Super-regular Steiner 2-designs

Marco Buratti *

Anamari Nakić †

July 12, 2022

Abstract

A design is additive under an abelian group G (briefly, G-additive) if, up to isomorphism, its point set is contained in G and the elements of each block sum up to zero. The only known Steiner 2-designs that are G-additive for some G have block size which is either a prime power or a prime power plus one. Indeed they are the point-line designs of the affine spaces $AG(n, q)$, the point-line designs of the projective planes $PG(2, q)$, the point-line designs of the projective spaces $PG(n, 2)$ and a sporadic example of a 2-(8191,7,1) design. In the attempt to find new examples, possibly with a block size which is neither a prime power nor a prime power plus one, we look for Steiner 2-designs which are strictly G-additive (the point set is exactly G) and G-regular (any translate of any block is a block as well) at the same time. These designs will be called "G-super-regular". Our main result is that there are infinitely many values of v for which there exists a super-regular, and therefore additive, 2-$(v, k, 1)$ design whenever k is neither singly even nor of the form $2^n3 \geq 12$. The case $k \equiv 2 \pmod 4$ is a genuine exception whereas $k = 2^n3 \geq 12$ is at the moment a possible exception. We also find super-regular 2-$(p^n, p, 1)$ designs with $p \in \{5, 7\}$ and $n \geq 3$ which are not isomorphic to the point-line design of $AG(n, p)$.

Keywords: (strictly) additive design; Steiner 2-design; automorphism group; regular design; (strong) difference family; cyclotomy; difference matrix.

*Dipartimento di Matematica e Informatica, Università di Perugia, via Vanvitelli 1, Italy. Email: buratti@dmi.unipg.it

†Faculty of Electrical Engineering and Computing, University at Zagreb, Croatia, email: anamari.nakic@fer.hr

1 Introduction

We recall that a t-(v,k,λ) design is a pair $\mathcal{D}=(V,\mathcal{B})$ with V a set of v *points* and $\mathcal{B}$ a collection of k-subsets of V, called *blocks*, such that any t-subset of V is contained in exactly λ blocks. It is understood that $1\le t\le k\le v$. The design is said to be *simple* if $\mathcal{B}$ is a set, i.e., if it does not have repeated blocks. When $v=k$ we necessarily have only one block, coincident with the whole point set V, repeated λ times; in this case the design is said to be *trivial.*

In the important case of $\lambda=1$ one speaks of a *Steiner t-design* and the notation $S(t,k,v)$ is often used in place of "t-$(v,k,1)$ design". An isomorphism between two designs $(V,\mathcal{B})$ and $(V',\mathcal{B}')$ is a bijection $f:V\longrightarrow V'$ turning $\mathcal{B}$ into $\mathcal{B}'$. Of course the study of t-designs is done up to isomorphism.

An *automorphism group* of a design $\mathcal{D}=(V,\mathcal{B})$ is a group G of permutations on V leaving $\mathcal{B}$ invariant, i.e., a group of isomorphisms of $\mathcal{D}$ with itself. If G acts regularly – i.e., sharply transitively – on the points, then $\mathcal{D}$ is said to be *regular* under G (briefly *G-regular*). Up to isomorphism, a G-regular design has point set G and any translate $B+g$ of any block B is a block as well.

For general background on t-designs we refer to [3] and [21].

Throughout the paper, every group will be assumed finite and abelian unless specified otherwise. A subset B of a group G will be said *zero-sum* if its elements sum up to zero. Representing the blocks of a design as zero-sum subsets of a commutative group turned out to provide an effective algebraic tool for studying their automorphisms (see, e.g., Example 3.7 in [19]). Also, some recent literature provides remarkable examples of usage of zero-sum blocks in the construction of combinatorial designs (see, e.g., [6, 26]). This gives even more value to the interesting theory on *additive designs* introduced in [18] by Caggegi, Falcone and Pavone. Other papers on the same subject by some of these authors are [16, 17, 24, 34]. They say that a design is additive if it is embeddable into an abelian group in such a way that the sum of the elements in any block is zero.

We reformulate just a little bit the terminology as follows.

Definition 1.1. A design $(V,\mathcal{B})$ is *additive under an abelian group G* (or briefly *G-additive*) if, up to isomorphism, we have:

(1) $V\subset G$;

(2) B is zero-sum $\forall B\in\mathcal{B}$.

If in place of condition (2) we have the much stronger condition

$(2)_s$ $\mathcal{B}$ is precisely the set of all zero-sum k-subsets of V,

then the design is *strongly G-additive.*

By saying that a design is additive (resp., strongly additive) we will mean that it is G-additive (resp., strongly G-additive) for at least one abelian group G. Note that we may have designs which are G-additive and H-additive at the same time even though none of them is isomorphic to a subgroup of the other. For instance, it is proved in [18] that if p is a prime, then the point-line design of the affine plane over $\mathbb{Z}_p$, which is obviously $\mathbb{Z}_p^2$-additive, is also strongly $\mathbb{Z}_p^{p(p-1)/2}$-additive.

In general, to establish whether an additive design is also strongly additive appears to be hard. Examples of additive 2-(v,k,λ) designs which are not strongly additive are given for $2 \leq \lambda \leq 6$ in [34]. The question on whether there exists an additive Steiner 2-design which is not strongly additive is still open.

We propose to consider the G-additive designs whose set of points is precisely G or $G \setminus \{0\}$.

Definition 1.2. An additive design is *strictly G-additive* or *almost strictly G-additive* if its point set is precisely G or $G \setminus \{0\}$, respectively.

Of course strictly additive (resp., almost strictly additive) means strictly G-additive (resp., almost strictly G-additive) for a suitable G. As it is standard, $\mathbb{F}_q$ will denote the field of order q and also, by abuse of notation, its additive group. It is quite evident that the 2-$(q^n,q,1)$ design of points and lines of $AG(n,q)$ (the n-dimensional affine geometry over $\mathbb{F}_q$) is strictly $\mathbb{F}_{q^n}$-additive.

As observed in [17], every 2-$(2^v-1,2^k-1,\lambda)$ design over $\mathbb{F}_2$ is almost strictly $\mathbb{F}_{2^v}$-additive[1]. Thus there exists an almost strictly $\mathbb{Z}_2^v$-additive 2-$(2^v-1,7,7)$ design for any odd $v \geq 3$ in view of the main results in [11, 36]. Also, there is an almost strictly $\mathbb{Z}_2^{v+1}$-additive 2-$(2^{v+1}-1,3,1)$ design that is the point-line design of $PG(v,2)$ (the v-dimensional projective geometry over $\mathbb{F}_2$). Finally, each of the well-celebrated designs found in [5] and revisited in [13] is an almost strictly $\mathbb{Z}_2^{13}$-additive 2-$(8191,7,1)$ design.

Almost all known additive designs have quite large values of λ. For instance, it is proved in [35] that if p is an odd prime and $k=mp$ does not exceed p^n, then all zero-sum k-subsets of $\mathbb{F}_{p^n}$ form the block-set of a strongly additive 2-(p^n,k,λ) design with $\lambda = \frac{1}{p^n}\binom{p^n-2}{k-2} + \frac{k-1}{p^n}\binom{p^{n-1}-1}{m-1}$. Applying this with $p=3$, $n=4$ and $k=6$, one finds a strongly additive 2-$(81,6,18551)$ design.

A sporadic example with $\lambda = 2$ is the strictly $\mathbb{Z}_3^4$-additive 2-$(81,6,2)$ design given in [30] and some more classes with a relatively small λ will be given in [12]. Anyway, what is most striking is the shortage of additive Steiner 2-designs. Up to now, only three classes were known:

[1] A 2-design is *over* $\mathbb{F}_q$ if its points are those of a projective geometry over $\mathbb{F}_q$ and the blocks are suitable subspaces of this geometry.

C1. the designs of points and lines of the affine geometries over any field $\mathbb{F}_q$ (which are strictly additive);

C2. the designs of points and lines of the projective geometries over $\mathbb{F}_2$ (which are almost strictly additive);

C3. the designs of points and lines of the projective planes over any field $\mathbb{F}_q$ (which are strongly additive under a "big" group [18]).

Nothing else was known, except for the sporadic example of the 2-$(8191, 7, 1)$ design mentioned above.

Hence to find additive Steiner 2-designs with new parameters, in particular with block size which is neither a prime power nor a prime power plus one, appears to be challenging.

Note that the 2-$(q^n, q, 1)$ designs mentioned above are also $\mathbb{F}_{q^n}$-regular. This fact suggests that a natural approach for reaching our target is to look for strictly G-additive Steiner 2-designs which are also G-regular. Let us give a name to the designs with these properties.

Definition 1.3. A design is *super-regular* under an abelian group G (or briefly *G-super-regular*) if it is G-regular and strictly G-additive at the same time.

Similarly as above, super-regular will mean G-super-regular for a suitable G. Super-regular Steiner 2-designs will be the central topic of this paper. Our main result will be the following.

Theorem 1.4. *Given $k \geq 3$, there are infinitely many values of v for which there exists a super-regular 2-$(v, k, 1)$ design with the genuine exceptions of the singly even values of k and the possible exceptions of all $k = 2^n 3 \geq 12$.*

As an immediate consequence, we have the existence of a strictly additive Steiner 2-design with block size k for any k with the same exceptions as in the above statement.

A major disappointment is that the smallest v for which, fixed k, we are able to say that a super-regular 2-$(v, k, 1)$ design exists, is huge. Suffice it to say that for $k = 15$ this value is $3 \cdot 5^{31}$. Consider, however, that there are several asymptotic results proving the existence of some designs as soon as the number of points is admissible and greater than a bound which is not even quantified. This happens, for instance, in the outstanding achievement by P. Keevash [26] on the existence of Steiner t-designs. Usually, these asymptotic results are obtained via probabilistic methods and are not constructive. Our methods are algebraic and "half constructive". We actually give a complete recipe for building a super-regular 2-$(kq, k, 1)$ design under $G \times \mathbb{F}_q$ (with G a suitable group of order k) whenever q is an admissible power of a prime divisor of k sufficiently large. Yet, in building every *base block* we have to pick the second coordinates of its elements, one by one, in a way that suitable cyclotomic conditions are satisfied and these choices are not "concrete"; they are realizable only in view of some theoretical arguments deriving from the *theorem of Weil on multiplicative character sums.*

In the penultimate section we will have a look at the super-regular non-Steiner 2-designs.

The paper will be organized as follows. In the next section we first prove two elementary necessary conditions for the existence of a strictly G-additive 2-$(v,k,1)$ design: G cannot have exactly one involution, and every prime factor of v must divide k.

In Section 3 we recall some basic facts on regular designs and show that any super-regular design can be completely described in terms of differences. In particular, we prove that a sufficient condition for the existence of a $(G\times\mathbb{F}_q)$-super-regular design with G a non-binary group of order k and q a power of a prime divisor of k is the existence of an additive $(G\times\mathbb{F}_q, G\times\{0\},k,1)$ difference family. This is a set $\mathcal{F}$ of zero-sum k-subsets of $G\times\mathbb{F}_q$ whose list of differences is $(G\times\mathbb{F}_q)\setminus(G\times\{0\})$. In Section 4 we prove that such an $\mathcal{F}$ cannot exist for $k=2^n3\geq 12$, clarifying in this way why this case is so hard.

In Sections 5 it is shown that a difference family as above can be realized by suitably lifting the blocks of an additive (G,k,λ) strong difference family, that is a collection of zero-sum k-multisets on G whose list of differences is λ times G.

In Section 6, as a first application of the method of strong difference families, we construct a $\mathbb{F}_{p^n}$-super-regular 2-$(p^n,p,1)$ design not isomorphic to the point-line design of $AG(n,p)$ for $p\in\{5,7\}$ and every integer $n\geq 3$.

In Section 7 a combined use of strong difference families and cyclotomy leads to a very technical asymptotic result. As a consequence of this result, the crucial ingredient for proving the main theorem is an additive (G,k,λ) strong difference family with G a non-binary group of order k and $\gcd(k,\lambda)=1$.

