



The first families of highly symmetric Kirkman Triple Systems whose orders fill a congruence class

Simona Bonvicini¹ · Marco Buratti²  · Martino Garonzi³ · Gloria Rinaldi⁴ · Tommaso Traetta⁵

Received: 8 April 2021 / Revised: 18 August 2021 / Accepted: 14 September 2021 /
Published online: 7 October 2021
© The Author(s) 2021

Abstract

Kirkman triple systems (KTSs) are among the most popular combinatorial designs and their existence has been settled a long time ago. Yet, in comparison with Steiner triple systems, little is known about their automorphism groups. In particular, there is no known congruence class representing the orders of a KTS with a number of automorphisms at least close to the number of points. We partially fill this gap by proving that whenever $v \equiv 39 \pmod{72}$, or $v \equiv 4^e 48 + 3 \pmod{4^e 96}$ and $e \geq 0$, there exists a KTS on v points having at least $v - 3$ automorphisms. This is only one of the consequences of an investigation on the KTSs with an automorphism group G acting sharply transitively on all but three points. Our methods are all constructive and yield KTSs which in many cases inherit some of the automorphisms of G , thus increasing the total number of symmetries. To obtain these results it was necessary to introduce new types of difference families (the doubly disjoint ones) and difference matrices (the splittable ones) which we believe are interesting by themselves.

Keywords Steiner triple system · Kirkman triple system · Group action · Difference family · Difference matrix

Mathematics Subject Classification Primary 05B07 · Secondary 20B25

1 Introduction

Steiner and Kirkman triple systems are undoubtedly amongst the most popular discrete structures. A *Steiner triple system* of order v , briefly $\text{STS}(v)$, is a pair (V, B) where V is a set of v points and B is a set of 3-subsets (*blocks*) of V with the property that any two distinct points are contained in exactly one block. A *Kirkman triple system* of order v , briefly $\text{KTS}(v)$, is an $\text{STS}(v)$ together with a *resolution* R of its block-set B , that is a partition of B into classes (*parallel classes*) each of which is, in its turn, a partition of the point-set V . It has been known since the mid-nineteenth century that a $\text{STS}(v)$ exists if and only if $v \equiv 1$ or $3 \pmod{6}$ [40]. The analogous result for KTSs has been instead solved more than a century

Communicated by D. Jungnickel.

Extended author information available on the last page of the article

later: a $\text{KTS}(v)$ exists if and only if $v \equiv 3 \pmod{6}$. The first published solution was by Ray-Chaudhuri and Wilson [53] but the problem was solved at least 8 years earlier by Lu [43] (see [17], p. 13).

An automorphism of a STS is a permutation of its points leaving the block-set invariant. Analogously, an automorphism of a KTS is a permutation of its points leaving the resolution invariant. Thus an automorphism of a KTS is automatically an automorphism of the underlying STS though the converse is not true in general.

For general background on these topics we refer to [18].

In the next section we will give a brief survey of the automorphism groups of STSs and KTSs. Looking at the results it will be evident how little we know about KTSs in comparison with STSs. For instance, it has been known for close to a century that there is an $\text{STS}(v)$ with an automorphism group of order v for any admissible v . Yet, we are still quite far from a similar result for KTSs. At the moment the existence of a $\text{KTS}(v)$ with an automorphism group of order v or $v - 1$ is known only when v has a special prime factorization. In particular, there is no known congruence $v \equiv k \pmod{n}$ which guarantees the existence of a $\text{KTS}(v)$ with an automorphism group of order close to v .

Adopting the combinatorial-analog of the famous *Erlangen program* by Klein [34], we believe that the interest of a discrete structure is proportional to the number of its automorphisms. Motivated by this and by the shortage of results mentioned above, in this paper we deeply investigate Kirkman triple systems which are *3-pyramidal*, i.e., admitting an automorphism group acting sharply transitively on all but three points.

Now we make a short digression to explain why adopting this "philosophy" also brings practical benefits. Given the definition of a discrete structure, the first natural target, which could be very difficult, is to determine under which constraints it exists. The second is to give an explicit construction for this structure; in some cases this could be even more difficult. For instance, thanks to the recent seminal work of Keevash [39], it is known that a *Steiner t -design* exists provided that the trivial necessary conditions are satisfied and that its order is sufficiently large (the case $t = 2$, due to Wilson [58–60], dates back to the 70's). This is an outstanding achievement which seemed completely out of reach only a decade ago; yet, the probabilistic methods used by Keevash are non-constructive, and do not provide an explicit lower bound on the order of a t -design that guarantees its existence. On the contrary, the request to have many symmetries, besides being in compliance with the Erlangen program, allows to develop constructive algebraic methods. This paper gives the complete recipe to construct, explicitly, a $\text{KTS}(v)$ for any v as in (i), (ii), (iii) of our main result below.

Theorem 1.1 *A necessary condition for the existence of a 3-pyramidal $\text{KTS}(v)$ is that $v = 24n + 9$ or $v = 24n + 15$ or $v = 48n + 3$ for some n which, in the last case, must be of the form $4^e m$ with m odd. This condition is also sufficient in each of the following cases:*

- (i) $v = 24n + 9$ and $4n + 1$ is a sum of two squares;
- (ii) $v = 24n + 15$ and either $2n + 1 \equiv 0 \pmod{3}$ or the square-free part of $2n + 1$ does not have any prime $p \equiv 11 \pmod{12}$;
- (iii) $v = 48n + 3$.

In particular, (ii) and (iii) allow us to reach our main target of getting some families of highly symmetric KTSs whose orders fill a congruence class.

Corollary 1.2 *There exists a 3-pyramidal $\text{KTS}(v)$ for all $v \equiv 39 \pmod{72}$, and for all $v \equiv 4^e 48 + 3 \pmod{4^e 96}$ whatever the non-negative integer e is.*

We point out that in many cases the constructed 3-pyramidal KTSs inherit some automorphisms of the group G acting sharply transitively on all but three points. This permits to increase their number of symmetries considerably (see Remarks 11.2, 11.4 and 11.6).

After the brief survey of Sect. 2 concerning some results on the automorphism groups of Steiner and Kirkman triple systems, the article will be structured as follows. In Sect. 3 we provide the difference methods to construct a 3-pyramidal KTS and we prove that each group having a 3-pyramidal action on a KTS fixes one parallel class and acts transitively on the remaining ones. We also prove that such a group must have exactly three involutions, and these involutions are pairwise conjugate. Groups with this property will be called *pertinent*. Although in literature there is no lack of articles on groups with three involutions (see, for example, [36,41]), none of them allows us to determine the set of “relevant” orders. We prove (Theorem 3.9) that such orders are precisely those of the form $12n + 6$ or $4^\alpha(24n + 12)$, and from this we partially derive the necessary condition in Theorem 1.1. The proof of the “only if” part of Theorem 3.9 is purely group theoretical and for this reason the whole Sect. 4 is dedicated to it. However, its reading is not necessary for understanding the rest of the article, whose nature is purely combinatorial.

The constructive part of Theorem 1.1 will be proven in Sect. 11 and it is the result of numerous direct constructions (Sects. 6, 7 and the Appendix) and recursive constructions (Sects. 8, 9, 10). These results are preceded by a brief section (Sect. 5) useful for understanding the notation and terminology used throughout the rest of the paper. The recursive constructions required the introduction of new concepts such as *doubly disjoint difference family* and *splittable difference matrix* which we believe may be important by themselves.

The article concludes (Sect. 12) with a short list of open problems.

2 A brief survey of the automorphism groups of Steiner and Kirkman triple systems

The literature on Steiner and Kirkman triple systems having an automorphism with a prescribed property or an automorphism group with a prescribed action is quite extensive.

For instance the set of values of v for which there exists an STS(v) with an involutory automorphism fixing exactly one point (*reversed* STS) has been established in [25,54,57]: it exists if and only if $v \equiv 1, 3, 9$ or $19 \pmod{24}$. Results concerning the *full* automorphism group of a STS have been obtained by Mendelsohn [44] and Lovegrove [42].

Here, we just provide a brief survey of what is known on the existence of systems whose number of automorphisms are at least close to the number of points.

Adopting a terminology coined by Mendelsohn and Rosa [45], we say that a combinatorial design is *f-pyramidal* if it admits an automorphism group G fixing f points and acting sharply transitively on the others. If $f = 0$ one usually speaks of a *regular* design and, more specifically, of a *cyclic design* if the group G is cyclic. If $f = 1$ one usually speaks of a *1-rotational design*.

It was proved a long time ago [51] that there exists a cyclic STS(v) for all admissible values of v except $v = 9$. On the other hand the unique STS(9), that is the point-line design associated with the affine plane of order 3, is clearly regular under the action of \mathbb{Z}_3^2 . Thus there exists a regular STS(v) for all admissible values of v .

The analogous problem of determining the set of values of v for which there exists a regular KTS(v) is almost completely open and it appears to be very difficult. The few known results on this problem are the following. The parallel classes of the point-line design associated

with the n -dimensional affine space over the field of order 3 clearly give a $\text{KTS}(3^n)$ that is regular under the action of \mathbb{Z}_3^n . A necessary condition given in [46] for the existence of a cyclic $\text{KTS}(6n+3)$ is that $2n+1$ is not a prime power congruent to 5 (mod 6). This condition is also sufficient up to $n = 32$ [46] and when all prime factors of n are congruent to 1 (mod 6) [31].

The existence of a 1-rotational $\text{STS}(v)$ has been thoroughly investigated in [3,6,47,52] leaving the problem open only for the orders v satisfying, simultaneously, the following conditions: $v = (p^3 - p)n + 1 \equiv 1 \pmod{96}$ with p a prime; $n \not\equiv 0 \pmod{4}$; the odd part of $v - 1$ is square-free and without prime factors $\equiv 1 \pmod{6}$.

The 1-rotational KTS s have a very nice structure. Indeed a group with a 1-rotational action on them (necessarily *binary*, i.e., admitting exactly one involution) is transitive on the parallel classes. On the other hand, as in the regular case, very little is known about their existence which has been proved only for orders v of the the following types: v is a power of 3 (the already mentioned regular $\text{KTS}(3^n)$ is also 1-rotational); all prime factors of $\frac{v-1}{2}$ are congruent to 1 (mod 12) [13]; $v = 8n + 1$ with all the prime factors of n congruent to 1 (mod 6) [14].

An f -pyramidal $\text{STS}(v)$ with $f \neq 0$ may exist only for $f \equiv 1$ or $3 \pmod{6}$ with $f < v/2$ or $f = v$ (see Lemma 1.1 in [12]). The existence problem for 3-pyramidal STS s was completely settled in [12].

Theorem 2.1 *There exists a 3-pyramidal $\text{STS}(v)$ if and only if $v \equiv 7, 9, 15 \pmod{24}$ or $v \equiv 3, 19 \pmod{48}$.*

As an obvious consequence of Theorem 2.1, a 3-pyramidal $\text{KTS}(v)$ may exist only when $v \equiv 9 \pmod{24}$ or $v \equiv 15 \pmod{24}$ or $v \equiv 3 \pmod{48}$. The main result of this paper (Theorem 1.1) provides, in particular, a complete answer in the last case $v \equiv 3 \pmod{48}$.

Finally, a $\text{STS}(v)$ is called 1-*transrotational* if it has an automorphism group G that fixes exactly one point, switches two points, and acts sharply transitively on the remaining $v - 3$. This terminology was first used in [29] under the assumption that G is cyclic, though G just need to be binary. One cannot fail to notice a certain kinship between 3-pyramidal and 1-transrotational STS s, but apart from the fact that their groups are deeply different, the sets of orders for which they exist do not coincide. Indeed it was proved in [29] that a 1-transrotational $\text{STS}(v)$ under the cyclic group exists if and only if $v \equiv 1, 7, 9$ or $15 \pmod{24}$. It is easy to check that the same holds if we remove the assumption that the group be cyclic. As far as we are aware, nobody studied 1-transrotational $\text{KTS}(v)$. Considering the above, they might exist only for $v \equiv 9$ or $15 \pmod{24}$ but it is not difficult to exclude the case $v \equiv 15 \pmod{24}$. This will be shown in a paper in preparation [11] where we will deal with the case $v \equiv 9 \pmod{24}$.

3 Difference families and 3-pyramidal Kirkman triple systems

In this section we show that the existence of a 3-pyramidal KTS over a group G is equivalent to constructing a suitable *difference family* (DF) in G relative to a *partial spread*, a concept introduced by the second author in [6]. We point out that throughout the paper, except for Sect. 4, every group will be denoted additively.

A partial spread of a group G is a set Σ of subgroups of G whose mutual intersections are trivial. If $\tau = \{d_1^{e_1}, \dots, d_n^{e_n}\}$ is the multiset (written in "exponential" notation) of the orders of all subgroups belonging to Σ , we say that Σ is of *type* τ or a τ -partial spread. A *spread*

(or *partition*) of G is a partial spread whose members between them cover the whole group G .

The *list of differences* of a triple $B = \{x, y, z\}$ of elements of G is the multiset ΔB of size 6 defined by

$$\Delta B = \{\pm(x - y), \pm(x - z), \pm(y - z)\}.$$

The list of differences of a family \mathcal{F} of 3-subsets of G , denoted by $\Delta\mathcal{F}$, is the multiset union of the lists of differences of all its triples. Also, the *flatten* of F , denoted by $\Phi(\mathcal{F})$, is the multiset union of all the triples of \mathcal{F} .

$$\Delta\mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B; \quad \Phi(\mathcal{F}) = \bigcup_{B \in \mathcal{F}} B.$$

A $(G, \Sigma, 3, 1)$ *difference family* (DF) is a family \mathcal{F} of 3-subsets of G (*base blocks*) whose list of differences is the set of all elements of G not belonging to any member of the partial spread Σ . If $\Sigma = \{H\}$ we write $(G, H, 3, 1)$ -DF or simply $(G, 3, 1)$ -DF when $H = \{0\}$. If Σ is a partial spread of type τ , we also use the notation $(G, \tau, 3, 1)$ -DF.

If F is a $(G, H, 3, 1)$ -DF, then its size is clearly equal to $\frac{|G \setminus H|}{6}$ and then its flatten $\Phi(F)$ has size $\frac{|G \setminus H|}{2}$. Thus, if J is a subgroup of H of order 2, one can ask whether $\Phi(F)$ is a complete system of representatives for the left cosets of J that are not contained in H . In the affirmative case we say that F is J -resolvable.

Definition 3.1 Let F be a $(G, H, 3, 1)$ -DF and let J be a subgroup of H of order 2. We say that F is J -resolvable if its flatten is a complete system of representatives for the left cosets of J in G that are not contained in H . So, equivalently, if we have $\Phi(F) + J = G \setminus H$.

We note that the development of a J -resolvable $(G, H, 3, 1)$ -DF is a *Kirkman frame* [56] admitting G as a sharply point transitive automorphism group.

A *multiplier* of a J -resolvable $(G, H, 3, 1)$ -DF, say F , is an automorphism μ of G leaving F invariant. We say that μ is a *strong multiplier* if it fixes H element-wise.

The following fact is straightforward.

Proposition 3.2 Let $G = H_n \geq \dots \geq H_1 \geq J$ be a chain of subgroups of G with J of order 2. If there exists a J -resolvable $(H_{i+1}, H_i, 3, 1)$ -DF, say F_i , for $1 \leq i \leq n - 1$, then

$$F = \bigcup_{i=1}^{n-1} F_i \text{ is a } J\text{-resolvable } (G, H_1, 3, 1)\text{-DF.}$$

Furthermore, F inherits the strong multipliers of F_{n-1} .

Difference families are a crucial topic in Design Theory [2,17]. In particular, as a special case of Theorem 2.1 in [12], it is possible to characterize the 3-pyramidal STS(6n + 3) in terms of difference families as follows.

Theorem 3.3 There exists a 3-pyramidal STS(6n + 3) if and only if there exists a $(G, \{2^3, 3^e\}, 3, 1)$ -DF for a suitable group G of order 6n with exactly three involutions, and a suitable integer e .

In the following lemma we recall what the 3-pyramidal STS(6n + 3) generated by a $(G, \{2^3, 3^e\}, 3, 1)$ -DF looks like.

