Some progress on the existence of 1-rotational Steiner Triple Systems

Simona Bonvicini [*] Marco Buratti [†]

Gloria Rinaldi [‡] Tommaso Traetta [§]

Abstract

A Steiner Triple System of order v (briefly $STS(v)$) is 1-rotational under G if it admits G as an automorphism group acting sharply transitively on all but one point. The spectrum of values of v for which there exists a 1-rotational $STS(v)$ under a cyclic, an abelian, or a dicyclic group, has been established in [16], [8] and [15], respectively. Nevertheless, the spectrum of values of v for which there exists a 1-rotational $STS(v)$ under an arbitrary group has not been completely determined yet. This paper is a considerable step forward to the solution of this problem. In fact, we leave as uncertain cases only those for which we have $v = (p^3 - p)n + 1 \equiv 1 \pmod{96}$ with p a prime, $n \not\equiv 0 \pmod 4$, and the odd part of $(p^3 - p)n$ that is square-free and without prime factors congruent to $1 \pmod 6$.

Keywords: 1-rotational Steiner triple system; binary group; special linear group; octahedral binary group; even starter; extended Skolem sequence.

[*]Dipartimento di Scienze e Metodi dell'Ingegneria, Università di Modena e Reggio Emilia, via Amendola, Italy. email: simona.bonvicini@unimore.it

[†]Dipartimento di Matematica e Informatica, Università di Perugia, via Vanvitelli 1 email: buratti@mat.uniroma1.it

[‡]Dipartimento di Scienze e Metodi dell'Ingegneria, Università di Modena e Reggio Emilia, via Amendola, Italy. email: rinaldi.gloria@unimore.it

[§]Dipartimento di Matematica, Università Sapienza di Roma, Piazzale Aldo Moro 5, email: traetta@mat.uniroma1.it

1 Introduction

A *Steiner* 2-*design* of order v and block-size k, briefly $S(2,k,v)$, is a pair $\mathcal{D} = (V, \mathcal{B})$ where V is a set of v *points* and $\mathcal{B}$ is a set of k-subsets of V (*blocks*) such that every 2-subset of V is contained in exactly one block. An automorphism group of such a design is a group G of bijections on V preserving $\mathcal{B}$. The design is 1-*rotational* under G if G fixes one point ∞ and acts regularly (i.e., sharply transitively) on the others. In this case it is natural to identify the point-set V with $G \cup \{\infty\}$ and the action of G on V with the multiplication (or addition) on the right with the rule that $\infty \cdot g = \infty$ (or $\infty + g = \infty$) for every $g \in G$.

An $S(2,3,v)$ is usually called a *Steiner triple system* of order v, briefly STS(v), and it is very well known that an $STS(v)$ exists if and only if $v \equiv 1$ or 3 (mod 6) (see [6, 10]). In this paper we carry on the investigation, begun in [8], regarding the existence of a 1-rotational STS of an assigned order v. The spectrum $\mathcal{C}_{1r}$ of values v for which there exists a 1-rotational $STS(v)$ under the cyclic group, namely under $\mathbb{Z}_{v-1}$, was determined by Phelps and Rosa [16]:

$$\mathcal{C}_{1r} = \{v \mid v \equiv 3 \text{ or } 9 \pmod{24}\}.$$

The spectrum $\mathcal{A}_{1r}$ of values of v for which there exists a 1-rotational $STS(v)$ under a suitable abelian group was determined by the second author [8]:

$$\mathcal{A}_{1r} = \mathcal{C}_{1r} \cup \{v \mid v \equiv 1 \text{ or } 19 \pmod{72}\}. \qquad (1)$$

Finally, the spectrum $\mathcal{Q}_{1r}$ of values of v for which there exists a 1-rotational $STS(v)$ under the *dicyclic* group[1] was determined by Mishima [15]:

$$\mathcal{Q}_{1r} = \{v \mid v \equiv 9 \pmod{24}\}.$$

Nevertheless, the spectrum $\mathcal{G}_{1r}$ of all values of v for which there exists a 1-rotational $STS(v)$ under an arbitrary group G has not been completely determined yet. As observed in [8] every 1-rotational STS is, in particular, a *reverse* STS, i.e., it admits an involutory automorphism. So $\mathcal{G}_{1r}$ is obviously contained in the set (determined by Rosa, Doyen and Teirlinck [17, 13, 19]) of values of v for which there exists a reverse STS(v):

$$\mathcal{G}_{1r} \subset \{v \mid v \equiv 1 \text{ or } 3 \text{ or } 9 \text{ or } 19 \pmod{24}\}.$$

Thus, in view of (1), the problem of determining $\mathcal{G}_{1r}$ reduces to that of establishing for which $v \equiv 25$ or 43 or 49 or 67 (mod 72) there exists a

[1] The dicyclic group of order $4n$ has *presentation* $< x, y \mid x^{2n} = 1, y^2 = x^n, xy = yx^{-1} >$

1-rotational STS(v) under a suitable group of order $u = v - 1$. Some partial answers have been already got in [8]. For instance it was proved that the existence is ensured in the case that u has at least one prime factor $p \equiv 1 \pmod 6$.
As a consequence of more general results concerning Steiner 2-designs, we briefly recall how 1-rotational STSs can be constructed. The *list of differences* of a given subset B of an additive (or multiplicative) group G is the multiset ΔB consisting of all possible differences $x - y$ (or quotients xy^{-1}) between two distinct elements x and y of B. A *partial spread* (PS) of a group G is a set Σ of subgroups of G intersecting each other trivially. A (G, Σ, k, λ) *difference family* (DF) is a set $\mathcal{F} = \{B_1, ..., B_t\}$ of k-subsets of G whose list of differences $\Delta\mathcal{F} = \Delta B_1 \cup ... \cup \Delta B_t$ is disjoint with every group of the partial spread Σ and covers exactly λ times all elements of G not lying in some group of Σ. In other words, every $g \in G - \bigcup_{S\in\Sigma} S$ is representable in exactly λ ways in the form $g = x - y$ (or $g = xy^{-1}$) with (x, y) an ordered pair of distinct elements of some $B \in \mathcal{F}$, while no element of $\bigcup_{S\in\Sigma} S$ admits such a representation. Note that a (G, Σ, k, λ)-DF in which Σ contains only the trivial subgroup of G is an *ordinary* difference family; one usually says that it is a (v, k, λ)-DF in G where v denotes the order of G (see [1] or [6]).
A k-PS of a group G is a partial spread of G all members of which have order k; a k^*-PS of G is a partial spread of G with exactly one member of order $k - 1$ and all the others of order k. If k is a prime, every S$(2, k, v)$ admitting an automorphism group G acting sharply transitively on the points is completely equivalent to a $(G, \Sigma, k, 1)$-DF where Σ is a k-PS (see [7]). Similarly, for k a prime, every S$(2, k, v)$ design that is 1-rotational under G is completely equivalent to a $(G, \Sigma, k, 1)$-DF with Σ a k^*-PS of G (see [9]). Thus, in particular, we can state:

Theorem 1.1. *Every 1-rotational STS(v) under G is completely equivalent to a $(G, \Sigma, 3, 1)$-DF with Σ a 3^*-PS in G.*

