Further 6-sparse Steiner triple systems

A. D. Forbes[1], M. J. Grannell[2] and T. S. Griggs[3]

Department of Mathematics, The Open University, Walton Hall, Milton Keynes MK7 6AA, UK.
[1] e-mail: anthony.d.forbes@gmail.com
[2] e-mail: m.j.grannell@open.ac.uk
[3] e-mail: t.s.griggs@open.ac.uk

Abstract. We give a construction that produces 6-sparse Steiner triple systems of order v for all sufficiently large v of the form $3p$, p prime and $p \equiv 3 \pmod 4$. We also give a complete list of all 429 6-sparse systems with $v < 10000$ produced by this construction.

Key words. Steiner triple system, 6-sparse, Pasch configuration, mitre configuration, crown configuration.

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 $3 \pmod 6$. Such values are called *admissible*.

For any two points a and b in an STS(v), $(V, \mathcal{B})$, we define the *cycle graph* $G_{a,b}$ as follows. The vertex set of $G_{a,b}$ is $V \setminus \{a, b, a * b\}$, where we denote by $x * y$ the third point in a block containing the pair $\{x, y\}$. The edge set of $G_{a,b}$ is the set of pairs $\{x, y\}$ such that either $\{x, y, a\}$ is a block or $\{x, y, b\}$ is a block. Clearly, $G_{a,b}$ is a set of disjoint cycles $\{C_{n_1}, C_{n_2}, \ldots, C_{n_r}\}$, where $n_1 + n_2 + \ldots + n_r = v - 3$ and for $i = 1, 2, \ldots, r$, n_i is even and $n_i \geq 4$.

A *configuration* in the context of a Steiner triple system is a set of triples, also called blocks, 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 $\mathcal{D}$. For 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 of the configuration which contain that point. We sometimes write blocks with set brackets and commas omitted, so that for example $\{0, 1, 3\}$ might be written as 013.

In this paper we will be concerned with configurations having n blocks and $n+2$ points. Such configurations are of particular interest because of the following result proved in [4].

Table 1. Configurations having n blocks and $n+2$ points, $4 \leq n \leq 6$.

n	Name	Blocks	Comment
4	Pasch	012, 034, 135, 245	
5	mitre	012, 034, 135, 236, 456	
5		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

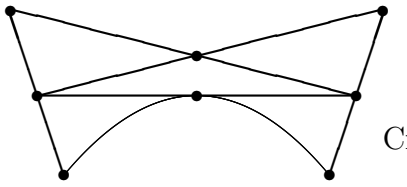
Theorem 1. *For every integer $d \geq 3$ and for every integer n satisfying $n \geq \lceil \frac{d}{2} \rceil$ there exists $v_0(n,d)$ such that for all admissible $v \geq v_0(n,d)$, every STS(v) contains a configuration having n blocks and $n+d$ points.*

Here, the value of d is sharp. For $d = 2$, the theorem does not hold. Indeed, the case $d = 2$ is the subject of a conjecture of Erdös [3]: *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 $4 \leq k' \leq k$.

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 [1], [8], [10] and [7].

There is, up to isomorphism, only one Pasch-free configuration having five blocks and seven points, namely the mitre. This is also shown in Table 1. In [2], [9] and [5], culminating in recent work by Fujiwara and Wolfe [6], [12], it is established that anti-mitre systems exist for all admissible orders except $v = 9$. Systems which are 5-sparse, that is, both anti-Pasch and anti-mitre, are known for $v \equiv 1, 19 \pmod{54}$, except possibly $v = 109$, and for many other sporadic values [9], [6]. Also we are aware that there exists a 5-sparse STS(109) [13]. Substantial further progress has recently been made by Wolfe in [14], where it is shown that 5-sparse STS(v)s exist for almost all admissible v (meaning arithmetic set density 1 in the set of all admissible orders), and in [15], where existence for all $v \equiv 3 \pmod{6}$ with $v \geq 21$ is established.

There are, up to isomorphism, two Pasch-free and mitre-free configurations having six blocks and eight points, of which one is the 6-cycle. The other configuration is called the *crown*, a word that is suggested by following diagram.