Lemma 3.4 Up to isomorphism, (V, B) is a STS(6n + 3) that is 3-pyramidal under G if and only if the following facts hold:

- (i) $V = G \cup \{\infty_1, \infty_2, \infty_3\}$;
- (ii) the action of G on V is the addition on the right with the rule that $\infty_i + g = \infty_i$ for each $g \in G$ and for $i = 1, 2, 3$;
- (iii) G has exactly three involutions, say j_1, j_2, j_3 ;
- (iv) a system of representatives for the G -orbits on B is of the form

$$\{B_\infty, B_1, B_2, B_3\} \cup H \cup F$$

where:

- $B_\infty = \{\infty_1, \infty_2, \infty_3\}$;
- $B_i = \{\infty_i, 0, j_i\}$ for $i = 1, 2, 3$;
- H is a set of e subgroups of G of order 3;
- F is a $(G, \Sigma, 3, 1)$ -DF with $\Sigma = \{0, j_1\}, \{0, j_2\}, \{0, j_3\} \cup H$.

Definition 3.5 Throughout this paper a finite group G will be called “pertinent” if it has precisely three involutions, and the three of them are pairwise conjugate in G .

Obviously, a pertinent group is necessarily non-abelian. Up to isomorphism, the smallest pertinent group is \mathbb{D}_6 , i.e., the dihedral group of order 6. The next one is \mathbb{A}_4 , the alternating group of degree 4.

As already said, we prefer to write every group in additive notation. So, differently from the mostly used representation, we prefer to see \mathbb{D}_6 as the additive group D with underlying set $\mathbb{Z}_2 \times \mathbb{Z}_3$ and operation law $\hat{+}$ defined by $(a, b) \hat{+} (c, d) = (a + c, (-1)^c b + d)$. Adopting this representation, it is easy to see that the difference $\hat{-}$ in D works as follows:

$$(a, b) \hat{-} (c, d) = (a - c, (-1)^c (b - d)).$$

The three involutions of D are $(1, 0)$, $(1, 1)$ and $(1, 2)$. The fact that

$$(1, 1) \hat{+} (1, 0) \hat{-} (1, 1) = (1, 2) \quad \text{and} \quad (1, 2) \hat{+} (1, 0) \hat{-} (1, 2) = (1, 1)$$

confirms that D is pertinent.

The alternating group \mathbb{A}_4 will be also represented additively as the first term of an infinite series of pertinent additive groups that we will construct in the proof of the “if” part of Theorem 3.9.

The crucial ingredient to characterize and construct the 3-pyramidal KTSs are some special $(G, \{2^3, 3\}, 3, 1)$ -DFs with G pertinent defined as follows.

Definition 3.6 Let F be a $(G, \{2^3, 3\}, 3, 1)$ -DF with G pertinent and let J be a subgroup of G of order 2. We say that F is J -resolvable if there exists $a, b \in G$ such that

- $J, a + J - a$ and $b + J - b$ are the three subgroups of order 2 of G ;
- $\Phi(\mathcal{F}) \cup \{0, a, b\}$ is a complete system of representatives for the left cosets of J in G .

The following fact is straightforward.

Proposition 3.7 Let J be a subgroup of order 2 of a pertinent group G and let H be a pertinent subgroup of G containing J . If \mathcal{F}_0 is a J -resolvable $(H, \{2^3, 3\}, 3, 1)$ -DF and F is a J -resolvable $(G, H, 3, 1)$ -DF, then $F \cup \mathcal{F}_0$ is a J -resolvable $(G, \{2^3, 3\}, 3, 1)$ -DF.

Speaking of a $(G, \{2^3, 3\}, 3, 1)$ -RDF with G pertinent, we will mean a J -resolvable $(G, \{2^3, 3\}, 3, 1)$ -DF with J one of the three subgroups of G of order 2.

The following result gives a characterization of the 3-pyramidal KTSs and, more importantly, a way to construct them.

Theorem 3.8 *There exists a 3-pyramidal KTS(6n + 3) with n > 0, if and only if there exists a (G, {2³, 3}, 3, 1)-RDF for a suitable pertinent group G of order 6n.*

Proof (⇒). Let (V, B, R) be a KTS(6n + 3) that is 3-pyramidal under G. Thus (V, B) is a STS(6n + 3) that is 3-pyramidal under G, hence we can assume that V and B satisfy the conditions listed in Lemma 3.4.

Let P be the parallel class containing the block B_∞. Obviously, we have P + g = P for each g ∈ G. It follows that the distinct right translates of the block H of P through 0 form a partition of G. This clearly implies that H is a subgroup of G and that the blocks of P are B_∞ and all the right cosets of H in G.

Now let Q be the parallel class of R containing the block B₁ = {∞₁, 0, j₁}. Since G fixes ∞₁, we see that the G-stabilizer of Q coincides with the G-stabilizer of B₁ that is J := {0, j₁}. Thus, for i = 2, 3, the block of Q through ∞_i is of the form {∞_i, g_i, g_i + j₁} for a suitable group element g_i. This block necessarily belongs to the orbit of B_i, hence we have {∞_i, 0, j_i} + t_i = {∞_i, g_i, g_i + j₁} for a suitable t_i. This equality implies that

$$\text{either } \begin{cases} t_i = g_i \\ j_i + t_i = g_i + j_1 \end{cases} \quad \text{or} \quad \begin{cases} t_i = g_i + j_1 \\ j_i + t_i = g_i \end{cases}$$

In both cases we get j_i = g_i + j₁ - g_i, hence the three involutions j₁, j₂, j₃ are pairwise conjugate, i.e., G is pertinent.

The fact that the G-stabilizer of Q is J also implies that the 2n - 2 triples of Q not containing the “points at infinity” can be grouped into pairs {A_i, A_i + j₁}, 1 ≤ i ≤ n - 1, and that the G-orbit Orb(Q) of Q has length $\frac{|G|}{2} = 3n$. Then, given that the resolution of a KTS(6n + 3) has size 3n + 1, we deduce that R = {P} ∪ Orb(Q). Also, if we set F = {A_i | 1 ≤ i ≤ n - 1}, we can claim that a set of base blocks for B is given by

$$\{B_\infty, B_1, B_2, B_3, H\} \cup F.$$

It follows, by condition (iv) in Lemma 3.4, that F is a (G, {2³, 3}, 3, 1)-DF.

Given that the blocks of Q partition V, we have (Φ(F) ∪ {0, g₂, g₃}) + J = G. This means that Φ(F) ∪ {0, g₂, g₃} is a complete system of representatives for the left cosets of J in G, i.e., F is J-resolvable.

(⇐). Let G be a pertinent group of order 6n whose involutions are j₁, j₂, j₃, and assume that F is a {0, j₁}-resolvable (G, {2³, 3}, 3, 1)-DF. There are suitable group elements g₂, g₃ such that j_i = g_i + j₁ - g_i, for i = 2, 3, and (Φ(F) ∪ {0, g₂, g₃}) + {0, j₁} = G. Let H be the subgroup of G of order 3 belonging to the partial spread associated with F. Two parallel classes of the STS(6n + 3) generated by F are clearly the following:

$$\mathcal{P} = \{B_\infty\} \cup \{\text{right cosets of } H \text{ in } G\};$$

$$Q = \{\{\infty_i, g_i, g_i + j_1\} \mid i = 1, 2, 3\} \cup \{A, A + j_1 \mid A \in \mathcal{F}\}.$$

Their G-stabilizers are, respectively, G and {0, j₁} so that their G-orbits have size 1 and 3n. It easily follows that {P} ∪ Orb(Q) is a G-invariant resolution of the STS(6n + 3) generated by F, namely a 3-pyramidal KTS(6n + 3). □

In view of Theorem 3.8, it is important to determine the set of pertinent numbers, i.e., the set of orders of the pertinent groups.

Theorem 3.9 *There exists a pertinent group of order n if and only if n ≡ 6 (mod 12) or n = 4^αm with α > 0 and m ≡ 3 (mod 6).*

Proof The proof of the “only if” part is purely group theoretical and for convenience it is postponed to Sect. 4. Here we prove the “if” part.

If $n \equiv 6 \pmod{12}$, we have $n = 6m$ for a suitable odd integer m . Then, recalling that the dihedral group D is pertinent, it is clear that $D \times H$ is a pertinent group of order $6m$ for every group H of order m .

Now let $n = 4^\alpha m$ with $\alpha > 0$ and $m \equiv 3 \pmod{6}$. Consider the matrix $\Theta = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}$

and let G_α be the group with underlying set $\mathbb{Z}_3 \times \mathbb{Z}_{2^\alpha} \times \mathbb{Z}_{2^\alpha}$ and operation $\hat{+}$ defined by the rule

$$(a, b, c) \hat{+} (d, e, f) = (a, b, c) \cdot \Theta^d + (d, e, f).$$

This is, up to isomorphism, the outer semidirect product of $\mathbb{Z}_{2^\alpha}^2$ and \mathbb{Z}_3 with respect to the group homomorphism $\theta : \mathbb{Z}_3 \rightarrow \text{Aut}(\mathbb{Z}_{2^\alpha}^2)$ defined by the rule

$$\theta(1)(x, y) = (-y, x - y) \quad \forall (x, y) \in \mathbb{Z}_{2^\alpha}^2.$$

The difference of two triples (a, b, c) and (d, e, f) of the group has a convenient form; it is the usual difference in the abelian group $\mathbb{Z}_3 \times \mathbb{Z}_{2^\alpha}^2$ multiplied by the inverse of Θ^d :

$$(a, b, c) \hat{-} (d, e, f) = (a - d, b - e, c - f) \cdot \Theta^{-d}. \tag{3.1}$$

More explicitly, we have

$$(a, b, c) \hat{-} (d, e, f) = \begin{cases} (a - d, b - e, c - f) & \text{if } d = 0 \\ (a - d, e - b + c - f, e - b) & \text{if } d = 1 \\ (a - d, f - c, b - e + f - c) & \text{if } d = 2 \end{cases}$$

It is a simple exercise to check that G_α has exactly three involutions that are

$$(0, 2^{\alpha-1}, 0), \quad (0, 0, 2^{\alpha-1}), \quad (0, 2^{\alpha-1}, 2^{\alpha-1})$$

and that they are pairwise conjugate. Indeed we have:

$$\begin{aligned} (1, 0, 0) \hat{+} (0, 2^{\alpha-1}, 0) \hat{-} (1, 0, 0) &= (0, 2^{\alpha-1}, 2^{\alpha-1}); \\ (2, 0, 0) \hat{+} (0, 0, 2^{\alpha-1}) \hat{-} (2, 0, 0) &= (0, 2^{\alpha-1}, 2^{\alpha-1}) \end{aligned}$$

Thus G_α is a pertinent group of order $4^\alpha 3$. Then, if H is any group of odd order m , it is clear that the direct product $G_\alpha \times H$ is a pertinent group of order $3 \cdot 4^\alpha m$ whose involutions are $(0, 2^{\alpha-1}, 0, 0)$, $(0, 0, 2^{\alpha-1}, 0)$ and $(0, 2^{\alpha-1}, 2^{\alpha-1}, 0)$. □

The alternating group A_4 can be seen, up to isomorphism, as the group G_1 .

4 Pertinent groups

Here we prove the “only if” part of Theorem 3.9. Considering that the arguments used are purely group theoretical, the reading of this section can be postponed to a later time without compromising the understanding of the rest of the article. Also, we point out that in this section, unlike the rest of the paper, we prefer to denote groups in multiplicative notation.

In the following, let G be a pertinent group and denote by K the subgroup of G generated by the three involutions i, j, k . Let $C_G(K)$ be the centralizer of K in G , that is

$$C_G(K) = \{g \in G : g^{-1}kg = k \text{ for every } k \in K\},$$

and set $C = C_G(K)$. Clearly, K is a characteristic subgroup of G , so both K and C are normal in G . Since G acts on $\{i, j, k\}$ by conjugation with kernel C , the quotient G/C is isomorphic to a transitive subgroup of S_3 , so either $G/C \cong S_3$ or $G/C \cong A_3$ (here A_3 denotes the alternating group of degree 3). Observe in particular that G has an element of order a power of 3 acting “cyclically” on the involutions (meaning that it sends i to j , j to k and k to i). Recall that if H is a subgroup of G the “normalizer” of H in G is $N_G(H) = \{g \in G : H^g = H\}$, where $H^g = g^{-1}Hg$ is a “conjugate” of H in G .

We will make use of the following well-known result in group theory.

Lemma 4.1 (*Frattini’s Argument*) *If X is a normal subgroup of G and Q is a Sylow p -subgroup of X , then $G = XN_G(Q)$.*

We start providing sufficient conditions for a pertinent group to have subgroups or quotients that are pertinent.

Lemma 4.2 *Let H be a subgroup of G . Then*

- (i) *If H has even order and $HC = G$, then H is pertinent.*
- (ii) *If Q is a Sylow p -subgroup of C and $H = N_G(Q)$, then H is pertinent.*
- (iii) *If H has even order and contains a Sylow 3-subgroup of G , then H is pertinent.*
- (iv) *Suppose the involutions of G commute pairwise. If H is normal in G and $|H|$ is odd then G/H is pertinent.*

Proof (i) Since H has even order, it contains at least one involution. Considering that $HC = G$, it follows that the action of H on the involutions is transitive. Therefore, $K \leq H$ and H is pertinent.
 (ii) By Lemma 4.1, we have that $HC = G$. Since $Q \leq C$, it follows that K centralizes Q , hence $K \leq H$, therefore H has even order. By point (1), we obtain that H is pertinent.
 (iii) Since $|H|$ is even, H contains at least one involution. Since $|G/C|$ is a multiple of 3, a Sylow 3-subgroup S of G is not contained in C , hence S acts transitively on $\{i, j, k\}$. Therefore, H contains all three involutions and then it is pertinent.
 (iv) Suppose H is normal of odd order in G and the involutions commute pairwise. Denote by i, j, k the involutions of G . Since $ij = ji$, the element ij is an involution distinct from i and from j so $ij = k$ and the elements $iH, jH, kH \in G/H$ are involutions of G/H and G/H acts transitively by conjugation on them (because G acts transitively by conjugation on i, j, k), moreover they are pairwise distinct, for example $iH \neq jH$ because $i^{-1}j = ij = k \notin H$. We are left to show that G/H has precisely three involutions. If xH is an involution of G/H then $x^2 \in H$ so x has order $2t$ with t odd (being $|H|$ odd), x^t is an involution of G , and $xH = (xH)^t = x^tH$. This means that the involutions of G/H are of the form yH with y an involution in G , so they are precisely iH, jH, kH and we deduce that G/H is pertinent. \square

For a pertinent group of order $2^n \cdot d$ with d odd, the following two lemmas give us sufficient or necessary conditions for n to be even or odd.

Lemma 4.3 *Suppose G has a normal 2-subgroup H of order 2^m . Then m is even.*

Proof G has an element g of order a power of 3 acting cyclically on the three involutions. We claim that g does not fix any non-trivial element of H . Indeed if $1 \neq h \in H$ is fixed by g then a suitable power of h is an involution fixed by g , but g does not fix any involution. This implies that the $\langle g \rangle$ -orbits of H distinct from $\{1\}$ have size divisible by 3 so $2^m = |H| \equiv 1 \pmod{3}$ therefore m is even. \square

Lemma 4.4 *Suppose 4 divides $|G|$. Then K is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. Moreover writing $|G| = 2^n \cdot d$ with d odd, if n is even then $G/C \cong A_3$, and if n is odd then $G/C \cong S_3$.*

Proof First, we show that i, j, k commute pairwise, so that $K = \{1, i, j, k\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. It is enough to show that two involutions, say i and j , commute, because then ij has order 2 so $ij = k$ (it cannot be $ij = i$ nor $ij = j$) therefore i and j commute with k . If this is not the case, then C must have odd order (otherwise an involution in C should commute with the others). But then the order of G/C is a multiple of $2^n \geq 4$ contradicting the fact that G/C is isomorphic to either A_3 or S_3 .

Write $|G| = 2^n \cdot d$ with d odd. We know that G/C is isomorphic to either A_3 or S_3 . Letting Q be a Sylow 2-subgroup of C , $N = N_G(Q)$ is pertinent by Lemma 4.2, so writing $|Q| = 2^m$, m is even by Lemma 4.3. If $G/C \cong A_3$ then Q is a Sylow 2-subgroup of G , so $n = m$ is even. Conversely if $G/C \cong S_3$ then $n = m + 1$ is odd. □

To prove the main result of this section, we need the following result.

