}$ and it is easy to check that the desired difference family is $\mathcal{F}=\{B_1,B_2,B_3,B_4\}$ with

$$B_1=\{g,g^{12},g^{16},g^{39}\};\quad B_2=\{g^3,g^4,g^{13},g^{48}\};$$
$$B_3=\{g^6,g^8,g^{26},g^{45}\};\quad B_4=\{g^7,g^{10},g^{15},g^{36}\}.$$

The above 1-rotational difference family $\mathcal{F}$ has the very special property to be *resolvable* (see [17]). It essentially means that the design generated by $\mathcal{F}$ is resolvable. Its resolution is $\{g^h\mathcal{P}_0 \mid 0\leq h\leq 16\}$ with

$$\mathcal{P}_0=\{g^{17i}B_j \mid 0\leq i\leq 2; 1\leq j\leq 4\}\ \cup\ \{B_0\}$$

where $B_0=\{0,1,g^{17},g^{34}\}$. Thus we can state the following.

Theorem 3.1. *There exists an additive* $(52,4,1)$*-design that is both* 1*-rotational and resolvable.*

This design, together with the additive $(124,4,1)$-design constructed in [11] is, up to now, the only known handy example of a Steiner 2-design whose parameters are not "geometric", namely neither of the form $(q^n,q,1)$, nor of the form $(\frac{q^n-1}{q-1},\frac{q^k-1}{q-1},1)$.

Yet, the above constructed design has something geometric anyway. Indeed we have discovered that it is isomorphic to the 1-rotational resolvable $(52,4,1)$-design in [28] which is proved to be embeddable in the desarguesian projective plane of order 16.

It may be interesting to know that we established their isomorphism by checking that they both have 2-*rank* 41 whereas the 2-rank of any other 1-rotational resolvable $(52,4,1)$ design is either 51 or 49. We recall that there are precisely twenty-two 1-rotational resolvable $(52,4,1)$ designs; they have been explicitly given in [18].

4 Three new $\mathrm{EA}(3^5)$-additive $(121,4,1)$-designs

It is well-known that the point-line incidence structure associated with the projective space $\mathrm{PG}(n-1,q)$ is a $(\frac{q^n-1}{q-1}, q+1, 1)$-design. As recalled in the introduction, it has been proved that this design is $\mathrm{EA}(q^n)$-additive.

On the other hand, it is possible that Theorem 2.3 may lead to at least two non-isomorphic additive designs with parameters $(\frac{q^n-1}{q-1}, q+1, 1)$. We verified this for $q=3$ and $n=5$.

Theorem 4.1. *There exist at least four pairwise non-isomorphic* $\mathrm{EA}(3^5)$-*additive* $(121,4,1)$-*designs.*

Proof. Given that $(121,4,1)$ are the parameters of the point-line design associated with $\mathrm{PG}(4,3)$, we already know that there is at least one additive design with these parameters. We now investigate whether other additive $(121,4,1)$-designs can be obtained via Theorem 2.3. Here we have $v=121$ and $k=4$ so that $\frac{v-k}{k-1} = \frac{117}{3} = 39$. Hence, the admissible values of q are the powers of 3 or 13. The least power of 3 of the form $vn+1$ is $q=3^5$.

For applying Theorem 2.3 we have to find a cyclic $(R_{q,121},4,1)$ difference family whose base blocks are all zero-sum in $\mathbb{F}_q$. We are going to describe four of these difference families.

One can check that $p(x) = x^5+2x+1$ is a primitive polynomial over $\mathbb{Z}_3$ so that we can write $\mathbb{F}_q = \mathbb{Z}_3[x]/(p(x))$ and x is a primitive element of $\mathbb{F}_q$. Given that $3^5 = 121\cdot 2+1$, the group $R_{q,121}$ can be viewed as the group of non-zero squares of $\mathbb{F}_{121}$. Hence $g := x^2$ is a generator of $R_{q,121}$.

Consider the 4-subsets of $R_{q,121}$

$$A_1 = \{1, g, g^5, g^{69}\}, \quad A_2 = \{1, g, g^{21}, g^{55}\},$$

$$A_3 = \{1, g, g^{52}, g^{93}\}, \quad A_4 = \{1, g, g^{65}, g^{78}\},$$

$$B_1 = \{1, g^2, g^{46}, g^{74}\}, \quad B_2 = \{1, g^4, g^{79}, g^{95}\},$$

$$B_3 = \{1, g^4, g^{15}, g^{78}\}, \quad B_4 = \{1, g^2, g^{25}, g^{116}\},$$

and set, for $1 \le i \le 4$,

$$\mathcal{F}_i = \{g^{3^j} A_i, g^{3^j} B_i \mid 0 \le j \le 4\}.$$

One can check that each $\mathcal{F}_i$ is a cyclic $(R_{q,121},4,1)$ difference family whose base blocks are zero-sum in $\mathbb{F}_q$. Using GAP [27] we also checked that the designs generated by them are pairwise non-isomorphic. In particular, the design generated by $\mathcal{F}_1$ is the point-line design associated with $\mathrm{PG}(4,3)$. $\square$

5 On the possible existence of an additive $(511, 7, 1)$-design

As a special case of Theorem 2.3 we have the following.