Crown configuration

Thus a system is 6-sparse if and only if it contains no Pasch configurations, no mitres, no 6-cycles and no crowns. In [4] we presented the first known non-trivial examples of 6-sparse Steiner triple systems. Our results depended on two basic theorems. The first of these is the following.

Theorem 2. *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).*

Using Theorem 2, we obtained 29 6-sparse systems with 27 different prime orders $v \equiv 7 \pmod{12}$. Furthermore, by employing Weil's theorem on bounding character sums [11, page 43] we were able to show that our list of such systems is complete.

The other theorem from [4] asserts that the standard product construction preserves 6-sparseness under certain conditions.

Theorem 3. *Suppose that $S = (V, \mathcal{B})$ is a block transitive Steiner triple system of order v, with α and χ as in Theorem 2 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*

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

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, if both S and S^* are 6-sparse, if

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

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

Having shown that (1) holds for each of our original 29 block transitive systems, we can repeatedly apply Theorem 3, choosing, for example, $\beta = \alpha$ and $\gamma = 1/\alpha$, to establish that there are infinitely many 6-sparse Steiner triple systems.

In this paper we prove a theorem analogous to Theorem 2 for the case $v = 3p$, where p is prime and $p \equiv 3 \pmod 4$. Using this theorem we are able to construct 6-sparse Steiner triple systems of order $3p$ for all sufficiently large primes $p \equiv 3 \pmod 4$.

2. Steiner triple systems with $v \equiv 9 \pmod{12}$

For the remainder of the paper, p will always denote a prime congruent to 3 modulo 4, and θ will denote the quadratic character modulo p. Thus if $x \not\equiv 0 \pmod p$, $\theta(x) = (x/p)$, the Legendre symbol, and if $x \equiv 0 \pmod p$, $\theta(x) = 0$.

Theorem 4. *Let $p = 2s + 1 \geq 7$ be a prime such that $p \equiv 3 \pmod 4$ and let $v = 3p$. Let τ be an integer modulo v such that $\tau \not\equiv 0 \pmod 3$ and τ is a primitive root modulo p. Let $\omega = \tau^2 \bmod v$. Choose α modulo v such that either (i) $\alpha \equiv 0 \pmod 3$ and $\theta(\alpha - 1) = 1$, or (ii) $\alpha \equiv 1 \pmod 3$ and $\theta(-\alpha) = 1$. Then, with all arithmetic modulo v,*

$$\begin{aligned}\{\{m, m + \omega^i, m + \alpha\omega^i\} : i = 0, 1, \ldots, s-1, m = 0, 1, \ldots, v-1\} \\ \cup \ \{\{n, n + \tfrac{1}{3}v, n + \tfrac{2}{3}v\} : n = 0, 1, \ldots, \tfrac{1}{3}v - 1\}\end{aligned}$$

is the set of blocks of an STS(v), defined on $\{0,1,\ldots,v-1\}$*, which is generated by* $\{0,1,\alpha\}$ *and* $\{0,v/3,2v/3\}$ *under the action of the group of mappings*

$$G \;=\; \{x \mapsto \omega^i\, x + m \bmod v,\;\; i = 0,1,\ldots,s-1,\;\; m = 0,1,\ldots,v-1\}.$$

Proof. In this proof and the remarks which follow we shall tacitly assume that unless otherwise specified all arithmetic is performed modulo v.

Clearly, the orbit of the starter block $\{0,p,2p\}$ under the action of G is $\{\{n,n+p,n+2p\} : n = 0,1,\ldots,p-1\}$. Let

$$\Omega(x) = \{x\,\omega^i \bmod v : i = 0,1,\ldots,s-1\}$$

and observe that for any x modulo v, we have

$$\theta(x\omega) = \theta(x), \qquad x\omega \equiv x \pmod 3$$

and

$$\Omega(x) = \{y \bmod v : \theta(y) = \theta(x) \text{ and } y \equiv x \pmod 3\}.$$

Therefore we can prove the theorem by showing that the six differences ± 1, $\pm\alpha$ and $\pm(1-\alpha)$ generated by the triple $\{0,1,\alpha\}$ have distinct combinations of quadratic character modulo p and residue class modulo 3. Since $\theta(-1) = -1$, this is possible if and only if α satisfies (i) or (ii) in the statement of the theorem. □