Let $\mathcal{F}$ be a difference family as in the above theorem and let $\mathcal{D}$ be the STS generated by it. A complete system of representatives for the G-orbits of the blocks of $\mathcal{D}$ is given by

$$\{S_0 \cup \infty\} \ \cup \ (\Sigma - \{S_0\}) \ \cup \ \mathcal{F}$$

where S_0 is the component of Σ of order 2.
Observe that if $\mathcal{F}$ is a $(G, \Sigma, 3, 1)$-DF with Σ a 3^*-PS, then G has exactly one involution, namely the involution of the unique component of Σ of order 2. In the opposite case we would have another involution h representable as a difference $x - y$ (or xy^{-1}) of a block of $\mathcal{F}$. It would follow that $h = y - x$

(or $h = yx^{-1}$) is another representation of h as a difference from $\mathcal{F}$, that is absurd.
A group G with exactly one involution g^* is usually said *binary* and its unique subgroup of order 2, that is $\{0, g^*\}$, will be denoted by $\Lambda(G)$. In view of the above paragraph an STS may be 1-rotational under G only if G is binary. Throughout the paper, in most cases the group G will be denoted additively. Sometimes, however, we will also adopt the multiplicative notation according to the situations.
Now observe that if $\mathcal{F}$ is a $(G, \Sigma, 3, 1)$-DF with Σ a 3^*-PS, then we have $6|\mathcal{F}| = |G| - 2|\Sigma|$ since every triple of $\mathcal{F}$ produces exactly 6 differences and the union of all subgroups in Σ has size $2|\Sigma|$. Thus, if G has order divisible by 3 the size of Σ is also divisible by 3, i.e., the number of its components of order 3 is congruent to 2 (mod 3) and hence G, besides being binary, must have at least two subgroups of order 3.
For this reason, throughout the paper, any binary group with more than one subgroup of order 3 will be said *admissible*. Hence we can state

Proposition 1.2. *A necessary condition for the existence of a* 1*-rotational STS*(v) *with* $v \equiv 1$ *or* 19 (*mod* 24) *is that* $v-1$ *is the order of an admissible group.*

In the next section we will determine the set of all *admissible orders* $v-1$. The third section will deal with *even starters* in a binary group, a concept allowing us, in the fourth section, to establish the existence of a 1-rotational STS(v) for every $v \equiv 1$ or 19 (mod 24) such that the odd part of $v-1$ is not square-free. In the fifth section we will give an explicit construction for a 1-rotational STS(v) for any $v \equiv 25$ (mod 48) and any $v \equiv 49$ (mod 96). Putting together all these results with those obtained in [8], we conclude that the existence question for a 1-rotational STS(v) remains open only in the very special cases that the following conditions simultaneously hold:

- $v = (p^3 - p)n + 1$ with $n \not\equiv 0 \pmod 4$ and p a prime;
- $(p^3 - p)n = 2^\ell 3 p_1 p_2 ... p_t$ with $\ell \geq 5$ and the p_i's pairwise distinct primes congruent to 5 modulo 6.

Note that the second of the above conditions can be equivalently formulated by saying that $v-1$ is divisible by 96 and that its odd part is square-free and without prime factors congruent to 1 (mod 6).

2 On the existence of admissible groups of order $24n + 18$ or $24n$

In this section we are able to establish the set of values of $u \equiv 0$ or 18 (mod 24) for which at least one admissible group of order u exists obtaining in this way some non-existence results for 1-rotational STS($24n + 1$).
First recall the following known result (see Example 3 at page 106 in [18]).

Theorem 2.1. *The number of Sylow p-subgroups of a finite group G can be expressed as a product of integers each of which is either a prime power $\equiv 1$ (mod p) or the number of Sylow p-subgroups of a composition factor of G.*

As a consequence of the above lemma we get the following.

Lemma 2.2. *Let G be a group of order $3t$ with t a square-free integer whose prime factors are all congruent to 2 (mod 3). Then G has exactly one Sylow 3-subgroup.*

Proof. By Sylow's theorem, the number n_3 of Sylow 3-subgroups of G is a divisor of t and by assumption on the prime factors of t it is obvious that there is no prime power divisor of t that is congruent to 1 (mod 6). Hence n_3 can be expressed as a product of integers each of which is the number of Sylow 3-subgroups of a composition factor of G by Theorem 2.1. On the other hand G is solvable since its order is not divisible by 4. Hence every composition factor of G has prime order so that the number of its Sylow 3-subgroups is 0 or 1. We conclude that $n_3 = 1$. □

From now on, V_q will denote the elementary abelian group of order q, namely the additive group of the field $\mathbb{F}_q$ with q elements.
The set of all $u \equiv 18$ (mod 24) which are orders of an admissible group was essentially established in [8] (see Theorem 3.2)

Theorem 2.3. *There exists an admissible group of order $u = 24n + 18$ if and only if the following condition DOES NOT hold:*

($*$) $4n+3$ *is square-free and all its prime factors are congruent to* 2 (mod 3).

Proof. If ($*$) holds, the assertion follows from Lemma 2.2.
If ($*$) does not hold we can write $4n + 3 = 3t$ or $4n + 3 = qt$ for a suitable prime power $q \equiv 1$ (mod 6). In the former case an admissible group of order u is given by $\mathbb{Z}_{2t} \times V_9$ while, in the latter, it is given by $\mathbb{Z}_{2t} \times (\mathbb{Z}_3 +_\epsilon V_q)$ where ϵ is a cubic primitive root of unity of $\mathbb{F}_q$ and where $+_\epsilon$ is the semidirect product of $\mathbb{Z}_3$ by V_q defined by the rule $(a, b) +_\epsilon (a', b') = (a+a', \epsilon^{a'} b+b')$. □

For convenience of the reader we recall the basic definitions about some classical groups. The *general linear group of degree n over $\mathbb{F}_q$* is the group $GL_n(q)$ of all $n \times n$ invertible matrices with elements in $\mathbb{F}_q$. The center of this group is the set of all *scalar* matrices, namely those of the form kI_n with $k \in \mathbb{F}_q - \{0\}$ and where I_n is the $n \times n$ identity matrix.
The *special linear group* $SL_n(q)$ is the subgroup of $GL_n(q)$ consisting of all matrices with determinant 1. Its center has order $\gcd(n, q-1)$ and consists of all scalar matrices kI_n with k a n-th root of unity in $\mathbb{F}_q$. We note, in particular, that $SL_2(q)$ is an admissible group for every odd prime power q.
The *projective linear group* $PGL_n(q)$ and the *projective special linear group* $PSL_n(q)$ are the quotients of $GL_n(q)$ and $SL_n(q)$ by their centers, respectively.
Finally, the *general semilinear group* $\Gamma L_n(q)$ and the *projective semilinear group* $P\Gamma L_n(q)$ are the semidirect products of $Aut(\mathbb{F}_q)$ by $GL_n(q)$ and by $PGL_n(q)$, respectively, where $Aut(\mathbb{F}_q)$ is the group of field automorphisms of $\mathbb{F}_q$. When q is a prime it is clear that we have $\Gamma L_n(q) = GL_n(q)$ and $P\Gamma L_n(q) = PGL_n(q)$.

A binary 2–group is well known to be either cyclic or dicyclic (in the second case it is also called a *generalized quaternion group*). Now note that if S is a cyclic or dicyclic group, then the quotient $S/\Lambda(G)$ is cyclic or dihedral, respectively. Hence, if S is a Sylow 2–subgroup of a binary group G, then $S/\Lambda(G)$ is to be either cyclic or dihedral. So the structure of binary groups is intimately related to the one of groups with cyclic or dihedral Sylow 2–subgroups, and it admits the following description which exploits the Burnside's Transfer Theorem and the Gorenstein–Walter Theorem [14].