Corollary 5.1. *If there exists a cyclic* $(\mathbb{F}_{2^v}^*, k, 1)$ *difference family whose base blocks are all zero-sum in* $\mathbb{F}_{2^v}$*, then there exists an* $\mathrm{EA}(2^v)$*-additive* $(2^v - 1, k, 1)$*-design.*

By interpreting $\mathbb{F}_{2^v}$ as the v-dimensional vector space over $\mathbb{Z}_2$, the set of points of $\mathrm{PG}(v-1, 2)$ is $\mathbb{F}_{2^v}^*$, whereas the $(k-1)$-dimensional subspaces of $\mathrm{PG}(v-1, 2)$ are the $(2^k - 1)$-subsets of $\mathbb{F}_{2^v}^*$ which, together with the zero vector, form a k-dimensional subspace of $\mathbb{F}_{2^v}$. We have the following remarkable variant of Corollary 5.1, which can be deduced from Theorem 6.4 in [15]. We prove it anyway along the lines of Theorem 2.3 for the convenience of the reader.

Theorem 5.2. *If there exists a cyclic* $(\mathbb{F}_{2^v}^*, 2^k - 1, 1)$ *difference family whose base blocks are all* $(k-1)$*-dimensional subspaces of* $\mathrm{PG}(v-1, 2)$*, then there exists the* 2*-analog of a* $(v, k, 1)$*-design.*

Proof. Let $\mathcal{F}$ be a difference family as in the assumption. By Theorem 2.2, any block of the cyclic $(2^v - 1, 2^k - 1, 1)$-design generated by $\mathcal{F}$ is of the form Bg with $B \in \mathcal{F}$ and $g \in \mathbb{F}_{2^v}^*$ or, possibly, a coset of the subgroup of $\mathbb{F}_{2^v}^*$ of order $2^k - 1$ in the case that k is a divisor of v. The fact that B is a $(k-1)$-dimensional subspace of $\mathrm{PG}(v-1, 2)$ easily implies that the block Bg has the same property. Also note that when k divides v every coset of the subgroup of $\mathbb{F}_{2^v}^*$ of order $2^k - 1$ is also a $(k-1)$-dimensional subspace of $\mathrm{PG}(v-1, 2)$.

Thus, all the blocks of the design generated by $\mathcal{F}$ are $(k-1)$-dimensional subspaces of $\mathrm{PG}(v-1, 2)$ and the assertion follows. □

The parameters of the additive designs with less than 100,000 points which are potentially obtainable from Corollary 5.1 are only the following:

$$(127, 7, 1),\ (511, 6, 1),\ (511, 7, 1),\ (8191, 6, 1),\ (8191, 7, 1),\ (8191, 10, 1).$$

Among them, the 2-analogs which are potentially obtainable from Theorem 5.2 have parameters

$$(127, 7, 1), \quad (511, 7, 1), \quad (8191, 7, 1).$$

They would be 2-analogs of a $(v, 3, 1)$ design with $v = 7, 9$ and 13, respectively.

As a matter of fact the existence of a $(127, 7, 1)$-design is not known even without any special requisite. Also, it has been proved that the automorphism group of a putative 2-analog of a $(7, 3, 1)$-design has order at most

2 (see [2, 31]) so that Theorem 5.2 cannot lead to such a 2-analog. The 2-analog of a $(13, 3, 1)$-design has been constructed in [5] with the implicit use of Theorem 5.2.

Given that cyclic $(511, 7, 1)$-designs exist (see Theorem 3.1 in [9]), it makes sense to try using Theorem 2.3. For now, however, an exhaustive computer search with the only use of this theorem seems to be unfeasible.

Unfortunately, Theorem 5.2 does not lead to any 2-analog of a $(9, 3, 1)$-design. Hence, we obtain the following result.

Theorem 5.3. *A putative* 2*-analog of a* $(9, 3, 1)$*-design cannot be cyclic.*

This will be proved by means of two different approaches in the next subsections.

5.1 Proof of Theorem 5.3 via Kramer-Mesner method

A straightforward approach to the construction of a $(v, k, 1)$-design $(V, \mathcal{B})$ is to consider the matrix

$$M_k^v := (m_{i,j}), \quad i = 1, \ldots, \binom{v}{2}, \ j = 1, \ldots, \binom{v}{k},$$

where the rows of M_k^v are indexed by the set $\binom{V}{2}$ of all 2-subsets of V and the columns by the set $\binom{V}{k}$ of all k-subsets of V. If the i-th 2-subset is contained in the j-th k-subset, $m_{i,j} = 1$, otherwise $m_{i,j} = 0$. Then, a $(v, k, 1)$-design corresponds to $\{0, 1\}$-solutions x of the system of linear equations

$$M_k^v \cdot x = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

over the rationals. In computer science, the above linear system is known as *exact cover problem*, see [32], and is well-known to be NP-hard.