The choice of τ is immaterial, subject to $\tau \not\equiv 0 \pmod 3$ and τ being a primitive root modulo p. To see this, suppose $\tau' \not\equiv 0 \pmod 3$ is also a primitive root modulo p and let $\omega' = (\tau')^2$. Then $\tau' \equiv \tau^t \pmod p$ for some t with $(t, p-1) = 1$ and it is plain that for any x,

$$\Omega(x) = \{x\,(\omega')^i \bmod v : i = 0,1,\ldots,s-1\}.$$

If $\alpha \equiv 0 \pmod 3$, the four STS(v)s generated by the blocks $\{0,1,\delta\}$ and $\{0,v/3,2v/3\}$ for $\delta \in \{\alpha, 1-\alpha, 1/(1-\alpha), 1-1/(1-\alpha)\}$ are isomorphic under the mappings $x \mapsto 1-x$, $x \mapsto (x-1)/(\alpha-1)$ and $x \mapsto (\alpha-x)/(\alpha-1)$. If $\alpha \equiv 1 \pmod 3$, the four STS(v)s generated by the blocks $\{0,1,\delta\}$ and $\{0,v/3,2v/3\}$ for $\delta \in \{\alpha, 1-\alpha, 1/\alpha, 1-1/\alpha\}$ are isomorphic under the mappings $x \mapsto 1-x$, $x \mapsto x/\alpha$ and $x \mapsto 1-x/\alpha$.

The above observations may be used to reduce the size of a search for 6-sparse systems obtained from Theorem 4. A complete list, up to isomorphism, of such 6-sparse Steiner triple systems for $v < 10000$ is given in Table 2. Systems with the same value of v are pairwise non-isomorphic, as can be seen by examining the structure of the cycle graphs $G_{0,1}$, $G_{0,\alpha}$, $G_{1,\alpha}$ and $G_{0,v/3}$. We refer to a system created by Theorem 4 as a *two-generator system* with parameters v and α.

The special mitres and Pasch configurations that are shown in [4] to be unavoidable in all systems with sufficiently large order obtained from Theorem 2 do not form in the two-generator systems of Theorem 4. We now prove that there is no such blocking mechanism to prevent the formation of 6-sparse two-generator systems of arbitrarily large orders.

Theorem 5. *For all sufficiently large* v *with* $v = 3p$*,* p *prime and* $p \equiv 3 \pmod 4$*, there exists* α *such that the two-generator system of Theorem 4 with parameters* v *and* α *is 6-sparse.*