In Section 8 this ingredient is finally obtained, also via difference matrices, for all the relevant values of k and then the main theorem is proved.

As mentioned above, the final construction leads to super-regular Steiner 2-designs with a huge number of points. In Section 9 it is shown that when $k=15$ the smallest v given by this construction is $3\cdot 5^{9565939}$. On the other hand we also show that a clever use of strong difference families and cyclotomy allows to obtain smaller values of v. Still in the case $k=15$, we first obtain $v=3\cdot 5^{187}$ and then $v=3\cdot 5^{31}$ by means of two variations of the main construction. We also suggest a possible attempt to obtain $v=3\cdot 5^{7}$ by means of a computer search.

In Section 10 we sketch how the same tools used with so much labor to construct "huge" super-regular Steiner 2-designs allow to rapidly obtain super-regular non-Steiner 2-designs with a "reasonably small" v at the expense of a possibly large λ and the loss of simplicity (each of them has $\frac{v}{k}$ blocks repeated λ times). For instance, we will show the existence of a non-simple super-regular 2-design with block size 15 having only $3 \cdot 5^3$ points and with $\lambda = 21$.

In the last section we list some open questions.

2 Elementary facts about strictly additive Steiner 2-designs

In these preliminaries we establish some constraints on the parameters of a strictly additive Steiner 2-design. First, it is useful to show two very elementary facts which we believe are folklore.

Fact 2.1. Every non-trivial subgroup of $\mathbb{F}_q^*$ (the multiplicative group of $\mathbb{F}_q$) is zero-sum.

Proof. Let $B \neq \{1\}$ be a subgroup of $\mathbb{F}_q^*$ and let n be its order. Then, if b is a generator of B, we have $b^n - 1 = 0$, i.e., $(b-1)(\sum_{i=0}^{n-1} b^i) = 0$ in $\mathbb{F}_q$. Thus $\sum_{i=0}^{n-1} b^i$, which is the sum of all elements of B, is equal to zero. □

The subgroup of an abelian group G consisting of all the involutions of G and zero will be denoted by $I(G)$, i.e., $I(G) = \{g \in G : 2g = 0\}$. We say that G is *binary* when $I(G)$ has order 2, i.e., when G has exactly one involution.

Fact 2.2. An abelian group G is not zero-sum if and only if it is binary.

Proof. The elements of $G \setminus I(G)$ are partitionable into 2-subsets consisting of opposite elements $\{g, -g\}$ so that $G \setminus I(G)$ is zero-sum. Then the sum of all elements of G is equal to the sum of all elements of $I(G)$. Now note that either $I(G) = \{0\}$ or $I(G)$ is isomorphic to $\mathbb{Z}_2^n$ for some n. If $n = 1$, then G is binary and the sum of all elements of G is the non-zero element of $I(G)$, that is the only involution of G. If $n > 1$, then G is not binary and $I(G) \setminus \{0\}$ can be viewed as the multiplicative group of $\mathbb{F}_{2^n}^*$, hence it is zero-sum by Fact 2.1. □

From the above fact we immediately establish when the trivial $S(2, k, k)$ is strictly additive.

Proposition 2.3. *The trivial* 2-$(k, k, 1)$ *design is strictly additive if and only if* $k \not\equiv 2$ $(mod\ 4)$.

Proof. It is evident that the trivial 2-$(k, k, 1)$ design is strictly additive if and only if there exists an abelian zero-sum group of order k. Then we get the assertion from Fact 2.2 and the following observations.

Every group of odd order k is not binary.

Every group of singly even order k is binary.

Among the groups of doubly even order k we have $G = \mathbb{Z}_2^2 \times \mathbb{Z}_{k/4}$ which is not binary. □

We recall that the *radical* of an integer n, denoted by $rad(n)$, is the product of all prime factors of n. Thus, the fact that a finite field $\mathbb{F}_q$ has characteristic p can be also expressed by saying that $rad(q) = p$. The following property reduces significantly the admissible parameters for a strictly additive 2-$(v, k, 1)$ design.

Proposition 2.4. *If a strictly G-additive* 2-$(v, k, 1)$ *design exists, then G is zero-sum and the radical of v is a divisor of k.*

Proof. Let $\mathcal{D} = (G, \mathcal{B})$ be a 2-$(v, k, 1)$ design which is strictly additive under G. For any fixed element g of G, let $\mathcal{B}_g$ be the set of blocks through g and recall that its size r (the so-called *replication number* of $\mathcal{D}$) does not depend on g. Now consider the double sum

$$\sigma_g = \sum_{B \in \mathcal{B}_g} \big(\sum_{b \in B} b\big).$$

We have $\sum_{b \in B} b = 0$ for every $B \in \mathcal{B}_g$ because $\mathcal{D}$ is strictly additive, hence σ_g is null. Also note that in the expansion of σ_g the fixed element g appears as an addend exactly r times whereas any other element h of G appears as an addend exactly once. Thus σ_g can be also expressed as $(r-1)g + \sum_{h \in G} h$. We conclude that we have

$$(r-1)g + \sum_{h \in G} h = 0 \quad \forall g \in G.$$

Specializing this to the case $g = 0$ we get $\sum_{h \in G} h = 0$ which means that G is zero-sum. Hence the first assertion is proved and we can write

$$(r-1)g = 0 \quad \forall g \in G.$$

This means that the order of every element of G is a divisor of $r - 1$. Let p be a prime divisor of v, set $v = pw$, and take an element g of G of order p (which exists by the theorem of Cauchy). For what we said, p divides $r - 1$. Now recall that $r = \frac{v-1}{k-1}$, hence $r - 1 = \frac{v-k}{k-1}$. Thus we can write $\frac{pw-k}{k-1} = pn$ for some integer n which gives $pw - k = (k-1)pn$. This equality implies that p divides k. Thus every prime factor of v is also a prime factor of k and the second assertion follows. □

In particular, considering that every abelian group of singly even order is binary, we can state the following.

Corollary 2.5. *A strictly additive* 2-$(v, k, 1)$ *design with v singly even cannot exist.*

In the next section we will see that in a super-regular 2-$(v, k, 1)$ design the radicals of v and k are even equal.

3 Difference families

We need to recall some classic results on regular designs.

The *list of differences* of a subset B of a group G is the multiset ΔB of all possible differences $x - y$ with (x, y) an ordered pair of distinct elements of B. More generally, if $\mathcal{F}$ is a set of subsets of G, the list of differences of $\mathcal{F}$ is the multiset union $\Delta\mathcal{F} = \biguplus_{B\in\mathcal{F}} \Delta B$.

Let H be a subgroup of a group G. A set $\mathcal{F}$ of k-subsets of G is a $(G, H, k, 1)$ difference family (briefly DF) if $\Delta\mathcal{F} = G \setminus H$.

The members of such a DF are called *base blocks* and their number is clearly equal to $\frac{v-h}{k(k-1)}$ where v and h are the orders of G and H, respectively. Thus a necessary condition for its existence is that $v - h$ is divisible by $k(k-1)$. It is also necessary that $I(G)$ is a subgroup of H since in a list of differences every involution necessarily appears an even number of times.

If G has order v and $H = \{0\}$, one usually speaks of an *ordinary* $(v, k, 1)$-DF in G. Instead, when $|H| = h > 1$ one speaks of a $(v, h, k, 1)$-DF in G *relative to* H or, more briefly, of a *relative* $(v, h, k, 1)$-DF.

For general background on difference families as above we refer to [3, 21].

More generally, one can speak of a *difference family relative to a partial spread of* G, that is a notion introduced by the first author in [9]. A *partial spread* of a group G is a set $\mathcal{H}$ of subgroups of G whose mutual intersections are trivial. It is a *spread* of G when the union of its members is the whole G. Also, it is said *of type* τ to express that the multiset of the orders of its members is τ. In particular, to say that $\mathcal{H}$ is of type $\{k^s\}$ means that $\mathcal{H}$ has exactly s members and all of them have order k.

Given a partial spread $\mathcal{H}$ of a group G, a set $\mathcal{F}$ of k-subsets of G is said to be a $(G, \mathcal{H}, k, 1)$ difference family if $\Delta\mathcal{F}$ is the set of all elements of G not belonging to any member of $\mathcal{H}$. If G has order v and $\mathcal{H}$ is of type τ, one also speaks of a $(v, \tau, k, 1)$-DF in G relative to $\mathcal{H}$. If $\tau = \{k^s\}$ for some s, the obvious necessary conditions for its existence are the following:

$$k \mid v; \quad \frac{v}{k} \equiv 1 \pmod{k-1}; \quad s \equiv 1 \pmod{k}; \quad I(G) \subset \bigcup_{H\in\mathcal{H}} H \tag{3.1}$$

Clearly, a $(G, H, k, 1)$-DF can be seen as a difference family relative to a partial spread of size 1.

The following theorem is a special case of a general result concerning regular *linear spaces* [9].

Theorem 3.1. *Let G be an abelian group of order v. A G-regular 2-$(v, k, 1)$ design may exist only for $v \equiv 1$ or k (mod $k(k-1)$) and it is equivalent to:*

- *an ordinary $(v, k, 1)$-DF in G when $v \equiv 1$ (mod $k(k-1)$);*
- *a $(v, \{k^s\}, k, 1)$-DF in G for some s when $v \equiv k$ (mod $k(k-1)$).*

We remark that the above theorem is false when G is non-abelian.

Remark 3.2. It is useful to recall the constructive part of the proof of the above theorem (which also works when G is not abelian).

(r1) The set of all the translates of the base blocks of an ordinary $(v, k, 1)$-DF in G form the block-set of a G-regular 2-$(v, k, 1)$ design.

(r2) If $\mathcal{F}$ is a $(v, \{k^s\}, k, 1)$-DF in G relative to $\mathcal{H}$, then the set of all the translates of the base blocks of $\mathcal{F}$ together with all the right cosets of all the members of $\mathcal{H}$ form the block-set of a G-regular 2-$(v, k, 1)$ design.

It is immediate from Theorem 3.1 that any G-super-regular 2-$(v, k, 1)$ design is generated by a suitable difference family. Let us see some other consequences.

Proposition 3.3. *If there exists a G-super-regular 2-$(v, k, 1)$ design, then we have:*

(i) the order of every element of G is a divisor of k;

(ii) $v \equiv k$ (mod $k(k-1)$);

(iii) $rad(v) = rad(k)$;

(iv) k is not singly even.

Proof. Let $\mathcal{D}$ be a G-super-regular 2-$(v, k, 1)$ design.

(i). Take any element g of G and any block B of $\mathcal{D}$. By definition of a G-regular design $B + g$ is a block of $\mathcal{D}$ as well. Also, by definition of strictly G-additive design both B and $B + g$ are zero-sum. Thus, considering that the elements of $B + g$ sum up to $(\sum_{b \in B} b) + kg$, we deduce that $kg = 0$, i.e., the order of g divides k.

(ii). If $v \equiv 1$ (mod $k(k-1)$), then k divides $v - 1$. By (i), the order of any $g \in G$ divides k, hence it also divides $v - 1$. On the other hand $ord(g)$ divides v by Lagrange's theorem. Thus $ord(g)$ would be a common divisor of v and $v - 1$ whichever is $g \in G$. This would imply $v = 1$ which is absurd. We conclude, by Theorem 3.1, that we have $v \equiv k$ (mod $k(k-1)$).

(iii). We already know from Proposition 2.4 that $rad(v)$ divides $rad(k)$. On the other hand k divides v because of condition (ii) proved above, hence $rad(k)$ divides $rad(v)$ and the assertion follows.

(iv). $\mathcal{D}$ has at least one block B which is a subgroup of G of order k in view of (ii) and Remark 3.2(r2). Considering that B is zero-sum by assumption, the group B is not binary by Fact 2.2, hence $k \not\equiv 2$ (mod 4). $\square$

Note that condition (i) of the above lemma implies, in particular, that if p is a prime factor of k but p^2 does not divide k, then the Sylow p-subgroup of G is elementary abelian. Hence, when k is square-free, G is necessarily a direct product of elementary abelian groups.