For the most interesting parameters v, k, the size of the matrix M_k^v will be prohibitively large and even the fastest computers available are not able to solve these systems of $\binom{v}{2}$ linear equations.

However, by assuming a group action on V, sometimes the size of M_k^v can be dramatically reduced. A group G acting on V induces also an action on $\binom{V}{2}$ and $\binom{V}{k}$. Now, $M_k^G = (m_{i,j})$ denotes the matrix where m_{ij} counts how often a representative of the i-th orbit on $\binom{V}{2}$ is contained in the j-th orbit on $\binom{V}{k}$. Kramer and Mesner observed the following.

Theorem 5.4. *([35]) A* $(v, k, 1)$*-design with an automorphism group* G *exists if and only if there is a* $\{0, 1\}$*-solution* x *to the linear system of equations*

$$M_k^G \cdot x = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

over the rationals.

The matrix M_k^G is now called Kramer-Mesner matrix, since it was first introduced formally by Kramer and Mesner in [35], albeit this approach had been used implicitly by others before.

The same approach can be applied to search for q-analogs of $(v, k, 1)$-designs. That is, we search for a q-analog of a $(v, k, 1)$-design having a given group $G \leq \mathrm{PGL}(v, q)$ as a group of automorphisms. Instead of orbits on 2-subsets and k-subsets, G-orbits on 2-dimensional subspaces and k-dimensional subspaces have to be considered, see [3, 4] for the full details and results.

Analog to classic designs, the set of blocks of a q-analog of a $(v, k, 1)$-design with an automorphism group $G \leq \mathrm{PGL}(v, q)$, would be the union of orbits of k-dimensional subspaces under the action of G. Now, the Kramer-Mesner matrix M_k^G carries the information, how many elements of the orbit K^G for a given k-dimensional subspace $K \leq \mathbb{F}_q^v$ contain a given 2-dimensional subspace $T \leq \mathbb{F}_q^v$.

The q-analog version of Theorem 5.4 by Kramer and Mesner is that a q-analog of a $(v, k, 1)$-design with an automorphism group G exists if and only if there is a $\{0, 1\}$-solution x of the system of linear equations

$$M_k^G \cdot x = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$$

over the rationals.

In the special case of a *cyclic* 2-analog of a $(9, 3, 1)$-design, the set of blocks would be the union of orbits of 3-dimensional subspaces of $\mathbb{F}_2^9$ under the action of the cyclic group $G = \mathbb{F}_{2^9}^*$ (a Singer cycle) of order 511.

The action of G partitions the 43 435 2-dimensional subspaces into 85 orbits, all of size 511. Similarly, the 788 035 3-dimensional subspaces are partitioned by G into 1543 orbits, where one orbit is of size 73 and all the others are of size 511.

Among the 1543 orbits on 3-dimensional subspaces, 1459 might be used for the construction of a putative 2-analog of a $(9, 3, 1)$ design. The other orbits are incompatible and can be ignored because at least one of the 2-dimensional subspaces is already contained in more than one of their orbit members, i.e., the corresponding column of the Kramer-Mesner matrix would have an entry larger than one.

In a straightforward Python implementation of the last author, the construction of the Kramer-Mesner matrix M_3^G for a putative 2-analog of a $(9, 3, 1)$-design takes 33 seconds (using `pypy3`). The exhaustive enumeration of all solutions of the resulting linear system needs approximately 20 seconds using either one of the exact cover algorithms by Knuth [32, 33], implemented by him in C. The computation shows that a putative 2-analog of a $(9,3,1)$-design cannot be cyclic.

The computations were performed on an Intel(R) Xeon(R) E-2288G CPU (3.70GHz) running Linux, Debian 13.

We do not claim that we are the first to show with the Kramer-Mesner approach that a 2-analog of a $(9,3,1)$-design cannot be cyclic. The same group and design parameters had already been tested by the authors of [5] after their construction of a 2-analog of a $(13,3,1)$-design. However, apparently this negative result was never published.

5.2 Proof of Theorem 5.3 via some geometric arguments

Let $\mathcal{D}=(V,\mathcal{B})$ be the 2-analog of the point-line design of $\mathrm{AG}(2,3)$. Then V coincides with the point-set of $\mathrm{PG}(8,2)$ and $\mathcal{B}$ consists of some suitable copies of $\mathrm{PG}(2,2)$. Here, we assume that $\mathcal{D}$ admits $G\cong\mathbb{Z}_{511}$ as a point-regular automorphism group. Therefore, G is a Singer subgroup of $\mathrm{PGL}(9,2)$, and hence G preserves a unique Desarguesian 2-spread Σ of $\mathrm{PG}(8,2)$, namely a set of 73 pairwise disjoint planes of $\mathrm{PG}(8,2)$, by [25, Lemma 2.1]. Thus, G preserves a copy of the plane $\mathrm{PG}(2,8)$, where the points are the elements of Σ and the lines are the 5-dimensional subspaces of $\mathrm{PG}(8,2)$ generated by any two elements of Σ. In particular, G acts on $\mathrm{PG}(2,8)$ in a natural way inducing $W\cong\mathbb{Z}_{73}$ on it.

