On 6-sparse Steiner triple systems

A. D. Forbes, M. J. Grannell and T. S. Griggs
Department of Pure Mathematics
The Open University
Walton Hall
Milton Keynes MK7 6AA
UNITED KINGDOM

tonyforbes@ltkz.demon.co.uk
m.j.grannell@open.ac.uk
t.s.griggs@open.ac.uk

Abstract

We give the first known examples of 6-sparse Steiner triple systems by constructing 29 such systems in the residue class 7 modulo 12, with orders ranging from 139 to 4447. We then present a recursive construction which establishes the existence of 6-sparse systems for an infinite set of orders. Observations are also made concerning existing construction methods for perfect Steiner triple systems, and we give a further example of such a system. This has order 135 859 and is only the fourteenth known. Finally, we present a uniform Steiner triple system of order 180 907.

AMS classification: 05B07.
Keywords: Steiner triple system, k-sparse Steiner triple system, Pasch configuration, mitre configuration, crown configuration, perfect Steiner triple system.

1 Introduction

A *Steiner triple system* of order v, STS(v), is a pair $(V, \mathcal{B})$ where V is a set of cardinality v of *elements*, or *points*, and $\mathcal{B}$ is a collection of *triples*, also called *blocks*, which has the property that every pair of distinct elements of V occurs in precisely one triple. It is well known that an STS(v) exists if and only if $v \equiv 1$ or 3 (mod 6). Such values are called *admissible*.

A *configuration* in a Steiner triple system is a collection of triples which has the property that every pair of distinct elements occurs in at most one triple. If $\mathcal{C}$ is a configuration, we denote by $P(\mathcal{C})$ its set of points. Two configurations $\mathcal{C}$ and $\mathcal{D}$ are said to be *isomorphic*, in symbols $\mathcal{C} \cong \mathcal{D}$, if there exists a bijection $\phi : P(\mathcal{C}) \to P(\mathcal{D})$ such that for each triple $T \in \mathcal{C}$, $\phi(T)$ is a triple in $\mathcal{D}$. Given a Steiner triple system $(V, \mathcal{B})$, the set $\mathcal{B}$ itself may be regarded as a configuration with $P(\mathcal{B}) = V$. The *degree* of a point in a configuration is the number of blocks which contain it. We will often write blocks with set brackets and commas omitted, so that for example $\{0, 1, 3\}$ might be written as 013.

In 1973, Erdös [5] conjectured that for every integer $k \geq 4$, there exists $v_0(k)$ such that if $v > v_0(k)$ and if v is admissible, then there exists an STS(v) with the property that it contains no configurations having n blocks and $n+2$ points for any n satisfying $4 \leq n \leq k$. Such an STS(v) is said to be *k-sparse*. Clearly, a k-sparse system is also k'-sparse for every k' satisfying $4 \leq k' \leq k$. The reason why configurations having two more points than blocks form the focus of the conjecture lies in the following result and its corollary. The essence of this result must have been known to Erdös, although we can find no explicit statement of it in the literature.

Theorem 1.1 *Suppose that $n \geq 2$ and that v is admissible with $v \geq n + 3$. Then any STS(v) contains a configuration having n blocks and $n + 3$ points.*

Proof. It is easy to see that for admissible $v \geq 7$, every STS(v) contains a copy of $\mathcal{C} = \{012, 034, 056, 246\}$; in fact [8] gives a formula for the number of occurrences of such configurations in an STS(v). Note that $\mathcal{C}$ has 4 blocks and 7 points. It also contains the configuration $\{012, 034, 246\}$ which has 3 blocks and 6 points, and the configuration $\{012, 034\}$ which has 2 blocks and 5 points. Thus the result certainly holds for $n = 2, 3$ and 4.

Now suppose, inductively, that the result holds for all n satisfying $4 \leq n \leq n_0$. We show that it also holds for $n = n_0 + 1$. Take $v \geq n_0 + 4$ and admissible, and select any STS(v), say $\mathcal{S}$. By the inductive hypothesis, $\mathcal{S}$

contains a configuration $\mathcal{C}$ having n_0 blocks and n_0+3 points. The set $P(\mathcal{C})$ generates $\binom{n_0+3}{2}$ pairs of which $3n_0$ appear in the blocks of $\mathcal{C}$, so there exist pairs not appearing in a block of $\mathcal{C}$. Each of these pairs lies in a unique block of $\mathcal{S}$ and so generates a third point of $\mathcal{S}$. Either

(a) there exists a pair whose third point lies outside $P(\mathcal{C})$, or

(b) every such pair generates its third point inside $P(\mathcal{C})$.

In case (a) we add the third point and corresponding block to $\mathcal{C}$ to obtain a configuration in $\mathcal{S}$ having n_0+1 blocks and n_0+4 points.

In case (b), the points of $P(\mathcal{C})$ generate an STS(n_0+3), $\mathcal{S}_0$, contained within $\mathcal{S}$. Then $7 \leq n_0+3 < v$ and $\mathcal{S}_0$ will contain a configuration $\mathcal{D}$ having n_0-1 blocks and n_0+2 points. Let x denote the unique point of $\mathcal{S}_0$ not lying in $P(\mathcal{D})$. The number of pairs from $P(\mathcal{D})$ which do not lie in blocks of $\mathcal{D}$ and which do not lie in blocks containing x is given by

$$\binom{n_0+2}{2} - 3(n_0-1) - \frac{n_0+2}{2} = \frac{(n_0-2)^2}{2} + 1 > 0.$$

So at least one pair from $P(\mathcal{D})$ lies in a block of $\mathcal{S}_0$ outside $\mathcal{D}$ whose third point lies in $P(\mathcal{D})$. If this block is added to $\mathcal{D}$ then we obtain a configuration $\mathcal{D}'$ having n_0 blocks and n_0+2 points. Now choose a point y of $\mathcal{S}$, not lying in $\mathcal{S}_0$, and choose any point $a \in P(\mathcal{D})$. There is a block $\{a, y, z\}$ of $\mathcal{S}$ with z not lying in $\mathcal{S}_0$. By adding this block to $\mathcal{D}'$, we form a configuration in $\mathcal{S}$ having n_0+1 blocks and n_0+4 points.

The result now follows by induction. □

Corollary 1.1.1 *For every integer $d \geq 3$ and for every integer n satisfying $n \geq \lceil \frac{d}{2} \rceil$ there exists $v_0(n,d)$ such that for all admissible $v \geq v_0(n,d)$, every STS(v) contains a configuration having n blocks and $n+d$ points.*

Proof. By the theorem, if $d=3$ we may take $v_0(n,d) = n+3$. So assume, inductively, that the result is true for $d = d_0 \geq 3$. We show that it also holds for $d = d_0+1$.

First we deal with the case when d_0 is odd and $n = \lceil \frac{d_0+1}{2} \rceil$. We must show that for every sufficiently large admissible v, every STS(v) contains a configuration having n blocks and $3n$ points. But such a configuration is a partial parallel class having n blocks, and the result follows from [1].

For all remaining cases, namely if d_0 is even and $n = \lceil \frac{d_0+1}{2} \rceil$, or if d_0 has either parity and $n > \lceil \frac{d_0+1}{2} \rceil$, we have $n - 1 \geq \lceil \frac{d_0}{2} \rceil$. So, by the inductive hypothesis, there exists $v_0(n-1, d_0)$ such that for all admissible $v \geq v_0(n-1, d_0)$ every STS(v) contains a configuration having $n-1$ blocks and $n-1+d_0$ points. If $v_0(n, d_0+1)$ is taken sufficiently large then any STS(v) with $v > v_0(n, d_0+1)$ will contain such a configuration $\mathcal{C}$ and have a block $\{x, y, z\}$ with $x \in P(\mathcal{C})$ and $y, z \notin P(\mathcal{C})$. If such a block is added to $\mathcal{C}$, then we obtain a configuration having n blocks and $n + (d_0 + 1)$ points.

The result now follows by induction. □

Up to isomorphism, there is only one configuration having four blocks and six points, namely the Pasch configuration, also known as a quadrilateral; this is shown in Table 1. The existence of 4-sparse (better known as anti-Pasch) STS(v)s for all admissible v, except $v = 7$ and 13, was established in a series of papers [2, 11, 13, 10]. The length and complexity of the proof which established this result may indicate the difficulty inherent in Erdös' original conjecture which relates to every $k \geq 4$ rather than just to $k = 4$.

n	Name	Blocks	Comment
4	Pasch	012, 034, 135, 245	
5	mitre	012, 034, 135, 236, 456	
5	mia	012, 034, 135, 245, 056	contains Pasch
6	6-cycle	012, 034, 135, 246, 257, 367	
6	crown	012, 034, 135, 236, 147, 567	
6		012, 034, 135, 236, 146, 057	contains Pasch
6		012, 034, 135, 236, 146, 247	contains Pasch
6		012, 034, 135, 236, 147, 257	contains mitre

Table 1: Configurations having n blocks and $n + 2$ points.