Table 2. 6-sparse systems with $v \equiv 9 \pmod{12}$

v	α	v	α	v	α	v	α	v	α	v	α	v	α
489	135	3837	880	5277	1377	6429	129	7977	1960	8637	919	9357	18
501	160	3849	1263	5277	1486	6429	1462	7977	2404	8637	1393	9357	390
1077	75	3909	544	5277	2074	6429	2097	7977	2944	8637	2046	9357	403
1101	379	3909	1063	5349	15	6537	915	7989	402	8637	2077	9357	1033
1149	328	3981	1627	5361	835	6537	1068	7989	657	8637	4141	9357	1516
1329	309	4101	265	5361	1075	6609	31	7989	2298	8661	490	9357	2152
1437	12	4101	427	5361	1377	6609	810	7989	3429	8661	1011	9357	2403
1461	13	4101	561	5469	84	6717	954	8013	348	8661	1254	9357	2643
1461	42	4281	204	5469	415	6753	1551	8013	496	8661	1918	9489	1048
1509	490	4317	201	5469	1114	6753	2184	8013	549	8661	2901	9489	1191
1569	232	4317	432	5469	1516	6861	385	8013	793	8709	42	9489	1809
1641	223	4317	658	5493	430	6861	604	8013	1009	8709	99	9489	4314
1689	276	4317	693	5493	1576	6933	933	8013	2353	8709	250	9501	168
1857	141	4317	744	5541	1104	6933	3030	8049	570	8709	705	9501	471
1857	328	4317	993	5541	1707	7017	81	8049	1173	8709	1296	9501	486
1929	502	4353	660	5541	2344	7017	240	8061	3	8709	1395	9501	1605
1929	508	4353	1057	5601	1065	7017	1117	8061	18	8709	1695	9501	2514
1941	3	4377	58	5613	1470	7041	351	8061	57	8709	2010	9501	3609
1941	736	4377	184	5613	1900	7041	1009	8061	439	8709	3925	9561	148
1977	519	4377	409	5613	2218	7041	1305	8061	576	8781	366	9561	4164
2157	36	4449	94	5613	2343	7041	1392	8061	1270	8781	498	9561	4273
2157	186	4497	430	5637	880	7053	520	8061	1333	8781	685	9573	54
2181	9	4569	370	5721	1594	7053	985	8061	1531	8781	979	9573	162
2217	193	4569	1402	5853	376	7053	1650	8097	666	8781	2251	9573	391
2229	880	4569	1837	5853	435	7053	2227	8121	307	8781	3706	9573	687
2361	979	4593	117	5853	1677	7113	2404	8121	1231	8817	571	9573	1093
2433	594	4593	1210	5853	2064	7149	714	8121	1347	8817	1552	9573	1350
2589	684	4629	366	5937	1365	7197	966	8133	292	8817	1969	9573	2085
2649	421	4629	1699	5937	1606	7197	1138	8133	1386	8817	2991	9573	2202
2649	609	4677	12	5961	358	7233	1794	8133	2764	8913	694	9609	306
2721	534	4677	78	5961	1540	7269	85	8133	3225	8913	1725	9609	721
2733	24	4677	99	5997	643	7341	1390	8157	2062	8913	3289	9609	1191
2733	240	4677	126	5997	1372	7341	1597	8193	160	8997	150	9609	1260
2733	585	4677	583	6009	360	7377	891	8193	1153	8997	351	9609	1731
2733	682	4677	1240	6009	900	7377	2287	8301	700	8997	367	9609	1783
2841	447	4701	76	6009	1167	7401	87	8301	835	8997	753	9609	2994
2949	711	4701	337	6033	126	7401	3546	8301	871	8997	955	9609	3166
2949	906	4701	430	6033	792	7509	907	8301	994	8997	1227	9753	2193
2949	919	4701	499	6033	2251	7509	1293	8301	1011	8997	2253	9753	3313
2973	288	4749	418	6081	457	7509	1762	8301	2398	8997	2857	9753	3454
2973	309	4749	1239	6081	1360	7593	103	8373	537	8997	3295	9777	364
3057	954	4749	1294	6117	604	7593	219	8373	1657	8997	3606	9777	903
3093	445	4821	43	6117	2373	7593	1108	8373	2697	9033	273	9813	1743
3093	610	4821	565	6117	2490	7617	85	8373	2913	9033	1582	9813	3049
3117	345	4821	826	6189	63	7617	223	8409	630	9033	3421	9897	1206
3117	579	4821	1240	6189	1429	7617	231	8409	1927	9057	397	9921	96
3189	318	4821	1587	6189	2224	7617	816	8409	2554	9057	720	9921	910
3261	9	4857	163	6249	69	7617	864	8457	685	9057	1308	9921	3514
3261	409	4857	1057	6249	561	7629	141	8529	57	9057	2643	9921	3865
3261	735	4881	942	6249	2653	7629	876	8529	471	9069	2761	9957	99
3309	390	4881	1761	6261	907	7653	162	8529	507	9201	486	9957	144
3309	940	4989	336	6261	1200	7653	366	8529	3192	9201	595	9957	2194
3453	802	5001	919	6261	1219	7653	498	8553	444	9201	946	9957	4138
3513	223	5001	1530	6261	1422	7653	1440	8553	568	9201	1327	9969	619
3513	598	5001	1608	6297	286	7653	1612	8553	1189	9201	2146	9969	2410
3561	313	5097	70	6297	1278	7737	1192	8553	1738	9201	2365	9969	2565
3669	87	5097	633	6297	1983	7773	1327	8553	2931	9237	648	9993	2443
3669	231	5097	1227	6333	135	7773	2185	8637	52	9237	693		
3669	520	5097	1747	6333	648	7773	2239	8637	232	9237	2287		
3693	102	5169	915	6333	810	7773	3270	8637	432	9249	556		
3693	544	5241	538	6333	2242	7941	1864	8637	523	9249	3069		
3693	838	5241	2160	6429	72	7977	1107	8637	744	9249	3339		

The proof of this theorem makes use of the following lemmas, the last of which relies on extensive computations.