Let B be any block of $\mathcal{D}$ such that $B\notin\Sigma$, then $|B\cap X|\leq 1$ for any $X\in\Sigma$ since $\lambda=1$ and X is also a block of $\mathcal{D}$. Therefore, the incidence structure π_B, whose point-set consists of the 7 elements of Σ intersecting B in a point and whose block-set consists of the intersections of B with any 5-dimensional subspace of $\mathrm{PG}(8,2)$ generated by two elements of Σ, is an isomorphic copy of $\mathrm{PG}(2,2)$ naturally embedded in $\mathrm{PG}(2,8)$.

Lemma 5.5. *Let $\mathcal{D}'=(V',\mathcal{B}')$, where V' is the point-set of* $\mathrm{PG}(2,8)$ *and $\mathcal{B}'=\{\pi_B\mid B\in\mathcal{B}\setminus\Sigma\}$. Then the following hold:*

1. *$\mathcal{D}'=(V',\mathcal{B}')$ is a 2-$(73,7,7)$ design admitting W as a point-regular automorphism group;*
2. *$\mathcal{B}'$ consists of 12 orbits under W.*

Proof. It follows from its definition that $\mathcal{D}'$ has $v'=73$ points, and each block of $\mathcal{D}'$ has $k'=7$ points. Clearly, $\pi_{B'}=\pi_B$ for each $B'\in B^C$, where C is the subgroup of order 7 of G. Conversely, suppose that $\pi_{B'}=\pi_B$. Let $X_i\in\Sigma$, $i=1,\ldots,7$, be such that $|B\cap X_i|=1$. Then $|B'\cap X_i|=1$ for each $i=1,\ldots,7$. Hence, $\{X_1,X_2,\ldots,X_7\}$ and B^C are the two systems of a Segre variety $\mathcal{S}_{2,2}$ of $\mathrm{PG}(8,2)$, by [29, Section 25.5]. Therefore, $B'\in B^C$ by [29, Theorem 25.5.11], since $\pi B'=\pi_B$. Thus, $\pi_{B'}=\pi_B$ if and only if $B'\in B^C$.

Let X, Y be any two distinct points of $\mathcal{D}'$. Then they correspond to two disjoint copies of $\mathrm{PG}(2,2)$ inside $\mathrm{PG}(8,2)$. Now, for any $x \in X$ and $y \in Y$, there exists a unique block B of $\mathcal{D}$ containing them, since $\mathcal{D}$ is a 2-design with $\lambda = 1$. Moreover, $B \cap X = \{x\}$ and $B \cap Y = \{y\}$. Therefore, the number of blocks intersecting X and Y in a point is 49.

On the other hand, each element of $(B')^C$ intersects X and Y in a point, and these correspond to the same element $\pi_{B'}$ of $\mathcal{B}'$. Thus, the number of blocks of $\mathcal{D}'$ intersecting X and Y is precisely 7. Hence, $\mathcal{D}'$ is a 2-$(73,7,7)$ design.

Clearly, W is a point-regular automorphism group of $\mathcal{D}'$, and we obtain (1). Furthermore, $W \cong \mathbb{Z}_{73}$ acts semiregularly on $\mathcal{B}'$. Hence, (2) holds true since

$$|\mathcal{B}'| = \frac{|\mathcal{B}| - |\Sigma|}{7} = \frac{6205 - 73}{7} = 876 = 12 \cdot 73.$$

□

Lemma 5.6. *If $\pi, \pi' \in \mathcal{B}'$ are such $\pi \cap \ell = \pi' \cap \ell$ with $|\pi \cap \ell| = 3$, then $\pi = \pi'$.*

Proof. Let $\pi, \pi' \in \mathcal{B}'$ be such that $\pi \cap \ell = \pi' \cap \ell$ with $|\pi \cap \ell| = 3$. Then there exist two blocks of $\mathcal{D}$, say $B = \langle e_1, e_2, e_3 \rangle^*$ and $B' = \langle e_1', e_2', e_3' \rangle^*$, with

$$B \cap \langle e_i \rangle_{\mathbb{F}_8}^* = \langle e_i \rangle_{\mathbb{F}_2}^*, \quad B \cap \langle e_1 + e_2 \rangle_{\mathbb{F}_8}^* = \langle e_1 + e_2 \rangle_{\mathbb{F}_2}^*,$$

and

$$B' \cap \langle e_i \rangle_{\mathbb{F}_8}^* = \langle e_i' \rangle_{\mathbb{F}_2}^*, \quad B' \cap \langle e_1 + e_2 \rangle_{\mathbb{F}_8}^* = \langle e_1' + e_2' \rangle_{\mathbb{F}_2}^*.$$