In the following a $(G, \mathcal{H}, k, 1)$-DF will be said *additive* if all its base blocks are zero-sum and all the members of $\mathcal{H}$ are zero-sum (i.e., not binary) as well.

The above results (Theorem 3.1, Remark 3.2 and Proposition 3.3) allow us to state the following.

Lemma 3.4. *There exists a G-super-regular 2-$(v, k, 1)$ design if and only if G satisfies conditions (i), (ii) of Proposition 3.3 and there exists an additive $(G, \mathcal{H}, k, 1)$-DF of type $\{k^s\}$ for some s.*

The next lemma will be our main tool to construct super-regular Steiner 2-designs.

Lemma 3.5. *Let G be a zero-sum group of order k and let $q \equiv 1 \pmod{k-1}$ be a power of a prime divisor p of k. If there exists an additive $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF, then there exists a $(G \times \mathbb{F}_{q^n})$-super-regular 2-$(kq^n, k, 1)$ design for every $n \geq 1$.*

Proof. The hypotheses easily imply that $G \times \mathbb{F}_{q^n}$ satisfies conditions (i), (ii) of Proposition 3.3 for every n. Let $\mathcal{F}$ be an additive $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF, and let S be a complete system of representatives for the cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^n}^*$. For every base block B of $\mathcal{F}$ and every $s \in S$, let $B \circ s$ be the subset of $\mathbb{F}_{q^n}^*$ obtained from B by multiplying the second coordinates of all its elements by s. It is easy to see that $\mathcal{F} \circ S := \{B \circ s \mid B \in \mathcal{F}; s \in S\}$ is an additive $(G \times \mathbb{F}_{q^n}, G \times \{0\}, k, 1)$-DF. The assertion then follows from Lemma 3.4. $\square$

Recall that, for the time being, only three classes of non-trivial additive Steiner 2-designs are known, that are classes C1, C2, C3 mentioned in the introduction. The set of their block sizes clearly coincides with the set $Q \cup (Q + 1)$ where Q is the set of all prime powers. Thus, for now, we do not have any example of an additive non-trivial Steiner 2-design whose block size is neither a prime power nor a prime power plus one. Also, for $k \in (Q+1) \setminus Q$ we have only one example that is the projective plane of order $k-1$. Let us examine which is the very first possible attempt of filling these gaps using the above lemma. The first k which is neither a prime power nor a prime power plus one is 15. We can try to find a super-regular 2-$(15q, 15, 1)$ design using Lemma 3.5, i.e., via an additive $(\mathbb{Z}_{15} \times \mathbb{F}_q, \mathbb{Z}_{15} \times \{0\}, 15, 1)$-DF with q a power of 3 or a power of 5. The first case is ruled out by Theorem 4.1 in the next section. Thus q has to be taken among the powers of 5. More precisely, in view of the condition $q \equiv 1 \pmod{14}$, we have to take $q = 5^{6n}$ for some n. We conclude that 2-$(15 \cdot 5^6, 15, 1)$ is the first parameter set of a super-regular Steiner 2-design with block size belonging to $(Q+1) \setminus Q$ potentially obtainable via Lemma 3.5. Unfortunately, we are not able to construct a design with these parameters. In the penultimate section we indicate a possible attempt to get it by means of a computer search. In that same section we will prove the existence of a super-regular 2-$(15 \cdot 5^{30}, 15, 1)$ design.

4 One more necessary condition and the hard case $k = 2^n 3$ with $n \geq 2$

The following result will lead to one more condition on the parameters of a super-regular Steiner 2-design. This result will also imply that a non-trivial super-regular 2-$(v, k, 1)$ design with $k = 2^n 3$ may be generated by an additive $(v, k, k, 1)$-DF only if a very strong condition on n holds. As a matter of fact we suspect that this conditions is never satisfied. This is why in our main result we are not able to say anything about the case $k = 2^n 3$ which appears to us very hard.

Theorem 4.1. *If a super-regular* 2-$(v, k, 1)$ *design is generated by an additive* $(v, k, k, 1)$*-DF and* $k \equiv \pm 3 \pmod 9$*, then* $\frac{v}{k} \equiv 1 \pmod 3$*.*

Proof. Let $\mathcal{F}$ be an additive $(G, H, k, 1)$-DF generating a G-super-regular 2-$(v, k, 1)$ design with $k \equiv \pm 3 \pmod 9$. Thus G is a group of order $v \equiv k \pmod{k(k-1)}$, say $v = kv_1$, and H is a subgroup of G of order $k = 3k_1$ with k_1 not divisible by 3. For what we observed immediately after Proposition 3.3 the Sylow 3-subgroup of G is elementary abelian. For this reason, for every two subgroups of G of order 3 there exists an automorphism of G mapping one into the other. Then, up to isomorphism, we may assume that $G = \mathbb{Z}_3 \times G_1$ with G_1 of order $k_1 v_1$ and $H = \mathbb{Z}_3 \times H_1$ with H_1 a subgroup of G_1 of order k_1.

For each $B \in \mathcal{F}$, let $\overline{B}$ be the k-multiset on $\mathbb{Z}_3$ that is the projection of B on $\mathbb{Z}_3$ and set $\overline{\mathcal{F}} = \{\overline{B} \mid B \in \mathcal{F}\}$. It is clear that $\Delta\overline{\mathcal{F}}$ is the projection of $\Delta\mathcal{F}$ on $\mathbb{Z}_3$. Thus, considering that $\Delta\mathcal{F} = (\mathbb{Z}_3 \times G_1) \setminus (\mathbb{Z}_3 \times H_1)$ by assumption, it is clear that $\Delta\overline{\mathcal{F}}$ is λ times $\mathbb{Z}_3$ with λ equal to the size of $G_1 \setminus H_1$, i.e., $\lambda = k_1(v_1 - 1)$. Using some terminology that we will recall in the next section, $\overline{\mathcal{F}}$ is essentially a $(\mathbb{Z}_3, k, \lambda)$ *strong difference family.*

Take any block $\overline{B}$ of $\overline{\mathcal{F}}$ and for $i = 0, 1, 2$, let μ_i be the multiplicity of i in $\overline{B}$. Clearly, we have $\mu_0 + \mu_1 + \mu_2 = k$, hence $\mu_0 + \mu_1 + \mu_2 \equiv 0 \pmod 3$. Considering that $\mathcal{F}$ is additive, B is zero-sum and then $\overline{B}$ is zero-sum as well. It follows that $\mu_1 + 2\mu_2 = 0$ in $\mathbb{Z}_3$, i.e., $\mu_1 \equiv \mu_2 \pmod 3$. We easily conclude that

$$\mu_0 \equiv \mu_1 \equiv \mu_2 \pmod 3 \tag{4.1}$$

Now, let ν be the multiplicity of zero in $\Delta\overline{B}$ and note that we have

$$\nu = \mu_0(\mu_0 - 1) + \mu_1(\mu_1 - 1) + \mu_2(\mu_2 - 1),$$

hence $\nu \equiv 0 \pmod 3$ in view of (4.1).

Note that λ can be seen as the sum of the multiplicities of zero in the lists of differences of the blocks of $\overline{\mathcal{F}}$. For what we just saw, all these multiplicities are zero (mod 3) and then $\lambda \equiv 0 \pmod 3$. Recalling that $\lambda = k_1(v_1 - 1)$ we conclude that $v_1 \equiv 1 \pmod 3$ which is the assertion. $\square$

As a consequence, we get the following non-existence result.

Theorem 4.2. *A super-regular* 2-$(v, k, 1)$ *design with* $k \equiv \pm 3$ $(mod\ 6)$ *and* $\frac{v}{k} \equiv 2$ $(mod\ 3)$ *cannot exist.*

Proof. Assume that there exists a G-super-regular 2-$(v, k, 1)$ design $\mathcal{D}$ with v and k as in the statement. Then $\mathcal{D}$ cannot be generated by an additive $(v, k, k, 1)$-DF by Theorem 4.1. It follows that $\mathcal{D}$ is generated by an additive $(v, \{k^s\}, k, 1)$-DF for a suitable $s > 1$ by Theorem 3.4. On the other hand the hypothesis obviously imply that v, as k, is divisible by 3 but not by 9. Thus G necessarily has only one subgroup of order 3, hence it cannot have a partial spread with two distinct members of order k. We got a contradiction. $\square$

Each of the following pairs (v, k) satisfies the admissibility conditions $v \equiv k \pmod{k(k-1)}$ and $rad(v) = rad(k)$ given by Proposition 3.3. Yet, for each of them no super-regular 2-$(v, k, 1)$ design exists in view of the above theorem.

v	k
$3 \cdot 2^6 \cdot 5^{10}$	$3 \cdot 2^2 \cdot 5$
$3 \cdot 2^{18} \cdot 11^{10}$	$3 \cdot 2^2 \cdot 11$
$3 \cdot 5 \cdot 11^7$	$3 \cdot 5 \cdot 11$
$3 \cdot 2^{21} \cdot 7^3$	$3 \cdot 2^3 \cdot 7$
$3 \cdot 5^{22} \cdot 13^4$	$3 \cdot 5 \cdot 13$
$3 \cdot 2^{26} \cdot 5^6$	$3 \cdot 2^4 \cdot 5$

Another consequence of Theorem 4.1 is the following.

Theorem 4.3. *Let* $k = 2^n 3$ *and assume that there exists a super-regular* 2-$(v, k, 1)$ *design generated by an additive* $(v, k, k, 1)$*-DF. Then* $v = 2^{oi+n}3$ *where* o *is the order of* 2 *in the group of units* $(mod\ k-1)$ *and* $0 \leq i \leq \lfloor \frac{n^2-n}{o} \rfloor$.

Proof. Let $\mathcal{D}$ be a G-super-regular 2-$(v, k, 1)$ design with $k = 2^n 3$ and assume that $\mathcal{D}$ is generated by an additive $(G, H, k, 1)$-DF so that G has order v and H is a subgroup of G of order k. By Proposition 3.3 (ii) and (iii) we have $v = 2^a 3^b \equiv k \pmod{k(k-1)}$. Thus, reducing mod k and mod $k-1$ we respectively get

$$2^a 3^b \equiv 2^n 3 \ (mod\ 2^n 3) \quad \text{and} \quad 2^a 3^b \equiv 1 \ (mod\ 2^n 3 - 1) \tag{4.2}$$

From the first of the above congruences we deduce that $a \geq n$ and $b \geq 1$. By Theorem 4.1 we must have $2^{a-n}3^{b-1} \equiv 1 \pmod 3$ which implies $b = 1$. Hence $v = 2^a 3$ with $a \geq n$. Multiplying the second congruence in (4.2) by 2^n (which is the inverse of 3 mod $k-1$), we get $2^a \equiv 2^n \pmod{k-1}$, i.e., $2^{a-n} \equiv 1 \pmod{k-1}$. This, by definition of o, means that $a = oi + n$ for some integer i. Hence we have

$$v = 2^{oi+n}3 \tag{4.3}$$

Now let 2^t be the order of $I(G)$ and recall that $I(G)$ is necessarily contained in H so that we have $t \leq n$. Up to isomorphism, by the fundamental theorem on abelian groups, we have $G = \mathbb{Z}_{2^{\alpha_1}} \times \cdots \times \mathbb{Z}_{2^{\alpha_t}} \times \mathbb{Z}_3$ for a suitable t-tuple $(\alpha_1, \ldots, \alpha_t)$ of positive integers summing up to a. For $i = 1, \ldots, t$, there are elements of G of order 2^{α_i}; for instance the element whose ith coordinate is 1 and all the other coordinates are zero. Hence 2^{α_i} divides k by Proposition 3.3(i) and then $\alpha_i \leq n$ for $i = 1, \ldots, t$. We deduce that we have

$$v = |G| \leq (2^n)^t 3 \leq 2^{n^2}3 \tag{4.4}$$

Comparing (4.3) and (4.4) we get $oi + n \leq n^2$, i.e., $i \leq \lfloor \frac{n^2-n}{o} \rfloor$ and the assertion follows. □

Corollary 4.4. *If $k = 2^n 3$ and there exists a non-trivial super-regular 2-$(v, k, 1)$ design generated by an additive $(v, k, k, 1)$-DF, then the order of 2 in the group of units of $\mathbb{Z}_{k-1}$ is less than $n^2 - n$.*

We suspect that the order of 2 in the group of units of $\mathbb{Z}_{2^n 3-1}$ is always greater than $n^2 - n$ but we are not able to prove it. For now, we are able to say that it is true for $n \leq 1000$ (checked by computer) and whenever $2^n 3 - 1$ has a prime factor greater than $(n^2 - n)^2$; this is a consequence of a result proved in [31] according to which the order of 2 modulo an odd prime p is almost always as large as the square root of p. Thus, for now, we can state the following.