Lemma 4.5 *Suppose $|G| = 2^n \cdot d$ where $n \geq 3$ is odd. Then G contains a pertinent subgroup L of order $2^n \cdot 3^s$ for some positive integer s .*

Proof Let Q be a Sylow 2-subgroup of C and recall that $|G/C| \in \{3, 6\}$. Therefore, if $|Q| = 2^m$, then $m = n$ or $n - 1$ according to whether $|G/C| = 3$ or 6. By Lemma 4.2, we have that $N = N_G(Q)$ is a pertinent group, and since Q is normal in N , by Lemma 4.3 we have that m is even, hence $m = n - 1$ (since n is odd by assumption) and $|G/C| = 6$. Considering that $Q \leq C \cap N$, and $G = NC$ (by Lemma 4.1), it follows that $|N/Q|$ is a multiple of $|N/(C \cap N)| = |NC/C| = |G/C| = 6$, hence 2^n divides $|N|$.

We recall that every group of singly even order has a subgroup of index 2 (see, e.g., Theorem 1.35 in [35]). Thus, since $|N/Q| \equiv 2 \pmod{4}$, there exists a normal subgroup D/Q of N/Q of index 2. In particular, all the Sylow 3-subgroups of N/Q are contained in D/Q , so the number of Sylow 3-subgroups of N/Q is odd. Let P/Q be a subgroup of N/Q of order 2. Since P/Q acts by conjugation on the family consisting of the Sylow 3-subgroups of N/Q , there exists one of them, say H/Q , normalized by P/Q . This implies that $PH/Q = (P/Q)(H/Q) \leq N/Q$ hence $L = PH \leq N$. Moreover $|L| = |Q| \cdot |L/Q| = |Q| \cdot |P/Q| \cdot |H/Q| = 2^n \cdot 3^s$ where $3^s = |H/Q|$. Now L has even order and contains a Sylow 3-subgroup of N , hence L is pertinent by Lemma 4.2. □

We are now ready to prove the “only if” part of Theorem 3.9.

Theorem 4.6 *If G is a pertinent group of order $2^n d$ with d odd and $n \geq 2$, then n is even.*

Proof We prove the result by contradiction. Let G be a counterexample of minimal order, that is, assume that there exists a pertinent group G such that $|G| = 2^n \cdot d$ is minimal with respect to the property that both n and d are odd, and $n \geq 3$. By Lemma 4.5, we have that G has a pertinent subgroup of order $2^n \cdot 3^s$ for some positive integer s , so by the minimality of $|G|$ we must have $d = 3^s$. Recall that $K \cong C_2 \times C_2$ and $G/C \cong S_3$ by Lemma 4.4.

Let S be a Sylow 3-subgroup of C and note that $|S| = 3^{s-1}$ since $|G/C| = 6$. Now, by Lemma 4.2 we have that $N = N_G(S)$ is pertinent; in particular, $K \leq N$ hence 4 is a divisor of $|N|$. Also, since $CN = G$ (by Lemma 4.1) and $C \cap N = C_N(K)$, it follows that $N/C_N(K) = N/(C \cap N) \cong NC/C = G/C \cong S_3$. Considering that S is a Sylow 3-subgroup of $C_N(K)$ of order 3^{s-1} , we have that $|N| = 2^m \cdot 3^s$, for some $2 \leq m \leq n$. Also, by Lemma 4.4, it follows that m is odd. Finally, since S is a normal subgroup of N of odd

order, Lemma 4.2 guarantees that N/S is pertinent. Since $|N/S| = 2^m \cdot 3$ and $m \geq 3$ is odd, by the minimality of $|G|$ we must have $s = 1$, hence $|G| = 2^n \cdot 3$.

We are reduced to the case $|G| = 2^n \cdot 3$. Let $H := C_G(i)$ be the centralizer of i in G . We have $|G : H| = 3$ because i has 3 conjugates in G , in other words $|H| = 2^n$ and H is a Sylow 2-subgroup of G . Let P be a Sylow 3-subgroup of G , then $P = \langle g \rangle$ is a cyclic group of order 3. Clearly $g \notin H$ because $|H| = 2^n$, so P acts transitively on the three involutions of G . We prove that $N_G(P) = P$. Suppose for a contradiction that $N_G(P) \neq P$, then there is an involution, say i , normalizing P , hence $\langle P, i \rangle$ is a group of order 6 containing all three involutions, hence $K \leq \langle P, i \rangle$, which is a contradiction since $|K| = 4$. So $N_G(P) = P$. We now prove that H is normal in G . Since $N_G(P) = P$, the subgroup P has precisely $|G : P| = 2^n$ conjugates in G therefore G has precisely $(|P| - 1) \cdot 2^n = 2 \cdot 2^n$ elements of order 3. Since $|G| = 3 \cdot 2^n$ we deduce that the number of elements of G of order not equal to 3 is 2^n hence there is room in G for only one Sylow 2-subgroup. We deduce that the Sylow 2-subgroups are normal hence $H \trianglelefteq G$, so n is even by Lemma 4.3. This is a contradiction and the result is proved. \square

5 Notation and terminology

A maximal prime power divisor of any integer n will be called a *component* of n . As it is standard, given a prime power q , we denote by \mathbb{F}_q the field of order q . We extend this notation to any integer $n > 1$ denoting by \mathbb{F}_n the ring which is direct product of all the fields whose orders are the components of n . Thus, for instance, $\mathbb{F}_{45} = \mathbb{F}_5 \times \mathbb{F}_9$. The additive group of the ring \mathbb{F}_n will be denoted by V_n and we set $V_n^* := V_n \setminus \{0\}$. If $n = 1$, then V_n is the trivial group with one element. If d is a divisor of n , any subgroup S of V_n of order d is clearly isomorphic to V_d and therefore, by abuse of notation, such a subgroup S will be often denoted by V_d .

The group of units of \mathbb{F}_n will be denoted by $\mathbb{U}(\mathbb{F}_n)$ and its order by $\psi(n)$. Obviously, in the particular case that $n = q$ is a prime power, $\mathbb{U}(\mathbb{F}_n)$ is nothing but the multiplicative group \mathbb{F}_q^* of the field \mathbb{F}_q and $\psi(n) = q - 1$. Otherwise, if n has more than one component, say q_1, \dots, q_ω , then $\mathbb{U}(\mathbb{F}_n) = \mathbb{F}_{q_1}^* \times \dots \times \mathbb{F}_{q_\omega}^*$ and $\psi(n) = \prod_{i=1}^\omega (q_i - 1)$. The set of non-zero squares and of non-squares of the field \mathbb{F}_q will be denoted by \mathbb{F}_q^\square and \mathbb{F}_q^\square , respectively.

If A, B are non-empty subsets of \mathbb{F}_n , then AB will denote the multiset $\{ab \mid a \in A; b \in B\}$. If $A = \{a\}$ or $B = \{b\}$, then AB will be written as aB or Ab , respectively.

Let q_1, \dots, q_ω be the components of an odd integer n . For every non-empty I belonging to the power-set $2^{\{1, \dots, \omega\}}$, choose an element $c(I) \in I$ and consider the subset $S(I)$ of V_n^* defined as follows:

$$S(I) = S_1(I) \times \dots \times S_\omega(I) \quad \text{with} \quad S_j(I) = \begin{cases} \{0\} & \text{if } j \notin I; \\ \mathbb{F}_{q_j}^\square & \text{if } j = c(I); \\ \mathbb{F}_{q_j}^* & \text{if } j \in I \setminus \{c(I)\}. \end{cases}$$

Then define $S := \bigcup_{I \in 2^{\{1, \dots, \omega\}} \setminus \{\emptyset\}} S(I)$. Such a set S has size $\frac{n-1}{2}$ and then will be called a *halving* of V_n^* . It is easy to see that it has the following property:

$$x, y \in \mathbb{F}_n \quad \text{and} \quad x_i y_i \in \mathbb{F}_{q_i}^\square \quad \text{for } 1 \leq i \leq \omega \implies \{x, y\}S = V_n^*. \tag{5.1}$$

Given a group G and an element s of \mathbb{F}_n , the endomorphism of $G \times V_n$ mapping (x, y) to (x, ys) will be denoted by μ_s . It is evident that if $s \in \mathbb{U}(\mathbb{F}_n)$, then μ_s is an automorphism of $G \times V_n$.

Given $\alpha \geq 1$, remember that throughout the paper G_α will denote the group defined in the “if” part of Theorem 3.9. By *canonical involution* of G_α we will mean $(0, 2^{\alpha-1}, 2^{\alpha-1})$. Also, the canonical involution of $G_\alpha \times V_n$ will be $(0, 2^{\alpha-1}, 2^{\alpha-1}, 0)$. Speaking of a $(G, H, 3, 1)$ -RDF with $G = G_\alpha$ or $G = G_\alpha \times V_n$, we will mean a $\{0, j\}$ -resolvable $(G_\alpha, H, 3, 1)$ -DF where j is the canonical involution of G .

6 The smallest examples

The five smallest *pertinent* values of n are 6, 12, 30, 36 and 48. In the following, for each of these values, a 3-pyramidal $KTS(n + 3)$ will be given by means of a $(G, \{2^3, 3\}, 3, 1)$ -RDF with $G = D, G_1, D \times V_5, G_1 \times V_3$ and G_2 , respectively. By way of illustration, in the first two cases we follow the instructions of Theorem 3.8 and we concretely construct a 3-pyramidal $KTS(9)$ and a 3-pyramidal $KTS(15)$.

The realizations of these five small KTSs allow us to state the following.

Proposition 6.1 *Assume that F is a $(G, H, 3, 1)$ -RDF with G pertinent of order n and H isomorphic to one of the following groups: $D, G_1, D \times V_5, G_1 \times V_3$ and G_2 . Then there exists a 3-pyramidal $KTS(n + 3)$.*

Furthermore, if M is a group of m strong multipliers of F , the obtained $KTS(n + 3)$ admits at least mn automorphisms.

Proof The first assertion follows immediately from Proposition 3.7. For the second assertion, it is enough to observe that the semidirect product $G \rtimes M$ is a group of automorphisms of the obtained $KTS(n + 3)$. □

Proposition 6.1 will enable us to construct infinite classes of 3-pyramidal KTSs in the subsequent sections.

6.1 A 3-pyramidal KTS(9)

The set of all non-trivial subgroups of D is a spread of type $\{2^3, 3\}$. Thus the empty family can be seen as a J -resolvable $(D, \{2^3, 3\}, 3, 1)$ -DF with J any of the three subgroups of D of order 2. Applying Theorem 3.8 with $(j_1, j_2, j_3) = ((1, 0), (1, 1), (1, 2))$ and $(g_2, g_3) = ((1, 2), (1, 1))$, we get a 3-pyramidal representation of the unique $KTS(9)$ (that is the affine plane of order 3) with point-set $D \cup \{\infty_1, \infty_2, \infty_3\}$ and the following parallel classes:

$$\begin{array}{lll}
 \{\infty_1, \infty_2, \infty_3\} & \{(0, 0), (0, 1), (0, 2)\} & \{(1, 0), (1, 1), (1, 2)\} \\
 \{\infty_1, (0, 0), (1, 0)\} & \{\infty_2, (0, 1), (1, 2)\} & \{\infty_3, (0, 2), (1, 1)\} \\
 \{\infty_1, (0, 1), (1, 1)\} & \{\infty_2, (0, 2), (1, 0)\} & \{\infty_3, (0, 0), (1, 2)\} \\
 \{\infty_1, (0, 2), (1, 2)\} & \{\infty_2, (0, 0), (1, 1)\} & \{\infty_3, (0, 1), (1, 0)\}.
 \end{array}$$

6.2 A 3-pyramidal KTS(15)

The set of all non-trivial subgroups of G_1 is a spread of this group of type $\{2^3, 3^4\}$. Let Σ be the $\{2^3, 3\}$ -partial spread obtained from it by removing all the 3-subgroups except

$H = \{(0, 0, 0), (1, 0, 0), (2, 0, 0)\}$. Consider the 3-subset $B = \{(0, 0, 1), (1, 1, 0), (2, 1, 1)\}$ of G_1 . Looking at its “difference table”

$\hat{\cdot}$	(0, 0, 1)	(1, 1, 0)	(2, 1, 1)
(0, 0, 1)	•	(2, 0, 1)	(1, 0, 1)
(1, 1, 0)	(1, 1, 1)	•	(2, 1, 1)
(2, 1, 1)	(2, 1, 0)	(1, 1, 0)	•

we see that ΔB is the set of all the 3-elements of G_1 not belonging to H . Thus the singleton $F = \{B\}$ is a $(G_1, \Sigma, 3, 1)$ -DF.

Now consider the subgroup $J = \{(0, 0, 0), (0, 1, 1)\}$ of G_1 . The other two subgroups of order 2 are $a + J - a$ and $b + J - b$ with $a = (1, 1, 1)$ and $b = (2, 0, 1)$. Now partition G_1 into the left cosets of J indicating in boldface the elements of $B \cup \{0, a, b\}$:

$$\{\mathbf{(0, 0, 0)}, (0, 1, 1)\}, \quad \{\mathbf{(0, 0, 1)}, (0, 1, 0)\}, \quad \{(1, 0, 0), \mathbf{(1, 1, 1)}\}, \\ \{(1, 0, 1), \mathbf{(1, 1, 0)}\}, \quad \{(2, 0, 0), \mathbf{(2, 1, 1)}\}, \quad \{\mathbf{(2, 0, 1)}, (2, 1, 0)\}.$$

We see that $B \cup \{0, a, b\}$ is a system of representatives for the left cosets of J in G_1 , i.e., F is J -resolvable. Following the instructions given in the proof of the “if” part of Theorem 3.8, we obtain the following 3-pyramidal representation of a KTS(15) where, to save space, each element $(a, b, c) \in G_1$ is written as abc .

$$\{\infty_1, \infty_2, \infty_3\} \{000, 100, 200\} \{001, 101, 201\} \{010, 110, 210\} \{011, 111, 211\} \\ \{\infty_1, 000, 011\} \{\infty_2, 111, 100\} \{\infty_3, 201, 210\} \{001, 110, 211\} \{010, 101, 200\} \\ \{\infty_1, 001, 010\} \{\infty_2, 110, 101\} \{\infty_3, 200, 211\} \{000, 111, 210\} \{011, 100, 201\} \\ \{\infty_1, 100, 110\} \{\infty_2, 210, 200\} \{\infty_3, 011, 001\} \{111, 201, 010\} \{101, 211, 000\} \\ \{\infty_1, 101, 111\} \{\infty_2, 211, 201\} \{\infty_3, 010, 000\} \{110, 200, 011\} \{100, 210, 001\} \\ \{\infty_1, 200, 201\} \{\infty_2, 001, 000\} \{\infty_3, 110, 111\} \{210, 011, 101\} \{211, 010, 100\} \\ \{\infty_1, 211, 210\} \{\infty_2, 010, 011\} \{\infty_3, 101, 100\} \{201, 000, 110\} \{200, 001, 111\}$$

It is known that, up to isomorphism, there exist exactly seven KTS(15), i.e., there are seven non-isomorphic solutions to the well-known Kirkman fifteen schoolgirls problem. It is possible to show, applying the proposition on page 894 of [27], that the solution above is necessarily isomorphic to the original solution given by Kirkman, that is the solution denoted by 1a in [17] Table 1.28, p. 30.

6.3 A 3-pyramidal KTS(33)

Let $G = D \times V_5$ and consider the following four 3-subsets of G :

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

One can check that they form a $(G, \Sigma, 3, 1)$ -DF where Σ is the unique $\{2^3, 3\}$ -partial spread of G , that is the set of all non-trivial subgroups of D . Then check that this difference family is J -resolvable with $J = \{(0, 0, 0), (1, 0, 0)\}$; two elements a, b as in Definition 3.6 are $(1, 1, 0)$ and $(1, 2, 0)$.