Theorem 2.4. *Let G be a binary group and let $O(G)$ be the largest normal subgroup of G of odd order. Then $G/(\Lambda(G) \cdot O(G))$ is either a 2–group or isomorphic to one of the following groups:*

(i) *a subgroup of $P\Gamma L_2(q)$ containing $PSL_2(q)$ for a suitable odd prime power q;*

(ii) *the alternating group $\mathbb{A}_7$.*

We also need the following theorem.

Theorem 2.5. *For an abstract group G, there exists a unique binary group $\overline{G}$ such that $\overline{G}/\Lambda(\overline{G})$ is isomorphic to G if and only if the Sylow 2-subgroups of G are cyclic or dihedral.*

As already observed in [5], the result of Theorem 2.5 is known to some group theorists, but we are not aware of an original proof in the literature. We refer to [5] for a proof suggested by Glaubermann.

Here is the main result of this section.

Theorem 2.6. *There exists an admissible group of a given order* $u \equiv 0 \pmod{24}$ *if and only if at least one of the following* good *conditions hold:*

(γ_0) *u is divisible by* 9*;*

(γ_1) *u is divisible by a prime power (possibly a prime)* $q \equiv 1 \pmod 6$*;*

(γ_2) $u = (p^3 - p)n$ *with p an odd prime and* $n \not\equiv 0 \pmod 4$.

Proof. ($\Longrightarrow$) Let G be a binary group of order $u \equiv 0 \pmod{24}$ and assume that none of the conditions (γ_0), (γ_1), (γ_2) hold. First observe that the order of G is not divisible by 7 otherwise condition (γ_1) would be met. Hence no quotient of G can be isomorphic to $\mathbb{A}_7$.
Now assume that $G/(\Lambda(G) \cdot O(G))$ is isomorphic to a subgroup S of $P\Gamma L_2(q)$ containing $PSL_2(q)$ for a suitable odd prime power q, say $q = p^\alpha$ with p a prime and α a positive integer. In this case q is a divisor of $|G|$ since the order of $PSL_2(q)$ is divisible by q. It follows that $\alpha = 1$ otherwise p^2 would be a prime power divisor of u which contradicts the assumption that neither (γ_0) nor (γ_1) holds considering that we have $p^2 = 9$ or $p^2 \equiv 1 \pmod 6$ according to whether $p = 3$ or not. Hence $q = p$, namely $P\Gamma L_2(q) = PGL_2(p)$. Now consider that we have $|PGL_2(p)| = p^3 - p$ and $|PSL_2(p)| = \frac{p^3-p}{2}$ so that S is either $PGL_2(p)$ or $PSL_2(p)$. We have $|G| = 2(p^3 - p)|O(G)|$ in the former case and $|G| = (p^3 - p)|O(G)|$ in the latter contradicting the fact that condition (γ_2) does not hold.
Then $G/(\Lambda(G) \cdot O(G))$ is a 2-group by Theorem 2.4 and hence the order of $O(G)$ coincides with the largest odd divisor of the order of G. This implies that every subgroup of G of odd order is necessarily contained in $O(G)$. We have $|O(G)| = 3t$ with t a square-free integer whose prime factors are all congruent to 2 (mod 3) since we are supposing that neither (γ_0) nor (γ_1) holds. Thus, by Lemma 2.2, $O(G)$ has exactly one subgroup of order 3 that, consequently, is also the the unique subgroup of G of order 3. In conclusion, G is not admissible.
($\Longleftarrow$) Assume that $u \equiv 0 \pmod{24}$ and that at least one of the three good conditions (γ_0), (γ_1), (γ_2) hold. We have to show that there exists an admissible group of order u.
If (γ_0) holds we have $u = 72t$ for a suitable t and $\mathbb{Z}_{8t} \times V_9$ is an admissible

group of order u.
If (γ_1) holds we have $u = 24tq$ for a suitable t and a suitable prime power $q \equiv 1 \pmod 6$. In this case an admissible group of order u is given by $\mathbb{Z}_{8t} \times (\mathbb{Z}_3 +_\epsilon V_q)$ where ϵ is a cubic primitive root of unity of $\mathbb{F}_q$ and where $+_\epsilon$ is the semidirect product of $\mathbb{Z}_3$ by V_q defined by the rule $(a,b) +_\epsilon (a',b') = (a+a', \epsilon^{a'}b + b')$.
If (γ_2) holds we can write $u = (p^3-p)m$ or $u = 2(p^3-p)m$ for a suitable odd prime p and a suitable odd integer m. In the first case an admissible group of order u is given by $SL_2(p) \times \mathbb{Z}_m$. In the second case, considering that the Sylow 2-subgroups of $PGL_2(p)$ are dihedral (see, e.g., [11]), there exists a (unique) binary group G such that $G/\Lambda(G) \simeq PGL_2(p)$ by Theorem 2.5. This group G obviously possesses more than one subgroup of order 3 since this is also true for its quotient $PGL_2(p)$. Hence it is clear that $G \times \mathbb{Z}_m$ is an admissible group of order $2(p^3-p)m$. □

As a consequence of the above theorem we deduce the non-existence of a 1-rotational STS(v) for infinitely many values of $v \equiv 1 \pmod{24}$. For instance, it is an easy matter to see that the following result holds.

Corollary 2.7. *If $v = 2^\ell 3 p_1 p_2 ... p_t + 1$ with $\ell \geq 5$ and the p_i's are pairwise distinct primes congruent to 5 (mod 6) with $p_i \not\equiv \pm 1$ (mod $2^{\ell-2}$) for any i, then no 1-rotational STS(v) exists.*

So, in particular, there is no 1-rotational STS($2^\ell 3 + 1$) with $l \geq 5$.

3 Some even starters with a prescribed missing element

An *even starter* of a binary group G is a set E of $|G|/2 - 1$ pairs partitioning $G - \{0, m_E\}$ for a suitable $m_E \in G - \{0\}$ and whose differences partition $G - \Lambda(G)$ (see [12]). We will call m_E the *missing element* of E. An earlier result on this concept was given by B.A. Anderson who proved that every *symmetrically sequenceable binary group*[2] admits an even starter (see [2], Theorem 2). In the same paper it is observed that the symmetric sequenceability is a sufficient but not necessary condition since, for instance, even though the *quaternion group* of order 8 (that is the multiplicative group

[2] An additive group G is sequenceable if there is a permutation $(a_0 = 0, a_1, ..., a_{|G|-1})$ of its elements such that all the partial sums $\sum_{i=0}^{j} a_i$ are pairwise distinct. A binary additive group G is symmetrically sequenceable if there is a permutation as above with $a_{\frac{|G|}{2}-i} = -a_{\frac{|G|}{2}+i}$ for $0 \leq i \leq \frac{|G|}{2}$. We have analogous definitions in multiplicative notation.

$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ with composition law defined by the rules $(-1)^2 = 1$ and $i^2 = j^2 = k^2 = ijk = -1$) does not admit a symmetric sequence, it is evident that

$$E = \Big\{\{i,j\}, \{-i,-k\}, \{-j,k\}\Big\}$$

is as an even starter of it with missing element -1.
We also recall that B.A. Anderson himself and E.C. Ihrig proved that every finite solvable binary group $G \neq Q_8$ is symmetrically sequenceable [3] and hence we can state:

Theorem 3.1. *Every finite solvable binary group admits an even starter.*

Our aim is to establish under which conditions a given binary group G may admit an even starter with an assigned missing element m_E.