Remark 4.5. Let $k = 2^n 3$ with $n \leq 1000$ or k has a prime factor greater than $(n^2 - n)^2$. Then there is no value of v for which a putative non-trivial super-regular 2-$(v, k, 1)$ design may be generated by an additive $(v, k, k, 1)$-DF.

The above leads us to believe that the existence of a non-trivial super-regular 2-$(v, 2^n 3, 1)$ design generated by a $(v, k, k, 1)$-DF is highly unlikely. On the other hand such a design might be obtained via a difference family relative to a partial spread of size greater than 1. For instance, we cannot rule out that there exists a G-super-regular 2-$(3^9 4^4, 12, 1)$ design generated by an additive $(G, \mathcal{H}, 12, 1)$-DF with $G = \mathbb{F}_{3^9} \times \mathbb{F}_{4^4}$ and $\mathcal{H}$ a partial spread of G of type $\{12^{85}\}$. Indeed G satisfies conditions (ii), (iii) of Propositions 3.3

and the necessary conditions (3.1) are also satisfied with an $\mathcal{H}$ constructible as follows. Take a (full) spread $\mathcal{H}_1$ of $\mathbb{F}_{4^4}$ consisting of subgroups of $\mathbb{F}_{4^4}$ of order 4 and note that it has size $\frac{4^4-1}{3} = 85$. Now take the (full) spread $\mathcal{H}_2$ of $\mathbb{F}_{3^9}$ consisting of all subgroups of $\mathbb{F}_{3^9}$ of order 3 which has size $\frac{3^9-1}{2} > 85$. Thus it is possible to choose an injective map $f : \mathcal{H}_1 \longrightarrow \mathcal{H}_2$ and we can take $\mathcal{H} := \{H \times f(H) \mid H \in \mathcal{H}_1\}$. On the other hand to realize an additive $(G, \mathcal{H}, 12, 1)$-DF with G and $\mathcal{H}$ as above appears to be unfeasible; suffice it to say that it would have 38,166 base blocks. Also, the fact that the literature is completely lacking of constructions for $(v, \{k^s\}, k, 1)$ difference families with $s > 1$, further underlines the difficulty of the problem.

5 Strong difference families

In view of Lemma 3.5 our target will be the construction of additive $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$ difference families with G of order k and q a power of a prime divisor of k. For this, we need one more variant of a difference family, that is a *strong difference family*.

The notion of list of differences of a subset of a group G can be naturally generalized to that of list of differences of a multiset on G as follows. If $B = \{b_1, \ldots, b_k\}$ is a multiset on a group G, then the list of differences of B is the multiset ΔB of all possible differences $b_i - b_j$ with (i, j) an ordered pair of distinct elements of $\{1, \ldots, k\}$.

It is evident that the multiplicity of zero in ΔB is even. Indeed if $b_i - b_j = 0$, then $b_j - b_i = 0$ as well. It is also evident that this multiplicity is equal to zero if and only if B does not have repeated elements, i.e., B is a set.

By list of differences of a collection $\mathcal{F}$ of multisets on G one means the multiset union $\Delta\mathcal{F} = \biguplus_{B \in \mathcal{F}} \Delta B$.

Definition 5.1. Let G be a group of order v and let $\mathcal{F}$ be a collection of k-multisets on G. One says that $\mathcal{F}$ is a (v, k, λ) strong difference family in G (or briefly a (G, k, λ)-SDF) if $\Delta\mathcal{F}$ covers every element of G (0 included) exactly λ times.

Note that if s is the number of blocks of a (G, k, λ)-SDF, then we necessarily have $\lambda|G| = sk(k-1)$.

A SDF with only one block is called a *difference multiset* [8] or also a *difference cover* [1].

Example 5.2. Take the 5-multiset $B = \{0, 1, 1, 4, 4\}$ on $\mathbb{Z}_5$. Looking at its "difference table"

	0	1	1	4	4
0	$\bullet$	**4**	**4**	**1**	**1**
1	**1**	$\bullet$	**0**	**2**	**2**
1	**1**	**0**	$\bullet$	**2**	**2**
4	**4**	**3**	**3**	$\bullet$	**0**
4	**4**	**3**	**3**	**0**	$\bullet$

we see that the singleton $\{B\}$ is a $(5, 5, 4)$-SDF in $\mathbb{Z}_5$.

Throughout the paper, the union of n copies of a set or multiset S will be denoted by $\underline{n}S$. Thus the difference multiset of the previous example can be denoted as $\{0\} \cup \underline{2}\{1, 4\}$. Much more in general, we recall that if q is an odd prime power and $\mathbb{F}_q^{\square}$ is the set of non-zero squares of $\mathbb{F}_q$, then $\{0\} \cup \underline{2}\mathbb{F}_q^{\square}$ is the so-called $(q, q, q-1)$ *Paley difference multiset of the first type* [8].

We will say that a multiset on a group G is zero-sum if the sum of all its elements (counting their multiplicities) is zero. A SDF in G will be said *additive* if all its members are zero-sum. In view of Fact 2.1 the Paley $(q, q, q-1)$ difference multisets of the first type are additive provided that $q \neq 3$.

Strong difference families are a very useful tool to construct relative difference families. Even though they were implicitly considered in some older literature, they have been formally introduced for the first time by the first author in [8]. After that, they turned out to be crucial in many constructions in design theory (see, e.g., [4, 10, 14, 15, 20, 22, 23, 25, 32, 38]).

The following construction explains how to use strong difference families in order to construct relative difference families.

Construction 5.3. *Let $\Sigma = \{B_1, \dots, B_s\}$ be a (G, k, λ)-SDF and let $q \equiv 1 \pmod{\lambda}$ be a prime power. Lift each block $B_h = \{b_{h1}, \dots, b_{hk}\}$ of Σ to a subset $\ell(B_h) = \{(b_{h1}, \ell_{h1}), \dots, (b_{hk}, \ell_{hk})\}$ of $G \times \mathbb{F}_q$. By definition of a strong difference family, we have $\Delta\mathcal{F} = \biguplus_{g \in G}\{g\} \times \Delta_g$ where each Δ_g is a λ-multiset on $\mathbb{F}_q$. Hence, if the liftings have been done appropriately, it may happen that there exists a $\frac{q-1}{\lambda}$-subset M of $\mathbb{F}_q^*$ such that $\Delta_g \cdot M = \mathbb{F}_q^*$ for each $g \in G$. In this case, it is easy to see that*

$$\mathcal{F} = \big\{\{(b_{h1}, \ell_{h1}m), \dots, (b_{hk}, \ell_{hk}m)\} \mid 1 \leq h \leq s; m \in M\big\}$$

is a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF. This DF is clearly additive in the additional hypothesis that Σ is additive and each $\ell(B_h)$ is zero-sum.

In most of the cases the above construction is applied when each Δ_g is a complete system of representatives for the cosets of the subgroup C^λ of $\mathbb{F}_q^*$ of index λ, that is the group of non-zero λ-th powers of $\mathbb{F}_q$. Indeed in this case we have $\Delta_g \cdot M = \mathbb{F}_q^*$ for each $g \in G$ with $M = C^\lambda$. Note, however, that Δ_g is of the form $\{1,-1\}\cdot\overline{\Delta}_g$ for every $g\in I(G)$, hence it contains pairs $\{x,-x\}$ of opposite elements. Thus, if the elements of Δ_g belong to pairwise distinct cosets of C^λ, we necessarily have $-1\notin C^\lambda$, i.e., $q\equiv\lambda+1 \pmod{2\lambda}$. This explains why in the next Theorems 7.2 and 7.3 we require that this congruence holds.

6 Anomalous 2-$(q^n, q, 1)$ designs

Let us say that a 2-$(q^n,q,1)$ design is *anomalous* if it is $\mathbb{F}_{q^n}$-super-regular but not isomorphic to the design of points and lines of $\mathrm{AG}(n,q)$.

Proposition 6.1. *If there exists an anomalous* 2-$(q^n,q,1)$ *design, then there exists an anomalous* 2-$(q^m,q,1)$ *design for any* $m\geq n$.

Proof. Let V be the n-dimensional subspace of $\mathrm{AG}(m,q)$ defined by the equations $x_i=0$ for $n+1\leq i\leq m$. Take the *standard* 2-$(q^m,q,1)$ design $(\mathbb{F}_q^m,\mathcal{B})$ and replace all its blocks contained in V with the blocks of an anomalous 2-$(q^n,q,1)$ design. We get, in this way, the block-set of an anomalous 2-$(q^m,q,1)$ design. □

In the next theorem we put into practice Lemma 3.5 and Construction 5.3 to get an anomalous 2-$(p^3,p,1)$ design for $p=5$ and $p=7$. Our proof is a slight modification of the construction for regular 2-$(pq,p,1)$ designs in [2] (improved in [7]) with p and q prime powers, $q\equiv 1 \pmod{p-1}$. In our construction below q coincides with p^2.

Theorem 6.2. *There exists an anomalous* 2-$(p^3,p,1)$ *design for* $p=5$ *and* $p=7$.

Proof. By Lemma 3.5 a super-regular 2-$(5^3,5,1)$ design can be realized by means of an additive $(\mathbb{Z}_5\times\mathbb{F}_{25},\mathbb{Z}_5\times\{0\},5,1)$-DF. We can obtain several DFs of the required kind using Construction 5.3 with Σ the additive $(5,5,4)$ difference multiset $B=\{0,1,1,4,4\}$ of Example 5.2. For instance, let us lift B to the subset $\ell(B)$ of $\mathbb{Z}_5\times\mathbb{F}_{25}$

$$\ell(B)=\{(0,0),(1,1),(1,-1),(4,\ell),(4,-\ell)\}$$

with ℓ a root of the primitive polynomial x^2+x+2. It is readily seen that $\ell(B)$ is zero-sum. Looking at its difference table

	$(0,0)$	$(1,1)$	$(1,-1)$	$(4,\ell)$	$(4,-\ell)$
$(0,0)$	$\bullet$	$\mathbf{(4,-1)}$	$\mathbf{(4,1)}$	$\mathbf{(1,-\ell)}$	$\mathbf{(1,\ell)}$
$(1,1)$	$\mathbf{(1,1)}$	$\bullet$	$\mathbf{(0,2)}$	$\mathbf{(2,1-\ell)}$	$\mathbf{(2,1+\ell)}$
$(1,-1)$	$\mathbf{(1,-1)}$	$\mathbf{(0,-2)}$	$\bullet$	$\mathbf{(2,-1-\ell)}$	$\mathbf{(2,-1+\ell)}$
$(4,\ell)$	$\mathbf{(4,\ell)}$	$\mathbf{(3,\ell-1)}$	$\mathbf{(3,1+\ell)}$	$\bullet$	$\mathbf{(0,2\ell)}$
$(4,-\ell)$	$\mathbf{(4,-\ell)}$	$\mathbf{(3,-1-\ell)}$	$\mathbf{(3,-\ell+1)}$	$\mathbf{(0,-2\ell)}$	$\bullet$

we see that $\Delta\ell(B) = \bigcup_{g=0}^{4}\{g\} \times \Delta_g$ with

$\Delta_0 = \{1, -1\} \cdot \{2, 2\ell\}$;

$\Delta_1 = \Delta_4 = \{1, -1\} \cdot \{1, \ell\}$;

$\Delta_2 = \Delta_3 = \{1, -1\} \cdot \{\ell - 1, \ell + 1\}$.