6.4 A 3-pyramidal KTS(39)

Let $G = G_1 \times V_3$ and consider the following five 3-subsets of G :

$$\begin{aligned} &\{(0, 0, 0, 2), (0, 1, 1, 1), (1, 0, 0, 1)\}, \\ &\{(0, 0, 1, 2), (2, 0, 1, 2), (2, 1, 0, 1)\}, \\ &\{(0, 1, 0, 0), (1, 0, 1, 2), (2, 0, 1, 0)\}, \\ &\{(0, 1, 0, 1), (1, 1, 1, 0), (2, 0, 0, 0)\}, \\ &\{(1, 0, 1, 1), (1, 1, 0, 0), (2, 1, 1, 2)\}. \end{aligned}$$

One can check that they form a $(G, \Sigma, 3, 1)$ -DF where Σ is the $\{2^3, 3\}$ -partial spread whose subgroup of order 3 is $\{0, x, -x\}$ with $x = (0, 0, 0, 1)$. Then check that this difference family is J -resolvable with $J = \{(0, 0, 0, 0), (0, 1, 1, 0)\}$; two elements a, b as in Definition 3.6 are $(1, 0, 0, 2)$ and $(2, 0, 0, 1)$.

6.5 A 3-pyramidal KTS(51)

One can check that the following six 3-subsets of G_2 :

$$\begin{aligned} B_1 &= \{(0, 0, 1), (2, 3, 0), (2, 3, 1)\}, & B_2 &= \{(0, 1, 1), (0, 1, 2), (0, 2, 1)\}, \\ B_3 &= \{(1, 1, 0), (1, 0, 1), (2, 1, 1)\}, & B_4 &= \{(1, 1, 2), (2, 0, 3), (1, 3, 1)\}, \\ B_5 &= \{(2, 1, 0), (1, 0, 3), (0, 3, 1)\}, & B_6 &= \{(0, 1, 0), (2, 2, 3), (1, 3, 3)\}, \end{aligned}$$

form a $(G_2, H, 3, 1)$ -RDF where H is the subgroup of G_2 with underlying-set $\mathbb{Z}_3 \times 2\mathbb{Z}_4 \times 2\mathbb{Z}_4$. The map $(a, b, c) \in G_1 \rightarrow (a, 2b, 2c) \in H$ is clearly an isomorphism between G_1 and H . Hence the singleton $\{B_7\}$ with $B_7 = \{(0, 0, 2), (1, 2, 0), (2, 2, 2)\}$ is a $(H, \{2^3, 3\}, 3, 1)$ -RDF for what we have seen in Subsect. 6.2. We conclude that $\{B_1, \dots, B_6, B_7\}$ is a $(G_2, \Sigma, 3, 1)$ -RDF where Σ is the $\{2^3, 3\}$ -partial spread whose subgroup of order 3 is $\{0, x, -x\}$ with $x = (1, 0, 0)$.

7 Three direct constructions

The action of a group U on a set V is said to be *semiregular* if the non-identity elements of U do not fix any element of V . The following fact is straightforward.

Proposition 7.1 *If U is a group of units of \mathbb{F}_n whose action by multiplication on V_n^* is semiregular and S is a complete system of representatives for the orbits of U on V_n^* , then we have $US = V_n^*$.*

We need the following lemma.

Lemma 7.2 *Let $n > 1$ be an integer whose components are all congruent to 1 (mod λ). Then there exist a unit u of \mathbb{F}_n of order λ and a subgroup T of $\mathbb{U}(\mathbb{F}_n)$ such that*

- (i) $u^j - 1$ is a unit for $1 \leq j \leq \lambda - 1$ and the group U generated by u acts semiregularly on V_n^* ;
- (ii) the order of T is the greatest divisor of $\psi(n)$ coprime with λ ;
- (iii) T leaves invariant a suitable complete system S of representatives for the orbits of U on V_n^* .

Proof Let q_1, \dots, q_ω be the components of n . For $1 \leq i \leq \omega$, let u_i be a generator of the subgroup U_i of $\mathbb{F}_{q_i}^*$ of order λ , and set $u = (u_1, \dots, u_\omega)$. It is very easy to prove that u satisfies (i) (see Corollary 3.3 and Lemma 3.2 in [7], in this order). Let T_i be the subgroup of $\mathbb{F}_{q_i}^*$ whose order is the greatest divisor of $q_i - 1$ coprime with λ , set $T = T_1 \times \dots \times T_\omega$, and let Σ_i be a complete system of representatives for the cosets of $T_i U_i$ in $\mathbb{F}_{q_i}^*$. Now, for every non-empty I belonging to the power-set $2^{\{1, \dots, \omega\}}$, choose an element $c(I) \in I$ and consider the subset $S(I)$ of V_n^* defined as follows:

$$S(I) = S_1(I) \times \dots \times S_\omega(I) \quad \text{with} \quad S_j(I) = \begin{cases} \{0\} & \text{if } j \notin I; \\ \Sigma_j T_j & \text{if } j = c(I); \\ \mathbb{F}_{q_j}^* & \text{if } j \in I \setminus \{c(I)\}. \end{cases}$$

Then set $S = \bigcup_{I \in 2^{\{1, \dots, \omega\}} \setminus \{\emptyset\}} S(I)$. It is not difficult to check that S is a complete system of representatives for the orbits of U on V_n^* and that T leaves S invariant. □

In this section we give three direct constructions which can be understood without any further explanation. Anyway, to be more informative, we emphasize that, in each case, a suitable *strong difference family* satisfying a special resolvability property has been used. These concepts are defined as follows.

Definition 7.3 Given a group G and an even integer λ , a $(G, 3, \lambda)$ *strong difference family* (SDF) is a collection of triples of elements of G whose list of differences covers each element of G , 0 included, exactly λ times.

If J is a subgroup of G of order 2, then we say that a $(G, 3, \lambda)$ -SDF is J -resolvable if its flatten contains exactly λ elements of each left coset of J in G .

Although the notion of a SDF was implicitly used in the literature for a long time, the formal definition has been given in [5]. Since then, SDFs have been crucial for the construction of various combinatorial designs in several papers such as [9,10,15,19,20,48,61]. As far as we are aware, the notion of a J -resolvable SDF is new.

Theorem 7.4 *If all the components of $4n + 1$ are congruent to 1 (mod 4), then there exists a $(D \times V_{4n+1}, D \times V_1, 3, 1)$ -RDF with a group of strong multipliers whose order is the greatest odd divisor of $\psi(4n + 1)$.*

Proof Take u, T and S as in the statement of Lemma 7.2 applied with $\lambda = 4$. Thus u is a unit of order 4 such that $u - 1$ is also a unit and $U := \langle u \rangle$ acts semiregularly on V_{4n+1}^* . Note that we necessarily have $u^2 = -1$, hence $U = \{\pm 1, \pm u\}$. Also note that we have $(u - 1)U = \{\pm(u - 1), \pm(u + 1)\}$.

Let us consider the set B consisting of the following triples of $D \times V_{4n+1}$ (recall that the underlying set of D is $\mathbb{Z}_2 \times \mathbb{Z}_3$; see Sect. 3):

$$\begin{aligned} & \{(0, 0, u), (0, 0, -u), (0, 2, -1)\}, \quad \{(0, 0, 1), (0, 1, u), (1, 2, -u)\}, \\ & \{(0, 0, -1), (0, 2, u), (1, 1, 1)\}, \quad \{(0, 1, 1), (0, 1, -1), (1, 1, -u)\}. \end{aligned}$$

It is straightforward to check that we have $\Delta B = \bigcup_{g \in D} \{g\} \times \Delta_g$ with

$$\Delta_g = \begin{cases} 2U & \text{if } g = (0, 0) \text{ or } g = (1, 1); \\ (u - 1)U & \text{otherwise.} \end{cases}$$

It is also readily seen that

$$\bigcup_{B \in B} B + J = \bigcup_{g \in D} \{g\} \times \Phi_g$$

with $J = \{(0, 0, 0), (1, 0, 0)\}$ and $\Phi_g = U$ for every $g \in D$. Now set

$$F = \{\mu_s(B) \mid s \in S; B \in B\}.$$

Given that S is a complete system of representatives for the orbits of U on V_{4n+1}^* , we have $US = V_{4n+1}^*$ by Proposition 7.1 and then, taking into account the previous identities, we easily obtain

$$\Delta F = (D \times V_{4n+1}) \setminus (D \times V_1) = \Phi(F) + J$$

which means that F is a $(D \times V_{4n+1}, D \times V_1, 3, 1)$ -RDF.

Finally, given that T is a subgroup of $\mathbb{U}(\mathbb{F}_n)$ which leaves S invariant, we infer that $\{\mu_t \mid t \in T\}$ is a group of strong multipliers of F . The assertion follows by observing that this group is clearly isomorphic to T and recalling that the order of T is the greatest odd divisor of $\psi(4n + 1)$. □

Observe that the set of *initial* base blocks B considered in Theorem 7.4 is a lifting of a J -resolvable $(D, 3, 4)$ -SDF.

If we apply Theorem 7.4 with $n = 1$ we are forced to take $u = 3$ and one can see that the resultant RDF is exactly the one given in Subsect. 6.3.

Theorem 7.5 *If all the components of n are congruent to 1 (mod 4), then there exists a $(G_1 \times V_n, G_1 \times V_1, 3, 1)$ -RDF with a group of strong multipliers whose order is the greatest odd divisor of $\psi(n)$.*

Proof Again, as in Theorem 7.4, take u, T and S as in the statement of Lemma 7.2 applied with $\lambda = 4$. Consider the set B consisting of the following eight 3-subsets of $G_1 \times V_n$ (recall that the underlying set of G_1 is $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; see Sect. 3):

$$\begin{aligned} & \{(0, 0, 0, -1), (0, 0, 0, 1), (2, 1, 0, -u)\}, & \{(0, 0, 0, -u), (0, 0, 0, u), (2, 1, 1, 1)\}, \\ & \{(0, 0, 1, 1), (0, 1, 0, -1), (1, 1, 0, -u)\}, & \{(0, 0, 1, u), (0, 1, 0, -u), (1, 1, 0, 1)\}, \\ & \{(1, 0, 0, -1), (1, 1, 1, 1), (2, 0, 1, u)\}, & \{(1, 0, 0, u), (1, 1, 1, -u), (2, 1, 1, -1)\}, \\ & \{(1, 0, 1, -1), (2, 0, 0, -u), (2, 1, 1, u)\}, & \{(1, 0, 1, u), (2, 0, 1, -1), (2, 1, 0, 1)\}. \end{aligned}$$

One can check that $\Delta B = \bigcup_{g \in G_1} \{g\} \times \Delta_g$ with $\Delta_g = 2U$ or $\Delta_g = (u - 1)U$ according to whether g belongs or does not belong to the Klein subgroup of G_1 , respectively.

Also, we have $\bigcup_{B \in B} B + J = \bigcup_{g \in G_1} \{g\} \times \Phi_g$ with $J = \{(0, 0, 0, 0), (0, 1, 1, 0)\}$ and $\Phi_g = U$ for every $g \in G_1$.

Reasoning as in Theorem 7.4, we can see that

$$F = \{\mu_s(B) \mid s \in S; B \in B\}$$

is a $(G_1 \times V_n, G_1 \times V_1, 3, 1)$ -RDF admitting $\{\mu_t \mid t \in T\}$ as a group of strong multipliers of order the greatest odd divisor of $\psi(n)$. □

Analogously to Theorem 7.4 the set of *initial* base blocks B considered above is a lifting of a J -resolvable $(G_1, 3, 4)$ -SDF.

Theorem 7.6 *If all the components of n are congruent to 1 (mod 6), then there exists a $(G_1 \times V_n, G_1 \times V_1, 3, 1)$ -RDF with a group of strong multipliers whose order is the greatest divisor of $\psi(n)$ coprime with 6.*

Proof Take u, T and S as in the statement of Lemma 7.2 applied with $\lambda = 6$. Thus u is a unit of $\mathbb{U}(\mathbb{F}_n)$ of order 6 such that $u^i - 1$ is a unit for $1 \leq i \leq 5$ and $U := \langle u \rangle$ acts semiregularly on V_n^* . Note that we necessarily have $u^3 = -1$ so that $U = \{\pm 1, \pm u, \pm u^2\}$, and the identity $u^2 - u + 1 = 0$ holds.¹ Consider the set B consisting of the following twelve 3-subsets of $G_1 \times V_n$:

$$\begin{aligned} &\{(0, 0, 0, 1), (0, 0, 0, -u), (0, 0, 0, u^2)\}; \\ &\{(0, 0, 0, u), (0, 1, 0, -u^2), (1, 1, 0, -1)\}; \\ &\{(0, 0, 1, -u), (1, 0, 0, u^2), (2, 0, 1, 1)\}; \\ &\{(0, 0, 1, u^2), (1, 0, 1, 1), (1, 1, 1, -u)\}; \\ &\{(0, 0, 1, 1), (1, 1, 0, u^2), (2, 0, 0, -u)\}; \\ &\{(0, 1, 0, u), (0, 1, 1, -u^2), (2, 0, 1, -1)\}; \\ &\{(0, 1, 0, -1), (1, 1, 1, u), (2, 0, 0, -u^2)\}; \\ &\{(0, 1, 1, -1), (1, 0, 0, -u^2), (2, 0, 1, u)\}; \\ &\{(1, 0, 0, 1), (1, 0, 1, -u), (2, 0, 1, u^2)\}; \\ &\{(1, 0, 1, -u^2), (1, 1, 1, -1), (2, 1, 1, u)\}; \\ &\{(1, 0, 1, u), (2, 0, 1, -u^2), (2, 1, 1, -1)\}; \\ &\{(2, 0, 0, u^2), (2, 0, 1, -u), (2, 1, 1, 1)\}. \end{aligned}$$

With a little bit of patience, taking into account the identity $u^2 = u - 1$, it is not difficult to check that we have:

$$\Delta B = \bigcup_{g \in G_1} \{g\} \times (u + 1)U \quad \text{and} \quad \bigcup_{B \in B} B + J = \bigcup_{g \in G_1} \{g\} \times U \tag{7.1}$$

where $J = \{(0, 0, 0, 0), (0, 1, 1, 0)\}$. We can write $u + 1 = -(u^4 - 1)$, hence $u + 1$ is a unit of \mathbb{F}_n by assumption on u . Now set

$$F = \{\mu_s(B) \mid s \in S; B \in B\}.$$

Given that S is a complete system of representatives for the orbits of U on V_{4n+1}^* , we have $US = V_n^*$ by Proposition 7.1 and then, taking into account (7.1), we easily obtain

$$\Delta F = \Phi(F) + J = (G_1 \times V_n) \setminus (G_1 \times V_1)$$

which means that F is a $(G_1 \times V_n, G_1 \times V_1, 3, 1)$ -RDF.

Finally, given that T is a subgroup of $\mathbb{U}(\mathbb{F}_n)$ which leaves S invariant, we infer that $\{\mu_t \mid t \in T\}$ is a group of strong multipliers of F . The assertion follows observing that this group is clearly isomorphic to T whose order is the greatest divisor of $\psi(n)$ coprime with 6. □

This time the set of *initial* base blocks B considered above is a lifting of a J -resolvable $(G_1, 3, 6)$ -SDF.

¹ By definition, we have $u^6 - 1 = 0$, hence $(u^3 - 1)(u + 1)(u^2 - u + 1) = 0$. It cannot be $u^3 - 1 = 0$ or $u + 1 = 0$ otherwise u would have order 3 or 2, respectively. It follows that $u^2 - u + 1 = 0$.

8 A composition construction via pseudo-resolvable difference families

Now we define a class of $(G, \{2^3, 3\}, 3, 1)$ -DFs, that we call pseudo-resolvable, that will be crucial for the construction of a 3-pyramidal KTS(v) with $v = 36n + 3$ or $v = 48n + 3$ or $v = 108n + 3$ with all the components of n congruent to 7 or 11 (mod 12).

Definition 8.1 Let G be a pertinent group of doubly even order and let F be a $(G, \Sigma, 3, 1)$ -DF with $\Sigma = \{\{0, j_1\}, \{0, j_2\}, \{0, j_3\}, \{0, x, -x\}\}$. We say that F is *pseudo-resolvable* (PRDF for short) if $\Phi(F) \cup \{0, j_\alpha, x\}$ is a complete system of representatives for the left cosets of $\{0, j_\beta\}$ in G for suitable involutions j_α, j_β .