Then there exist integers i, j, h such that

$$e_1' = e_1^{\varphi^i}, \quad e_2' = e_2^{\varphi^j}, \quad e_1' + e_2' = (e_1 + e_2)^{\varphi^h},$$

where $\langle \varphi \rangle = C$, since $\langle e_1 \rangle_{\mathbb{F}_8}^*$, $\langle e_2 \rangle_{\mathbb{F}_8}^*$, and $\langle e_1 + e_2 \rangle_{\mathbb{F}_8}^*$ are distinct C-orbits.

Then $e_1^{\varphi^i} + e_2^{\varphi^j} = e_1^{\varphi^h} + e_2^{\varphi^h}$, since φ is linear, and hence

$$e_1^{\varphi^{i-h}} + e_1 = e_2^{\varphi^{j-h}} + e_2,$$

which forces $\langle e_1 \rangle_{\mathbb{F}_8}^* = \langle e_2 \rangle_{\mathbb{F}_8}^*$, whereas $\langle e_1 \rangle_{\mathbb{F}_8}^*$ and $\langle e_2 \rangle_{\mathbb{F}_8}^*$ are distinct C-orbits. Therefore $h = i = j$, and hence $\{e_1', e_2'\} \subset B' \cap B^{\varphi^h}$.

Then $B^{\varphi^h} = B'$, since $\mathcal{D}$ is a 2-design with $\lambda = 1$, and so $\pi = \pi'$.

□

Definition 5.7. Let ℓ be any line of $\mathrm{PG}(2,8)$ and $\mathcal{O}$ be any block-W-orbit of $\mathcal{D}'$. The set

$$I(\mathcal{O}, \ell) = \{\pi \cap \ell \mid |\pi \cap \ell| = 3, \, \pi \in \mathcal{O}\}$$

is called the *imprint of* $\mathcal{O}$ on ℓ.

Corollary 5.8. *Let ℓ be any line of* $\mathrm{PG}(2,8)$ *and $\mathcal{O}$ be any block-W-orbit of $\mathcal{D}'$. Then $|I(\mathcal{O},\ell)| = 7$.*

Proof. The incidence structure $(\mathcal{O},\mathcal{B})$, with incidence relation given by the pairs $(\pi, m) \in \mathcal{O} \times \mathcal{B}$ such that $|\pi \cap m| = 3$, is a symmetric 1-design by [24, 1.2.6], since both $\mathcal{O}$ and $\mathcal{B}$ are W-orbits of size 73. Hence,

$$|\{\pi \mid |\pi \cap \ell| = 3,\ \pi \in \mathcal{O}\}| = 7,$$

since the number of lines of $\mathrm{PG}(2,8)$ secant to π is 7.

If $|I(\mathcal{O},\ell)| < 7$, then there exist $\pi_1, \pi_2 \in I(\mathcal{O},\ell)$ such that $\pi_1 \cap \ell = \pi_2 \cap \ell$ with $|\pi_1 \cap \ell| = 3$, and hence $\pi_1 = \pi_2$ by Lemma 5.6. Therefore,

$$7 \leq |I(\mathcal{O},\ell)| \leq |\{\pi \mid |\pi \cap \ell| = 3,\ \pi \in \mathcal{O}\}| = 7,$$

and hence $|I(\mathcal{O},\ell)| = 7$. $\square$

Definition 5.9. Let ℓ be any line of $\mathrm{PG}(2,8)$. A family $\mathcal{F}$ of copies of $\mathrm{PG}(2,2)$ provides a *perfect cover of ℓ* if

$$\{\pi \cap \ell \mid |\pi \cap \ell| = 3, \pi \in \mathcal{F}\}$$

is the set of all sublines $\mathrm{PG}(1,2)$ of ℓ.

Theorem 5.10. *Let $\mathcal{O}_j$, $j = 1,\ldots,12$, be the W-orbits on $\mathcal{B}'$. For each line ℓ of* $\mathrm{PG}(2,8)$*, the set*

$$\bigcup_{j=1}^{12} I(\mathcal{O}_j,\ell)$$

provides a perfect cover of ℓ.

Proof. It follows from Corollary 5.8 that $|I(\mathcal{O}_j,\ell)| = 7$ for each $j = 1,\ldots,12$. Therefore,

$$\left|\bigcup_{j=1}^{12} I(\mathcal{O}_j,\ell)\right| \leq 84.$$

If $I(\mathcal{O}_{j_1},\ell) \cap I(\mathcal{O}_{j_2},\ell) \neq \emptyset$ for some distinct $1 \leq j_1, j_2 \leq 12$, then there exist $\pi_1 \in \mathcal{O}_{j_1}$ and $\pi_2 \in \mathcal{O}_{j_2}$ with $|\pi_1 \cap \ell| = 3$ such that $\pi_1 \cap \ell = \pi_2 \cap \ell$. Hence, $\pi_1 = \pi_2$ by Lemma 5.6, so $\mathcal{O}_{j_1} = \mathcal{O}_{j_2}$, which is a contradiction since these are distinct W-orbits.