Some progress has also been made with 5-sparse systems. There are, up to isomorphism, two configurations having five blocks and seven points, namely the mitre and the mia. These are also shown in Table 1. The mia contains a copy of the Pasch configuration and so a system is 5-sparse if and only if it contains no Pasch configurations and no mitres. Thus 5-sparse systems are anti-mitre, but not necessarily vice-versa. In a sequence of papers [3, 12, 6] and culminating in the recent papers by Fujiwara and Wolfe [7, 16], it is established that anti-mitre systems exist for all admissible orders,

apart from $v = 9$. Systems which are 5-sparse are known for $v \equiv 1, 19 \pmod{54}$, except possibly $v = 109$, and for many other sporadic values [12, 7]. Furthermore, Wolfe has recently proved that 5-sparse systems exist for "almost all" admissible v (meaning arithmetic set density 1 in the set of all admissible orders) [17], and indeed for all $v \equiv 3 \pmod{6}$ with $v \geq 21$ [18].

As might be expected, the situation for 6-sparse systems is more complicated. There are, up to isomorphism, five configurations having six blocks and eight points. These are also shown in Table 1. Two of these contain a Pasch configuration and another one contains a mitre, leaving two configurations of which one is known as a 6-cycle and the other we will call a *crown*. Thus a system is 6-sparse if and only if it contains no Pasch configurations, no mitres, no 6-cycles and no crowns. Up to the time of the current paper, no 6-sparse systems were known. Although our primary focus in the current paper is on such systems, we remark that we have examined these systems to see if any are 7-sparse and we have found that they are not.

In the next section we give a construction method for block transitive Steiner triple systems. This construction was used in [9] to produce nine new perfect Steiner triple systems, that is STS(v)s having no k-cycle for $k < v - 3$. A k-cycle ($k \geq 4$ and even) is a configuration of k blocks having the form $\{\{a, 1, 2\}, \{b, 2, 3\}, \{a, 3, 4\}, \ldots, \{b, k, 1\}\}$. The Pasch configuration is a 4-cycle and the 6-cycle configuration given in Table 1 is a further example. Every STS(v) contains k-cycle configurations for some values of k satisfying $4 \leq k \leq v - 3$. To see this, take any STS(v)$= (V, \mathcal{B})$. Then for each pair $\{a, b\} \subset V$, define the *cycle graph* $G_{a,b}$ by taking its vertex set as $V \setminus \{a, b, c\}$ where $\{a, b, c\} \in \mathcal{B}$, and joining vertices x and y by an edge if and only if $\{a, x, y\}$ or $\{b, x, y\} \in \mathcal{B}$. Clearly $G_{a,b}$ is a union of disjoint cycles, the total of whose lengths is $v - 3$. Thus an STS(v) is perfect if and only if every cycle graph $G_{a,b}$ is a single cycle of length $v - 3$.

A perfect system is anti-Pasch, but perfect does not imply k-sparse for any $k > 4$. Nevertheless, there is an affinity between the two concepts since both relate to the avoidance of certain configurations, some of which are common. The construction given in section 2 has enabled us to produce 29 6-sparse block transitive Steiner triple systems. In section 3 we employ these in a recursive construction which generates infinitely many 6-sparse systems. Finally, in section 4, we show that the 29 systems form a complete listing of all 6-sparse systems obtainable from the construction of section 2, and we answer a question posed in [9] by showing that the same construction can only produce finitely many perfect systems.

2 A basic construction

The following theorem is a reformulation, in terms of multiplicative characters of $GF(v)$, of a result first presented in [9].

Theorem 2.1 *Suppose that v is a prime congruent to 7 modulo 12 and that χ is a multiplicative character of $GF(v)$ of order 6. Suppose also that $\alpha \in GF(v)$ has the property that $\chi(\alpha) \neq -1, 0, 1$ and that $\chi(1-\alpha)\chi(\alpha) = \pm 1$. Let G denote the group comprising all mappings on $GF(v)$ having the form $x \to ax + b$ for $a, b \in GF(v)$ with $\chi(a) = 1$. Then the orbit generated by the block $\{0, 1, \alpha\}$ under the action of G forms a block transitive STS(v).*

Proof. See [9]. □

In what follows we will refer to a system constructed in this fashion as a *block transitive* STS(v) *with parameter* α, tacitly assuming that $v \equiv 7 \pmod{12}$ is prime, that arithmetic is performed in $GF(v)$ and that χ is a multiplicative character of $GF(v)$ of order 6. The importance of Theorem 2.1 lies in the fact that a computer search can be employed to identify suitable values of α. Furthermore, since the STS(v) so generated is block transitive, only the three cycle graphs $G_{0,1}, G_{0,\alpha}$ and $G_{1,\alpha}$ need to be examined in order to determine whether the system is perfect, and this was the focus of the investigation in [9]. In the present paper, for each value of α, we examined the systems for sparseness, again using block transitivity to simplify the calculations. A further simplification is obtained by observing that, if α satisfies the conditions of the theorem then, as shown in [9], the six STS(v)s generated by the blocks $\{0, 1, \beta\}$ for $\beta \in \{\alpha, 1-\alpha, \frac{1}{1-\alpha}, \frac{\alpha}{\alpha-1}, 1-\frac{1}{\alpha}, \frac{1}{\alpha}\}$ are all isomorphic. This observation reduces the number of cases to be checked. Furthermore, if $\chi(2) = 1$ then the STS(v) with parameter α contains the Pasch configuration $\{\{0, 1, \alpha\}, \{0, 2, 2\alpha\}, \{1, 2, \alpha+1\}, \{\alpha, \alpha+1, 2\alpha\}\}$ and so cannot be 6-sparse.

The results of a computer search are collected in Table 2. Altogether we have found 29 6-sparse block transitive Steiner triple systems produced by the construction, including two non-isomorphic STS(139)s and two non-isomorphic STS(3259)s. We remark that the system with $v = 139$ and $\alpha = 51$ is isomorphic to the perfect block transitive STS(139) given in [9]. To construct that STS(139) the value $\alpha = 25$ was used, and this is related to ours by $51 \equiv 1 - 1/25 \pmod{139}$. The search was exhaustive for $v \leq 9\,150\,625$; the significance of this number will be made clear in section 4. None of the systems in Table 2 is 7-sparse.

The program that performed the search was very straightforward and based on the following mathematics.

For $x \not\equiv 0 \pmod{v}$, $\chi(x)$ was taken as $\exp(\pi\, i\, \mathrm{ind}_\omega(x)/3)$, where ω is the smallest primitive root modulo v, and $\mathrm{ind}_\omega(x) \in \{0, 1, \ldots, v-2\}$ is defined by $\mathrm{ind}_\omega(x) = y \Leftrightarrow \omega^y \equiv x \pmod{v}$.

For each prime $v \equiv 7 \pmod{12}$ satisfying $v < 9\,150\,625$ and $\mathrm{ind}_\omega(2) \not\equiv 0 \pmod{6}$, we considered each $\alpha = \omega^j \in GF(v)$ satisfying $j \equiv 1 \pmod{3}$, $\mathrm{ind}_\omega(1-\alpha) \equiv 2 \pmod{3}$, $j < \mathrm{ind}_\omega(1/(1-\alpha))$ and $j < \mathrm{ind}_\omega(1-1/\alpha)$. These conditions ensure that $\alpha^2 - \alpha + 1 \neq 0$. We rejected systems where there exists an x satisfying

$$\chi(x) = \chi(1-\alpha x) = \chi\left(\frac{\alpha(x-1)}{1-\alpha}\right) = \chi\left(\frac{(\alpha^2-\alpha+1)x-\alpha}{1-\alpha}\right) = 1,$$

since the system then contains a mitre (see the proof of Theorem 4.2). A test for 6-sparseness was performed on the remaining systems, all of which had $v \leq 9787$. By exploiting block transitivity this was a straightforward $O(v)$ process, examining triangles with vertices a, b, c, where $a, b \in \{0, 1, \alpha\}$ and $c \notin \{0, 1, \alpha\}$, to see if any formed part of a Pasch, mitre, 6-cycle or crown configuration.

v	α	v	α	v	α	v	α
139	51	907	68	1303	971	2707	1837
139	118	967	210	1531	42	3259	562
151	37	991	76	1699	506	3259	1286
463	261	1039	356	2083	800	3319	511
523	501	1051	660	2179	1820	4447	210
571	528	1087	519	2311	1593		
691	468	1171	931	2503	1287		
859	616	1291	833	2539	180		

Table 2: Block transitive 6-sparse Steiner triple systems.