Even though the definitions of resolvable and pseudo-resolvable difference families are very similar, they are independent. For instance, in spite of the fact that there exists a $(G_1, \{2^3, 3\}, 3, 1)$ -RDF (see Subsect. 6.2), there is no $(G_1, \{2^3, 3\}, 3, 1)$ -PRDF. Certainly, a $(G, \{2^3, 3\}, 3, 1)$ -DF cannot be resolvable and pseudo-resolvable at the same time. Here is a useful example in the groups $G_1 \times V_3$.

Example 8.2 Let Σ be the $\{2^3, 3\}$ -partial spread of $G_1 \times V_3$ whose member of order 3 is $\{0, x, -x\}$ with $x = (1, 0, 0, 0)$. One can check that the following five 3-subsets of $G_1 \times V_3$

$$\begin{aligned} B_1 &= \{(0, 0, 1, 2), (0, 1, 1, 1), (1, 0, 0, 2)\}, \\ B_2 &= \{(0, 1, 0, 1), (1, 0, 0, 1), (2, 1, 0, 0)\}, \\ B_3 &= \{(0, 1, 1, 2), (2, 0, 0, 0), (2, 0, 0, 1)\}, \\ B_4 &= \{(1, 0, 1, 1), (1, 1, 0, 0), (2, 1, 0, 2)\}, \\ B_5 &= \{(1, 1, 0, 2), (2, 0, 0, 2), (2, 0, 1, 1)\}, \end{aligned}$$

form a $(G_1 \times V_3, \Sigma, 3, 1)$ -PRDF.

The following Theorem 8.3 explains why pseudo-resolvable DFs can be helpful in the construction of some resolvable DFs.

Theorem 8.3 Assume that all the components of n are congruent to 3 (mod 4) but distinct from 3, and that there exists a $(G, \Sigma, 3, 1)$ -PRDF with G pertinent of doubly even order. Then there exists a $(G \times V_n, G \times V_1, 3, 1)$ -RDF with a group of strong multipliers of order the greatest odd divisor of $\psi(n)$.

Proof The fact that G is pertinent of doubly even order implies that its three involutions j_1, j_2, j_3 , together with zero, form the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$ (see Lemma 4.4). Thus we have $j_\alpha + j_\beta = j_\gamma$ for every permutation (α, β, γ) of $(1, 2, 3)$.

Let F be a $(G, \Sigma, 3, 1)$ -PRDF and let H be the union of the members of Σ . Thus $H = \{0, j_1, j_2, j_3, x, -x\}$ for a suitable element x of order 3. By definition, up to a reordering of $\{j_1, j_2, j_3\}$, we have

$$\Delta F = G \setminus H \quad \text{and} \quad \Phi(F) + \{0, j_1\} = G \setminus L \tag{8.1}$$

where $L = \{0, j_1, j_2, j_3, x, x + j_1\}$.

Let $n = q_1 \dots q_\omega$ be the prime power factorization of n . By assumption we have $q_i \equiv 3 \pmod{4}$, hence $-1 \in \mathbb{F}_{q_i}^\times$ for $1 \leq i \leq \omega$. Take any element σ_i of $\mathbb{F}_{q_i}^\times \setminus \{1\}$ and set $y_i = \frac{\sigma_i + 1}{\sigma_i - 1}$. Set $y = (y_1, \dots, y_\omega)$ and consider the following two 3-subsets of $G \times \mathbb{F}_n$:

$$A_1 = \{(0, 1), (x, y), (x, -y)\}, \quad A_2 = \{(0, -1), (j_2, y), (j_3, -y)\}.$$

Note that we have $\Delta\{A_1, A_2\} = \bigcup_{h \in H} \{h\} \times \Delta_h$ with

$$\begin{aligned} \Delta_0 &= \Delta_{j_1} = \{2y, -2y\}; \\ \Delta_{j_2} &= \{y + 1, -(y + 1)\}; & \Delta_{j_3} &= \{y - 1, -(y - 1)\}; \\ \Delta_x &= \{y - 1, -(y + 1)\}; & \Delta_{-x} &= \{y + 1, -(y - 1)\}. \end{aligned}$$

We have $\frac{y_i+1}{y_i-1} = \sigma_i \in \mathbb{F}_{q_i}^\square$, thus $y_i - 1$ and $y_i + 1$ are both squares or both non-squares of \mathbb{F}_{q_i} . Also, we have $q_i \equiv 3 \pmod{4}$ for each i so that $-1 \in \mathbb{F}_{q_i}^\square$. On the basis of these facts it is evident that the projection of each Δ_h on $\mathbb{F}_{q_i}^\square$ consists of a non-zero square and a non-square of \mathbb{F}_{q_i} . As a consequence, if S is any halving of V_n^* , we have $S\Delta_h = V_n^*$ for every $h \in H$. Thus, the set of triples $A =: \{\mu_s(A_i) \mid i = 1, 2; s \in S\}$ has list of differences $\Delta A = H \times V_n^*$, i.e.,

$$\Delta A = (H \times V_n) \setminus (H \times V_1) \tag{8.2}$$

Now note that we have

$$(A_1 \cup A_2) + \{(0, 0), (j_1, 0)\} = \bigcup_{\ell \in L} \{\ell\} \times \{\phi_\ell, -\phi_\ell\}$$

with $\phi_0 = \phi_{j_1} = 1$, and $\phi_\ell = y$ for $\ell \in L \setminus \{0, j_1\}$. We clearly have $\{\phi_\ell, -\phi_\ell\} \cdot S = V_n^*$ for each $\ell \in L$ and then

$$\Phi(A) + \{(0, 0), (j_1, 0)\} = (L \times V_n) \setminus (L \times V_1). \tag{8.3}$$

Take a triple $\{u_1, u_2, u_3\}$ of units of \mathbb{F}_n with the property that the elements of its list of differences $\Delta\{u_1, u_2, u_3\}$ are also units. For instance, one could take $\{u_1, u_2, u_3\} = \{1, -1, y\}$. Now lift each triple $B = \{b_1, b_2, b_3\} \in F$ to the triple $B^+ = \{(b_1, u_1), (b_2, u_2), (b_3, u_3)\}$ and set

$$F^+ = \{\mu_z(B^+) \mid B \in F; z \in V_n^*\}.$$

We note that the contribution of a single $B \in F$ to ΔF^+ and $\Phi(F^+)$ is $(\Delta B) \times V_n^*$ and $B \times V_n^*$, respectively. Thus that the two equalities in (8.1) imply that we have:

$$\Delta F^+ = (G \setminus H) \times (V_n \setminus V_1); \tag{8.4}$$

$$\Phi(F^+) + \{(0, 0), (j_1, 0)\} = (G \setminus L) \times (V_n \setminus V_1). \tag{8.5}$$

It is clear that $A \cup F^+$ is a $(G \times V_n, G \times V_1, 3, 1)$ -RDF. Indeed (8.2) and (8.4) imply that $\Delta(A \cup F^+) = (G \times V_n) \setminus (G \times V_1)$. Also, (8.3) and (8.5) imply that $\Phi(A \cup F^+) + \{(0, 0), (j_1, 0)\} = (G \times V_n) \setminus (G \times V_1)$.

Letting q_1, \dots, q_ω be the components of n , we finally note that

$$\{\mu_s \mid s \in \mathbb{F}_{q_1}^\square \times \dots \times \mathbb{F}_{q_\omega}^\square\}$$

is a group of strong multipliers of F^+ and its order is the greatest odd divisor of $\psi(n)$ since each $q_i \equiv 3 \pmod{4}$. The assertion follows. \square

Letting $G = G_1 \times V_3$ and applying Theorem 8.3 to the $(G, \Sigma, 3, 1)$ -PRDF given in Example 8.2, we obtain the following important result.

Corollary 8.4 *If all the components of n are greater than 3 and congruent to 3 modulo 4, then there exists a $(G_1 \times V_{3n}, G_1 \times V_3, 3, 1)$ -RDF with a group of strong multipliers of order the greatest odd divisor of $\psi(n)$.*

In Appendices A and B we will give an example of a $(G, \{2^3, 3\}, 3, 1)$ -PRDF with both $G = G_1 \times V_9$ and $G = G_2$. Thus, as another important application of Theorem 8.3 we get the following.

Corollary 8.5 *If all the components of n are greater than 3 and congruent to 3 modulo 4, then there exists a $(G_1 \times V_{9n}, G_1 \times V_9, 3, 1)$ -RDF with a group of strong multipliers of order the greatest odd divisor of $\psi(n)$.*

Corollary 8.6 *If all the components of n are greater than 3 and congruent to 3 modulo 4, then there exists a $(G_2 \times V_n, G_2 \times V_1, 3, 1)$ -RDF with a group of strong multipliers of order the greatest odd divisor of $\psi(n)$.*

9 Doubly disjoint difference families

A $(G, H, 3, 1)$ -DF is said to be *disjoint* if its blocks are pairwise disjoint and do not meet the subgroup H . It is well known that there exists a disjoint $(\mathbb{Z}_{6n+1}, 3, 1)$ -DF and a disjoint $(\mathbb{Z}_{6n+3}, \{0, 2n+1, 4n+2\}, 3, 1)$ -DF for every positive integer n (see [8,22,23]). There is an intriguing conjecture by Novák [49] according to which every cyclic STS $(6n+1)$ is generated by a suitable disjoint $(\mathbb{Z}_{6n+1}, 3, 1)$ -DF. In a very recent paper [28] it has been proved that this conjecture is true with the possible exception of finitely many composite orders $6n+1$.

Let us say that two difference families are *strongly equivalent* if each block of the first is a suitable translate of a block of the second.²

Definition 9.1 A $(G, H, 3, 1)$ -DF is *doubly disjoint* if its blocks tile $G \setminus H$ together with the blocks of another DF strongly equivalent to it.

Note how Definition 9.1 reminds a bit of the notion introduced in [21] of a (v, k, λ) tiling of a group G , that is a set of mutually disjoint (v, k, λ) difference sets in G partitioning $G \setminus \{0\}$. Needless to say, however, that two distinct members of a (v, k, λ) tiling of G cannot be strongly equivalent.

Note that any $\{0, j\}$ -resolvable $(G, H, 3, 1)$ -DF, say $F = \{B_1, \dots, B_n\}$, is doubly disjoint. Indeed, setting $B'_i = B_i + j$ for $i = 1, \dots, n$, it is clear that F and $F' := \{B'_1, \dots, B'_n\}$ are strongly equivalent. Also, by definition, we have $\Phi(F) + \{0, j\} = G \setminus H$ and this is equivalent to say that the blocks of F and F' form a partition of $G \setminus H$.

In the next section we will give a composition construction for RDFs where doubly disjoint difference families play a crucial role. For this reason, it is worth studying their possible existence. In particular, we are interested in $(\mathbb{Z}_3 \times V_{2n+1}, \mathbb{Z}_3 \times V_1, 3, 1)$ -DFs. We are going to prove their existence in the case that all the components of $2n+1$ are congruent to 1 (mod 4).

Theorem 9.2 *If the components of n are all congruent to 1 (mod 4), then there exists a doubly disjoint $(\mathbb{Z}_3 \times V_n, \mathbb{Z}_3 \times V_1, 3, 1)$ -DF.*

Proof First observe that if $q \equiv 1 \pmod{4}$ is a prime power, then the set $X = \{x \in \mathbb{F}_q^{\square} : x - 2 \in \mathbb{F}_q^{\square}\}$ is not empty. For instance, using the *cyclotomic numbers* of order 2 (see, e.g.,

² We cannot simply say that they are *equivalent* since two difference families in a group G , say $F = \{B_1, \dots, B_n\}$ and $F' = \{B'_1, \dots, B'_n\}$, are usually said to be equivalent if, up to the order, we have $B'_i = \alpha(B_i) + t_i$ for a suitable $\alpha \in \text{Aut}(G)$ and suitable $t_1, \dots, t_n \in G$.

[24]) one can see that X has size $\frac{q-1}{4}$. More elementarily and constructively, an element of X can be found as follows. Take any y of $\mathbb{F}_q^\square \setminus \{2\}$ and check that the set

$$X' = \{y, y + 1, 1 - y, 4 - 2y, \frac{2}{y + 1}, \frac{2y}{y - 1}\}$$

has at least one element in common with X .

Thus, if $n = q_1 \dots q_\omega$ with $q_i \equiv 1 \pmod{4}$ is a prime power for $1 \leq i \leq \omega$, we can construct an element $x = (x_1, \dots, x_\omega) \in \mathbb{F}_n$ with the property that $x_i \in \mathbb{F}_{q_i}^\square$ and $x_i - 2 \in \mathbb{F}_{q_i}^\square$ for $1 \leq i \leq \omega$. Consider the 3-subsets A and B of $\mathbb{Z}_3 \times V_n$ defined as follows:

$$A = \{(0, 1), (1, x), (1, 2 - x)\}; \quad B = \{(0, x), (2, x^2), (2, 2x - x^2)\}.$$

We have

$$\Delta A \cup \Delta B = \bigcup_{h=0}^2 \{h\} \times \{1, -1\} \cdot \Delta_h$$

with $\Delta_0 = \{2(x - 1), 2x(x - 1)\}$ and $\Delta_1 = \Delta_2 = \frac{1}{2}\Delta_0$. Also, we have

$$A \cup B = \bigcup_{h=0}^2 \{h\} \times \Phi_h$$

with $\Phi_0 = \{1, x\}$, $\Phi_1 = \{x, 2 - x\}$, and $\Phi_2 = \{x^2, x(2 - x)\}$.

Now take a halving S of V_n^* (see Sect. 5). In view of the choice of the element x , we see that the projection of each Δ_h and each Φ_h on \mathbb{F}_{q_i} consists of a square and a non-square. Thus, by (5.1), we have $\Delta_h S = \Phi_h S = V_n^*$ for $h = 0, 1, 2$.

For each $s \in S$ set $A_s = \mu_s(A)$, $B_s = \mu_s(B)$, and consider the family $F = \{A_s, B_s \mid s \in S\}$. We obviously have $\Delta A_s = \mu_s(\Delta A)$ and $\Delta B_s = \mu_s(\Delta B)$. Thus we have

$$\Delta F = \bigcup_{h=0}^2 \{h\} \times (\{1, -1\} \cdot \Delta_h \cdot S) = \bigcup_{h=0}^2 \{h\} \times (\{1, -1\} \cdot V_n^*)$$

that is two times $(\mathbb{Z}_3 \times V_n) \setminus (\mathbb{Z}_3 \times V_1)$.

We also have:

$$\Phi(F) = \bigcup_{h=0}^2 \{h\} \times (\Phi_h \cdot S) = \bigcup_{h=0}^2 \{h\} \times V_n^* = (\mathbb{Z}_3 \times V_n) \setminus (\mathbb{Z}_3 \times V_1).$$

Note that the chosen halving S is *symmetric*, i.e., we have $-S = S$. Then there exists a subset T of S for which we have $S = T \cup (-T)$ so that F is splittable in the two families

$$F^+ = \{A_t, B_t \mid t \in T\}, \quad F^- = \{A_{-t}, B_{-t} \mid t \in T\}.$$

Now note that A_{-t} is a translate of A_t and that B_{-t} is a translate of B_t for every $t \in T$. Indeed it is readily seen that we have:

$$A_t + (0, -2t) = A_{-t}; \quad B_t + (0, -2xt) = B_{-t}.$$

We deduce, in particular, that $\Delta A_t = \Delta A_{-t}$ and $\Delta B_t = \Delta B_{-t}$ for every $t \in T$. It follows that $\Delta F^+ = \Delta F^-$. Thus, considering that ΔF is twice $\mathbb{Z}_3 \times V_n^*$, we necessarily have $\Delta F^+ = \Delta F^- = \mathbb{Z}_3 \times V_n^*$. This means that both F^+ and F^- are $(\mathbb{Z}_3 \times V_n, \mathbb{Z}_3 \times V_1, 3, 1)$ -DFs.

Considering that each block of F^- is a translate of a block of F^+ and that $\Phi(F^+ \cup F^-) = \Phi(F) = (\mathbb{Z}_3 \times V_n) \setminus (\mathbb{Z}_3 \times V_1)$, we conclude that F^+ is doubly disjoint and the assertion follows. \square

10 Composition constructions via difference matrices

We recall that a $(h, k, 1)$ difference matrix in a group H of order h , briefly denoted by $(H, k, 1)$ -DM, is a $k \times h$ matrix with elements from H in which the difference of any two distinct rows is a permutation of H .