Thus, the sets $I(\mathcal{O}_j,\ell)$ are pairwise disjoint, and hence

$$\left|\bigcup_{j=1}^{12} I(\mathcal{O}_j,\ell)\right| = 84.$$

On the other hand, the set of all sublines $\mathrm{PG}(1,2)$ of ℓ has size $|\mathrm{PSL}_2(8) : \mathrm{PSL}_2(2)| = 84$, and hence $\bigcup_{j=1}^{12} I(\mathcal{O}_j,\ell)$ provides a perfect cover of ℓ. $\square$

We implemented an algorithm that uses Theorem 5.10 to show the non-existence of $\mathcal{D}'$ and hence it provides a proof of Theorem 5.3. We operate as follows.

5.2.1 Description of the algorithm

This algorithm tests whether there exist twelve distinct orbits $\mathcal{O}_i$ of blocks in $\mathrm{PG}(2,8)$ under the action of the group $W \cong \mathbb{Z}_{73}$ such that their imprints $I(\mathcal{O}_i, \ell)$ on a fixed line ℓ are pairwise disjoint.

The procedure has two phases. Phase A constructs $n \leq 7$ such orbits; Phase B searches for the remaining $12-n$, if they exist. The entire algorithm has been implemented and executed using a Python program.

• **Phase A:** We first fix the line $\ell = \{1, 2, 35, 37, 42, 45, 47, 54, 63\}$ and its seven 3-point *sublines* s_i of the form $\{1, 2, x\}$, for $i = 1, \ldots, 7$. All orbits are precomputed (via GAP [27]) and loaded from disk. For each orbit $\mathcal{O}$ we compute its imprint on ℓ, thereby forming a list L of pairs $(\mathcal{O}, I(\mathcal{O}, \ell))$. We then define 7 new lists as follows:

$$L_i = \left\{ \big(\mathcal{O}, I(\mathcal{O}, \ell)\big) \in L \;\middle|\; s_i \in I(\mathcal{O}, \ell) \right\}, \qquad i = 1, \ldots, 7.$$

Each L_i has 105 elements (clearly, the L_i's are not mutually disjoint). We iterate over L_1 with an outer for-loop, fixing an element $(\mathcal{O}_1, I_1) \in L_1$. The goal is to filter the remaining sets $L_2, \ldots, L_7$ to those orbits whose imprints are disjoint from I_1. Proceeding in the fixed order $L_2, L_3, \ldots$ may prematurely eliminate feasible solutions: a priori we do not know whether a supposed solution present, for example, s_1 and s_2 in the imprint of the same orbit. If this happen, then L_2 filtered by disjointness from I_1 will be empty and the loop would stop without further exploring this option.

Therefore, after fixing $(\mathcal{O}_1, I_1)$ we filter *each* of $L_2, \ldots, L_7$, producing six lists

$$\left\{ \big(\mathcal{O}, I(\mathcal{O}, \ell)\big) \in L_i \;\middle|\; I(\mathcal{O}, \ell) \cap I_1 = \emptyset \right\}, \qquad i = 2, \ldots, 7.$$

Among these we select the one of maximum size and call it L'_2; we denote by i_2 the index from which it originates (i.e., L'_2 is L_{i_2} filtered). If two different lists have maximum size, then we fix the first one encountered.

If $L'_2 \neq \emptyset$, we iterate over $(\mathcal{O}_2, I_2) \in L'_2$. Next, for the remaining five lists with $i \in \{2, \ldots, 7\} \setminus \{i_2\}$ we filter by disjointness from both I_1 and I_2,

$$\left\{ \big(\mathcal{O}, I(\mathcal{O}, \ell)\big) \in L_i \;\middle|\; I(\mathcal{O}, \ell) \cap I_j = \emptyset,\ j = 1, 2 \right\},$$

and select the largest filtered list L'_3 with its index i_3.

If $L'_3 \neq \emptyset$, we fix $(\mathcal{O}_3, I_3) \in L'_3$ and repeat.

At step k, we iterate $(\mathcal{O}_k, I_k) \in L'_k$. For the remaining $7-k$ lists with $i \in \{2, \ldots, 7\} \setminus \{i_2, i_3, \ldots, i_k\}$, we filter by disjointness from all I_1, I_2,..., I_k, creating the following new lists:

$$\left\{ \big(\mathcal{O}, I(\mathcal{O}, \ell)\big) \in L_i \;\middle|\; I(\mathcal{O}, \ell) \cap I_j = \emptyset,\ j = 1, 2, \ldots, k \right\},$$

We select the largest filtered list L'_{k+1} with its index i_{k+1}. If $L'_{k+1} \neq \emptyset$, we fix $(\mathcal{O}_{k+1}, I_{k+1}) \in L'_{k+1}$ and repeat.