In the next section some elementary properties of the construction are required. We obtain these properties in the following lemmas.

Lemma 2.1 *Let $S = (V, \mathcal{B})$ be a block transitive STS(v) with parameter α. Then (i) $\alpha \notin \{0, 1, -1, 2, \frac{1}{2}\}$ and (ii) $\alpha^2 \notin \{-1, 2\alpha - 2, \alpha - \frac{1}{2}\}$.*

Proof. For (i), there is in each case either a block which does not have three distinct points or a pair which appears in more than one block. For (ii), since $v \equiv 3 \pmod 4$, -1 is not a quadratic residue modulo v, and consequently $\alpha^2 + 1 = 0$, $\alpha^2 - 2\alpha + 2 = 0$ and $2\alpha^2 - 2\alpha + 1 = 0$ are not solvable in $GF(v)$. □

Lemma 2.2 *Let $S = (V, \mathcal{B})$ be a block transitive STS(v) with parameter α. Suppose $\{x, y, z\}$ and $\{\mu x, \mu y, \mu z\}$ are blocks of S. Then either $\chi(\mu) = 1$ or $\alpha^2 = \alpha - 1$.*

Proof. We may assume that $x = q, y = p + q, z = p\alpha + q$, and that

$$\{\mu x, \mu y, \mu z\} = \{s, r + s, r\alpha + s\} \tag{1}$$

where $p, q, r, s \in GF(v)$ and $\chi(p) = \chi(r) = 1$. We examine each of the six permutations of (1). Taking first the case when $\mu x = s$ and $\mu y = r + s$, we have $(\mu y - \mu x)/(y - x) = r/p$, so $\mu = r/p$ and hence $\chi(\mu) = 1$. In the remaining five cases we compute μ in two ways from the ratios $(\mu y - \mu x)/(y - x)$ and $(\mu z - \mu x)/(z - x)$. This yields the following implications.

$$\begin{aligned}
\mu x = s,\ \mu y = r\alpha + s \quad &\Rightarrow \quad \alpha^2 = 1, \\
\mu x = r + s,\ \mu y = s \quad &\Rightarrow \quad \alpha = \frac{1}{2}, \\
\mu x = r + s,\ \mu y = r\alpha + s \quad &\Rightarrow \quad \alpha^2 = \alpha - 1, \\
\mu x = r\alpha + s,\ \mu y = s \quad &\Rightarrow \quad \alpha^2 = \alpha - 1, \\
\mu x = r\alpha + s,\ \mu y = r + s \quad &\Rightarrow \quad \alpha = 2.
\end{aligned}$$

If $\alpha^2 = 1$ then $\alpha = \pm 1$, and these values together with the values $\frac{1}{2}$ and 2 are excluded by Lemma 2.1. □

Lemma 2.3 *Let $S = (V, \mathcal{B})$ be a block transitive STS(v) with parameter α. Suppose that $\mu \neq 0$ and that $\{c, d, g\}$ and $\{b, e, h\}$ are blocks of S. Then the two equalities*

$$b - e = (d - c)\mu \quad \textit{and} \quad h - b = (d - g)\mu \tag{2}$$

cannot hold simultaneously unless

$$\alpha^2 \in \{1 - \alpha, \alpha + 1, 3\alpha - 1\}. \tag{3}$$

Proof. Assume that $\{c, d, g\} = \{q, p+q, p\alpha+q\}$ and $\{b, e, h\} = \{s, r+s, r\alpha+s\}$ where $p, q, r, s \in GF(v)$ and $\chi(p) = \chi(r) = 1$. Given these representations of the blocks $\{c, d, g\}$ and $\{b, e, h\}$, we refer to the coefficient of p for c, d and g, and the coefficient of r for b, e and h, as the *type* of the point. The type is thus 0, 1 or α.

For each of the 36 valid ways to combine the types of c, d, g, b, e and h, we compute $\mu p/r$ in two ways, one for each of the equalities in (2). We may assume that either c has type 0, or c has type 1 and g has type α. For otherwise we make the two interchanges $c \leftrightarrow g$ and $e \leftrightarrow h$ (which involve pairs in the same block). Then (2) becomes $b - h = (d - g)\mu$ and $e - b = (d - c)\mu$, which is the same as (2) but with μ replaced by $-\mu$. Hence there are only 18 cases to consider.

We present the analysis of these cases in Table 3 which shows the two values of $\mu p/r$ (column 4) and their common solution, if any, for α (column 5) for each combination of the types of c, d, g (column 2) and b, e, h (column 3). It is straightforward to verify the contents of the table. In rows 1, 3, 11, 13 and 15, the expressions for $\mu p/r$ yield a contradiction. In rows 4, 5, 8, 9, 12, 14 and 18, the expression in column 5 contradicts Lemma 2.1. In the remaining cases, rows 2, 6, 7, 10, 16 and 17, each pair of expressions for $\mu p/r$ implies (3).

	$c\,d\,g$ type	$b\,e\,h$ type	$\mu p/r$	solution
1	$0\,1\,\alpha$	$0\,1\,\alpha$	$-1,\ \alpha/(1-\alpha)$	$-$
2	$0\,1\,\alpha$	$0\,\alpha\,1$	$-\alpha,\ 1/(1-\alpha)$	$\alpha^2=\alpha+1$
3	$0\,1\,\alpha$	$1\,0\,\alpha$	$1,\ -1$	$-$
4	$0\,1\,\alpha$	$1\,\alpha\,0$	$1-\alpha,\ 1/(\alpha-1)$	$\alpha^2=2\alpha-2$
5	$0\,1\,\alpha$	$\alpha\,0\,1$	$\alpha,\ 1$	$\alpha=1$
6	$0\,1\,\alpha$	$\alpha\,1\,0$	$-1+\alpha,\ \alpha/(\alpha-1)$	$\alpha^2=3\alpha-1$
7	$0\,\alpha\,1$	$0\,1\,\alpha$	$-1/\alpha,\ \alpha/(\alpha-1)$	$\alpha^2=1-\alpha$
8	$0\,\alpha\,1$	$0\,\alpha\,1$	$-1,\ 1/(\alpha-1)$	$\alpha=0$
9	$0\,\alpha\,1$	$1\,0\,\alpha$	$1/\alpha,\ 1$	$\alpha=1$
10	$0\,\alpha\,1$	$1\,\alpha\,0$	$-1+1/\alpha,\ 1/(1-\alpha)$	$\alpha^2=3\alpha-1$
11	$0\,\alpha\,1$	$\alpha\,0\,1$	$1,\ -1$	$-$
12	$0\,\alpha\,1$	$\alpha\,1\,0$	$(\alpha-1)/\alpha,\ \alpha/(1-\alpha)$	$2\alpha^2=2\alpha-1$
13	$1\,0\,\alpha$	$0\,1\,\alpha$	$1,\ -1$	$-$
14	$1\,0\,\alpha$	$0\,\alpha\,1$	$\alpha,\ -1/\alpha$	$\alpha^2=-1$
15	$1\,0\,\alpha$	$1\,0\,\alpha$	$-1,\ -1+1/\alpha$	$-$
16	$1\,0\,\alpha$	$1\,\alpha\,0$	$-1+\alpha,\ 1/\alpha$	$\alpha^2=\alpha+1$
17	$1\,0\,\alpha$	$\alpha\,0\,1$	$-\alpha,\ (\alpha-1)/\alpha$	$\alpha^2=1-\alpha$
18	$1\,0\,\alpha$	$\alpha\,1\,0$	$1-\alpha,\ 1$	$\alpha=0$

Table 3: Lemma 2.3. □

Lemma 2.4 *Let $S=(V,\mathcal{B})$ be a block transitive STS(v) with parameter α. Suppose that $\mu\neq 0$ and that $\{a,g,h\}$ and $\{b,d,f\}$ are blocks of S for which the two equalities*

$$b-d=(h-g)\mu \quad \textit{and} \quad b-f=(h-a)\mu \tag{4}$$

hold simultaneously. Then either $\chi(\mu)=1$ or $\alpha^2=\alpha-1$.