Now note that each of the 2-sets $\overline{\Delta}_0 = \{2, 2\ell\}$, $\overline{\Delta}_1 = \{1, \ell\}$ and $\overline{\Delta}_2 = \{\ell - 1, \ell + 1\}$ contains a non-zero square and a non-square of $\mathbb{F}_{25}$. Thus, if M is a complete system of representatives for the cosets of $\{1, -1\}$ in $\mathbb{F}_{25}^{\square}$, we clearly have $\Delta_g \cdot M = \mathbb{F}_{25}^{*}$. Hence

$$\mathcal{F} = \big\{\{(0, 0), (1, m), (1, -m), (4, \ell m), (4, -\ell m)\} \mid m \in M\big\}$$

is an additive $(\mathbb{Z}_5 \times \mathbb{F}_{25}, \mathbb{Z}_5 \times \{0\}, 5, 1)$-DF. If we take, for instance, $M = \{\ell^{2i} \mid 0 \leq i \leq 5\}$ then the blocks of $\mathcal{F}$, written in additive notation, are the following:

$$B_1 = \{(0, 0, 0), (1, 0, 1), (1, 0, 4), (4, 1, 0), (4, 4, 0)\};$$

$$B_2 = \{(0, 0, 0), (1, 4, 3), (1, 1, 2), (4, 4, 2), (4, 1, 3)\};$$

$$B_3 = \{(0, 0, 0), (1, 3, 2), (1, 2, 3), (4, 4, 4), (4, 1, 1)\};$$

$$B_4 = \{(0, 0, 0), (1, 0, 2), (1, 0, 3), (4, 2, 0), (4, 3, 0)\};$$

$$B_5 = \{(0, 0, 0), (1, 3, 1), (1, 2, 4), (4, 3, 4), (4, 2, 1)\};$$

$$B_6 = \{(0, 0, 0), (1, 1, 4), (1, 4, 1), (4, 3, 3), (4, 2, 2)\}.$$

We can check, by hand, that the super-regular 2-$(125, 5, 1)$ design $\mathcal{D}$ generated by $\mathcal{F}$ is anomalous. Assume for contradiction that it is isomorphic to the point-line design of AG$(3, 5)$. It is then natural to speak of *lines* of $\mathcal{D}$ rather than blocks. Also, it makes sense to speak of the *planes* of $\mathcal{D}$ and a line containing two distinct points of a plane π is clearly contained in π.

Let π be the plane of $\mathcal{D}$ containing the two lines through the origin $B_0 = \{(0, 0, 0), (1, 0, 0), (2, 0, 0), (3, 0, 0), (4, 0, 0)\}$ and B_1. Of course, if $\mathcal{B}_\pi$ is the set of lines of $\mathcal{D}$ contained in π, then $(\pi, \mathcal{B}_\pi)$ is isomorphic to the affine plane over $\mathbb{F}_5$. The line through $(1, 0, 0) \in B_0$ and $(1, 0, 1) \in B_1$ is

$$C = B_4 + (0, 0, 3) = \{(0, 0, 3), (\mathbf{1}, \mathbf{0}, \mathbf{0}), (\mathbf{1}, \mathbf{0}, \mathbf{1}), (4, 2, 3), (4, 3, 3)\}$$

and belongs to $\mathcal{B}_\pi$ since it joins two points of π. The line through $(1, 0, 4) \in B_1$ and $(0, 0, 3) \in C$ is

$$D = B_1 + (0, 0, 3) = \{(\mathbf{0}, \mathbf{0}, \mathbf{3}), (\mathbf{1}, \mathbf{0}, \mathbf{4}), (1, 0, 2), (4, 1, 3), (4, 4, 3)\}.$$

The line through $(1, 0, 4) \in B_1$ and $(4, 2, 3) \in C$ is

$$D' = B_6 + (0, 4, 0) = \{(0, 4, 0), (\mathbf{1}, \mathbf{0}, \mathbf{4}), (1, 3, 1), (\mathbf{4}, \mathbf{2}, \mathbf{3}), (4, 1, 2)\}.$$

These two lines D and D' also belong to $\mathcal{B}_\pi$ since they also join two points of π. We also note that they are both disjoint with the line $B_0 \in \mathcal{B}_\pi$. This contradicts the Euclid's parallel axiom: there is a point of π (that is $(1,0,4)$) and two distinct lines of π through this point (D and D') which are both disjoint with a line of π (that is B_0).

Now consider the $(7,7,6)$ Paley difference multiset of the first type, that is $\{0\} \cup \underline{2}\{1,2,4\}$, and apply Construction 5.3 lifting it to a suitable 7-subset of $\mathbb{F}_{49}$. Without entering all the details, we just list the base blocks of the resultant $(\mathbb{Z}_7^3, \mathbb{Z}_7 \times \{0\} \times \{0\}, 7, 1)$-DF.

$$\{(0,0,0),(1,1,0),(1,6,0),(2,2,1),(2,5,6),(4,2,0),(4,5,0)\}$$

$$\{(0,0,0),(1,2,4),(1,5,3),(2,0,3),(2,0,4),(4,4,1),(4,3,6)\}$$

$$\{(0,0,0),(1,2,2),(1,5,5),(2,2,6),(2,5,1),(4,4,4),(4,3,3)\}$$

$$\{(0,0,0),(1,3,5),(1,4,2),(2,1,6),(2,6,1),(4,6,3),(4,1,4)\}$$

$$\{(0,0,0),(1,0,1),(1,0,6),(2,6,2),(2,1,5),(4,0,2),(4,0,5)\}$$

$$\{(0,0,0),(1,3,2),(1,4,5),(2,4,0),(2,3,0),(4,6,4),(4,1,3)\}$$

$$\{(0,0,0),(1,5,2),(1,2,5),(2,1,2),(2,6,5),(4,3,4),(4,4,3)\}$$

$$\{(0,0,0),(1,2,3),(1,5,4),(2,1,1),(2,6,6),(4,4,6),(4,3,1)\}$$

One can check that the design generated by the above DF is anomalous with the same isomorphism test used for getting the anomalous 2-$(5^3,5,1)$ design. $\square$

The above results allow us to state the following.

Corollary 6.3. *There exists an anomalous* 2-$(p^n,p,1)$ *design for* $p \in \{5,7\}$ *and any integer* $n \geq 3$.

We tried to get an anomalous 2-$(11^3,11,1)$ design with the same method used in the proof of Theorem 6.2, i.e., by means of a suitable lifting of the $(11,11,10)$ Paley difference multiset $\{0\} \cup \{1,3,4,5,9\}$, but we fail.

7 Cyclotomy

Starting from the fundamental paper of Wilson [37], cyclotomy has been very often crucial in the construction of many classes of difference families. Here it is also crucial for getting a good lifting of a SDF as required by Construction 5.3.

Given a prime power $q \equiv 1 \pmod{\lambda}$, let C^λ be the subgroup of $\mathbb{F}_q^*$ of index λ. If r is a fixed primitive element of $\mathbb{F}_q$, then $\{r^iC^\lambda \mid 0 \leq i \leq \lambda-1\}$ is the set of cosets of C^λ in $\mathbb{F}_q^*$. For $i = 0,1,\ldots,\lambda-1$, the coset r^iC^λ

will be denoted by C_i^λ and it is called *the i-th cyclotomic class of order* λ. Note that we have $C_i^\lambda \cdot C_j^\lambda = C_{i+j\ (mod \lambda)}^\lambda$. We will need the following lemma deriving from the theorem of Weil on multiplicative character sums (see [28], Theorem 5.41).

Lemma 7.1. [14] *Let $q \equiv 1 \pmod{\lambda}$ be a prime power and let t be a positive integer. Then, for any t-subset $C = \{c_1, \ldots, c_t\}$ of $\mathbb{F}_q$ and for any ordered t-tuple $(\gamma_1, \ldots, \gamma_t)$ of $\mathbb{Z}_\lambda^t$, the set $X := \{x \in \mathbb{F}_q : x - c_i \in C_{\gamma_i}^\lambda \text{ for } i = 1, \ldots, t\}$ has arbitrarily large size provided that q is sufficiently large.*

In particular, we have $|X| > 2\lambda^{t-1}$ for $q > t^2\lambda^{2t}$.

In most cases the above lemma has been used to prove that the set X is not empty. But this is not enough for our purposes. The last sentence in the above statement is formula (2) in [14].

The following theorem is essentially Corollary 5.3 in [14] where it appeared as a special consequence of a more general result. Here, for convenience of the reader, it is better to show its proof directly. Then we will see how this proof can be modified in order to get its *additive version*.

Theorem 7.2. *If there exists a (G, k, λ)-SDF, then there exists a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF for every prime power $q \equiv \lambda + 1$ (mod 2λ) provided that $q > (k-1)^2\lambda^{2k-2}$.*

Proof. Let $\Sigma = \{B_1, \ldots, B_s\}$ be a (G, k, λ)-SDF with $B_h = \{b_{h1}, \ldots, b_{hk}\}$ for $1 \leq h \leq s$. Let T be the set of all triples (h, i, j) with $h \in \{1, \ldots, s\}$ and i, j distinct elements of $\{1, \ldots, k\}$. For every $g \in G$, let T_g be the set of triples (h, i, j) of T such that $b_{h,i} - b_{h,j} = g$. Note that $\bigcup_{g \in G} T_g$ is a partition of T and that each T_g has size λ by definition of a (G, k, λ)-SDF. Thus it is possible to choose a map $\psi : T \longrightarrow \mathbb{Z}_\lambda$ satisfying the following conditions:

1) the restriction $\psi|_{T_g}$ is bijective for any $g \in G$;

2) $\psi(h, j, i) = \psi(h, i, j) + \lambda/2$ for every pair of distinct i, j.

As a matter of fact the number Ψ of all maps ψ satisfying the above conditions is huge. If $\lambda = 2\mu$ and $|G| = 2^n m$ where 2^n is the order of $I(G)$, it is easy to see that $\Psi = \lambda!^{2^{n-1}(m-1)}(2^\mu\mu!)^{2^n}$.

Now lift each B_h to a subset $\ell(B_h) = \{(b_{h1}, \ell_{h1}), \ldots, (b_{hk}, \ell_{hk})\}$ of $G \times \mathbb{F}_q$ by taking the first element $\ell_{h,1}$ arbitrarily and then by taking the other elements $\ell_{h,2}$, $\ell_{h,3}$, $\ldots$, $\ell_{h,k}$ iteratively, one by one, according to the rule that once that $\ell_{h,i-1}$ has been chosen, we pick $\ell_{h,i}$ arbitrarily in the set

$$X_{h,i} = \{x \in \mathbb{F}_q \ : \ x - \ell_{h,j} \in C_{\psi(h,i,j)}^\lambda \quad \text{for } 1 \leq j \leq i-1\}.$$

Note that $\{\ell_{h,1}, ..., \ell_{h,i-1}\}$ is actually a set, i.e., it does not have repeated elements. Indeed given two elements $j_1 < j_2$ in $\{1, \ldots, i-1\}$, we have $\ell_{h,j_2} - \ell_{h,j_1} \in C_{\psi(h,j_2,j_1)}^\lambda$ since ℓ_{h,j_2} has been picked in X_{h,j_2}. Thus we cannot have $\ell_{h,j_2} = \ell_{h,j_1}$. It follows that $X_{h,i}$ is not empty by Lemma 7.1, hence an element $\ell_{h,i}$ with the above requirement can be actually chosen.

Also note that we have

$$\ell_{h,i} - \ell_{h,j} \in C^{\lambda}_{\psi(h,i,j)} \quad \forall (h,i,j) \in T \tag{7.1}$$

This is clear if $i > j$ considering the rule that we followed for selecting the $\ell_{h,i}$'s. If $i < j$, for the same reason, we have $\ell_{h,j} - \ell_{h,i} \in C^{\lambda}_{\psi(h,j,i)}$, i.e., $\ell_{h,j} - \ell_{h,i} \in C^{\lambda}_{\psi(h,i,j)+\lambda/2}$ in view of the second property of ψ. Multiplying by -1 and considering that $-1 \in C^{\lambda}_{\lambda/2}$ since $q \equiv \lambda + 1 \pmod{2\lambda}$, we get (7.1) again.