In particular, an $(H, 3, 1)$ -DM is equivalent to a *complete mapping* of H . There is a large literature on complete mappings starting with the famous conjecture of Hall and Paige [32] according to which a group H of even order admits a complete mapping if and only if it is *admissible*, i.e., if and only if its 2-Sylow subgroups are not cyclic. The conjecture has been finally proved in [26].

Definition 10.1 A $(H, k, 1)$ difference matrix is *homogeneous* if each row is also a permutation of H .

It is quite evident that there exists a homogeneous $(H, k, 1)$ -DM if and only if there exists an $(H, k+1, 1)$ -DM. Indeed, adding a null-row to a homogeneous $(H, k, 1)$ -DM one gets an $(H, k+1, 1)$ -DM. Conversely, if M is a $(H, k+1, 1)$ -DM with rows M_1, \dots, M_{k+1} , then one gets a homogeneous $(H, k, 1)$ -DM whose rows are $M_2 - M_1, \dots, M_{k+1} - M_1$.

Thus, as immediate consequence of the main results on $(H, 4, 1)$ -DM (see [30,50]), we have the following.

Theorem 10.2 *There exists a homogeneous $(H, 3, 1)$ -DM with H abelian of odd order if and only if $|H| > 3$, except possibly when H is cyclic and $|H| \equiv 9 \pmod{27}$ (the exception is definite when $H \simeq \mathbb{Z}_9$).*

There exists a homogeneous $(H, 3, 1)$ -DM with H abelian of even order if and only if the 2-Sylow subgroup of H is not cyclic.

Corollary 10.3 *There exists a homogeneous $(V_n, 3, 1)$ -DM if and only if $3 < n \not\equiv 2 \pmod{4}$.*

Difference matrices are also a crucial topic of Design Theory [2,17]. They have been used explicitly or implicitly in a lot of papers especially for the composition constructions of designs with a regular automorphism group starting from some early work by Jungnickel [37] and by Colbourn and Colbourn [16]. Homogeneous difference matrices have been used later for the composition constructions of several kinds of resolvable designs (see, e.g., [1]). As far as we are aware the quite appropriate term *homogeneous* was coined in [38] when other authors choose other terms as *good* [13] about the same time.

We need to devise a new type of difference matrix that we call *splittable*.

Definition 10.4 Let J be a subgroup of order 2 of a group H and let M be a $(H, 3, 1)$ -DM. We say that M is *J-splittable* if the first half and the second half of each row of M is a complete system of representatives for the left cosets of J in H .

We give three examples of splittable difference matrices that will be crucial for the construction of some classes of resolvable difference families.

Example 10.5 Consider the following matrix M with elements in G_1

$$\left(\begin{array}{cccccc|cccccc} 000 & 010 & 100 & 110 & 200 & 210 & 011 & 001 & 111 & 101 & 211 & 201 \\ 000 & 100 & 210 & 010 & 110 & 200 & 000 & 101 & 010 & 210 & 200 & 100 \\ 010 & 200 & 210 & 100 & 000 & 110 & 101 & 001 & 200 & 011 & 201 & 111 \end{array} \right)$$

where, to save space, each element (a, b, c) has been denoted by abc . It is straightforward to check that M is a J -splittable $(G_1, 3, 1)$ -DM with $J = \{(0, 0, 0), (0, 1, 1)\}$.

Example 10.6 Consider the following matrix M with elements in $\mathbb{Z}_2 \times \mathbb{Z}_6$

$$\left(\begin{array}{cccccc|cccccc} 00 & 01 & 02 & 03 & 04 & 05 & 10 & 11 & 12 & 13 & 14 & 15 \\ 00 & 12 & 15 & 04 & 01 & 03 & 00 & 13 & 11 & 05 & 02 & 04 \\ 03 & 01 & 15 & 12 & 00 & 04 & 11 & 05 & 04 & 03 & 12 & 00 \end{array} \right)$$

where, to save space, each element (a, b) has been denoted by ab . It is straightforward to check that M is a J -splittable $(\mathbb{Z}_2 \times \mathbb{Z}_6, 3, 1)$ -DM with $J = \{(0, 0), (1, 0)\}$.

Example 10.7 Consider the following matrix M with elements in $\mathbb{Z}_4 \times \mathbb{Z}_4$

$$\left(\begin{array}{cccccc|cccccc} 00 & 30 & 11 & 20 & 01 & 10 & 31 & 21 & 22 & 12 & 33 & 02 & 23 & 32 & 13 & 03 \\ 22 & 11 & 30 & 10 & 21 & 23 & 02 & 31 & 13 & 20 & 32 & 00 & 12 & 33 & 01 & 03 \\ 22 & 31 & 03 & 01 & 10 & 30 & 20 & 33 & 32 & 12 & 00 & 21 & 13 & 23 & 11 & 02 \end{array} \right)$$

where, to save space, each element (a, b) has been denoted by ab . It is straightforward to check that M is a J -splittable $(\mathbb{Z}_4 \times \mathbb{Z}_4, 3, 1)$ -DM with $J = \{(0, 0), (2, 2)\}$.

The matrix of the third example is also homogeneous. The following Theorem 10.8 explains how doubly disjoint or resolvable difference families in a quotient group G/H can be combined with homogeneous or splittable difference matrices in H for the construction of resolvable difference families in G .

Theorem 10.8 *Let H be a normal subgroup of a pertinent group G and let L be a subgroup of G containing H . Assume that F is a $(G/H, L/H, 3, 1)$ -DF and M is a $(H, 3, 1)$ -DM. Then there exists a $(G, L, 3, 1)$ -DF.*

Moreover, let j be an involution of G and assume that one of the following additional hypotheses holds.

- (i) $j \notin H$, F is $\{H, j + H\}$ -resolvable, and M is homogeneous;
- (ii) $j \in H$, F is doubly disjoint, and M is $\{0, j\}$ -splittable.

Then there exists a $\{0, j\}$ -resolvable $(G, L, 3, 1)$ -DF.

Proof The first part of the statement has been already proved in [4] (see Corollary 5.8). It is convenient, however, to recall how the $(G, L, 3, 1)$ -DF can be constructed. Let $\bar{\cdot} : g \in G \rightarrow \bar{g} = g + H \in G/H$, be the canonical epimorphism from G to G/H , let $F = \{\bar{B}_i \mid i \in I\}$ with $B_i = \{b_{i,1}, b_{i,2}, b_{i,3}\}$, and let $M = (m_{r,c})$. For every block \bar{B}_i of F and for every column $M^c = (m_{1,c}, m_{2,c}, m_{3,c})$ of M , set $\bar{B}_i \circ M^c = \{b_{i,1} + m_{1,c}, b_{i,2} + m_{2,c}, b_{i,3} + m_{3,c}\}$. Then

$$F \circ M := \{\bar{B}_i \circ M^c \mid i \in I; 1 \leq c \leq |H|\}$$

is a $(G, L, 3, 1)$ -DF.

Assume that condition (i) holds.

If two elements $\phi_1 = b_{i_1,r_1} + m_{r_1,c_1}$ and $\phi_2 = b_{i_2,r_2} + m_{r_2,c_2}$ of $\Phi(F \circ M)$ are in the same left coset of $\{0, j\}$ in G , then we have

$$-m_{r_1,c_1} - b_{i_1,r_1} + b_{i_2,r_2} + m_{r_2,c_2} \in \{0, j\}.$$

Reducing modulo H we get $-\overline{b_{i_1,r_1}} + \overline{b_{i_2,r_2}} \in \{\overline{0}, \overline{j}\}$. This necessarily implies that $(i_1, r_1) = (i_2, r_2)$ because F is $\{\overline{0}, \overline{j}\}$ -resolvable. Thus, setting $r_1 = r_2 = r$, we have $-m_{r,c_1} + m_{r,c_2} \in \{0, j\}$. It cannot be $-m_{r,c_1} + m_{r,c_2} = j$ since j does not belong to H , hence $-m_{r,c_1} + m_{r,c_2} = 0$, i.e., $m_{r,c_1} = m_{r,c_2}$. This implies that $c_1 = c_2$ because M is homogeneous. We conclude that the two triples (i_1, r_1, c_1) and (i_2, r_2, c_2) coincide, i.e., $F \circ M$ is $\{0, j\}$ -resolvable.

Now assume that condition (ii) holds.

For each $i \in I$ there is a suitable translate of $\overline{B_i}$, say $\overline{B'_i} = \overline{B_i} + \overline{\tau_i}$, such that F and $F' = \{\overline{B'_i} \mid i \in I\}$ are $(G/H, L/H, 3, 1)$ -DFs with $\Phi(F) \cup \Phi(F')$ a partition of $(G/H) \setminus (L/H)$. Note that we can rewrite each $\overline{B'_i}$ in the form $\overline{B'_i} = \overline{B_i} + \overline{t_i}$ for a suitable t_i which commutes with j . Indeed we have $\tau_i + j - \tau_i = j_i$ with j_i one of the three involutions of G . The fact that $j \in H \trianglelefteq G$ implies that H is pertinent so that there exists $h_i \in H$ such that $h_i + j_i - h_i = j$. Then, setting $t_i = h_i + \tau_i$, it is easy to see that $\overline{B'_i} = \overline{B_i} + \overline{t_i}$ and that $t_i + j = j + t_i$.

Set

$$F \blacklozenge M = \{\overline{B_i} \circ M^c \mid i \in I; 1 \leq c \leq \frac{|H|}{2}\} \cup \{\overline{B_i} \circ M^c + t_i \mid i \in I; \frac{|H|}{2} < c \leq |H|\}.$$

Of course $F \blacklozenge M$ is a $(G, H, k, 1)$ -DF which is strongly equivalent to $F \circ M$. Let us show that it is $\{0, j\}$ -resolvable. We have:

$$\Phi(F \blacklozenge M) = \{\phi_{i,r,c} \mid i \in I; 1 \leq r \leq 3; 1 \leq c \leq |H|\}$$

with

$$\phi_{i,r,c} = \begin{cases} b_{i,r} + m_{r,c} & \text{if } c \leq |H|/2; \\ b_{i,r} + m_{r,c} + t_i & \text{if } c > |H|/2. \end{cases}$$

Assume that we have

$$-\phi_{i_1,r_1,c_1} + \phi_{i_2,r_2,c_2} \in \{0, j\} \tag{10.1}$$

for suitable triples (i_1, r_1, c_1) and (i_2, r_2, c_2) . We have to prove that these triples are necessarily equal. Without loss of generality we can assume that $c_1 \leq c_2$. So we have the following three possible cases.

1st case: $c_1 \leq c_2 \leq |H|/2$.

Here (10.1) implies that $-m_{r_1,c_1} - b_{i_1,r_1} + b_{i_2,r_2} + m_{r_2,c_2} \in \{0, j\}$. Reducing modulo H we get $\overline{b_{i_1,r_1}} = \overline{b_{i_2,r_2}}$ and then $(i_1, r_1) = (i_2, r_2)$ because F is disjoint. Thus, setting $r_1 = r_2 = r$, we have $-m_{r,c_1} + m_{r,c_2} \in \{0, j\}$ that is possible only for $c_1 = c_2$ because M is $\{0, j\}$ -splittable. We conclude that $(i_1, r_1, c_1) = (i_2, r_2, c_2)$.

2nd case: $|H|/2 < c_1 \leq c_2 \leq |H|$.

Here (10.1) implies that $-t_{i_1} - m_{r_1,c_1} - b_{i_1,r_1} + b_{i_2,r_2} + m_{r_2,c_2} + t_{i_2} \in \{0, j\}$. Reducing modulo H we get $\overline{b_{i_1,r_1}} + \overline{t_{i_1}} = \overline{b_{i_2,r_2}} + \overline{t_{i_2}}$ and then $(i_1, r_1) = (i_2, r_2)$ because F' is disjoint. Thus, setting $i_1 = i_2 = i$ and $r_1 = r_2 = r$, we have $-m_{r,c_1} + m_{r,c_2} \in \{0, t_i + j - t_i\} = \{0, j\}$,

the last equality being true since t_i commutes with j . This is possible only for $c_1 = c_2$ because M is $\{0, j\}$ -splittable. We conclude that $(i_1, r_1, c_1) = (i_2, r_2, c_2)$.

3rd case: $c_1 \leq |H|/2; c_2 > |H|/2$.

Here (10.1) gives $-m_{r_1, c_1} - b_{i_1, r_1} + b_{i_2, r_2} + m_{r_2, c_2} + t_i \in \{0, j\}$. Reducing modulo H we get $\overline{b_{i_1, r_1}} = \overline{b_{i_2, r_2}} + \overline{t_i}$. On the other hand $\overline{b_{i_2, r_2}}$ and $\overline{b_{i_1, r_1}} + \overline{t_i}$ belong to $\Phi(F)$ and $\Phi(F')$, respectively. This is absurd since $\Phi(F)$ and $\Phi(F')$ are disjoint. \square

As an important consequence of Theorem 10.8 we get the following corollaries.

Corollary 10.9 *If the components of n are all congruent to 1 (mod 4), then there exists a $(G_1 \times V_{3n}, G_1 \times V_3, 3, 1)$ -RDF.*

Proof Consider the group $G = G_1 \times V_{3n}$ and its subgroups $L = G_1 \times V_3$, and $H = G_1 \times V_1$. We have $G/H \simeq V_{3n}$ and $L/H \simeq V_3$, hence there exists a doubly disjoint $(G/H, L/H, 3, 1)$ -DF by Theorem 9.2. There also exists a splittable $(H, 3, 1)$ -DM by Example 10.5. Thus, by Theorem 10.8(ii), there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_1 \times V_{3n}, G_1 \times V_3, 3, 1)$ -RDF. \square

Corollary 10.10 *If the components of n are all congruent to 1 (mod 4), then there exists a $(G_2 \times V_n, G_1 \times V_1, 3, 1)$ -RDF.*

Proof Consider the group $G = G_2 \times V_n$ and its subgroups $L = G_1 \times V_n$, and $H = \{0\} \times V_n$. We have $G/H \simeq G_2$ and $L/H \simeq G_1$, hence there exists a doubly disjoint $(G/H, L/H, 3, 1)$ -DF (see Subsect. 6.5). There also exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. Thus there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_2 \times V_n, G_1 \times V_n, 3, 1)$ -RDF by Theorem 10.8(i). Now recall that there exists a $(G_1 \times V_n, G_1 \times V_1, 3, 1)$ -RDF by Theorem 7.5. We get the assertion by applying Proposition 3.2 with the chain $G_2 \times V_n \geq G_1 \times V_n \geq G_1 \times V_1$. \square

11 Main results

We are finally able to prove the sufficient conditions given by the main Theorem 1.1.

11.1 3-pyramidal KTS(24n + 9)

Recall that Theorem 7.4 says that there exists a $(D \times V_{4n+1}, D \times V_1, 3, 1)$ -RDF whenever the prime decomposition of $4n + 1$ does not contain primes $p \equiv 3 \pmod{4}$ raised to an odd power. Equivalently, whenever $4n + 1$ is a sum of two squares (see, e.g., [55]). Thus, considering that $24n + 9 = 6(4n + 1) + 3$ and that $D \times V_{4n+1}$ is a pertinent group of order $6(4n + 1)$, we get Theorem 1.1(i) by applying Proposition 6.1.

Theorem 11.1 *If $4n + 1$ is a sum of two squares, then there exists a 3-pyramidal KTS(24n + 9).*

Remark 11.2 Recall that Theorem 7.4 assures a group of strong multipliers of order the greatest odd divisor of $\psi(4n + 1)$. Therefore, Proposition 6.1 guarantees that the number of symmetries of each KTS(24n + 9) obtainable via Theorem 11.1 is at least equal to $(24n + 6)m$, where m is the greatest odd divisor of $\psi(4n + 1)$.

11.2 3-pyramidal $KTS(24n + 15)$

Here we prove Theorem 1.1(ii), that is our main result on 3-pyramidal $KTS(24n + 15)$.

Theorem 11.3 *There exists a 3-pyramidal $KTS(24n + 15)$ whenever one of the following conditions holds:*

- (1) $2n + 1$ is divisible by 3;
- (2) the square-free part of $2n + 1$ does not contain primes congruent to 11 (mod 12).