Proof. Let $b'=b+a\mu-f$, $d'=d+a\mu-f$, and $f'=a\mu$. By block transitivity, $\{b',d',f'\}$ is a block in $\mathcal{B}$. Furthermore, (4) implies $\{b',d',f'\}=\{a\mu,g\mu,h\mu\}$. Hence the result follows from Lemma 2.2. □

3 Tripling and product constructions

The following theorem is our main tool in establishing the existence of an infinite number of 6-sparse Steiner triple systems.

Theorem 3.1 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α, and $V = GF(v)$. Put $V' = V \times \{0, 1, 2\}$ and let*

$$\begin{aligned} \mathcal{B}' &= \{\{a_i, b_i, c_i\} : \{a, b, c\} \in \mathcal{B},\ i = 0, 1, 2\} \\ &\cup\ \{\{x_0, y_1, (x\beta + y\gamma)_2\} : x, y \in GF(v)\}, \end{aligned}$$

where $\beta, \gamma \neq 0$ are fixed parameters in $GF(v)$. Then $S' = (V', \mathcal{B}')$ is a Steiner triple system of order $3v$. Furthermore

(i) if S is anti-Pasch, then S' is also anti-Pasch;

(ii) if S is anti-mitre, $\alpha^2 \neq \alpha - 1$, and $\chi(\beta), \chi(\gamma), \chi(-\beta/\gamma) \neq 1$, then S' is also anti-mitre;

(iii) if S has no crowns and $\alpha^2 \notin \{1 - \alpha, \alpha + 1, 3\alpha - 1\}$, then S' also has no crowns;

(iv) if S has no 6-cycles, $\alpha^2 \neq \alpha - 1$, and $\chi(\beta), \chi(\gamma), \chi(-\beta/\gamma) \neq -1$, then S' also has no 6-cycles.

As a consequence, if S is 6-sparse, $\alpha^2 \notin \{\alpha - 1, 1 - \alpha, \alpha + 1, 3\alpha - 1\}$, and $\chi(\beta), \chi(\gamma), \chi(\beta/\gamma) \neq \pm 1$, then S' is also 6-sparse.

Proof. It is worth remarking that the conditions on β and γ in the final sentence can be achieved, for example, by taking $\beta = \alpha$ and $\gamma = 1/\alpha$. It is easily verified that if β and γ are non-zero modulo v, the operation defined by $x \circ y = x\beta + y\gamma$ satisfies the axioms of a quasigroup. The construction itself is an application of the generalized direct product (see [4] page 39, for example), and so S' is an STS($3v$).

If x_i is a point of V', we refer to i as the *level* of x_i. We describe a block of $\mathcal{B}'$ as *horizontal* if all of its points have the same level; otherwise we describe it as *vertical*. A vertical block contains a point at each of the three levels 0, 1 and 2.

For each of the Pasch, mitre, crown, and 6-cycle configurations, we assume that S, but not S', is free of that configuration, and we deduce a contradiction. The arguments are independent of each other.

Case (i) The Pasch configuration.

Suppose $\mathcal{C}$ is a Pasch configuration in S'. It is easy to show that if $\mathcal{C}$ has a horizontal block, then all blocks of $\mathcal{C}$ are horizontal, contrary to the hypothesis that S does not contain a Pasch configuration. Therefore C has no horizontal blocks. Indeed, by exploiting the symmetry of the Pasch configuration, we can assume that

$$\mathcal{C} = \{\{a_0, b_1, c_2\}, \{a_0, e_1, d_2\}, \{f_0, b_1, d_2\}, \{f_0, e_1, c_2\}\}.$$

Then $c = a\beta + b\gamma = f\beta + e\gamma$ and $d = a\beta + e\gamma = f\beta + b\gamma$. Hence $(b-e)\gamma = (e-b)\gamma$ and therefore $b_1 = e_1$, a contradiction.

Case (ii) The mitre.

Suppose $\mathcal{D}$ is a mitre in S'. It is straightforward to verify that the number of horizontal blocks containing the apex (i.e. the unique point of degree 3 in this configuration) of $\mathcal{D}$ is either zero or one.

Case (ii.a) No horizontal block contains the apex.

The two disjoint blocks must be horizontal. We consider three cases according to the level of the apex.

If the apex has level 0, we can assume that

$$\mathcal{D} = \{\{a_0, b_1, e_2\}, \{a_0, c_1, f_2\}, \{a_0, d_1, g_2\}, \{b_1, c_1, d_1\}, \{e_2, f_2, g_2\}\}.$$

Then $e = a\beta + b\gamma$, $f = a\beta + c\gamma$, $g = a\beta + d\gamma$. By block transitivity, $\{b\gamma, c\gamma, d\gamma\} = \{e - a\beta, f - a\beta, g - a\beta\} \in \mathcal{B}$. But by Lemma 2.2 this implies $\chi(\gamma) = 1$, a contradiction.

If the apex has level 1, we can assume that

$$\mathcal{D} = \{\{a_1, b_0, e_2\}, \{a_1, c_0, f_2\}, \{a_1, d_0, g_2\}, \{b_0, c_0, d_0\}, \{e_2, f_2, g_2\}\}.$$

Then $e = b\beta + a\gamma$, $f = c\beta + a\gamma$, $g = d\beta + a\gamma$ and $\{b\beta, c\beta, d\beta\} = \{e - a\gamma, f - a\gamma, g - a\gamma\} \in \mathcal{B}$; hence by Lemma 2.2 $\chi(\beta) = 1$, a contradiction.

If the apex has level 2, we can assume that

$$\mathcal{D} = \{\{a_2, b_0, e_1\}, \{a_2, c_0, f_1\}, \{a_2, d_0, g_1\}, \{b_0, c_0, d_0\}, \{e_1, f_1, g_1\}\}.$$

Then $a = b\beta + e\gamma = c\beta + f\gamma = d\beta + g\gamma$, $\{-b\beta/\gamma, -c\beta/\gamma, -d\beta/\gamma\} = \{e - a/\gamma, f - a/\gamma, g - a/\gamma\} \in \mathcal{B}$, and, again by Lemma 2.2, $\chi(-\beta/\gamma) = 1$, a contradiction.

Case (ii.b) One horizontal block contains the apex.

The two disjoint blocks must be vertical, and there are three sub-cases to consider.

If the horizontal block has level 0, we can assume that

$$\mathcal{D} = \{\{a_0, b_0, e_0\}, \{a_0, c_1, f_2\}, \{a_0, d_2, g_1\}, \{b_0, c_1, d_2\}, \{e_0, f_2, g_1\}\}.$$

Then $d = a\beta + g\gamma = b\beta + c\gamma$ and $f = a\beta + c\gamma = e\beta + g\gamma$.

If the horizontal block has level 1, we can assume that

$$\mathcal{D} = \{\{a_1, b_1, e_1\}, \{a_1, c_0, f_2\}, \{a_1, d_2, g_0\}, \{b_1, c_0, d_2\}, \{e_1, f_2, g_0\}\}.$$

Then $d = g\beta + a\gamma = c\beta + b\gamma$ and $f = c\beta + a\gamma = g\beta + e\gamma$.

If the horizontal block has level 2, we can assume that

$$\mathcal{D} = \{\{a_2, b_2, e_2\}, \{a_2, c_0, f_1\}, \{a_2, d_1, g_0\}, \{b_2, c_0, d_1\}, \{e_2, f_1, g_0\}\}.$$

Then $a = c\beta + f\gamma = g\beta + d\gamma$, $b = c\beta + d\gamma$ and $e = g\beta + f\gamma$.

In each of these three sub-cases we have $a - b = e - a$, a contradiction, since, by transitivity, the block $\{a, b, e\}$ of S cannot have identical differences $a - b$ and $e - a$.

Case (iii) The crown.

Let $\{\{a', b', c'\}, \{a', d', e'\}, \{b', d', f'\}, \{c', d', g'\}, \{b', e', h'\}, \{f', g', h'\}\}$ be a crown in S'. It is easy to see that $\{c', d', g'\}$ and $\{b', e', h'\}$ must be horizontal blocks at different levels and that all other blocks must be vertical. There are six possible combinations of the levels of these horizontal blocks, but consideration may be reduced to three by noting that $\pi = (b'\ d')(c'\ e')(g'\ h')$ is an automorphism of the crown which exchanges $\{c', d', g'\}$ and $\{b', e', h'\}$.

If the horizontal blocks are $\{c_0, d_0, g_0\}$ and $\{b_1, e_1, h_1\}$ (corresponding to $\{c', d', g'\}$ and $\{b', e', h'\}$, respectively) and the other points are a_2 and f_2 (corresponding to a' and f'), then $a = c\beta + b\gamma = d\beta + e\gamma$ and $f = g\beta + h\gamma = d\beta + b\gamma$. Hence $b - e = (d - c)\beta/\gamma$ and $h - b = (d - g)\beta/\gamma$.