Lemma 3.2. *Let G be a binary group admitting an even starter E_0 with missing element $m_{E_0} = g^*$. Then, for any group H of odd order and for any even starter E_1 of $\Lambda(G) \times H$, there exists an even starter E_2 of $G \times H$ with $m_{E_2} = m_{E_1}$.*

Proof. Consider the set

$$E_0' = \Big\{\{(x,h), (y,-h)\} \mid \{x,y\} \in E_0; h \in H\Big\}$$

and observe that its pairs, and their differences as well, partition $(G \times H) - (\Lambda(G) \times H)$. It is then obvious that $E_2 := E_0' \cup E_1$ is an even starter of $G \times H$ with the desired property. □

Lemma 3.3. *Let E be an even starter of $\mathbb{Z}_2 \times H$ with H of odd order n. Then m_E lies in $\{0\} \times H$ or $\{1\} \times H$ according to whether $n \equiv 3$ or 1 $(mod\ 4)$, respectively.*

Proof. Let us say that an element of $\mathbb{Z}_2 \times H$ is *even* or *odd* according to whether it lies in $\{0\} \times H$ or $\{1\} \times H$, respectively.
Also, let us say that a pair $\{(a,b), (c,d)\}$ of elements of $\mathbb{Z}_2 \times H$ is of type t_{00} or t_{11} or t_{01} according to whether we have $a = c = 0$ or $a = c = 1$ or $a \neq c$, namely according to whether the number of its even elements is 2 or 0 or 1, respectively.
Denote by x_{ij} the number of pairs of E of type t_{ij}. The size of E is $n-1$ so that we have $x_{00} + x_{11} + x_{01} = n - 1$.
Now note that the two differences of any given pair of E are both even or both odd and that the latter case happens exactly when the given pair is of type

t_{01}. Thus $2x_{01}$ gives the number of odd elements of $(\mathbb{Z}_2 \times H) - \{(0,0),(1,0)\}$, namely $2x_{01} = n-1$.
Finally, the number $2x_{00}+x_{01}$ of even elements covered by the pairs of E must be equal to the number of even elements of the set $(\mathbb{Z}_2 \times H) - \{(0,0), m_E\}$ so that we have

$$2x_{00} + x_{01} = \begin{cases} n-2 & \text{if } m_E \text{ is even;} \\ n-1 & \text{if } m_E \text{ is odd.} \end{cases}$$

It is straightforward to see that the above equalities give

$$(x_{00}, x_{11}, x_{01}) = \begin{cases} (\frac{n-3}{4}, \frac{n+1}{4}, \frac{n-1}{2}) & \text{if } m_E \text{ is even;} \\ (\frac{n-1}{4}, \frac{n-1}{4}, \frac{n-1}{2}) & \text{if } m_E \text{ is odd.} \end{cases}$$

The assertion immediately follows. □

Given k, with $1 \leq k \leq 2n+1$, a *k-extended Skolem sequence* of order n is a sequence $(s_1, ..., s_n)$ of n integers such that

$$\bigcup_{i=1}^{n} \{s_i, s_i - i\} = \{1, 2, ..., 2n+1\} - \{k\}.$$

The following Baker's theorem [4] holds.

Theorem 3.4. *There exists a k-extended Skolem sequence of order n with k odd [even] if and only if $n \equiv 0$ or 1 [$n \equiv 2$ or 3] (mod 4).*

Now note that k-extended Skolem sequences also produce some even starters.

Lemma 3.5. *If $\{s_1, ..., s_{n-1}\}$ is a k-extended Skolem sequence of order $n-1$, then $E = \{\{s_i, s_i - i\} \mid 1 \leq i \leq n-1\}$ is an even starter of $\mathbb{Z}_{2n}$ with missing element k.*

Proof. Straightforward. □

Here is an immediate special consequence of the above lemma and the theorem of Baker.

Lemma 3.6. *If $G = \mathbb{Z}_{2n}$ with $n \equiv 0$ or 1 (mod 4), then there exists an even starter of G with missing element $g^* = n$.*

The following two lemmas are crucial for proving the result of the next section.

Lemma 3.7. *Let $np^\alpha \equiv 3 \pmod 4$ with p a prime not dividing n. There exists an even starter of $\mathbb{Z}_{2n} \times V_{p^\alpha}$ with missing element $\overline{m}$ for any prescribed $\overline{m} \in \{0\} \times (V_{p^\alpha} - \{0\})$.*

Proof. It is enough to prove that there exists an even starter E of $\mathbb{Z}_{2n} \times V_{p^\alpha}$ whose missing element m_E lies in $\{0\} \times V_{p^\alpha}$. In this case in fact m_E is mapped into $\overline{m}$ by a suitable automorphism ϕ of $\mathbb{Z}_{2n} \times V_{p^\alpha}$ and hence it is clear that $\phi(E)$ is an even starter of $\mathbb{Z}_{2n} \times V_{p^\alpha}$ with missing element $\overline{m}$.

1^{st} case: $n \equiv 1 \pmod 4$.
Set $G = \mathbb{Z}_{2n}$ and $H = V_{p^\alpha}$. By Lemma 3.6 there exists an even starter of G with missing element $g^* = n$. Thus applying Lemma 3.2 we get an even starter of $G \times H$ with missing element m_E where E is an even starter of $\Lambda(G) \times H$ whose existence is ensured by Theorem 3.1. Now note that $n \equiv 1 \pmod 4$ implies that $|H| = p^\alpha \equiv 3 \pmod 4$ and hence, by Lemma 3.3, we necessarily have $m_E \in \{0\} \times H$.

2^{nd} case: $n \equiv p \equiv 3 \pmod 4$.
Set $G = \mathbb{Z}_{2np}$ and $H = V_{p^{\alpha-1}}$. We have $np \equiv 1 \pmod 4$ and hence, by Lemma 3.6, there exists an even starter of G with missing element $g^* = np$. Applying Lemma 3.2 we get an even starter of $G \times H$ with missing element m_E where E is an even starter of $\Lambda(G) \times H$ whose existence is ensured by Theorem 3.1. Also here we have $|H| = p^{\alpha-1} \equiv 3 \pmod 4$ and hence, by Lemma 3.3, we necessarily have $m_E \in \{0\} \times H$.