Proof We have $24n + 15 = 12(2n + 1) + 3$ and $G_1 \times V_{2n+1}$ is a pertinent group of order $12(2n + 1)$. Hence, by Proposition 6.1, it is enough to prove the existence of a $(G_1 \times V_{2n+1}, G_1 \times V_i, 3, 1)$ -RDF with $i = 1$ or 3.

Case 1): $2n + 1 \equiv 0 \pmod{3}$.

Set $e = 2$ if 9 is a component of $2n + 1$, otherwise set $e = 1$. Now let $(2n + 1)/3^e = PQ$ where P and Q are the product of all the components of $(2n + 1)/3^e$ congruent to 3 and 1 (mod 4), respectively. Note that 3 is not a component of P , otherwise $3^{e+1} = \begin{cases} 9 & \text{if } e = 1 \\ 27 & \text{if } e = 2 \end{cases}$ would be a component of $2n + 1$, contradicting the definition of the integer e .

Consider the group $G = G_1 \times V_{2n+1}$ and its subgroups $L = G_1 \times V_{3^e Q}$ and $H = \{0\} \times V_Q$. Since $G/H \simeq G_1 \times V_{3^e P}$ and $L/H \simeq G_1 \times V_{3^e}$, by Corollaries 8.4 and 8.5, there exists a $(G/H, L/H, 3, 1)$ -RDF. Also, there exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. Thus, by Theorem 10.8(i), there exists a $(G, L, 3, 1)$ -RDF. There is also an $(L, G_1 \times V_{3^{2-e}}, 3, 1)$ -RDF by Theorem 7.5 (when $e = 2$) and Corollary 10.9 (when $e = 1$). Therefore, by applying Proposition 3.2 with the chain $G \geq L \geq G_1 \times V_{3^{2-e}}$ we get a $(G, G_1 \times V_{3^{2-e}}, 3, 1)$ -RDF.

Case 2): the square-free part of $2n + 1$ does not contain any prime congruent to 11 (mod 12). We can assume that $2n + 1$ is not divisible by 3 in view of Case 1). Thus, by assumption, we can write $2n + 1 = PQ$ where P is the product of all components of $2n + 1$ that are congruent to 7 modulo 12 and Q is the product of all components of n that are congruent to 1 modulo 4. Of course it is understood that P and/or Q may be equal to 1 in the case that the components of the respective kinds do not exist. If $P = 1$ or $Q = 1$, we have a $(G_1 \times V_{2n+1}, G_1 \times V_1, 3, 1)$ -RDF by Theorem 7.5 or Theorem 7.6, respectively. If both P and Q are greater than 1, consider the group $G = G_1 \times V_{2n+1}$ and its subgroups $L = G_1 \times V_P$ and $H = \{0\} \times V_P$. We have $G/H \simeq G_1 \times V_Q$ and $L/H \simeq G_1 \times V_1$. Thus there exists a $(G/H, L/H, 3, 1)$ -RDF by Theorem 7.5. Also, there exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. It follows, by Theorem 10.8(i), that there exists a $(G, L, 3, 1)$ -RDF, i.e. a $(G_1 \times V_{2n+1}, G_1 \times V_P, 3, 1)$ -RDF. We also have a $(G_1 \times V_P, G_1 \times V_1, 3, 1)$ -RDF by Theorem 7.6. Applying Proposition 3.2 with the chain $G_1 \times V_{2n+1} \geq G_1 \times V_P \geq G_1 \times V_1$ we get a $(G_1 \times V_{2n+1}, G_1 \times V_1, 3, 1)$ -RDF. □

Remark 11.4 We recall that Theorems 7.5 and 7.6, and Corollaries 8.4 and 8.5 show the existence of a group of strong multipliers. Therefore, it is not difficult to check that Propositions 3.2 and 6.1 guarantee that

1. the number of symmetries of each KTS $(72n' + 39)$ obtainable via Theorem 11.3.(1) is at least equal to $m(72n' + 39)$, where m is the greatest odd divisor of $\psi(P)$ and $P > 1$ is the product of all the components of $2n' + 1$ congruent to 7 or 11 (mod 12);
2. the number of symmetries of each KTS $(24n + 15)$ built in Theorem 11.3.(2) is at least equal to $m(24n + 15)$ where m is defined as follows:
 - (a) if $Q > 1$ is the product of all the components of $2n + 1$ congruent to 1 (mod 4), then m is the greatest odd divisor of $\psi(Q)$;
 - (b) if all the components of $2n + 1$ are congruent to 7 (mod 12), then m is the greatest odd divisor of $\psi(2n + 1)$ coprime with 6.

11.3 3-pyramidal KTS $(48n + 3)$

In this subsection we will prove that the necessary condition for the existence of a KTS (v) is also sufficient when $v \equiv 3 \pmod{48}$, that is Theorem 1.1(iii).

We recall that $\{G_\alpha : \alpha \geq 1\}$ is the series of pertinent groups considered in Sect. 3. For $0 \leq i \leq \alpha - 1$, the subgroup of G_α with underlying-set $\mathbb{Z}_3 \times 2^i \mathbb{Z}_{2^\alpha} \times 2^i \mathbb{Z}_{2^\alpha}$ is isomorphic to $G_{\alpha-i}$. Hence, by abuse of notation, this subgroup will be denoted by $G_{\alpha-i}$ in the following.

Theorem 11.5 *There exists a KTS $(4^e 48n + 3)$ for every non-negative integer e and every positive odd integer n .*

Proof Set $\alpha = e + 2$ and note that $G_\alpha \times V_n$ is a pertinent group of order $4^e 48n$. Hence, by Proposition 6.1, it is enough to prove the existence of a $(G_\alpha \times V_n, G_1 \times V_i, 3, 1)$ -RDF with $i = 1$ or 3 for any $\alpha \geq 2$ and any odd $n \geq 1$.

We distinguish five cases.

1st case: $n = 1$.

Let us prove the existence of a $(G_\alpha, G_1, 3, 1)$ -RDF for every $\alpha \geq 2$. A $(G_2, G_1, 3, 1)$ -RDF has been given in Subsect. 6.5 and a $(G_3, G_2, 3, 1)$ -RDF can be found in Appendix D. Now let $\alpha \geq 4$ and assume, by induction, that there exists a $(G_\beta, G_{\beta-1}, 3, 1)$ -RDF for $2 \leq \beta < \alpha$. Set $G = G_\alpha$, $L = G_{\alpha-1}$, and let H be the subgroup of G with underlying set $\{0\} \times 2^{\alpha-2} \mathbb{Z}_{2^\alpha} \times 2^{\alpha-2} \mathbb{Z}_{2^\alpha}$. Note that H is isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4$ so that there exists a splittable $(H, 3, 1)$ -DM by Example 10.7. The quotient groups G/H and L/H are isomorphic to $G_{\alpha-2}$ and $G_{\alpha-3}$, respectively. Thus, by the induction hypothesis, there exists a $(G/H, L/H, 3, 1)$ -RDF. Applying Theorem 10.8(ii) we get a $(G, L, 3, 1)$ -RDF, i.e., a $(G_\alpha, G_{\alpha-1}, 3, 1)$ -RDF. Applying Proposition 3.2 with the chain $G_\alpha \geq G_{\alpha-1} \geq \dots \geq G_2 \geq G_1$ we get a $(G_\alpha, G_1, 3, 1)$ -RDF.

2nd case: $n = 3$.

A $(G_2 \times V_3, G_1 \times V_3, 3, 1)$ -RDF will be given in Appendix C. Let $\alpha \geq 3$ and let β be any integer of the closed interval $[3, \alpha]$. Consider the group $G = G_\beta \times V_3$ and its subgroups $L = G_{\beta-1} \times V_3$ and $H = K \times V_3$ where K is the Klein subgroup of G_β . We have $G/H \simeq G_{\beta-1}$ and $L/H \simeq G_{\beta-2}$ so that there exists a $(G/H, L/H, 3, 1)$ -RDF (see 1st case). Also, $H \simeq \mathbb{Z}_2 \times \mathbb{Z}_6$ so that there exists a splittable $(H, 3, 1)$ -DM by Example 10.6. Thus, by Theorem 10.8(ii), there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_\beta \times V_3, G_{\beta-1} \times V_3, 3, 1)$ -RDF.

Applying Proposition 3.2 with the chain

$$G_\alpha \times V_3 \geq G_{\alpha-1} \times V_3 \geq \dots \geq G_2 \times V_3 \geq G_1 \times V_3$$

we get a $(G_\alpha \times V_3, G_1 \times V_3, 3, 1)$ -RDF.

3rd case: $3 < n \equiv 0 \pmod{3}$.

Consider the group $G = G_\alpha \times V_n$ and its subgroups $L = G_1 \times V_n$ and $H = \{0\} \times V_n$. We have $G/H \simeq G_\alpha$ and $L/H \simeq G_1$ so that there exists a $(G/H, L/H, 3, 1)$ -RDF (see first case). There also exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. It follows that there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_\alpha \times V_n, G_1 \times V_n, 3, 1)$ -RDF by Theorem 10.8(i). From the proof of Case 1) of Theorem 11.3 we also have a $(G_1 \times V_n, G_1 \times V_i, 3, 1)$ -RDF with $i = 1$ or 3. Thus we have a $(G_\alpha \times V_n, G_1 \times V_i, 3, 1)$ -RDF by Proposition 3.2.

4th case: $1 < n \not\equiv 0 \pmod{3}$ and $\alpha = 2$.

Write $n = PQ$ where P is the product of all the components of n congruent to 3 (mod 4) and Q is the product of all the components of n congruent to 1 (mod 4). If $Q = 1$, we get the required $(G_2 \times V_n, G_2 \times V_1, 3, 1)$ -RDF from Corollary 8.6. If $Q > 1$, consider the group $G = G_2 \times V_n$ and its subgroups $L = G_2 \times V_Q$ and $H = \{0\} \times V_Q$. We have $G/H \simeq G_2 \times V_P$ and $L/H \simeq G_2$ so that there exists a $(G/H, L/H, 3, 1)$ -RDF either trivially if $P = 1$, or by Corollary 8.6 if $P > 1$. There also exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. It follows that there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_2 \times V_n, G_2 \times V_Q, 3, 1)$ -RDF by Theorem 10.8(i). We also have a $(G_2 \times V_Q, G_2 \times V_1, 3, 1)$ -RDF because of Corollary 10.10 and, from the first case, a $(G_2 \times V_1, G_1 \times V_1, 3, 1)$ -RDF. Thus, applying Proposition 3.2 with the chain $G_2 \times V_n \geq G_2 \times V_Q \geq G_2 \times V_1 \geq G_1 \times V_1$ we finally get a $(G_2 \times V_n, G_1 \times V_1, 3, 1)$ -RDF.

5th case: $n > 3$ and $\alpha > 2$.

Let $\alpha \geq 3$ and let $2 \leq \beta \leq \alpha$. Consider the group $G = G_\beta \times V_n$ and its subgroups $L = G_{\beta-1} \times V_n$ and $H = \{0\} \times V_n$. We have $G/H \simeq G_\beta$ and $L/H \simeq G_{\beta-1}$ so that there exists a $(G/H, L/H, 3, 1)$ -RDF (see 1st case). Also, there exists a homogeneous $(H, 3, 1)$ -DM by Theorem 10.2. Thus there exists a $(G, L, 3, 1)$ -RDF, i.e., a $(G_\beta \times V_n, G_{\beta-1} \times V_n, 3, 1)$ -RDF by Theorem 10.8(i). Applying Proposition 3.2 with the chain

$$G_\alpha \times V_n \geq G_{\alpha-1} \times V_n \geq \dots \geq G_2 \times V_n$$

we get a $(G_\alpha \times V_n, G_2 \times V_n, 3, 1)$ -RDF. From either the third or the fourth case we also have a $(G_2 \times V_n, G_1 \times V_i, 3, 1)$ -RDF with $i = 1$ or 3. Then, by Proposition 3.2 again, we have a $(G_\alpha \times V_n, G_1 \times V_i, 3, 1)$ -RDF with $i = 1$ or 3. □

Remark 11.6 We recall that Corollary 8.6 shows the existence of a group of strong multipliers. Therefore, it is not difficult to check that Propositions 3.2 and 6.1 guarantee that the number of symmetries of each KTS($48n + 3$) obtainable via Theorem 11.5, when n is not divisible by 3, is at least equal to $m(48n + 3)$, where m is the greatest odd divisor of $\psi(P)$ and $P > 1$ is the product of all the components of n congruent to 3 (mod 4).

12 Open problems

The problem of classifying the 3-pyramidal KTS(v) remains open in the following cases.

- $v - 3 = 24n + 6$ and $4n + 1$ is not a sum of two squares;
- $v - 3 = 72n \pm 12$ and its prime decomposition contains a prime factor $p \equiv 11 \pmod{12}$ raised to an odd power;

The open cases above could be closed if one solves the following problems, respectively.

Problem 12.1 Determine a $(D \times V_{pq}, D \times V_1, 3, 1)$ -RDF for every pair (p, q) of distinct primes congruent to 3 modulo 4.

Problem 12.2 Determine a $(G_1 \times V_p, G_1 \times V_1, 3, 1)$ -RDF for every prime $p \equiv 11$ modulo 12.

Our research naturally leads to consider also the following collateral problems which, in our opinion, are interesting on their own.

Problem 12.3 Determine the admissible groups H for which there exists a splittable $(H, 3, 1)$ difference matrix.

Problem 12.4 Determine the set of all values of n for which there exists a doubly disjoint $(\mathbb{Z}_3 \times V_{2n+1}, \mathbb{Z}_3 \times V_1, 3, 1)$ difference family.

Acknowledgements The authors gratefully acknowledge support from GNSAGA of Istituto Nazionale di Alta Matematica.

Funding Open access funding provided by University degli Studi di Perugia within the CRUI-CARE Agreement.

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

Appendix

A: Pseudo-resolvable $(G_1 \times V_9, \{2^3, 3\}, 3, 1)$ -DF

Let Σ be the $\{2^3, 3\}$ -partial spread of $G_1 \times V_9$ whose member of order 3 is $\{0, x, -x\}$ with $x = (1, 0, 0, 0, 0)$. The following seventeen 3-subsets of $G_1 \times V_9$

$$\begin{aligned} & \{(0, 0, 0, 0, 1), (0, 1, 1, 2, 0), (1, 0, 1, 1, 1)\}, \quad \{(0, 0, 0, 0, 2), (2, 0, 0, 2, 0), (2, 1, 0, 0, 0)\}, \\ & \{(0, 0, 0, 1, 0), (0, 1, 0, 2, 0), (1, 0, 0, 1, 2)\}, \quad \{(0, 0, 0, 1, 1), (2, 0, 0, 2, 1), (2, 0, 1, 2, 0)\}, \\ & \{(0, 0, 0, 1, 2), (0, 1, 0, 1, 0), (2, 0, 1, 1, 0)\}, \quad \{(0, 0, 0, 2, 1), (0, 1, 0, 0, 2), (1, 0, 1, 1, 2)\}, \\ & \{(0, 0, 0, 2, 2), (0, 0, 1, 0, 1), (2, 0, 0, 1, 2)\}, \quad \{(0, 0, 1, 1, 2), (1, 1, 1, 2, 0), (2, 1, 0, 2, 2)\}, \\ & \{(0, 0, 1, 2, 2), (1, 0, 1, 1, 0), (2, 0, 0, 2, 2)\}, \quad \{(0, 1, 0, 1, 1), (2, 0, 1, 0, 1), (2, 1, 1, 0, 0)\}, \\ & \{(0, 1, 0, 2, 1), (1, 1, 1, 2, 2), (2, 0, 0, 0, 1)\}, \quad \{(1, 0, 1, 0, 0), (1, 1, 1, 1, 0), (2, 1, 0, 1, 1)\}, \\ & \{(1, 0, 1, 0, 1), (1, 0, 1, 2, 1), (1, 0, 1, 2, 2)\}, \quad \{(1, 1, 0, 0, 2), (2, 0, 0, 1, 1), (2, 0, 1, 0, 2)\}, \\ & \{(1, 1, 0, 2, 0), (1, 1, 1, 1, 1), (2, 0, 1, 1, 2)\}, \quad \{(1, 1, 1, 0, 1), (2, 0, 1, 2, 1), (2, 1, 1, 0, 2)\}, \\ & \{(1, 1, 1, 0, 2), (1, 1, 1, 2, 1), (2, 1, 1, 1, 0)\} \end{aligned}$$

are the blocks of a $(G_1 \times V_9, \Sigma, 3, 1)$ -PRDF.