Two outcomes are possible: either we reach $k = 7$ or the current maximal filtered list L'_n is empty (and hence all other filtered lists are empty, since L'_n has maximal cardinality). In the first case, each s_i lies in a different imprint I_j. In the second case, at least two sublines s_i, s_j appear in the same imprint. In both cases, the sublines $s_1, \ldots, s_7$ have been covered as required.

• **Phase B:** We then call a subroutine that attempts to build the remaining $12 - n$ orbits. Its input is a partial family $\{(\mathcal{O}_1, I_1), \ldots, (\mathcal{O}_n, I_n)\}$ of already constructed orbits and their imprints.

The subroutine proceeds as follows. First, it forms $L_{\text{partial}} \subseteq L$, consisting of all pairs $(\mathcal{O}, I(\mathcal{O}, \ell))$ whose imprints are disjoint from every I_i, $1 \leq i \leq n$. If $|L_{\text{partial}}|$ is strictly smaller than the number of orbits still required to reach 12, the subroutine terminates immediately (pruning the branch).

Otherwise, it performs a depth-first search using an explicit stack. Each stack level corresponds to selecting a new orbit, so at level k the algorithm has chosen $n + k + 1$ orbits (the search starts at level 0). At each step:

1. the current candidate list is scanned sequentially;

2. if the next candidate $(\mathcal{O}, I(\mathcal{O}, \ell))$ is *valid* (namely, the filtered list obtained by enforcing disjointness has cardinality greater than or equal to the number of orbits still required to reach 12) it is pushed on the stack together with its updated disjoint candidate list;

3. if no viable candidates remain, the algorithm backtracks to the previous level and continues with the next unexplored element.

If the depth reaches $11 - n$, a complete configuration of twelve orbits is found; the solution is written to file and the program terminates. This subroutine guarantees exhaustive exploration, while the pruning rule discards unpromising branches as early as possible. The explicit stack avoids deep recursion and keeps the search efficient and memory-safe.

If, for every partial family $\mathcal{O} = \{(\mathcal{O}_1, I_1), \ldots, (\mathcal{O}_n, I_n)\}$ generated by Phase A, Phase B never reaches twelve orbits, the program ends and reports that no solution was found.

5.3 Computational platform and runtime.

All computations were performed on a MacBook Air (13.6-inch, 2022) equipped with an Apple M2 processor (8-core CPU, 8-core GPU), 8 GB of unified memory, and a 512 GB SSD, running macOS Sequoia.

The algorithm completed the exhaustive search in approximately 7-8 hours of time. No complete solution was found within this runtime, which provides a proof for the non-existence of the desired design.

Acknowledgments

The first, second, and third author thank the Italian National Group for Algebraic and Geometric Structures and their Applications (GNSAGA-INdAM) for its support to their research.

References

[1] R.J.R. Abel, M. Buratti, *Difference families.* Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 392–410.

[2] M. Braun, M. Kiermaier, A. Nakic, *On the automorphism group of a binary q-analog of the Fano plane*, European Journal of Combinatorics **51**, 443–457 (2016).

[3] M. Braun, M. Kiermaier, A. Wassermann, *Computational methods in subspace designs*, In: Network Coding and Subspace Designs, Signals and Communication Technology, 213–244, Springer, (2018).

[4] M. Braun, M. Kiermaier, A. Wassermann, *q-analogs of designs: Subspace designs*, In: Network Coding and Subspace Designs, Signals and Communication Technology, 171–211, Springer, (2018).

[5] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy, A. Wassermann, *On the Existence of q-Analogs of Steiner Systems.* Forum of Mathematics, PI, 4 (2016).

[6] D. Bryant, C.J. Colbourn, D. Horsley, I.M. Wanless, *Steiner triple systems with high chromatic index*, SIAM J. Discrete Math. **31** (2017), 2603–2611.

[7] D. Bryant, D. Horsley, *A second infinite family of Steiner triple systems without almost parallel classes*, J. Comb. Theory Ser. A **120** (2013), 1851–1854.

[8] M. Buratti, *Recursive constructions for difference matrices and relative difference families*, J. Combin. Des. **6**, 165–182 (1998).

[9] M. Buratti, *Cyclotomic conditions leading to new Steiner* 2*-designs*, Finite Fields Appl. **3**, 300–313 (1997).

[10] M. Buratti, F. Martinovic, A. Nakic, $(27, 6, 5)$ *designs with a nice automorphism group*, Australas. J. Combin. **92**, 80–95 (2025).

[11] M. Buratti, F. Merola, A. Nakic, *Additive combinatorial designs*, Des. Codes Cryptogr. **93**, 2717–2740 (2025).