We finally note that we have $\biguplus_{h=1}^{s} \Delta\ell(B_h) = \biguplus_{g\in G}\{g\} \times \Delta_g$ with $\Delta_g = \{\ell_{h,i} - \ell_{h,j} \mid (h,i,j) \in T_g\}$. Thus, in view of (7.1) and the first property of ψ, we see that Δ_g is a complete system of representatives for the cyclotomic classes of order λ whichever is $g \in G$. At this point we get the required $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF by applying Construction 5.3 as pointed out at the end of Section 5. $\square$

The additive version of the above theorem is straightforward in the case that $rad(q)$ is not a divisor of k. On the contrary, if $rad(q)$ divides k, which in view of Lemma 3.5 is the case we are interesting in, we have to lift the base blocks of the given additive SDF much more carefully. Also, we need to raise the bound on q significantly, and to ensure that the order of G is not too large.

Theorem 7.3. *Assume that there exists an additive (G, k, λ)-SDF of size s with $k \neq 3$ and let $q \equiv \lambda + 1 \pmod{2\lambda}$ be a prime power. Then there exists an additive $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF in each of the following cases:*

(i) $rad(q)$ does not divide k and $q > (k-1)^2\lambda^{2k-2}$;

(ii) $rad(q)$ divides k, $|G| < 2\lambda^{2k-5}s$ and $q > (2k-3)^2\lambda^{4k-6}$.

Proof. Let $\Sigma = \{B_1, \ldots, B_s\}$ be a (G, k, λ)-SDF as in the proof of the previous theorem and let $q \equiv \lambda + 1 \pmod{2\lambda}$ be a prime power.

(i) k is not divisible by $rad(q)$, and $q > (k-1)^2\lambda^{2k-2}$.
Take a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF, say $\mathcal{F}$, which exists by Theorem 7.2. For every block $B \in \mathcal{F}$, let σ_B be the sum of the second coordinates of all elements of B and set $B' = B + (0, -\frac{\sigma_B}{k})$. It is evident that $\{B' \mid B \in \mathcal{F}\}$ is an additive $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF.

(ii) $rad(q)$ divides k, $|G| < 2\lambda^{2k-5}s$, and $q > (2k-3)^2\lambda^{4k-6}$.
We keep the same notation as in the proof of the above theorem and the procedure for getting $\ell(B_h)$ will be exactly the same until determining the element $\ell_{h,k-4}$. After that we have to be much more careful in picking the last four elements $\ell_{h,k-3}$, $\ell_{h,k-2}$, $\ell_{h,k-1}$ and $\ell_{h,k}$. In the following, we set $\sigma_{h,i} = \sum_{j=1}^{i} \ell_{h,j}$ once that all $\ell_{h,j}$'s with $1 \le j \le i$ have been chosen.

Choice of $\ell_{h,k-3}$.
If $rad(q) \neq 3$, just proceed as in the proof of Theorem 7.2; we can take $\ell_{h,k-3}$ in $X_{h,k-3}$ arbitrarily. If $rad(q) = 3$ we take it in $X_{h,k-3} \setminus \{-\sigma_{h,k-4}\}$. Note that $rad(q) = 3$ implies $k > 4$ since we have $k \neq 3$ by assumption, hence it makes sense to consider the sum $\sigma_{h,k-4}$.

Choice of $\ell_{h,k-2}$.
We pick this element in $X_{h,k-2} \setminus Y$, where Y is the union of the sets

$$Y_1 = \{-\sigma_{h,k-3} - \ell_{h,i} - \ell_{h,j} \mid 1 \leq i \leq j \leq k-3\},$$

$$Y_2 = \{-\sigma_{h,k-3} - \ell_{h,i} \mid 1 \leq i \leq k-3\}, \qquad Y_3 = \frac{1}{2}Y_2,$$

and, only in the case that $rad(q) \neq 3$, the singleton $Y_4 = \{-\frac{\sigma_{h,k-3}}{3}\}$. Note that this selection can be done since $|X_{h,k-2}| > |Y|$. Indeed we have $|X_{h,k-2}| > 2\lambda^{k-4}$ by Lemma 7.1 and $2\lambda^{k-4} > \frac{\lambda|G|}{s}$ in view of the upper bound on the order of G. Also, we have $\frac{\lambda|G|}{s} = k(k-1)$ since, as observed after Definition 5.1, we have $\lambda|G| = sk(k-1)$. Finally, it is evident that Y has size less than $k(k-1)$.

Choice of $\ell_{h,k-1}$.
We pick this element in the set

$$X'_{h,k-1} = \{x \in \mathbb{F}_q \ : \ x - c_{h,j} \in C^{\lambda}_{\gamma_{h,j}} \text{ for } 1 \leq j \leq 2k-3\}$$

with the pairs $(c_{h,j}, \gamma_{h,j})$ defined as follows:

$$c_{h,j} = \ell_{h,j} \quad \text{and} \quad \gamma_{h,j} = \psi(h, k-1, j) \quad \text{for } 1 \leq j \leq k-2;$$

$$c_{h,k-2+j} = -\sigma_{h,k-2} - \ell_{h,j} \quad \text{and} \quad \gamma_{h,k-2+j} = \psi(h,k,j) + \frac{\lambda}{2} \quad \text{for } 1 \leq j \leq k-2;$$

$$c_{h,2k-3} = -\frac{\sigma_{h,k-2}}{2} \quad \text{and} \quad \gamma_{h,2k-3} = \psi(h,k,k-1) - \alpha$$

where C^{λ}_{α} is the cyclotomic class of order λ containing -2.

Note that the first $k-2$ conditions required for the generic element of $X'_{h,k-1}$ are exactly the conditions for the generic element of $X_{h,k-1}$. Thus $X'_{h,k-1}$ is a subset of $X_{h,k-1}$.

Assume that $c_{h,j_1} = c_{h,j_2}$ with $1 \leq j_1 < j_2 \leq 2k-3$.

If $j_2 \leq k-2$, then we have $\ell_{h,j_1} = \ell_{h,j_2}$ which contradicts the fact that $\ell_{h,j_2} - \ell_{h,j_1} \in C^{\lambda}_{\psi(h,j_2,j_1)}$ (recall indeed that ℓ_{h,j_2} is in X_{h,j_2}).

For the same reason, we cannot have $k-1 \leq j_1 < j_2 \leq 2k-4$.

If $j_1 = k-2$ and $j_2 = 2k-3$ we get $-\sigma_{h,k-3} - 3\ell_{h,k-2}$. If $rad(q) = 3$, this means $\sigma_{h,k-3} = 0$, hence $\ell_{h,k-3} = -\sigma_{h,k-4}$ contradicting the choice of $\ell_{h,k-3}$ in this case. If $rad(q) \neq 3$, then we would have $\ell_{h,k-2} = -\frac{\sigma_{h,k-3}}{3}$ contradicting the choice of $\ell_{h,k-2}$ in this case.

In all the remaining cases the reader can check that we would get $\ell_{h,k-2} \in Y$. On the other hand, $\ell_{h,k-2}$ had been picked out of Y on purpose. We conclude that the $c_{h,j}$'s ($j = 1, 2, \ldots, 2k-3$) are pairwise distinct. Thus, Lemma 7.1 and the assumption $q > (2k-3)^2\lambda^{4k-6}$ guarantee that $X'_{h,k-1}$ is not empty and the selection of $\ell_{h,k-1}$ described above can be actually done.

Choice of $\ell_{h,k}$.
Take $\ell_{h,k} = -\sigma_{h,k-1}$. This last (obligatory) choice assures that $\ell(B_h)$ is zero-sum; the sum of the first coordinates of all its elements is zero because Σ is additive, and the sum of the second coordinates of all its elements is $\sigma_{h,k} = \sigma_{h,k-1} + \ell_{h,k} = 0$.

It is evident that $\ell_{h,i} \in X_{h,i}$ for $1 \leq i \leq k-1$. As a consequence of the fact that $\ell_{h,k-1} \in X'_{h,k-1}$, we show that this is true also for $i = k$, i.e., that we have $\ell_{h,k} - \ell_{h,j} \in C^\lambda_{\psi(h,k,j)}$ for $1 \leq j \leq k-1$.

$1 \leq j \leq k-2$: by definition of $X'_{h,k-1}$, we have

$$\ell_{h,k-1} - c_{h,k-2+j} \in C^\lambda_{\psi(h,k,j)+\lambda/2}. \tag{7.2}$$

Now note that $\ell_{h,k-1} - c_{h,k-2+j} = -\ell_{h,k} + \ell_{h,j}$ by the definitions of $c_{h,k-2+j}$ and $\ell_{h,k}$. Thus, multiplying (7.2) by -1 and recalling that $-1 \in C^\lambda_{\lambda/2}$, we actually get $\ell_{h,k} - \ell_{h,j} \in C^\lambda_{\psi(h,k,j)}$.

$j = k-1$: considering the last condition required for the generic element of $X'_{h,k-1}$, we have $\ell_{h,k-1} + \frac{\sigma_{h,k-2}}{2} \in C^\lambda_{\psi(h,k,k-1)-\alpha}$. Multiplying by -2 and remembering that $-2 \in C^\lambda_\alpha$ we get $-2\ell_{h,k-1} - \sigma_{h,k-2} \in C^\lambda_{\psi(h,k,k-1)}$ which is what we wanted. Indeed, by definition of $\ell_{h,k}$, we have $-2\ell_{h,k-1} - \sigma_{h,k-2} = \ell_{h,k} - \ell_{h,k-1}$.

We conclude that the above constructed liftings are in the same situation of the liftings constructed in the proof of Theorem 7.2, i.e., (7.1) holds. Thus, reasoning as at the end of that proof, we can say that they form a $(G \times \mathbb{F}_q, G \times \{0\}, k, 1)$-DF. The assertion follows considering that each of these liftings is zero-sum. □

We are going to see that the above theorem allows to obtain a difference family as required in Lemma 3.5 as soon as one has an additive (G, k, λ)-SDF with G a zero-sum group of order k and λ not divisible by $rad(k)$. This will be the crucial ingredient for proving our main result.

Lemma 7.4. *Assume that there exists an additive (G, k, λ)-SDF with G a zero-sum group of order k and assume that k has a prime divisor not dividing λ. Then there exists a G-super-regular 2-$(v, k, 1)$ design for infinitely many values of v.*

Proof. Let Σ be a SDF as in the statement and let p be a prime divisor of k not dividing λ. Let n be the order of p in the group of units of $\mathbb{Z}_\lambda$, let 2^e be the largest power of 2 dividing $\frac{p^n-1}{\lambda}$, and set $\lambda_1 = 2^e\lambda$. Clearly, $\underline{2^e}\Sigma$ is an additive (G,k,λ_1)-SDF. We have $p^n-1=2^e\lambda\mu$ with μ odd, hence $q^n\equiv\lambda_1+1 \pmod{2\lambda_1}$. It easily follows, by induction on i, that $p^{ni}\equiv\lambda_1+1 \pmod{2\lambda_1}$ for every odd i. It is obvious that $|G|=k<2\lambda_1^{2k-5}$ and of course there are infinitely many odd values of i for which $p^{ni}>(2k-3)^2\lambda_1^{4k-6}$. Hence, by Theorem 7.3, there exists an additive $(G\times\mathbb{F}_{p^{ni}}, G\times\{0\}, k, 1)$-DF for each of these odd values of i. The assertion then follows from Lemma 3.5. $\square$

8 The main result

For the proof of the main result we need one more ingredient, that is the notion of a *difference matrix*.

If G is an additive group of order v, a (v,k,λ) difference matrix in G (or briefly a (G,k,λ)-DM) is a $(k\times\lambda v)$-matrix with entries in G such that the difference of any two distinct rows contains every element of G exactly λ times. For general background on difference matrices we refer to [3, 21].

We will say that a DM is *additive* if each of its columns is zero-sum. An adaptation of an old construction for ordinary difference families by Jungnickel [29] allows us to prove the following.