If the horizontal blocks are $\{c_0, d_0, g_0\}$ and $\{b_2, e_2, h_2\}$ and the other points are a_1 and f_1, then $b = c\beta + a\gamma = d\beta + f\gamma$, $e = d\beta + a\gamma$ and $h = g\beta + f\gamma$. Hence $b - e = -(d - c)\beta$ and $h - b = -(d - g)\beta$.

If the horizontal blocks are $\{c_1, d_1, g_1\}$ and $\{b_2, e_2, h_2\}$ and the other points are a_0 and f_0, then $b = a\beta + c\gamma = f\beta + d\gamma$, $e = a\beta + d\gamma$ and $h = f\beta + g\gamma$. Hence $b - e = -(d - c)\gamma$ and $h - b = -(d - g)\gamma$.

In each of these three cases we obtain a contradiction by Lemma 2.3.

Case (iv) The 6-cycle.

Let $\{\{a',b',c'\},\{a',d',e'\},\{b',d',f'\},\{c',f',h'\},\{e',f',g'\},\{a',g',h'\}\}$ be a 6-cycle in S'. It is straightforward to show that either there are precisely two horizontal blocks at different levels, or all blocks are vertical.

Case (iv.a) Two horizontal blocks at different levels.

By symmetry we may assume that the horizontal blocks are $\{a',g',h'\}$ and $\{b',d',f'\}$. There are six possible combinations for the two levels involved but, again by symmetry, consideration can be reduced to three.

If the horizontal blocks are $\{a_0,g_0,h_0\}$ and $\{b_1,d_1,f_1\}$, let the other points be c_2 and e_2. Then $c=a\beta+b\gamma=h\beta+f\gamma$ and $e=a\beta+d\gamma=g\beta+f\gamma$. Hence $b-d=(h-g)\beta/\gamma$ and $b-f=(h-a)\beta/\gamma$.

If the horizontal blocks are $\{a_0,g_0,h_0\}$ and $\{b_2,d_2,f_2\}$, let the other points be c_1 and e_1. Then $b=a\beta+c\gamma$, $d=a\beta+e\gamma$ and $f=h\beta+c\gamma=g\beta+e\gamma$. Hence $b-d=-(h-g)\beta$ and $b-f=-(h-a)\beta$.

If the horizontal blocks are $\{a_1,g_1,h_1\}$ and $\{b_2,d_2,f_2\}$, let the other points be c_0 and e_0. Then $b=c\beta+a\gamma$, $d=e\beta+a\gamma$ and $f=c\beta+h\gamma=e\beta+g\gamma$. Hence $b-d=-(h-g)\gamma$ and $b-f=-(h-a)\gamma$.

In each of these three cases we obtain a contradiction by Lemma 2.4, since none of $\chi(\beta/\gamma),\chi(-\beta),\chi(-\gamma)$ takes the value 1.

Case (iv.b) There are no horizontal blocks.

It is easy to show that the two points of degree 3, a' and f', are at the same level. There are then three possibilities.

If the points of degree 3 have level 0, we may assume that the 6-cycle is

$$\{\{a_0,b_2,c_1\},\{a_0,d_1,e_2\},\{b_2,d_1,f_0\},\{c_1,f_0,h_2\},\{e_2,f_0,g_1\},\{a_0,g_1,h_2\}\}.$$

Then $b=a\beta+c\gamma=f\beta+d\gamma$, $e=a\beta+d\gamma=f\beta+g\gamma$ and $h=a\beta+g\gamma=f\beta+c\gamma$. Hence $c=d=g$, a contradiction since c_1, d_1 and g_1 are at the same level.

If the points of degree 3 have level 1, we may assume that the 6-cycle is

$$\{\{a_1,b_2,c_0\},\{a_1,d_0,e_2\},\{b_2,d_0,f_1\},\{c_0,f_1,h_2\},\{e_2,f_1,g_0\},\{a_1,g_0,h_2\}\}.$$

Then $b=c\beta+a\gamma=d\beta+f\gamma$, $e=d\beta+a\gamma=g\beta+f\gamma$, $h=g\beta+a\gamma=c\beta+f\gamma$ and, again, $c=d=g$, a contradiction.

If the points of degree 3 have level 2, we may assume that the 6-cycle is

$$\{\{a_2,b_1,c_0\},\{a_2,d_0,e_1\},\{b_1,d_0,f_2\},\{c_0,f_2,h_1\},\{e_1,f_2,g_0\},\{a_2,g_0,h_1\}\}.$$

Then $a=c\beta+b\gamma=d\beta+e\gamma=g\beta+h\gamma$, $f=d\beta+b\gamma=c\beta+h\gamma=g\beta+e\gamma$. Hence $b=e=h$, a contradiction, and this completes the proof. □

It is worth remarking that with minor changes the argument employed in case (iv.b) works for any k-cycle configuration where $k \geq 6$ is even. Moreover, if $\mathcal{C}$ is a k-cycle and $k \not\equiv 0 \pmod 6$, it is not possible to assign levels 0, 1 and 2 to the points of $\mathcal{C}$ in the manner described above unless either all blocks of $\mathcal{C}$ are horizontal at the same level, or all blocks of $\mathcal{C}$ are vertical. Hence, recalling that the Pasch configuration is a 4-cycle, we have the following extension of Theorem 3.1: *For $k \not\equiv 0 \pmod 6$, if S has no k-cycles then S' also has no k-cycles.*

The next theorem is also an extension of Theorem 3.1, to a product construction.

Theorem 3.2 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α, and $V = GF(v)$. Suppose also that $S^* = (W, \mathcal{B}^*)$ is a Steiner triple system of order w. For each block of $\mathcal{B}^*$ arbitrarily fix the order of the points, so that $\mathcal{B}^*$ may be regarded as a set of ordered triples (i, j, k) . Put $V' = V \times W$ and let*

$$\begin{aligned} \mathcal{B}' &= \{\{a_i, b_i, c_i\} : \{a, b, c\} \in \mathcal{B}, i \in W\} \\ &\quad \cup \ \{\{x_i, y_j, (x\beta + y\gamma)_k\} : x, y \in GF(v), \ (i, j, k) \in \mathcal{B}^*\}, \end{aligned}$$

where $\beta, \gamma \neq 0$ are fixed parameters in $GF(v)$. Then $S' = (V', \mathcal{B}')$ is a Steiner triple system of order vw. Furthermore

(i) if both S and S^* are anti-Pasch, then S' is also anti-Pasch;

(ii) if both S and S^* are anti-mitre, $\alpha^2 \neq \alpha - 1$, and $\chi(\beta), \chi(\gamma), \chi(-\beta/\gamma) \neq 1$, then S' is also anti-mitre;

(iii) if both S and S^* have no crowns and $\alpha^2 \notin \{1 - \alpha, \alpha + 1, 3\alpha - 1\}$, then S' also has no crowns;

(iv) if both S and S^* have no 6-cycles, $\alpha^2 \neq \alpha - 1$, and $\chi(\beta), \chi(\gamma), \chi(-\beta/\gamma) \neq -1$, then S' also has no 6-cycles.

As a consequence, if both S and S^* are 6-sparse,

$$\alpha^2 \notin \{\alpha - 1, 1 - \alpha, \alpha + 1, 3\alpha - 1\}, \tag{5}$$

and $\chi(\beta), \chi(\gamma), \chi(\beta/\gamma) \neq \pm 1$, then S' is also 6-sparse.

Proof. As in the previous theorem, the construction itself is an application of the generalized direct product, and so S' is an STS(vw). If x_i is a point of S', $x \in V, i \in W$, we refer to i as the *level* of x_i. As before, a block of S' is *horizontal* if all of its points have the same level; otherwise it is *vertical*. The elements of a vertical block have distinct levels which, as points of W, form a block of S^*.

Suppose that $\mathcal{C}$ is one of the configurations in question (Pasch, mitre, crown or 6-cycle) and that $\mathcal{C}$ is present in S' but not in S and S^*. Let

$$\mathcal{C}^* = \{\{i,j,k\} : \{x_i, y_j, z_k\} \in \mathcal{C},\ i \neq j\}.$$

Clearly, S^* contains $\mathcal{C}^*$ and therefore if $\mathcal{C}^* \cong \mathcal{C}$, we have a contradiction. Also, if $\mathcal{C}^*$ is a single block, we can relabel it as $\{0,1,2\}$ and then the proof of this theorem proceeds exactly as in Theorem 3.1. We now establish that these are the only possibilities for each of the four configurations: Pasch, mitre, crown and 6-cycle.