3^{rd} case: $n \equiv 3 \pmod 4$ and $p \equiv 1 \pmod 4$.
Set $G = \mathbb{Z}_2 \times V_{p^{\alpha-1}}$ and $H = \mathbb{Z}_p \times \mathbb{Z}_n$. By induction on α and using Lemmas 3.2 and 3.6, it is easy to see that there exists an even starter of G with missing element $g^* = (1, 0)$. Now note that by Baker's theorem there exists a $2n$-extended Skolem sequence of order $pn - 1$ which, by Lemma 3.5, yields an even starter of $\mathbb{Z}_{2pn}$ with missing element $2n$. Of course such an even starter can be also seen as an even starter of $\Lambda(G) \times H$ with missing element $((0, 0), (2n, 0))$ in view of the isomorphism $\mathbb{Z}_{2pn} \simeq \Lambda(G) \times H$.
Thus, applying Lemma 3.2 we get an even starter of $G \times H$ with missing element $((0, 0), (2n, 0))$ and the assertion very easily follows. □

Lemma 3.8. *Let $p > 3$ be a prime and let n not divisible by p. There exists an even starter of $\mathbb{Z}_{8n} \times V_{p^\alpha}$ with missing element $\overline{m}$ for any prescribed $\overline{m} \in \{0\} \times (V_{p^\alpha} - \{0\})$*

Proof. Reasoning as in Lemma 3.7 it suffices to prove that there exists an even starter of $\mathbb{Z}_{8n} \times V_{p^\alpha}$ with missing element in $\{0\} \times V_{p^\alpha}$.
By Baker's theorem there exists an $8n$-extended Skolem sequence of order $4np - 1$ which, by Lemma 3.5, yields an even starter of $\mathbb{Z}_{8np}$ with missing

element $8n$. So, identifying $\mathbb{Z}_{8np}$ with $\mathbb{Z}_{8n} \times V_p$ we have an even starter of $\mathbb{Z}_{8n} \times V_p$ with missing element in $\{0\} \times V_p$ and the assertion is true for $\alpha = 1$. Now assume $\alpha > 1$, set $8np = 4r$, and identify $\mathbb{Z}_{8n} \times V_{p^\alpha}$ with $G := \mathbb{Z}_{4r} \times V_{p^{\alpha-1}}$. Consider the set E_0 consisting of the following $4r$ pairs of elements of G where i runs, in each case, from 1 to $r-1$:

$$\begin{array}{cc} \{(0,1),(0,-1)\}; & \{(r,1),(3r,3)\}; \\ \{(2r-1,-1),(2r,1)\}; & \{(2r,-1),(2r+1,-3)\}; \\ \{(i,1),(4r-i,-1)\}; & \{(i,-1),(4r-i,1)\}; \\ \{(r+i-1,-1),(3r-i,3)\}; & \{(r+i,1),(3r-i+1,-3)\}. \end{array}$$

It is not difficult to check that we have:

$$\bigcup_{\{x,y\} \in E_0} \{x,y\} = \bigcup_{z=0}^{4r-1} \{z\} \times \{\gamma_z, -\gamma_z\}$$

with $\gamma_z = 3$ for $2r+1 \leq z \leq 3r$ and $\gamma_z = 1$ otherwise. We also have:

$$\Delta E_0 = \bigcup_{z=0}^{4r-1} \{z\} \times \{\delta_z, -\delta_z\}$$

with $\delta_z = 4$ for any odd $z \neq \pm 1$ and $\delta_z = 2$ otherwise. Thus, denoting by S a complete system of representatives for the cosets of $\{1,-1\}$ in the multiplicative group of $\mathbb{F}_{p^{\alpha-1}}$, we have

$$\{\gamma_z, -\gamma_z\} \cdot S = \{\delta_z, -\delta_z\} \cdot S = V_{p^{\alpha-1}} - \{0\} \quad \forall z \in \mathbb{Z}_{4r}$$

since we have supposed $p > 3$. This implies that

$$E_1 := \left\{ \{(as,bs),(cs,ds)\} \mid \{(a,b),(c,d)\} \in E_0; s \in S \right\}$$

is a set of pairs of G partitioning $G - (\mathbb{Z}_{4r} \times \{0\})$ and whose differences also partition $G - (\mathbb{Z}_{4r} \times \{0\})$.

As observed at the beginning of this proof, there exists an even starter E' of $\mathbb{Z}_{4r} = \mathbb{Z}_{8np}$ with missing element $8n$. So, if E_2 is the set of all pairs $\{(x,0),(y,0)\}$ of G with $\{x,y\}$ a pair of E', it is obvious that $E := E_1 \cup E_2$ is an even starter of $\mathbb{Z}_{8np} \times V_{p^{\alpha-1}}$ with missing element $(8n,0)$. The natural isomorphism between $\mathbb{Z}_{8np} \times V_{p^{\alpha-1}}$ and $\mathbb{Z}_{8n} \times V_{p^\alpha}$ maps this element into the pair $(0,m)$ where m is the α-tuple $(8n,0,...,0)$. Thus E can be viewed as an even starter of $\mathbb{Z}_{8n} \times V_{p^\alpha}$ with missing element $(0,m)$ and the assertion follows. □

4 1-rotational STS(v) with the odd part of $v-1$ non-square-free

We already mentioned that the existence of a 1-rotational STS(v) with $v \equiv 1$ or 19 (mod 24) whenever $v-1$ has a prime factor $p \equiv 1$ (mod 6) has been established in [8]. Using a similar construction, now we show how our results about even starters allow to prove that the existence is also guaranteed in the weaker hypothesis that $v-1$ is divisible by a prime power $q \equiv 1$ (mod 6).

Theorem 4.1. *If $v \equiv 1$ or 19 (mod 24) and the odd part of $v-1$ is not square-free, then there exists a 1-rotational STS(v).*

Proof. By assumption $u := v-1$ is divisible by p^2 for a suitable odd prime p. If $p=3$ we have $u \equiv 0$ or 18 (mod 72) and the assertion follows from (1). Assume $p \neq 3$ and set $u = 6np^\alpha$ where p^α is the largest power of p dividing u. Consider the group $H = K \times V_{p^2}$ where $K = \mathbb{Z}_{2n} \times V_{p^{\alpha-2}}$. We obviously have $p^2 \equiv 1$ (mod 6). Let ϵ be a primitive cubic root of unity of $\mathbb{F}_{p^2}$ and consider the unit $w = (1, \epsilon)$ of the ring with additive group H. Observe that $\epsilon^2 + \epsilon + 1 = 0$ so that we have $w^2 + w + 1 = (3, 0)$. This implies that $(w^2+w+1)h = 0$ for every $h \in \{0\} \times V_{p^2}$. Let $G = \mathbb{Z}_3 +_w H$ be the group with elements in the cartesian product $\mathbb{Z}_3 \times H$ and composition law $+_w$ defined by the rule

$$(a, h) +_w (a', h') = (a + a', w^{a'}h + h').$$

The hypothesis that $v \equiv 1$ or 19 (mod 24) implies that we have $np^\alpha \equiv 0$ or 3 (mod 4). By Lemma 3.8 in the former case and by Lemma 3.7 in the latter, there exists an even starter $E = \{\{x_i, y_i\} \mid 1 \leq i \leq np^\alpha - 1\}$ of H with missing element $m_E \in \{0\} \times V_{p^2}$. Consider the triples T_1, ..., $T_{np^\alpha-1}$ of elements of G defined as follows:

$$T_i = \{(0,0), (1, x_i), (1, y_i)\} \quad 1 \leq i \leq np^\alpha - 1.$$

Given $h \in H$, the opposites of $(0, h)$, $(1, h)$ and $(2, h)$ in G are $(0, -h)$, $(2, -w^2h)$ and $(1, -wh)$, respectively. Taking account of this, we easily see that

$$\Delta T_i = \{(0, w^2(x_i - y_i)), (0, w^2(y_i - x_i)), (1, x_i), (1, y_i), (2, -w^2x_i), (2, -w^2y_i)\}.$$