Lemma 8.1. *If Σ is an additive (G,k,λ)-SDF and M is an additive (H,k,μ)-DM, then there exists an additive $(G\times H,k,\lambda\mu)$-SDF.*

Proof. Let Σ be a (G,k,λ)-SDF and let $M=(m_{rc})$ be an (H,k,μ)-DM. For each block $B=\{b_1,\dots,b_k\}\in\Sigma$ and each column $M^c=(m_{1c},\dots,m_{kc})^T$ of M, consider the k-multiset $B\circ M^c$ defined as follows:

$$B\circ M^c=\{(b_1,m_{1c}),\dots,(b_k,m_{kc})\}.$$

It is straightforward to check that

$$\Sigma\circ M:=\{B\circ M^c \mid B\in\mathcal{F}; 1\le c\le\mu|H|\}$$

is a $(G\times H,k,\lambda\mu)$-SDF. It is clearly additive in the hypothesis that both Σ and M are additive. $\square$

In the proof of the following theorem we construct the crucial ingredient considered in Lemma 7.4.

Theorem 8.2. *Let k be a positive integer which is neither a prime power, nor singly even, nor of the form 2^n3. Then there exists an additive (G,k,λ)-SDF in a suitable zero-sum group of order k with* $\gcd(k,\lambda)=1$.

Proof. Let q be the largest odd prime power factor of k and set $k=qr$. The hypotheses on k guarantee that q is greater than 3. Now consider the k-multiset A on $\mathbb{F}_q$ which is union of r copies of the $(q,q,q-1)$ Paley difference multiset of the first type:

$$A=\underline{r}\{0\}\ \uplus\ \underline{2r}\mathbb{F}_q^\square.$$

Let $\alpha : \mathbb{F}_q \longrightarrow \mathbb{N}$ be the map where $\alpha(x)$ is the multiplicity of x in ΔA for every $x \in \mathbb{F}_q$. We have

$$\alpha(0) = r(r-1) + \frac{q-1}{2}2r(2r-1) = (2q-1)r^2 - qr.$$

Now let x be an element of $\mathbb{F}_q^*$ and distinguish two cases according to whether $q \equiv 1$ or $3 \pmod 4$.

1st case: $q \equiv 1 \pmod 4$. In this case it is well-known that $\mathbb{F}_q^{\square}$ is a partial $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$ difference set[2]. If $x \in \mathbb{F}_q^{\square}$, there are $\frac{q-5}{4}$ representations of x as a difference from $\mathbb{F}_q^{\square}$. Each of them has to be counted $(2r)^2$ times in the number of representations of x as a difference from A. The remaining representations of x as a difference from A are $x = x - 0$ ($2r \cdot r$ times) and $x = 0 - (-x)$ ($r \cdot 2r$ times). Thus we have $\alpha(x) = (4r^2)\frac{q-5}{4} + 2r^2 + 2r^2 = (q-1)r^2$.

If $x \in \mathbb{F}_q^{\boxslash}$, there are $\frac{q-1}{4}$ representations of x as a difference from $\mathbb{F}_q^{\square}$. Each of them has to be counted $(2r)^2$ times in the number of representations of x as a difference from A. There is no other representation of x as a difference from A. Hence we have $\alpha(x) = (4r^2)\frac{q-1}{4} = (q-1)r^2$.

2nd case: $q \equiv 3 \pmod 4$. Here, $\mathbb{F}_q^{\square}$ is a $(q, \frac{q-1}{2}, \frac{q-3}{4})$ difference set. Every $x \in \mathbb{F}_q^*$ admits precisely $\frac{q-3}{4}$ representations as a difference from $\mathbb{F}_q^{\square}$. Each of them has to be counted $(2r)^2$ times in the number of representations of x as a difference from A. The remaining representations of x as a difference from A are $x = x - 0$ ($2r \cdot r$ times) if x is a square, or $x = 0 - (-x)$ ($r \cdot 2r$ times) if x is not a square. Thus, for every $x \in \mathbb{F}_q^*$ we have $\alpha(x) = (4r^2)\frac{q-3}{4} + 2r^2 = (q-1)r^2$.

In summary, we have:

$$\alpha(0) = (2q-1)r^2 - qr \quad \text{and} \quad \alpha(x) = (q-1)r^2 \ \forall x \in \mathbb{F}_q^* \tag{8.1}$$

Now let $B = \underline{r}\mathbb{F}_q$ be the k-multiset which is union of r copies of $\mathbb{F}_q$ and let $\beta : \mathbb{F}_q \longrightarrow \mathbb{N}$ be the map of multiplicities of ΔB. It is quite evident that we have:

$$\beta(0) = qr(r-1) \quad \text{and} \quad \beta(x) = qr^2 \ \forall x \in \mathbb{F}_q^* \tag{8.2}$$

We claim that

$$\Sigma = \{A, \underbrace{B, \ldots, B}_{r-1 \text{ times}}\}$$

is a $(q, k, (k-1)r^2)$-SDF in $\mathbb{F}_q$. Indeed, if σ is the map of multiplicities of $\Delta\Sigma$, in view of (8.1) and (8.2) we have:

$$\sigma(0) = \alpha(0) + (r-1)\beta(0) = (2q-1)r^2 - qr + qr(r-1)^2 = (qr-1)r^2;$$

$$\sigma(x) = (q-1)r^2 + qr^2(r-1) = (qr-1)r^2 \quad \forall x \in \mathbb{F}_q^*.$$

[2] A k-subset B of an additive group G of order v is a (v, k, λ, μ) *partial difference set* if $\Delta B = \underline{\lambda}(B \setminus \{0\}) \ \cup \ \underline{\mu}(G \setminus (B \cup \{0\})$. If $\lambda = \mu$ then B is a (v, k, λ) *difference set.*

Considering that $\mathbb{F}_q^\square$ is a zero-sum subset of $\mathbb{F}_q$ for $q > 3$ (see Fact 2.2), the multiset A is zero-sum. Also, considering that $\mathbb{F}_q$ is zero-sum, B is zero-sum as well. We conclude that Σ is additive.

The hypothesis that k is not singly even implies that r is also not singly even. Hence we can take an abelian zero-sum group H of order r. Let M be the matrix whose columns are all possible zero-sum k-tuples of elements of H summing up to zero. Let (i, j) be any pair of distinct elements of $\{1, \dots, k\}$ and let h be any element of H. The number of zero-sum k-tuples $(m_1, ..., m_k)$ of elements of H such that $m_i - m_j = h$ is equal to r^{k-2}. Indeed each of these k-tuples can be constructed as follows. Fix any element ℓ in $\{1, ..., k\} \setminus \{i, j\}$, take m_x arbitrarily for $x \notin \{i, \ell\}$, and then we are forced to take $m_i = m_j + h$ and $m_\ell = -\sum_{x \neq \ell} m_x$.

The above means that there are exactly r^{k-2} columns $(m_{1,c}, \dots, m_{k,c})^T$ of M such that $m_{i,c} - m_{j,c} = h$. Equivalently, the difference between the ith row and the jth row of M covers the element h exactly r^{k-2} times. Thus, in view of the arbitrariness of i, j and h, M is a (r, k, r^{k-2}) difference matrix. Of course it is additive by construction.

Thus, applying Lemma 8.1, we can say that $\Sigma \circ M$ is an additive (k, k, λ)-SDF in $G := \mathbb{F}_q \times H$ with $\lambda = (k-1)r^k$. Recall that q is the largest odd prime power factor of k so that q is coprime with both $k - 1$ and $r = \frac{k}{q}$. Thus λ is coprime with k and the assertion follows. $\square$

Proof of Theorem 1.4. If k is a prime power we have the super-regular 2-$(k^n, k, 1)$ designs associated with $AG(n, k)$. The singly even values of k are genuine exceptions in view of Proposition 3.3(iv). Finally, if k is neither a prime power, nor singly even, nor of the form $2^n 3$, then the assertion follows from Theorem 8.2 and Lemma 7.4. $\square$

9 A huge number of points

As already mentioned in the introduction the super-regular Steiner 2-designs obtainable by means of the main construction (Theorem 8.2 combined with Lemma 7.4) have a huge number of points. On the other hand, there are some hopes to find more handleable super-regular Steiner 2-designs. We discuss this for the first relevant value of k, that is $k = 15$.

Let us examine, first, which is the smallest v for which the main construction leads to a non-trivial super-regular 2-$(v, 15, 1)$ design. Keeping the same notation as in Theorem 8.2, we have $q = 5$, $r = 3$ and $\Sigma \circ M$ is a $(15, 15, \lambda)$-SDF in $\mathbb{Z}_3 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{15}$ with $\lambda = 14 \cdot 3^{15}$. Now proceed as in the proof of Lemma 7.4 taking $p = 5$. The order of 5 in $\mathbb{Z}_\lambda$ is $n = 2 \cdot 3^{14} = 9565938$ and the largest power of 2 in $\frac{q^n-1}{\lambda}$ is 4. Thus $\underline{4}(\Sigma \circ M)$ is a $(15, 15, \lambda_1)$-SDF with $\lambda_1 = 4\lambda$ and we have $5^{ni} \equiv \lambda_1 + 1 \pmod{2\lambda_1}$ for every odd i. One can check that $5^n > (2k-3)^2 \lambda_1^{4k-6} = 27^2 \cdot (56 \cdot 3^{15})^{54}$. Hence we have an additive $(\mathbb{Z}_{15}\times\mathbb{F}_{5^n},\mathbb{Z}_{15}\times\{0\},15,1)$-DF. In conclusion, the first v for which the application of Lemma 7.4 with the use of $\Sigma\circ M$ leads to a super-regular 2-$(v,15,1)$ design is $3\cdot 5^{9565939}$.

On the other hand, in this specific case, we can find a much lower v with the use of another SDF. Consider the following three 15-multisets on $\mathbb{Z}_{15}$

$$B=\{0\}\ \cup\ \underline{2}\{1,2,3,7,9,11,12\};$$

$$B'=\{0\}\ \cup\ \underline{2}\{1,3,4,5,7,12,13\};$$

$$B''=\{0\}\ \cup\ \underline{2}\{1,5,8,10,11,12,13\}.$$

It is straightforward to check that $\Sigma'=\{B,B',B''\}$ is an additive $(15,15,\lambda')$-SDF with $\lambda'=42$. Let us apply Lemma 7.4 using Σ' rather than $\Sigma\circ M$. The order of $q=5$ in $\mathbb{Z}_{\lambda'}$ is $n=6$ and the largest power of 2 in $\frac{q^n-1}{\lambda'}$ is 4. Thus $\underline{4}\Sigma'$ is a $(15,15,\lambda'_1)$-SDF with $\lambda'_1=4\lambda'$ and we have $5^{6i}\equiv\lambda'_1+1 \pmod{2\lambda'_1}$ for every odd i. The first odd i for which $5^{ni}>(2k-3)^2{\lambda'_1}^{4k-6}$ is 31. Hence, the first v for which the use of Σ' in Lemma 7.4 gives a super-regular 2-$(v,15,1)$ design is $3\cdot 5^{187}$.