Case (i) The Pasch configuration.

As in Theorem 3.1 we can assume that all blocks of $\mathcal{C}$ are vertical. Then it is easy to see that either $|\mathcal{C}^*| = 1$ or $\mathcal{C}^* \cong \mathcal{C}$.

Case (ii) The mitre.

Either the two parallel blocks of the mitre are horizontal, or there is precisely one horizontal block, which contains the point of degree 3, or all blocks are vertical. In the first two cases $|\mathcal{C}^*| = 1$ and in the third case $\mathcal{C}^* \cong \mathcal{C}$.

Case (iii) The crown.

Let $\{\{a',b',c'\}, \{a',d',e'\}, \{b',d',f'\}, \{c',d',g'\}, \{b',e',h'\}, \{f',g',h'\}\}$ be a crown in S'. We can assume that either $\{c',d',g'\}$ and $\{b',e',h'\}$ are horizontal blocks at different levels and all other blocks are vertical, or all six blocks are vertical. In the former case $|\mathcal{C}^*| = 1$; in the latter case $\mathcal{C}^* \cong \mathcal{C}$.

Case (iv) The 6-cycle.

Either there are precisely two horizontal blocks at different levels, or all blocks are vertical. In the former case $|\mathcal{C}^*| = 1$; in the latter case either $|\mathcal{C}^*| = 1$ or $\mathcal{C}^* \cong \mathcal{C}$. This completes the proof. □

By applying the previous two theorems to the 6-sparse systems identified in section 2, we can prove the following.

Theorem 3.3 *There are infinitely many 6-sparse Steiner triple systems.*

Proof. It is easily verified that property (5) holds for each of the systems listed in Table 2. Therefore we can repeatedly apply Theorem 3.2, choosing, for example, $\beta = \alpha$ and $\gamma = 1/\alpha$. □

In fact, it is easy to see that Theorems 3.1 and 3.2 may be used to construct 6-sparse systems for all orders v of the form $v = 3^{j_0} \prod_{i=1}^{27} (v_i)^{j_i}$, where $j_0 = 0$ or 1, $j_i \geq 0$ for $i = 1, 2, \ldots, 27$, and $v_1, v_2, \ldots, v_{27}$ are the 27 distinct orders (i.e. $139, 151, \ldots, 4447$) given in Table 2.

4 The scope of the basic construction

In the previous section we have proved two theorems which have enabled us to construct infinitely many 6-sparse Steiner triple systems, using the 29 block transitive systems obtained by computation as described in section 2. In this section we study the scope of the basic construction method given in section 2 for the production of both 6-sparse and perfect systems. In particular, we prove that the list of 6-sparse systems given in Table 2 is a complete list of the systems obtainable using this method, by showing that the construction produces no 6-sparse STS(v)s with $v > 9\,150\,625$. By a similar method we show that there exists v^* such that the construction produces no perfect STS(v)s with $v > v^*$. The former result relies on proving the existence of a mitre, and the latter on proving the existence of a 12-cycle, in (almost) all sufficiently large systems.

In order to establish these results, we make use of the following theorem which is a consequence of a result of Weil.

Theorem 4.1 *Let χ be a multiplicative character of order $m > 1$ of $GF(q)$, and suppose that the polynomial $f(x)$ over $GF(q)$ has d distinct zeros in the algebraic closure of $GF(q)$ and is not a constant multiple of an m^{th} power. Then*

$$\left| \sum_{x \in GF(q)} \chi(f(x)) \right| \leq (d-1)q^{1/2}.$$

Proof. See [14], page 43. □

We now use this result to establish a useful lemma.

Lemma 4.1 *Suppose that v is prime and that χ is a multiplicative character of $GF(v)$ of order 6. Suppose also that $f_1(x), f_2(x), \ldots, f_n(x)$ are polynomials over $GF(v)$ of degree 1 in x, having distinct roots $\rho_1, \rho_2, \ldots, \rho_n$ respectively, with the additional property that for each i $(1 \le i \le n)$ there exists j $(1 \le j \le n)$ for which $\chi(f_j(\rho_i)) \ne 1$. Then if*

$$v > \left(\sum_{k=2}^{n}(k-1)\binom{n}{k}5^k\right)^2 = \left(6^{n-1}(5n-6)+1\right)^2, \tag{6}$$

there exists $x \in GF(v)$ such that

$$\chi(f_1(x)) = \chi(f_2(x)) = \ldots = \chi(f_n(x)) = 1. \tag{7}$$

Proof. Observe first that the possible values of $\chi(x)$ are the six sixth roots of unity when $x \ne 0$, and $\chi(0) = 0$. Put

$$\pi(x) = \left(\sum_{i_1=0}^{5}\chi(f_1(x)^{i_1})\right)\left(\sum_{i_2=0}^{5}\chi(f_2(x)^{i_2})\right)\ldots\left(\sum_{i_n=0}^{5}\chi(f_n(x)^{i_n})\right).$$

If (7) holds then $\pi(x) = 6^n$, while if $\chi(f_j(x)) \ne 1$ (including the possibility that $x = \rho_j$) then $\pi(x) = 0$. Thus $\pi(x) \ne 0$ if and only if (7) holds.

Next put $\Delta = \sum_{x \in GF(v)} \pi(x)$. Note that if we can prove that $\Delta \ne 0$ then it will follow that there exists an $x \in GF(v)$ which satisfies (7). But $\pi(x)$ has the form

$$\pi(x) = 1 + \sum_{\substack{i_1,i_2,\ldots,i_n=0 \\ i_1+i_2+\ldots+i_n \ne 0}}^{5} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}).$$

So

$$\Delta = v + \sum_{\substack{i_1,i_2,\ldots,i_n=0 \\ i_1+i_2+\ldots+i_n \ne 0}}^{5} \sum_{x \in GF(v)} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}).$$

Since the $f_i(x)$ are all first order polynomials in x with distinct roots, a product of the form $(f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n}$ with $0 \le i_1, i_2, \ldots, i_n \le 5$ cannot be a constant multiple of a sixth power of a polynomial in x unless $i_1 = i_2 = \ldots = i_n = 0$. Hence, by Theorem 4.1 and provided that $i_1 + i_2 + \ldots + i_n \ne 0$, we have

$$\left|\sum_{x \in GF(v)} \chi((f_1(x))^{i_1}(f_2(x))^{i_2}\ldots(f_n(x))^{i_n})\right| \le (r_{i_1,i_2,\ldots,i_n} - 1)\sqrt{v},$$

where $r_{i_1,i_2,\ldots,i_n}$ is the number of distinct roots of $f_1^{i_1} f_2^{i_2} \ldots f_n^{i_n}$ in $GF(v)$. But $r_{i_1,i_2,\ldots,i_n}$ is precisely the number of non-zero indices amongst $\{i_1, i_2, \ldots, i_n\}$ in the expression $\chi((f_1(x))^{i_1}(f_2(x))^{i_2} \ldots (f_n(x))^{i_n})$. Hence

$$|\Delta| \geq v - \sum_{k=2}^{n} (k-1) \binom{n}{k} 5^k \sqrt{v}.$$

This is strictly positive if (6) holds. □

With the aid of the preceding lemma we can prove the following theorem.