[12] M. Buratti, A. Nakic, *Designs over finite fields by difference methods*, Finite Fields Appl. **57**, 128–138 (2019).

[13] M. Buratti, A. Nakic, *Super-regular Steiner* 2*-designs*, Finite Fields Appl. **85**, Article number 102116 (2023).

[14] M. Buratti, A. Nakic, *Additivity of symmetric and subspace* 2*-designs*, Des. Codes Cryptogr. **92**, 3561–3572 (2024).

[15] M. Buratti, A. Nakic, A. Wassermann, *Graph decompositions over projective geometries*, J. Combin. Des. 29, 149–174 (2021).

[16] M. Buratti, A. Pasotti, *Heffter spaces*, Finite Fields Appl. **98**, Article number 102464 (2024).

[17] M. Buratti, F. Zuanni, *G-invariantly resolvable Steiner* 2*-designs which are* 1*-rotational over G*, Bull. Belg. Math. Soc. **5** (1998), 221–235.

[18] M. Buratti, F. Zuanni, *The* 1*-rotational* $(52, 4, 1)$*-RBIBD's*, J. Combin. Math. Combin. Comput. **30**, 99–102 (1999).

[19] A. Caggegi, *A new family of additive designs*, Ars. Math. Contemp. **23**, P2.07 (2023).

[20] A. Caggegi, G. Falcone, *On* 2-$(n^2, 2n, 2n-1)$ *designs with three intersection numbers*, Des. Codes Crypt. **43**, 33–40 (2007).

[21] A. Caggegi, G. Falcone, M. Pavone, *On the additivity of block designs*, J. Algebr. Comb. **45**, 271–294 (2017).

[22] A. Caggegi, G. Falcone, M. Pavone, *Additivity of affine designs*, J. Algebr. Comb. **53**, 755–770 (2012).

[23] S. Cichacz, *Zero sum partition into sets of the same order and its applications*, Electron. J. Combin. **25** (2018), ♯P1.20.

[24] P. Dembowski, *Finite Geometries*, Springer, Berlin, Heidelberg, New York, 1968.

[25] K. Drudge, *On the orbits of Singer groups and their subgroups*, Electron. J. Combin. **9**, 1, Research Paper 15, pp. 10 (2002).

[26] J. Egan, I.M. Wanless, *Latin Squares with Restricted Transversals*, J. Combin. Des. **20** (2012), 344–361.

[27] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.4.12, (2008).

[28] Z.S. Huerta, V. Tonchev, M. Keranen, *On projective planes of order* 16 *associated with* 1*-rotational* 2-$(52, 4, 1)$ *designs*, https://arxiv.org/abs/2403.03189

[29] J.W.P. Hirschfeld, J.A. Thas, *General Galois Geometries*. Oxford University Press, Oxford (1991).

[30] P. Keevash, *The existence of designs*. Preprint, arXiv:1401.3665.

[31] M. Kiermaier, S. Kurz, A. Wassermann, *The order of the automorphism group of a binary q-analog of the Fano plane is at most two*, Des. Codes Cryptogr. **86**, 239–250 (2018)

[32] Knuth, D.E.: Introduction to Backtracking, The Art of Computer Programming, Vol. 4: Combinatorial Algorithms, Fascicle 5. Addison-Wesley (2020)

[33] Knuth, D.E.: Constraint Satisfaction, The Art of Computer Programming, Vol. 4: Combinatorial Algorithms, Fascicle 7. Addison-Wesley (2025)

[34] G. Falcone, M. Pavone, *Binary Hamming codes and Boolean designs*, Des. Codes Cryptogr. **89**, 1261–1277 (2021)

[35] E. S. Kramer, D. M. Mesner, *t-designs on hypergraphs*, Discrete Mathematics **15**, 263–296 (1976)

[36] A. Nakic, *The first example of a simple* $2-(81, 6, 2)$ *design*, Ex. Counterexamples **1**, Article number 100005 (2021)

[37] A. Pasotti, J.H. Dinitz, *A survey of Heffter arrays*, Fields Institute Communications **86**, 353–392 (2024)

[38] M. Pavone, *A quasidouble of the affine plane of order* 4 *and the solution of a problem on additive designs*, Finite Fields Appl. **92**, Article number 102277 (2023)

[39] S. Thomas, *Designs over finite fields*, Geom. Dedicata **24**, 237–242 (1987)

[40] I.M. Wanless, B.S. Webb, *The existence of latin squares without orthogonal mates*, Des. Codes Cryptogr. **40**, 131–135 (2006)

[41] M. Zhang, T. Feng, X. Wang, *The existence of cyclic* $(v, 4, 1)$*-designs*, Des. Codes Crypt. **90**, 1611–1628 (2022)

[42] C. Zhao, B. Zhao, Y. Chang, T. Feng, X. Wang, M. Zhang, *Cyclic relative difference families with block size four and their applications*, J. Comb. Theory Ser. A **206**, Article number 105890 (2024)