Now we show a more clever use of Σ' which exploits its nice form (every base block is of the form $\{0\}\ \cup\ \underline{2}A$ with A a 7-subset of $\mathbb{Z}_{15}\setminus\{0\}$). Let $q\equiv 1 \pmod{42}$ be a prime power and lift the blocks of Σ' to three zero-sum 15-subsets of $\mathbb{Z}_{15}\times\mathbb{F}_q$ of the form

$$\ell(B)=\{(0,0),(1,\pm\ell_1),(2,\pm\ell_2),(3,\pm\ell_3),(7,\pm\ell_4),(9,\pm\ell_5),(11,\pm\ell_6),(12,\pm\ell_7)\},$$

$$\ell(B')=\{(0,0),(1,\pm\ell'_1),(3,\pm\ell'_2),(4,\pm\ell'_3),(5,\pm\ell'_4),(7,\pm\ell'_5),(12,\pm\ell'_6),(13,\pm\ell'_7)\},$$

$$\ell(B'')=\{(0,0),(1,\pm\ell''_1),(5,\pm\ell''_2),(8,\pm\ell''_3),(10,\pm\ell''_4),(11,\pm\ell''_5),(12,\pm\ell''_6),(13,\pm\ell''_7)\},$$

where, to save space, we have written $(x,\pm y)$ to mean the two pairs (x,y) and $(x,-y)$. We have $\Delta\ell(B)\ \cup\ \Delta\ell(B')\ \cup\ \Delta\ell(B'')=\displaystyle\bigcup_{i=0}^{14}\{i\}\times\Delta_i$ with $\Delta_i=\{1,-1\}\cdot\overline{\Delta}_i$ where each $\overline{\Delta}_i$ is a list of 21 elements of $\mathbb{F}_q$. For instance, it is readily seen that $\overline{\Delta}_0=\{\ell_i,\ell'_i,\ell''_i\mid 1\leq i\leq 7\}$.

Assume that the above liftings are done in such a way that each $\overline{\Delta}_i$ is a complete system of representatives for the cyclotomic classes of order 21. In this case we have $\Delta_i\cdot M=\mathbb{F}_q^*$ with M a system of representatives for the cosets of $\{1,-1\}$ in C^{21} and then, by Construction 5.3, we get an additive $(\mathbb{Z}_{15}\times\mathbb{F}_q,\mathbb{Z}_{15}\times\{0\},15,1)$-DF. Reasoning as in the proof of Theorem 7.2, one can see that the required liftings certainly exist by Lemma 7.1 provided that $q>6^2\cdot 21^{12}$. Now note that we have $5^{6i}\equiv 1 \pmod{42}$ for every $i\geq 0$ and $5^{6i}>6^2\cdot 21^{12}$ as soon as $i\geq 5$. Thus we have an additive $(\mathbb{Z}_{15}\times\mathbb{F}_{5^{30}},\mathbb{Z}_{15}\times\{0\},15,1)$-DF. So the first v for which this construction leads, theoretically, to a strictly additive 2-$(v,15,1)$ design is $3\cdot 5^{31}$ that is dramatically smaller than the value obtained before by applying the main construction "with the blinkers". Yet, it is still huge! We cannot exclude, however, that by means of a (probably heavy) computer work one may realize a good lifting of Σ' with $q = 5^6$. In this case we should have a 2-$(3 \cdot 5^7, 15, 1)$ design.

10 Super-regular non-Steiner 2-designs

As underlined in the introduction, the paper is focused on super-regular Steiner 2-designs since their construction appears to be challenging. Here we just sketch how the methods used in the previous sections allow to obtain super-regular non-Steiner 2-designs much more easily and with a relatively "small" number of points. In particular, without any need of cyclotomy (that is the heaviest tool used) it is possible to show that every additive (k, k, λ)-SDF with k not singly even gives rise to a super-regular 2-(kq, k, λ) design for any power $q > k$ of a prime divisor of k.

First, we need to recall the following well known fact.

Proposition 10.1. *Let $\mathcal{F}$ be a (v, k, k, λ)-DF in G relative to H, let $\mathcal{C}$ be the set of right cosets of H in G, and set*

$$\mathcal{B} = \{B + g \mid B \in \mathcal{F}; g \in G\} \ \cup \ \underline{\lambda}\mathcal{C}.$$

Then $(G, \mathcal{B})$ is a G-regular 2-(v, k, λ) design.

The above is contained in Remark 3.2 (r2) for $\lambda = 1$ and produces a non-simple design for $\lambda > 1$.

Lemma 10.2. *If there exists an additive $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$-DF with G a zero-sum group of order k, then there exists a super-regular 2-(kq, k, λ) design.*

Proof. The $(G \times \mathbb{F}_q)$-regular 2-(kq, k, λ) design obtainable from $\mathcal{F}$ using Proposition 10.1 is clearly additive. The assertion follows. □

Theorem 10.3. *If there exists an additive (k, k, λ)-SDF with k not singly even, then there exists a super-regular 2-(kq, k, λ) design for every power $q > k$ of a prime divisor of k.*

Proof. Let $\Sigma = \{B_1, \dots, B_s\}$ be an additive (k, k, λ)-SDF in G and let q be a prime power as in the statement. Take a zero-sum k-subset $L = \{\ell_1, \dots, \ell_k\}$ of $\mathbb{F}_q$ whose existence is almost evident[3]. Lift each block $B_h = \{b_{h1}, \dots, b_{hk}\}$ of Σ to the subset $L_h = \{(b_{h1}, \ell_1), \dots, (b_{hk}, \ell_k)\}$ of $G \times \mathbb{F}_q^*$. By definition of a strong difference family, we have $\Delta\{L_1, ..., L_h\} = \biguplus_{g \in G}\{g\} \times \Delta_g$ where each Δ_g is a λ-multiset on $\mathbb{F}_q^*$ so that we have

$$\Delta_g \cdot \mathbb{F}_q^* = \underline{\lambda}\mathbb{F}_q^* \quad \forall g \in G. \tag{10.1}$$

[3]It is also an immediate consequence of a formula giving the precise number of k-subsets of $\mathbb{F}_q$ whose sum is an assigned $b \in \mathbb{F}_q$ (see Theorem 1.2 in [27] or, for an easier proof, Theorem 1.1(3) in [33]).

Given $m \in \mathbb{F}_q^*$, denote by $L_h \circ m$ the subset of $G \times \mathbb{F}_q$ obtained from L_h by multiplying the second coordinates of all its elements by m. Taking (10.1) into account, it is easily seen that

$$\mathcal{F} = \{L_h \circ m \mid 1 \leq h \leq s; m \in \mathbb{F}_q^*\} \tag{10.2}$$

is a $(G \times \mathbb{F}_q, G \times \{0\}, k, \lambda)$-DF. Also, we note that $\mathcal{F}$ is additive since Σ is additive and L is zero-sum. The assertion then follows from Lemma 10.2. □

Applying the above theorem using the $(15, 15, 42)$-SDF given in the previous section, we find a super-regular 2-$(15q, 15, 42)$ design for every power q of 3 or 5 not smaller than 25. Here, however, in view of the special form of the used $(15, 15, 42)$-SDF, one could see that if L is chosen more carefully as in Section 9 and if in (10.2) we make m vary in a system of representatives for the cosets of $\{1, -1\}$ in $\mathbb{F}_q^*$ rather than in the whole $\mathbb{F}_q^*$, we get an additive a $(\mathbb{Z}_{15} \times \mathbb{F}_q, \mathbb{Z}_{15} \times \{0\}, 15, \lambda)$-DF with $\lambda = 21$ rather than 42. Thus we can say that there exists a super-regular 2-$(15q, 15, 21)$ design for every power q of 3 or 5 not smaller than 25. In particular, using $q = 25$, we can say that there exists a super-regular 2-$(375, 15, 21)$ design.

11 Open questions

Our research leaves open several questions. The most intriguing is probably the following.

(Q1) Does there exist a strictly G-additive Steiner 2-design which is not G-regular?

Here are some other questions which naturally arise.

(Q2) Do there exist strictly additive 2-$(v, k, 1)$ designs with k singly even?

(Q3) Do there exist super-regular Steiner 2-designs with block size $k = 2^n 3 \geq 12$?

Finally, it would be desirable to solve the following problem.

(P) Find an additive Steiner 2-design with a non-primepower block size and a "reasonably small" number of points.

Acknowledgements

The authors wish to thank the anonymous referees for their careful reading and some helpful comments.

This work has been performed under the auspices of the G.N.S.A.G.A. of the C.N.R. (National Research Council) of Italy.

The second author is supported in part by the Croatian Science Foundation under the projects 9752 and 6732.

References

[1] K.T. Arasu, S. Sehgal, *Cyclic difference covers*, Aust. J. Combin. **32** (2005), 213–223.

[2] S. Bagchi, B. Bagchi, *Designs from pairs of finite fields I. A cyclic Unital $U(6)$ and other regular Steiner 2-designs*, J. Combin. Theory Ser. A **52** (1989), 51–61.

[3] T. Beth, D. Jungnickel and H. Lenz, Design Theory. Cambridge University Press, Cambridge, 1999.

[4] S. Bonvicini, M. Buratti, M. Garonzi, G. Rinaldi, T. Traetta, The first families of highly symmetric Kirkman triple systems whose orders fill a congruence class, Des. Codes Crypt. **89** (2021), 2725–2757.

[5] M. Braun, T. Etzion, P. R. J. Östergård, A. Vardy and 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] M. Buratti, *Cyclotomic conditions leading to new Steiner* 2*-designs*, Finite Fields Appl. **3** (1997), 300–313.

[8] M. Buratti, *Old and new designs via difference multisets and strong difference families*, J. Combin. Des. **7** (1999), 406-425.

[9] M. Buratti, *Constructions for point-regular linear spaces*, J. Statist. Plann. Inference **94** (2001), 139–146.

[10] M. Buratti, L. Gionfriddo, *Strong difference families over arbitrary groups*, J. Combin. Des. **16** (2008), 443-461.

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

[12] M. Buratti, A. Nakic, *New infinite classes of* 2*-designs with the method of partial differences*, in preparation.

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

[14] M. Buratti, A. Pasotti, *Combinatorial designs and the theorem of Weil on multiplicative character sums*, Finite Fields Appl. **15**, (2009), 332–344.

[15] M. Buratti, J. Yan, C. Wang, *From a* 1*-rotational RBIBD to a partitioned difference family*, Electronic J. Combin. **17** (2010), ♯R139.

[16] A. Caggegi, *A new family of additive designs*, preprint.

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

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

[19] A. Caggegi, G. Falcone, M. Pavone, Additivity of affine designs, J. Algebr. Comb. **53** (2021), 755–770.

[20] Y. Chang, S. Costa, T. Feng, X. Wang, *Strong difference families of special types*, Discrete Math. **343**, (2020), Nr. 111776.

[21] C.J. Colbourn, J.H. Dinitz, Handbook of Combinatorial Designs. Second Edition, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[22] S. Costa, T. Feng, X. Wang, *New* 2*-designs from strong difference families*, Finite Fields Appl. **50** (2018), 391–405.

[23] S. Costa, T. Feng, X. Wang, *Frame difference families and resolvable balanced incomplete block designs*, Des. Codes Cryptogr. **86** (2018), 2725–2745.

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

[25] C. Guo, T. Feng, X. Wang, *Cyclic balanced sampling plans excluding contiguous units with block size four*, Discrete Math. **345** (2022), 112899.

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

[27] J. Li, D. Wan, *On the subset sum problem over finite fields*, Finite Fields Appl. **14** (2008), 911–929.

[28] R. Lidl, H. Neiderreiter, Finite Fields, Encyclopedia Math., vol. 20, Cambridge University Press, Cambridge, UK, 1983.

[29] D. Jungnickel, *Composition theorems for difference families and regular planes*, Discrete Math. **23** (1978), 151–158.

[30] A. Nakic, *The first example of a simple* 2-$(81, 6, 2)$ *design*, Example and Counterexample **1** (2021), Article 100005.

[31] C. R. Matthews, *Counting Points Modulo p for some Finitely Generated Subgroups of Algebraic Groups*, Bull. London Math. Soc. **14** (1982), 149–154.

[32] K. Momihara, *Strong difference families, difference covers, and their applications for relative difference families*, Des. Codes Cryptogr., **51** (2008), 253–273.

[33] M. Pavone, *On the subset sum problem for finite fields*, Finite Fields Appl. **76** (2021), 101912.

[34] M. Pavone, *A quasidouble of the affine plane of order* 4 *and the solution of a problem on additive designs*, preprint.

[35] M. Pavone, Subset sums and block designs in a finite vector space, preprint.

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

[37] R.M. Wilson, *Cyclotomy and difference families in elementary abelian groups*, J. Number Theory 4 (1972), 17–47.

[38] J. Ying, X. Yang, Y. Li, *Some* 20*-regular CDP*$(5, 1; 20u)$ *and their applications*, Finite Fields Appl. **17** (2011), 317–328.