Theorem 4.2 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. Then if $v > 9\,150\,625$ and $\alpha^2 - \alpha + 1 \neq 0$, S contains a mitre.*

Proof. Consider the following five sets of points.

$$\begin{gathered}
\{0, 1, \alpha\}, \\
\{0, x, \alpha x\} = x\{0, 1, \alpha\}, \\
\{\alpha x, 1, \alpha + \alpha x - \alpha^2 x\} = (1 - \alpha x)\{0, 1, \alpha\} + \alpha x, \\
\left\{\frac{\alpha(1-\alpha x)}{1-\alpha}, \alpha x, \alpha\right\} = \left(\frac{\alpha(x-1)}{1-\alpha}\right)\{0, 1, \alpha\} + \frac{\alpha(1-\alpha x)}{1-\alpha}, \\
\left\{\frac{\alpha(1-\alpha x)}{1-\alpha}, x, \alpha + \alpha x - \alpha^2 x\right\} = \left(\frac{(\alpha^2 - \alpha + 1)x - \alpha}{1-\alpha}\right)\{0, 1, \alpha\} + \frac{\alpha(1-\alpha x)}{1-\alpha}.
\end{gathered}$$

These are five distinct blocks of S provided that x is selected to satisfy the following relationships.

$$\chi(x) = 1,\ \chi(1-\alpha x) = 1,\ \chi\left(\frac{\alpha(x-1)}{1-\alpha}\right) = 1,\ \chi\left(\frac{(\alpha^2-\alpha+1)x-\alpha}{1-\alpha}\right) = 1.$$

So put $f_1(x) = x,\ f_2(x) = 1 - \alpha x,\ f_3(x) = \frac{\alpha(x-1)}{1-\alpha},\ f_4(x) = \frac{(\alpha^2-\alpha+1)x-\alpha}{1-\alpha}$. Then, provided that $\alpha^2 - \alpha + 1 \neq 0$, each $f_i(x)$ is a polynomial of degree 1 in x. These four polynomials have the distinct roots $\rho_1 = 0,\ \rho_2 = \frac{1}{\alpha},\ \rho_3 = 1,\ \rho_4 = \frac{\alpha}{\alpha^2-\alpha+1}$. It is also easy to verify that for each i there exists j with $\chi(f_j(\rho_i)) \neq 1$. For example, $f_3(\rho_4) = (\alpha - 1)f_1(\rho_4)$, so either for $j = 1$ or for $j = 3$ we have $\chi(f_j(\rho_4)) \neq 1$. By applying the previous lemma, we find that there exists a suitable $x \in GF(v)$ provided that $v > (6^3 \cdot 14 + 1)^2 = 3025^2 = 9\,150\,625$. But then the five blocks form a mitre in S and the proof is complete. □

Corollary 4.2.1 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. Then if $v > 9\,150\,625$, S is not 6-sparse.*

Proof. In view of Theorem 4.2 it is only necessary to consider the case when $\alpha^2 - \alpha + 1 = 0$. Then α is a primitive sixth root of unity (which entails $v \not\equiv 19 \pmod{36}$) and the system S is the so-called Netto system described in [15, 4]. It is shown in [15] that such systems contain Pasch configurations when $v \equiv 7 \pmod{24}$, and in [9], using a result from [15], it is shown that such systems contain 6-cycles when $v \equiv 19 \pmod{24}$. □

The heuristic method by which the mitre of Theorem 4.2 was found can be used to search for a variety of configurations. To explain it, consider a mitre in a block transitive system S with parameter α. We may assume that the mitre has the blocks $\{0, 1, \alpha\}, \{a, b, c\}, \{0, a, d\}, \{1, b, d\}, \{\alpha, c, d\}$. First take permutations $\pi_1, \pi_2, \pi_3, \pi_4$ on three symbols. Then set up the four vector equations

$$\begin{aligned}
(a, b, c) &= \mu_1(\pi_1(0, 1, \alpha)) + \nu_1, \\
(0, a, d) &= \mu_2(\pi_2(0, 1, \alpha)) + \nu_2, \\
(1, b, d) &= \mu_3(\pi_3(0, 1, \alpha)) + \nu_3, \\
(\alpha, c, d) &= \mu_4(\pi_4(0, 1, \alpha)) + \nu_4.
\end{aligned}$$

Here we have twelve linear equations and twelve unknowns $(a, b, c, d, \{\mu_i\}, \{\nu_i\})$. It can happen that, for certain of the 6^4 choices of the permutations π_i, the equations are indeterminate and have a free parameter, say x. If we then express each μ_i in terms of x and if we can impose the condition $\chi(\mu_i) = 1$ for each i, then the blocks of the mitre will lie in S.

We have applied this method to prove the existence of 12-cycles in almost all sufficiently large block transitive systems which arise from the construction of section 2. The results are contained in the next two lemmas. Both lemmas involve the quantity 4 290 908 300 250 625 which we denote by v^*. We have tried the same approach with k-cycles for $k = 4, 6, 8$ and 10 without success.

Lemma 4.2 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. If $v > v^*$ and if all of $\alpha^2 - \alpha + 1$, $\alpha^2 - 3\alpha + 1$, $1 - 3\alpha$, $3 - \alpha$ are non-zero, then S contains a 12-cycle.*

Proof. The blocks of the 12-cycle will be denoted by $\mathbf{b}_i$ for $i = 1, 2, \ldots, 12$, where $\mathbf{b}_1 = \{0, z_1, z_2\}$, $\mathbf{b}_2 = \{a, z_2, z_3\}$, $\mathbf{b}_3 = \{0, z_3, z_4\}, \ldots,$ $\mathbf{b}_{12} = \{a, z_{12}, z_1\}$. The point a and the twelve points z_i are given in terms of a parameter x as follows.

$$\begin{aligned}
&a = (1-\alpha)x + \alpha, \quad z_1 = 1, \quad z_2 = \alpha, \quad z_3 = \alpha - \alpha x, \quad z_4 = 1 - x,\\
&z_5 = \frac{2(1-\alpha)x}{\alpha} + \frac{2\alpha - 1}{\alpha}, \quad z_6 = -2x + \frac{2\alpha - 1}{\alpha - 1},\\
&z_7 = -\frac{(\alpha+1)x}{\alpha - 1} + \frac{\alpha^2}{(\alpha-1)^2}, \quad z_8 = -\frac{\alpha(\alpha+1)x}{\alpha - 1} + \frac{\alpha^3}{(\alpha-1)^2},\\
&z_9 = 2\alpha x - \frac{\alpha^2}{\alpha - 1}, \quad z_{10} = 2\alpha(1-\alpha)x + \alpha^2, \quad z_{11} = \alpha x, \quad z_{12} = x.
\end{aligned}$$

Each block $\mathbf{b}_i$ can be expressed as $\mu_i\{0, 1, \alpha\} + \nu_i$ where the values of μ_i are as follows.

$$\begin{aligned}
&\mu_1 = 1, \quad \mu_2 = x, \quad \mu_3 = 1 - x, \quad \mu_4 = \frac{(2-\alpha)x}{\alpha} + \frac{\alpha - 1}{\alpha},\\
&\mu_5 = \frac{2x}{\alpha} + \frac{1 - 2\alpha}{\alpha(\alpha - 1)}, \quad \mu_6 = -\frac{(\alpha-3)x}{\alpha - 1} + \frac{\alpha^2 - 3\alpha + 1}{(\alpha-1)^2},\\
&\mu_7 = -\frac{(\alpha+1)x}{\alpha - 1} + \frac{\alpha^2}{(\alpha-1)^2}, \quad \mu_8 = \frac{(3\alpha-1)x}{\alpha - 1} + \frac{\alpha - 2\alpha^2}{(\alpha-1)^2},\\
&\mu_9 = -2\alpha x + \frac{\alpha^2}{\alpha - 1}, \quad \mu_{10} = (1-2\alpha)x + \alpha, \quad \mu_{11} = x, \quad \mu_{12} = 1 - x.
\end{aligned}$$

Thus the 12 blocks will lie in the system S provided that $\chi(\mu_i) = 1$ for each i. So take $f_i(x) = \mu_{i+1}$ for $i = 1, 2, \ldots, 9$. The reader can check that the conditions on α ensure that these nine functions of x are polynomials of degree 1 having distinct roots ρ_i with the additional property that for each i there exists j for which $\chi(f_j(\rho_i)) \neq 1$. Although this is lengthy and tedious, it is straightforward, and we leave the details to the reader. It may be helpful to point out that two particular conditions encountered in the checking process, namely $1 - 3\alpha + 2\alpha^2 - \alpha^3 \neq 0$ and $1 - 2\alpha + 3\alpha^2 - \alpha^3 \neq 0$, follow from the facts that neither $\chi(\alpha)$ nor $\chi(\alpha^2)$ can equal ± 1, and so $\alpha \neq (\alpha - 1)^3$ and $\alpha^2 \neq (\alpha - 1)^3$. It is also necessary to verify that the 12 blocks are distinct. An effective method for doing this is to show first that $a \neq 0$. This follows from the fact that if $a = 0$ then $x = -\alpha/(1-\alpha)$, and this leads to a contradiction between the conditions on α and the assumption that $\chi(x) = \chi(\mu_2) = 1$. It then follows that the six odd-numbered blocks are distinct from the six even-numbered blocks. It is also easy to show that for any i, $\mathbf{b}_i \neq \mathbf{b}_{i+2}$ (subscript

arithmetic modulo 12), that $\mathbf{b}_i = \mathbf{b}_{i+4}$ if and only if $z_j = z_{j+4}$ for each j, and that $\mathbf{b}_i = \mathbf{b}_{i+6}$ if and only if $z_j = z_{j+6}$ for each j. Since the pair of equations $z_1 = z_5, z_2 = z_6$ lead to a contradiction as does the pair $z_1 = z_7, z_6 = z_{12}$, it then follows that the 12 blocks are distinct. Finally, applying Lemma 4.1, we find that a suitable x may be chosen provided that $v > (6^8 \cdot 39 + 1)^2 = v^*$. □