Hence, by the definition of an even starter, we see that we have

$$\bigcup_{i=1}^{np^\alpha-1} \Delta T_i = G - \{(0,0), (0, h^*), (1, 0), (1, m_E), (2, 0), (2, -w^2m_E)\}$$

where h^* is the involution of H. Now note that the fact that $m_E \in \{0\} \times V_{p^2}$ implies that $(w^2 + w + 1)m_E = 0$ and hence that $(w + 1)m_E = -w^2 m_E$. It follows that $(1, m_E) + (1, m_E) = (2, (w + 1)m_E) = (2, -w^2 m_E) = -(1, m_E)$. Thus $\{(0, 0), (1, m_E), (2, -w^2 m_E)\}$ is a subgroup of G of order 3. We conclude that $\{T_1, ..., T_{np^\alpha - 1}\}$ is a $(G, 3, \Sigma, 1)$-DF where Σ is the following partial spread of G:

$$\Sigma = \Big\{\{(0,0),(0,h^*)\},\ \{(0,0),(1,0),(2,0)\},\ \{(0,0),(1,m_E),(2,-w^2m_E)\}\Big\}.$$

The assertion follows. □

5 Existence of a 1-rotational STS$(24n+1)$ with $n \not\equiv 0 \pmod 4$

In this section we prove that the existence of a 1-rotational STS(v) with $v \equiv 1 \pmod{24}$ is guaranteed in the case that the largest power of 2 in $v - 1$ does not exceed 16. Hence we prove that there exists a 1-rotational STS$(48n + 25)$ and a 1-rotational STS$(96n + 49)$ for every $n \geq 0$. We first need the following fundamental lemma.

Lemma 5.1. *Assume that there exists a* 1*-rotational STS*$(6m + 1)$ *under* G. *Also assume that for a given positive integer* n *there exist* $2m$ *triples* $T_1, ..., T_{2m}$ *of* $G \times \mathbb{Z}_{2n+1}$ *such that*

$$\bigcup_{i=1}^{2m} \Delta T_i = \bigcup_{g \in G} \{g\} \times \{\delta_g, -\delta_g\}$$

for suitable elements $\delta_g \in \mathbb{Z}_{2n+1}$ *with* $\gcd(\delta_g, 2n + 1) = 1$ *for every* $g \in G$. *Then there exists a* 1*-rotational STS*$(12mn + 6m + 1)$ *under* $G \times \mathbb{Z}_{2n+1}$.

Proof. By assumption, there exists a $(G, \Sigma, 3, 1)$-DF, say $\mathcal{F} = \{B_1, ..., B_t\}$, for a suitable partial spread $\Sigma = \{S_0, S_1, ..., S_u\}$ of G with $S_0 = \Lambda(G)$ and $|S_i| = 3$ for $i = 1, ..., u$.
For any given $j \in \mathbb{Z}_{2n+1} - \{0\}$, let ϕ_j be the endomorphism of $G \times \mathbb{Z}_{2n+1}$ defined by $\phi_j(g, z) = (g, jz)$ for every $(g, z) \in G \times \mathbb{Z}_{2n+1}$. Set $T_{ij} = \phi_j(T_i)$ for $1 \leq i \leq 2m$ and consider the set

$$\mathcal{F}' = \{T_{ij} \mid 1 \leq i \leq 2m; 1 \leq j \leq n\}.$$

Of course $\Delta T_{ij} = \phi_j(\Delta T_i)$ and hence we have:

$$\Delta\mathcal{F}' = \bigcup_{j=1}^{n} \phi_j \left(\bigcup_{i=1}^{2m} \Delta T_i \right) = \bigcup_{g \in G} \{g\} \times \bigcup_{j=1}^{n} \{j\delta_g, -j\delta_g\}.$$

Now consider that $\bigcup_{j=1}^{n}\{j\delta_g, -j\delta_g\} = \mathbb{Z}_{2n+1} - \{0\}$ for every $g \in G$ since we have $\gcd(\delta_g, 2n+1) = 1$ by assumption. Hence we can write:

$$\Delta\mathcal{F}' = \bigcup_{g\in G}\{g\} \times (\mathbb{Z}_{2n+1} - \{0\}) = (G \times \mathbb{Z}_{2n+1}) - (G \times \{0\}).$$

At this point it is clear that setting

$$\hat{\mathcal{F}} = \{B_1 \times \{0\}, ..., B_t \times \{0\}\} \quad \text{and} \quad \hat{\Sigma} = \{S_0 \times \{0\}, S_1 \times \{0\}, ..., S_u \times \{0\}\}$$

we have that $\hat{\mathcal{F}} \cup \mathcal{F}'$ is a $(G \times \mathbb{Z}_{2n+1}, \hat{\Sigma}, 3, 1)$-DF. The assertion follows. □

The constructions given in [8] and Theorem 4.1 allow to derive the existence of a 1-rotational STS$(48n + 25)$ for any n except when $2n + 1$ is a product of an odd number of pairwise distinct primes $\equiv 2 \pmod 3$. Now we are able to cover also these cases since the next construction gives such an STS, directly, for every n.

Theorem 5.2. *There exists a* 1*-rotational STS*$(48n + 25)$ *for every* $n \geq 0$.

Proof. The assertion is true for $n = 0$ since the existence of a 1-rotational STS(25) under $SL_2(3)$ has been proved in [8]. It is unique up to isomorphism and it is 1–rotational under the unique admissible group of order 24, that is the special linear group $SL_2(3)$.
The (unique) normal Sylow 2-subgroup of $SL_2(3)$ is $Q = \{q_0, q_1, ..., q_7\}$ where

$$q_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}; \quad q_1 = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix}; \quad q_2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}; \quad q_3 = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix};$$

$$q_4 = \begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}; \quad q_5 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}; \quad q_6 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}; \quad q_7 = \begin{pmatrix} 2 & 2 \\ 2 & 1 \end{pmatrix}.$$

We can write $SL_2(3) = Q \cup Qr \cup Qr^2$ with $r = \begin{pmatrix} 0 & 2 \\ 1 & 2 \end{pmatrix}$.
Suppose that $n \geq 1$ and consider the following eight triples of $SL_2(3) \times \mathbb{Z}_{2n+1}$:

$$\begin{array}{ll}
T_1 = \{(q_0, 0), (q_1 r, 1), (q_4 r, -1)\}; & T_2 = \{(q_0, 0), (q_2 r, 1), (q_7 r, -1)\}; \\
T_3 = \{(q_0, 0), (r, 1), (q_1 r, -1)\}; & T_4 = \{(q_0, 0), (q_3 r, 1), (q_6 r, -1)\}; \\
T_5 = \{(q_0, 0), (q_4 r, 1), (r, -1)\}; & T_6 = \{(q_0, 0), (q_5 r, 1), (q_5 r, -1)\}; \\
T_7 = \{(q_0, 0), (q_6 r, 1), (q_2 r, -1)\}; & T_8 = \{(q_0, 0), (q_7 r, 1), (q_3 r, -1)\}.
\end{array}$$

It is straightforward to check that we have

$$\bigcup_{i=1}^{8} \Delta T_i = \bigcup_{g\in SL_2(3)} \{g\} \times \{\delta_g, -\delta_g\}$$

where $\delta_g = 2$ or 1 according to whether $g \in Q$ or not. Thus the assertion follows from Lemma 5.1. $\square$

At the moment, the existence of a 1-rotational $STS(96n + 49)$ is uncertain in the case that $2n + 1$ is a square free product of primes $\equiv 2 \pmod 3$ and hence, in particular, for $n = 0$. Also here we are able to give a direct construction covering these cases.