B: Pseudo-resolvable $(G_2, \{2^3, 3\}, 3, 1)$ -DF

Let Σ be the $\{2^3, 3\}$ -partial spread of G_2 whose member of order 3 is $\{0, x, -x\}$ with $x = (1, 0, 0)$. The following seven 3-subsets of G_2

$$\begin{aligned} &\{(0, 0, 1), (0, 3, 1), (2, 1, 2)\}, \quad \{(0, 1, 0), (1, 0, 3), (2, 3, 2)\}, \\ &\{(0, 1, 1), (1, 3, 3), (2, 0, 2)\}, \quad \{(0, 1, 2), (1, 0, 2), (2, 1, 3)\}, \\ &\{(0, 2, 1), (2, 0, 0), (2, 0, 1)\}, \quad \{(1, 1, 0), (1, 2, 3), (1, 3, 1)\}, \\ &\{(1, 1, 2), (2, 0, 3), (2, 3, 3)\}, \end{aligned}$$

are the blocks of a pseudo-resolvable $(G_2, \Sigma, 3, 1)$ -DF.

C: $(G_2 \times V_3, G_1 \times V_3, 3, 1)$ -RDF

The following eighteen 3-subsets of $G_2 \times V_3$

$$\begin{aligned} &\{(0, 0, 1, 0), (1, 3, 1, 2), (2, 1, 0, 1)\}, \quad \{(0, 0, 1, 1), (0, 1, 0, 2), (1, 3, 3, 2)\}, \\ &\{(0, 0, 1, 2), (0, 3, 3, 1), (1, 1, 2, 0)\}, \quad \{(0, 0, 3, 0), (2, 3, 1, 2), (2, 3, 2, 0)\}, \\ &\{(0, 0, 3, 1), (0, 1, 3, 0), (1, 1, 0, 0)\}, \quad \{(0, 1, 0, 0), (1, 3, 1, 1), (2, 0, 1, 0)\}, \\ &\{(0, 1, 0, 1), (1, 0, 3, 1), (2, 3, 1, 1)\}, \quad \{(0, 1, 1, 0), (2, 2, 1, 2), (2, 3, 0, 1)\}, \\ &\{(0, 1, 2, 0), (0, 2, 1, 2), (1, 3, 3, 0)\}, \quad \{(0, 1, 2, 2), (0, 3, 1, 1), (2, 0, 1, 1)\}, \\ &\{(0, 1, 3, 2), (1, 0, 1, 2), (2, 3, 0, 0)\}, \quad \{(0, 3, 0, 1), (1, 0, 3, 2), (2, 1, 3, 0)\}, \\ &\{(0, 3, 3, 2), (1, 0, 3, 0), (2, 3, 0, 2)\}, \quad \{(1, 0, 1, 0), (1, 1, 2, 2), (1, 1, 3, 0)\}, \\ &\{(1, 0, 1, 1), (1, 1, 1, 1), (1, 1, 2, 1)\}, \quad \{(1, 1, 0, 1), (2, 0, 3, 0), (2, 1, 1, 0)\}, \\ &\{(1, 1, 0, 2), (2, 1, 1, 2), (2, 2, 1, 1)\}, \quad \{(2, 1, 0, 2), (2, 1, 1, 1), (2, 2, 3, 2)\} \end{aligned}$$

are the blocks of a $(G_2 \times V_3, G_1 \times V_3, 3, 1)$ -RDF.

D: $(G_3, G_2, 3, 1)$ -RDF

The following twentyfour 3-subsets of G_3

$$\begin{aligned} &\{(0, 0, 1), (0, 5, 2), (0, 7, 5)\}, \quad \{(0, 0, 3), (2, 1, 1), (2, 5, 2)\}, \\ &\{(0, 0, 5), (2, 1, 7), (2, 3, 6)\}, \quad \{(0, 0, 7), (0, 1, 1), (2, 7, 0)\}, \\ &\{(0, 1, 0), (0, 7, 3), (2, 6, 1)\}, \quad \{(0, 1, 4), (1, 4, 7), (2, 7, 5)\}, \\ &\{(0, 1, 5), (0, 5, 6), (2, 6, 7)\}, \quad \{(0, 1, 7), (1, 3, 2), (2, 4, 5)\}, \\ &\{(0, 2, 1), (2, 3, 5), (2, 5, 0)\}, \quad \{(0, 2, 5), (1, 1, 4), (1, 1, 5)\}, \\ &\{(0, 3, 0), (1, 1, 1), (1, 6, 1)\}, \quad \{(0, 3, 3), (2, 0, 3), (2, 1, 0)\}, \\ &\{(0, 3, 5), (1, 3, 6), (2, 2, 1)\}, \quad \{(0, 3, 6), (1, 2, 3), (1, 3, 5)\}, \\ &\{(0, 5, 7), (0, 7, 0), (1, 4, 5)\}, \quad \{(0, 6, 3), (1, 1, 2), (2, 3, 7)\}, \\ &\{(0, 6, 7), (1, 3, 3), (1, 5, 2)\}, \quad \{(0, 7, 6), (2, 6, 3), (2, 7, 7)\}, \\ &\{(1, 1, 0), (1, 4, 3), (2, 1, 5)\}, \quad \{(1, 1, 3), (1, 4, 1), (2, 7, 4)\}, \\ &\{(1, 1, 7), (2, 1, 2), (2, 4, 3)\}, \quad \{(1, 3, 7), (2, 4, 1), (2, 7, 6)\}, \end{aligned}$$

$$\{(1, 6, 3), (1, 7, 4), (2, 5, 7)\}, \quad \{(1, 6, 5), (1, 7, 0), (1, 7, 5)\}$$


are the blocks of a $(G_3, G_2, 3, 1)$ -RDF.

References

1. Anderson I.J., Finizio N.J., Leonard P.A.: New product theorems for Z -cyclic whist tournaments. *J. Comb. Theory Ser. A* **88**, 162–166 (1999).
2. Beth T., Jungnickel D., Lenz H.: *Design Theory*. Cambridge University Press, Cambridge (1999).
3. Bonvicini S., Buratti M., Rinaldi G., Traetta T.: Some progress on the existence of 1-rotational Steiner triple systems. *Des. Codes Cryptogr.* **62**, 63–78 (2012).
4. Buratti M.: Recursive constructions for difference matrices and relative difference families. *J. Comb. Des.* **6**, 165–182 (1998).
5. Buratti M.: Old and new designs via difference multisets and strong difference families. *J. Comb. Des.* **7**, 406–425 (1999).
6. Buratti M.: 1-rotational Steiner Triple Systems over arbitrary groups. *J. Comb. Des.* **9**, 215–226 (2001).
7. Buratti M.: On disjoint $(v, k, k - 1)$ difference families. *Des. Codes Cryptogr.* **87**, 745–755 (2019).
8. Buratti M., Ghinelli D.: On disjoint $(3t, 3, 1)$ cyclic difference families. *J. Stat. Plan. Inference* **140**, 1918–1922 (2010).
9. Buratti M., Gionfriddo L.: Strong difference families over arbitrary groups. *J. Comb. Des.* **16**, 443–461 (2008).
10. Buratti M., Pasotti A.: Combinatorial designs and the theorem of Weil on multiplicative character sums. *Finite Fields Appl.* **15**, 332–344 (2009).
11. Buratti, M., Nakic, A.: Transrotational Kirkman triple systems, in preparation.
12. Buratti M., Rinaldi G., Traetta T.: 3–pyramidal Steiner triple systems. *Ars Math. Contemp.* **13**, 95–106 (2017).
13. Buratti M., Zuanni F.: G -invariantly resolvable Steiner 2–designs which are 1-rotational over G . *Bull. Belg. Math. Soc.* **5**, 221–235 (1998).
14. Buratti M., Zuanni F.: Explicit constructions for 1-rotational Kirkman triple systems. *Utilitas Math.* **59**, 27–30 (2001).
15. Chang Y., Costa S., Feng T., Wang X.: Strong difference families of special types. *Discret. Math.* **343**, 111776 (2020).
16. Colbourn M.J., Colbourn C.J.: Recursive constructions for cyclic block designs. *J. Stat. Plan. Infer.* **10**, 97–103 (1984).
17. Colbourn C.J., Dinitz J.H.: *Handbook of Combinatorial Designs*, 2nd edn Chapman & Hall/CRC, Boca Raton, FL (2006).
18. Colbourn C.J., Rosa A.: *Triple Systems*. Clarendon Press, Oxford (1999).
19. Costa S., Feng T., Wang X.: New 2-designs from strong difference families. *Finite Fields Appl.* **50**, 391–405 (2018).
20. Costa S., Feng T., Wang X.: Frame difference families and resolvable balanced incomplete block designs. *Des. Codes Cryptogr.* **86**, 2725–2745 (2018).
21. Custic A., Krcadinac V., Zhou Y.: Tiling groups with difference sets. *Electron. J. Comb.* **22**, 2–56 (2015).
22. Dinitz J.H., Rodney P.: Block disjoint difference families for Steiner triple systems. *Utilitas Math.* **52**, 153–160 (1997).
23. Dinitz J.H., Shalaby N.: Block disjoint difference families for Steiner triple systems: $v \equiv 3 \pmod{6}$. *J. Stat. Plan. Inference* **106**, 77–86 (2002).
24. Dinitz J.H., Williams H.C.: Number Theory and Finite Fields. In: Colbourn C.J., Dinitz J.H. (eds.) *Handbook of Combinatorial Designs*, 2nd edn, pp. 791–818. Chapman & Hall/CRC, Boca Raton (2006).
25. Doyen J.: A note on reverse Steiner triple systems. *Discret. Math.* **1**, 315–319 (1972).
26. Evans A.B.: The admissibility of sporadic simple groups. *J. Algebra* **321**, 105–116 (2009).
27. Falcone G., Pavone M.: Kirkman’s tetrahedron and the fifteen schoolgirl problem. *Am. Math. Mon.* **118**, 887–900 (2011).
28. Feng, T., Horsley, D., Wang, X.: Novák’s conjecture on cyclic Steiner triple systems and its generalization. Preprint, [arXiv:2001.06995](https://arxiv.org/abs/2001.06995)
29. Gardner R.B.: Steiner triple systems with transrotational automorphisms. *Discret. Math.* **131**, 99–104 (1994).
30. Ge G.: On $(g, 4; 1)$ difference matrices. *Discret. Math.* **301**, 164–174 (2005).

31. Genma M., Mishima M., Jimbo M.: Cyclic resolvability of cyclic Steiner 2–designs. *J. Comb. Des.* **5**, 177–187 (1997).
32. Hall M., Paige L.J.: Complete mappings of finite groups *Pacific. J. Math.* **5**, 541–549 (1955).
33. Hanani H., Ray Chaudhuri D.K., Wilson R.M.: On resolvable designs. *Discret. Math.* **3**, 343–357 (1972).
34. Hawkins T.: The Erlanger program of Felix Klein: Reflections on its place in the history of mathematics. *Hist. Math.* **11**, 442–470 (1984).
35. Isaacs I.M.: *Finite Group Theory*. Graduate Studies in Mathematics, vol. 92. American Mathematical Society, Providence, RI (2008).
36. Janko Z.: A classification of finite 2–groups with exactly three involutions. *J. Algebra* **291**, 505–533 (2005).
37. Jungnickel D.: Composition theorems for difference families and regular planes. *Discret. Math.* **23**, 151–158 (1978).
38. Kageyama S., Miao Y.: A construction for resolvable designs and its generalizations. *Graphs Comb.* **14**, 11–24 (1998).
39. Keevash, P.: The existence of designs. Preprint, [arXiv:1401.3665](https://arxiv.org/abs/1401.3665)
40. Kirkman T.P.: On a problem in combinations. *Camb. Dublin Math. J.* **2**, 191–204 (1847).
41. Konvisser M.W.: 2–Groups which contain exactly three involutions. *Math. Z.* **130**, 19–30 (1973).
42. Lovegrove G.: The automorphism groups of Steiner triple systems obtained by the Bose construction. *J. Algebra Comb.* **18**, 159–170 (2003).
43. Lu J.X.: *Collected Works on Combinatorial Designs*. Inner Mongolia People’s Press, Hunhot, Mongolia (1990).
44. Mendelsohn E.: On the groups of automorphisms of Steiner triple and quadruple systems. *J. Comb. Theory Ser. A* **25**, 97–104 (1978).
45. Mendelsohn E., Rosa A.: One-factorizations of the complete graph: a survey. *J. Graph Theory* **9**, 43–65 (1985).
46. Meszka M., Rosa A.: Cyclic Kirkman triple systems. *Congr. Numer.* **188**, 129–136 (2007).
47. Mishima M.: The spectrum of 1-rotational Steiner triple systems over a dicyclic group. *Discret. Math.* **308**, 2617–2619 (2008).
48. Momihara K.: Strong difference families, difference covers, and their applications for relative difference families. *Des. Codes Cryptogr.* **51**, 253–273 (2008).
49. Novák, J.: A note on disjoint cyclic Steiner triple systems. In: *Recent Advances in Graph Theory (Proc. Symp. Prague 1974)*. Academia, Praha, pp. 439–440 (1975)
50. Pan R., Chang Y.: A note on difference matrices over non-cyclic finite abelian groups. *Discret. Math.* **339**, 822–830 (2016).
51. Peltesohn R.: Eine Lösung der beiden Heffterschen Differenzenprobleme. *Compos. Math.* **6**, 251–257 (1938).
52. Phelps K.T., Rosa A.: Steiner triple systems with rotational automorphisms. *Discret. Math.* **33**, 57–66 (1981).
53. Ray-Chaudhuri, D.K., Wilson, R.M.: Solution of Kirkman’s Schoolgirl Problem *Combinatorics*. Proc. Sympos. Pure Math., Univ. California Los Angeles 1968 **19** (1971), 187–203.
54. Rosa A.: On reverse Steiner triple systems. *Discret. Math.* **2**, 61–71 (1972).
55. Rosen K.H.: *Elementary Number Theory and its Applications*, 6th edn Pearson, New York (2000).
56. Stinson D.R.: Frames for Kirkman triple systems. *Discret. Math.* **65**, 289–300 (1987).
57. Teirlinck L.: The existence of reverse Steiner triple systems. *Discret. Math.* **6**, 220–245 (1973).
58. Wilson R.M.: An existence theory for pairwise balanced designs, I: Composition theorems and morphisms. *J. Comb. Theory Ser. A* **13**, 246–273 (1972).
59. Wilson R.M.: An existence theory for pairwise balanced designs, II: The structure of PBD-closed sets and the existence conjectures. *J. Comb. Theory Ser. A* **13**, 71–79 (1972).
60. Wilson R.M.: An existence theory for pairwise balanced designs, III: Proof of the existence conjectures. *J. Comb. Theory Ser. A* **18**, 71–79 (1975).
61. Ying J., Yang X., Li Y.: Some 20-regular CDP(5, 1; 20*u*) and their applications. *Finite Fields Appl.* **17**, 317–328 (2011).

Authors and Affiliations

Simona Bonvicini¹ · Marco Buratti²  · Martino Garonzi³ · Gloria Rinaldi⁴ · Tommaso Traetta⁵

✉ Marco Buratti
buratti@dmi.unipg.it

Simona Bonvicini
simona.bonvicini@unimore.it

Martino Garonzi
mgaronzi@gmail.com

Gloria Rinaldi
gloria.rinaldi@unimore.it

Tommaso Traetta
tommaso.traetta@unibs.it

- ¹ Dipartimento di Scienze Fisiche Informatiche Matematiche, Università di Modena e Reggio Emilia, via Campi 213/B, 41100 Modena, Italy
- ² Dipartimento di Matematica e Informatica, Università di Perugia, via Vanvitelli, 06123 Perugia, Italy
- ³ Departamento de Matemática, Universidade de Brasília, Campus Universitário Darcy Ribeiro, Brasília, DF, Brazil
- ⁴ Dipartimento di Scienze e Metodi dell'Ingegneria, Università di Modena e Reggio Emilia, viale Amendola 2, 42122 Reggio Emilia, Italy
- ⁵ DICATAM-Sezione Matematica, Università degli Studi di Brescia, via Branze 38, 25123 Brescia, Italy