Lemma 4.3 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. If $v > v^*$ and if all of $\alpha^2 - \alpha + 1,\ \alpha^2 + \alpha - 1,\ 2 - 3\alpha,\ 2 + \alpha$ are non-zero, then S contains a 12-cycle.*

Proof. The proof is similar to that of the previous lemma. We take

$$
\begin{aligned}
&a = \alpha x - \frac{1}{\alpha - 1}, \quad z_1 = 1, \quad z_2 = \alpha, \quad z_3 = (\alpha - 1)x + \frac{\alpha - 1}{\alpha},\\
&z_4 = -x - \frac{1}{\alpha}, \quad z_5 = -\frac{2\alpha x}{\alpha - 1} + \frac{2 - \alpha}{(\alpha - 1)^2}, \quad z_6 = 2\alpha x + \frac{\alpha - 2}{\alpha - 1},\\
&z_7 = (\alpha + 1)x - \frac{1}{\alpha(\alpha - 1)}, \quad z_8 = -\frac{(\alpha + 1)x}{\alpha - 1} + \frac{1}{\alpha(\alpha - 1)^2},\\
&z_9 = -\frac{2\alpha^2 x}{(\alpha - 1)^2} + \frac{\alpha}{(\alpha - 1)^3}, \quad z_{10} = -\frac{2\alpha x}{\alpha - 1} + \frac{1}{(\alpha - 1)^2},\\
&z_{11} = -x, \quad z_{12} = (\alpha - 1)x.
\end{aligned}
$$

These give

$$
\begin{aligned}
&\mu_1 = 1, \quad \mu_2 = -x + \frac{\alpha^2 - \alpha + 1}{\alpha(\alpha - 1)}, \quad \mu_3 = x + \frac{1}{\alpha},\\
&\mu_4 = \frac{(\alpha + 1)x}{\alpha - 1} - \frac{1}{\alpha(\alpha - 1)^2}, \quad \mu_5 = \frac{2\alpha x}{\alpha - 1} + \frac{\alpha - 2}{(\alpha - 1)^2},\\
&\mu_6 = x + \frac{1}{\alpha} = \mu_3, \quad \mu_7 = \frac{(\alpha + 1)x}{\alpha - 1} - \frac{1}{\alpha(\alpha - 1)^2} = \mu_4,\\
&\mu_8 = \frac{(\alpha^2 + 1)x}{(\alpha - 1)^2} - \frac{\alpha^2 - \alpha + 1}{\alpha(\alpha - 1)^3}, \quad \mu_9 = \frac{2\alpha x}{(\alpha - 1)^2} - \frac{1}{(\alpha - 1)^3},\\
&\mu_{10} = \frac{(\alpha + 1)x}{\alpha - 1} - \frac{1}{(\alpha - 1)^2}, \quad \mu_{11} = x, \quad \mu_{12} = -x + \frac{1}{\alpha - 1}.
\end{aligned}
$$

Now take the nine functions $f_i(x)$ to be the expressions μ_j with μ_1 and the replicated μ_6 and μ_7 excluded. The reader can again check that the conditions on α ensure that these nine functions of x are polynomials of degree 1 having distinct roots ρ_i with the additional property that for each i there exists j for which $\chi(f_j(\rho_i)) \neq 1$. To prove that the 12 blocks are distinct, we may

again argue that $a \neq 0$, and to see this consider the value of $\chi(\mu_3)$ when $x = 1/\alpha(\alpha - 1)$. The remainder of the argument is as in the previous lemma and, again applying Lemma 4.1, we find that a suitable x may be chosen provided that $v > (6^8 \cdot 39 + 1)^2 = v^*$. □

Theorem 4.3 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. If $v > v^*$ and if $\alpha^2 - \alpha + 1 \neq 0$, then S contains a 12-cycle.*

Proof. This follows from the previous two lemmas. □

Corollary 4.3.1 *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v with parameter α. If $v > v^*$, then S is not perfect.*

Proof. By the previous theorem, the result is true unless $\alpha^2 - \alpha + 1 = 0$. But in this exceptional case, as noted in Corollary 4.2.1, the system has either a 4-cycle or a 6-cycle. □

The bound v^* given in the preceding corollary is likely to be very much too large. We have checked for being perfect all systems obtained from the construction of section 2 up to $v = 760\,000$. In addition to the perfect systems identified in [9], we have found just one further perfect system at $v = 135\,859$ given by the parameter $\alpha = 49\,142$. We would not be surprised if this is the last perfect system which can be obtained by this method.

A related concept to a perfect Steiner triple system is that of a *uniform Steiner triple system*. This is a Steiner triple system in which the cycle graphs $G_{a,b}$ are all isomorphic. Perfect systems are uniform, but uniform systems are not necessarily perfect. We have also checked for uniformity all systems obtained from the construction of section 2, up to $v = 470\,000$. In addition to the four uniform (but not perfect) systems listed in [9], we have discovered a new uniform system at $v = 180\,907$ given by the parameter $\alpha = 68\,356$, and having cycle structure $\{4, 12, 180\,888\}$.

These searches for perfect and uniform systems were made with variants of the program used for the 6-sparse search. Both searches were run from $v = 7$ upwards, verifying the results of [9] in passing.

References

[1] N. Alon, J.-H. Kim and J. Spencer, Nearly perfect matchings in regular simple hypergraphs, *Israel J. Math.* **100** (1997), 171–187.

[2] A. E. Brouwer, Steiner triple systems without forbidden subconfigurations, Mathematisch Centrum Amsterdam, ZW 104/77, 1977.

[3] C. J. Colbourn, E. Mendelsohn, A. Rosa and J. Širáň, Anti-mitre Steiner triple systems, *Graphs Combin.* **10** (1994), 215–224.

[4] C. J. Colbourn and A. Rosa, *Triple systems*, Oxford University Press, New York 1999, ISBN 0-19-853576-7.

[5] P. Erdös, Problems and results in combinatorial analysis, *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973), Tomo II, pp. 3–17.* Atti dei Convegni Lincei, No. 17, *Accad. Naz. Lincei, Rome, 1976.*

[6] Y. Fujiwara, Constructions for anti-mitre Steiner triple systems, *J. Combin. Des.* **13** (2005), 286–291.

[7] Y. Fujiwara, Infinite classes of anti-mitre and 5-sparse Steiner triple systems, *J. Combin. Des.* **14** (2006) 237–250.

[8] M. J. Grannell, T. S. Griggs and E. Mendelsohn, A small basis for four-line configurations in Steiner triple systems, *J. Combin. Des.* **3** (1994), 51–59.

[9] M. J. Grannell, T. S. Griggs and J. P. Murphy, Some new perfect Steiner triple systems, *J. Combin. Des.* **7** (1999), 327–330.

[10] M. J. Grannell, T. S. Griggs and C. A. Whitehead, The resolution of the anti-Pasch conjecture, *J. Combin. Des.* **8** (2000), 300–309.

[11] T. S. Griggs, J. P. Murphy and J. S. Phelan, Anti-Pasch Steiner triple systems, *J. Combin. Inf. Syst. Sci.* **15** (1990), 79–84.

[12] A. C. H. Ling, A direct product construction for 5-Sparse Steiner triple systems, *J. Combin. Des.* **5** (1997), 443–447.

[13] A. C. H. Ling, C. J. Colbourn, M. J. Grannell and T. S. Griggs, Construction techniques for anti-Pasch Steiner triple systems, *J. London Math. Soc. (2)* **61** (2000), 641–657.

[14] W. M. Schmidt, *Equations over Finite Fields*, Lecture Notes in Mathematics **536**, Springer Verlag, Berlin 1976.

[15] R. M. Robinson, The structure of certain triple systems, *Math. Comp.* **29** (1975), 223–241.

[16] A. J. Wolfe, The resolution of the anti-mitre Steiner triple system conjecture, *J. Combin. Des.* **14** (2006), 229–236.

[17] A. J. Wolfe, 5-sparse Steiner triple systems of order n exist for almost all admissible n, *Electron. J. Combin.* **12** (2005), #R68, 42pp (electonic).

[18] A. J. Wolfe, Block transitive meager squares over $GF(q)$ for prime q, preprint, 2005, 15pp.