Theorem 5.3. *There exists a 1-rotational $STS(96n + 49)$ for every $n \geq 0$.*

Proof. Consider the *octahedral group* $O := PGL_2(3)$ of order 24. By Theorem 2.5 there exists exactly one binary group $\overline{O}$ such that $\overline{O}/\Lambda(\overline{O})$ is isomorphic to O. This is the so called *binary octahedral group* and, obviously, it is an admissible group of order 48. Up to isomorphism it can be viewed as a subgroup of the multiplicative group of the skew-field $\mathbb{H}$ of *quaternions* introduced by Hamilton that is an extension of the complex field $\mathbb{C}$. For convenience of the reader we recall the basic facts regarding $\mathbb{H}$. Its elements are all real linear combinations of 1, i, j and k. The sum and the product of two quaternions are defined in the natural way under the rules that $i^2 = j^2 = k^2 = ijk = -1$. The *conjugate* of a quaternion $q = a + bi + cj + dk$ is $\overline{q} = a - bi - cj - dk$ and its *norm* is the real number $||q|| = \sqrt{q\overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$. If $q \neq 0$, its inverse is given by $q^{-1} = \frac{\overline{q}}{||q||^2}$. The multiplicative group $\overline{O}$ under examination consists of the following quaternions:

± 1, $\pm i$, $\pm j$, $\pm k$;

$\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ with all possible choices of the signs;

$\frac{1}{\sqrt{2}}(\pm x \pm y)$ with $\{x, y\} \in \binom{\{1,i,j,k\}}{2}$ and all possible choices of the signs.

We see that Q_8 is a subgroup of $\overline{O}$ and we have $\Lambda(\overline{O}) = \{1, -1\}$. Also note that every element of $\overline{O}$ has norm 1 so that its inverse simply is its conjugate.

Now consider the following seven triples of elements of $\overline{O}$:

$$\begin{aligned}
B_1 = &\ \{1, \tfrac{1}{\sqrt{2}}(j-k), \tfrac{1}{2}(-1-i+j+k)\};\\
B_2 = &\ \{1, -j, k\};\\
B_3 = &\ \{1, \tfrac{1}{\sqrt{2}}(i+k), \tfrac{1}{\sqrt{2}}(1+i)\};\\
B_4 = &\ \{1, \tfrac{1}{2}(-1+i+j-k), -\tfrac{1}{\sqrt{2}}(j+k)\};\\
B_5 = &\ \{1, \tfrac{1}{2}(1+i+j+k), -\tfrac{1}{\sqrt{2}}(1+j)\};\\
B_6 = &\ \{1, \tfrac{1}{2}(1+i-j-k), \tfrac{1}{\sqrt{2}}(1-k)\};\\
B_7 = &\ \{1, \tfrac{1}{\sqrt{2}}(i-k), -\tfrac{1}{\sqrt{2}}(1+k)\}.
\end{aligned}$$

Let us calculate their lists of differences:

$$\begin{aligned}
\Delta B_1 = &\ \{\tfrac{1}{\sqrt{2}}(j-k), \tfrac{1}{2}(-1+i-j-k), \tfrac{1}{\sqrt{2}}(i+j)\}^{\pm 1}\\
\Delta B_2 = &\ \{i, j, k\}^{\pm 1}\\
\Delta B_3 = &\ \{\tfrac{1}{\sqrt{2}}(i+k), \tfrac{1}{\sqrt{2}}(1+i), \tfrac{1}{2}(1+i-j+k)\}^{\pm 1}\\
\Delta B_4 = &\ \{\tfrac{1}{2}(-1+i+j-k), \tfrac{1}{\sqrt{2}}(j+k), \tfrac{1}{\sqrt{2}}(i-j)\}^{\pm 1}\\
\Delta B_5 = &\ \{\tfrac{1}{2}(1+i+j+k), \tfrac{1}{\sqrt{2}}(-1+j), \tfrac{1}{\sqrt{2}}(-1+i)\}^{\pm 1}\\
\Delta B_6 = &\ \{\tfrac{1}{2}(1+i-j-k), \tfrac{1}{\sqrt{2}}(1+k), \tfrac{1}{\sqrt{2}}(1+j)\}^{\pm 1}\\
\Delta B_7 = &\ \{\tfrac{1}{\sqrt{2}}(i-k), \tfrac{1}{\sqrt{2}}(-1+k), \tfrac{1}{2}(1+i+j-k)\}^{\pm 1}
\end{aligned}$$

We see that

$$\bigcup_{i=1}^{7} \Delta B_i = \overline{O} - H$$

with

$$H = \{1, -1, \tfrac{1}{2}(-1+i+j+k), \tfrac{1}{2}(-1-i-j-k), \tfrac{1}{2}(-1+i-j+k), \tfrac{1}{2}(-1-i+j-k)\}.$$

Thus, observing that $S_1 = \{1, \frac{1}{2}(-1+i+j+k), \frac{1}{2}(-1-i-j-k)\}$ and $S_2 = \{1, \frac{1}{2}(-1+i-j+k), \frac{1}{2}(-1-i+j-k)\}$ are subgroups of $\overline{O}$ of order 3, we conclude that $\mathcal{F} = \{B_1, ..., B_7\}$ is a 1-rotational $(\overline{O}, \Sigma, 3, 1)$ difference family with $\Sigma = \{\Lambda(\overline{O}), S_1, S_2\}$, i.e., there exists a 1-rotational STS(49) under $\overline{O}$. Then the assertion is true for $n = 0$.
The assertion is also true when $2n+1 > 0$ is divisible by 3 in view of (1).

So assume that $2n+1>0$ is not divisible by 3 and consider the following sixteen triples of $\overline{O}\times\mathbb{Z}_{2n+1}$:

$$\begin{aligned}
T_1 &= \{(1,1),(1,-1),(\tfrac{1}{2}(1+i-j-k),0)\};\\
T_2 &= \{(1,0),(\tfrac{1}{2}(-1-i+j-k),3),(\tfrac{1}{2}(1+i-j+k),-1)\};\\
T_3 &= \{(1,0),(\tfrac{1}{2}(-1-i+j-k),-3),(-\tfrac{1}{\sqrt{2}}(1-k),-2)\};\\
T_4 &= \{(1,0),(\tfrac{1}{2}(1+i-j+k),1),(-\tfrac{1}{\sqrt{2}}(1-k),2)\};\\
T_5 &= \{(1,0),(k,1),(j,-1)\};\\
T_6 &= \{(1,0),(k,-1),(j,1)\};\\
T_7 &= \{(1,0),(\tfrac{1}{\sqrt{2}}(i+k),1),(-\tfrac{1}{2}(1+i+j-k),-1)\};\\
T_8 &= \{(1,0),(\tfrac{1}{\sqrt{2}}(i+k),-1),(-\tfrac{1}{2}(1+i+j-k),1)\};\\
T_9 &= \{(1,0),(\tfrac{1}{\sqrt{2}}(i-k),1),(\tfrac{1}{2}(-1-i+j+k),-1)\};\\
T_{10} &= \{(1,0),(\tfrac{1}{\sqrt{2}}(i-k),-1),(\tfrac{1}{2}(-1-i+j+k),1)\};\\
T_{11} &= \{(1,0),(-\tfrac{1}{\sqrt{2}}(i+j),1),(\tfrac{1}{\sqrt{2}}(-1+j),-1)\};\\
T_{12} &= \{(1,0),(-\tfrac{1}{\sqrt{2}}(i+j),-1),(\tfrac{1}{\sqrt{2}}(-1+j),1)\}\};\\
T_{13} &= \{(1,0),(\tfrac{1}{\sqrt{2}}(1+i),1),(\tfrac{1}{2}(1+i+j-k),-1)\};\\
T_{14} &= \{(1,0),(\tfrac{1}{\sqrt{2}}(1+i),-1),(\tfrac{1}{2}(1+i+j-k),1)\};\\
T_{15} &= \{(1,0),(\tfrac{1}{2}(1+i+j+k),1),(\tfrac{1}{\sqrt{2}}(j+k),-1)\};\\
T_{16} &= \{(1,0),(\tfrac{1}{2}(1+i+j+k),-1),(\tfrac{1}{\sqrt{2}}(j+k),1)\}.
\end{aligned}$$

It is tedious but not difficult to check that we have

$$\bigcup_{i=1}^{16}\Delta T_i=\bigcup_{g\in\overline{O}}\{g\}\times\{\delta_g,-\delta_g\}\quad\text{with } \delta_g\in\{1,2,3,4\}\ \forall\ g\in\overline{O}.$$

For the reader who would like to check the above calculation, we point out that we have $T_{2i}=\phi(T_{2i-1})$ for $3\le i\le 8$ where ϕ is the automorphism of $\overline{O}\times\mathbb{Z}_{2n+1}$ defined by $\phi(g,z)=(g,-z)$ for every $(g,z)\in\overline{O}\times\mathbb{Z}_{2n+1}$; hence we have $\Delta T_{2i}=\phi(\Delta T_{2i-1})$ for $3\le i\le 8$.
We have $\gcd(\delta_g,2n+1)=1$ for every g since we are supposing that 3 does not divide $2n+1$ and hence, considering that a 1-rotational STS(49) under $\overline{O}$ has been proved to exist, the assertion follows from Lemma 5.1. □

6 Conclusion

Putting together the results of [8] and those obtained in the previous sections we conclude that the existence of a 1-rotational STS(v) is uncertain only in the case of $v = (p^3 - p)n + 1 \equiv 1 \pmod{96}$ with p a prime, $n \not\equiv 0 \pmod 4$, the odd part of $v - 1$ square-free and without prime factors $\equiv 1 \pmod 6$.
At the moment solving these open cases does not seem an easy matter to us. Maybe, the first step could be to find a solution when $n = 1$ or 2. Thus we propose the following problems.

Problem 1. Given an odd prime p, does there exist an STS($2p^3 - 2p + 1$) that is 1-rotational under an extension of $PGL_2(p)$ by $\mathbb{Z}_2$?

Problem 2. Given an odd prime p, does there exist an STS($p^3 - p + 1$) that is 1-rotational under $SL_2(p)$?

For the time being, the above problems have been positively solved only in the smallest case of $p = 3$ (see the previous section). Also consider that the two solutions that we obtained in this special case allowed us, together with Lemmma 5.1, to prove the existence of a 1-rotational STS(v) for any $v \equiv 25 \pmod{48}$ and any $v \equiv 49 \pmod{96}$, namely the existence of a 1-rotational STS($(3^3 - 3)n + 1$) for any $n \not\equiv 0 \pmod 4$.
Thus, it is maybe possible that if one positively solves Problems 1 and 2 for any odd prime p, then a clever use of Lemma 5.1 allows us to find a 1-rotational STS($(p^3 - p)n + 1$) for any odd prime p and any $n \not\equiv 0$ (mod 4). In this case our main question about the set of values of v for which a 1-rotational STS(v) exists would be completely solved.
We point out, however, that even though Problems 1 and 2 are interesting in their own right, for our main purpose it is not necessary to solve them for all odd primes p. In Problem 1 it is enough to consider those primes $p \equiv \pm 1 \pmod 8$ for which the odd part of $p^3 - p$ is square-free and without prime factors $\equiv 1 \pmod 6$. Analogously, in Problem 2 it is enough to consider those primes $p \equiv \pm 1 \pmod{16}$ for which, again, the odd part of $p^3 - p$ is square-free and without prime factors $\equiv 1 \pmod 6$.
So, the primes $p < 1000$ for which our main question actually requires a solution to Problem 1 are 23, 47, 137, 263, 353, 383, 479, 641 and 983.
Instead, the primes $p < 1000$ for which our main question actually requires a solution to Problem 2 are only 47, 353, 383, 479 and 641.
Hence $v = 24289 = (23^3 - 23)2 + 1$ and $v = 103777 = 47^3 - 47 + 1$ are the first two values of v for which the existence of a 1-rotational STS(v) is open. If a 1–rotational STS(24289) exists, it is necessarily under an extension of

$PGL_2(23)$ by $\mathbb{Z}_2$; also, if a 1–rotational STS(103777) exists, it is necessarily under $SL_2(47)$.

Acknowledgement. We are very grateful to the referee for his/her suggestions which have been helpful in increasing the readibility of the paper.

References

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

[2] B.A. Anderson, *Sequencings and starters*, Pacific J. Math. **64** (1976), 17–24.

[3] B.A. Anderson and E. C. Ihrig, *Every finite solvable group with a unique element of order two, except the quaternion group, has a symmetric sequencing*, J. Combin. Des. **1** (1993), 3–14.

[4] C.A. Baker, *Extended Skolem sequences*, J. Combin. Des. **3** (1995), 363–379.

[5] L. Babai and P.J. Cameron, *Automorphisms and enumeration of switching classes of tournaments*, Electron. J. Combin. **7** (2000).

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

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

[8] M. Buratti, 1-*rotational Steiner triple systems over arbitrary groups*, J. Combin. Des. **9** (2001), 215–226.

[9] M. Buratti and F. Zuanni, *On singular* 1-*rotational Steiner* 2-*designs*, J. Combin. Theory Ser. A **86** (1999), 232–244.

[10] C. J. Colbourn and A. Rosa, *Triple Systems.* Clarendon Press, Oxford, 1999.

[11] L.E. Dickson, *Linear groups with an exposition of the Galois field theory* Dover Publications, Inc., New York, 1958.

[12] J.H. Dinitz, *Starters*, Handbook of Combinatorial Designs, Second Edition, C.J. Colbourn and J.H. Dinitz (Editors), Chapman & Hall/CRC, Boca Raton, FL, 2006, 622-628.

[13] J. Doyen, *A note on reverse Steiner triple systems*, Discrete Math. **1** (1972), 315–319.

[14] D. Gorenstein, *Finite groups.* Harper and Row, New York, 1968.

[15] M. Mishima, *The spectrum of* 1*-rotational Steiner triple systems over a dicyclic group*, Discrete Math. **308** (2008), 2617–2619.

[16] K.T. Phelps and A. Rosa, *Steiner triple systems with rotational automorphisms*, Discrete Math. **33** (1981), 57–66.

[17] A. Rosa, *On reverse Steiner triple systems*, Discrete Math. **2** (1972), 61–71.

[18] M. Suzuki, *Group theory I.* Springer-Verlag, Berlin, 1982.

[19] L. Teirlinck, *The existence of reverse Steiner triple systems*, Discrete Math. **6** (1973), 301–302.