Lemma 1. *Let n be a positive integer, let p be a prime, let*

$$\begin{aligned} a_{1,1}\,x_1 + a_{1,2}\,x_2 + \ldots + a_{1,n}\,x_n &\equiv c_1 \pmod p \\ a_{2,1}\,x_1 + a_{2,2}\,x_2 + \ldots + a_{2,n}\,x_n &\equiv c_2 \pmod p \\ &\ldots \\ a_{n,1}\,x_1 + a_{n,2}\,x_2 + \ldots + a_{n,n}\,x_n &\equiv c_n \pmod p \end{aligned} \tag{2}$$

be a set of linear congruences modulo p and let $\mathbf{A} = [a_{i,j}]$ be the corresponding matrix of coefficients. Suppose $|\mathbf{A}| \not\equiv 0 \pmod p$. Then there exists a unique solution of (2) in $GF(p)$. Furthermore, the solution is formally the same as that obtained by solving (2) over the rationals.

Proof. This is well known. □

Lemma 2. *Let $S = (V, \mathcal{B})$ be a two-generator Steiner triple system with parameters v and α containing one of the configurations Pasch, mitre, 6-cycle, crown. Let $V = \{0, 1, \ldots, v-1\}$ and let $\Gamma = \{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{13}\}$, where*

$$\begin{aligned}
\mathcal{G}_1 &= \{\{0,1,\alpha\},\{0,x_1,x_2\},\{1,x_2,x_3\},\{\alpha,x_1,x_3\}\},\\
\mathcal{G}_2 &= \{\{0,1,\alpha\},\{0,x_1,x_2\},\{0,x_3,x_4\},\{1,x_1,x_3\},\{\alpha,x_2,x_4\}\},\\
\mathcal{G}_3 &= \{\{0,1,\alpha\},\{1,x_1,x_2\},\{1,x_3,x_4\},\{0,x_1,x_3\},\{\alpha,x_2,x_4\}\},\\
\mathcal{G}_4 &= \{\{0,1,\alpha\},\{\alpha,x_1,x_2\},\{\alpha,x_3,x_4\},\{0,x_1,x_3\},\{1,x_2,x_4\}\},\\
\mathcal{G}_5 &= \{\{0,1,\alpha\},\{0,x_1,x_2\},\{0,x_3,x_4\},\{x_5,1,x_1\},\{x_5,\alpha,x_3\},\{x_5,x_2,x_4\}\},\\
\mathcal{G}_6 &= \{\{0,1,\alpha\},\{1,x_1,x_2\},\{1,x_3,x_4\},\{x_5,0,x_1\},\{x_5,\alpha,x_3\},\{x_5,x_2,x_4\}\},\\
\mathcal{G}_7 &= \{\{0,1,\alpha\},\{\alpha,x_1,x_2\},\{\alpha,x_3,x_4\},\{x_5,0,x_1\},\{x_5,1,x_3\},\{x_5,x_2,x_4\}\},\\
\mathcal{G}_8 &= \{\{0,1,\alpha\},\{0,x_1,x_2\},\{0,x_3,x_5\},\{1,x_1,x_4\},\{\alpha,x_1,x_5\},\{x_2,x_3,x_4\}\},\\
\mathcal{G}_9 &= \{\{0,1,\alpha\},\{0,x_1,x_2\},\{0,x_3,x_5\},\{\alpha,x_1,x_4\},\{1,x_1,x_5\},\{x_2,x_3,x_4\}\},\\
\mathcal{G}_{10} &= \{\{0,1,\alpha\},\{1,x_1,x_2\},\{1,x_3,x_5\},\{0,x_1,x_4\},\{\alpha,x_1,x_5\},\{x_2,x_3,x_4\}\},\\
\mathcal{G}_{11} &= \{\{0,1,\alpha\},\{1,x_1,x_2\},\{1,x_3,x_5\},\{\alpha,x_1,x_4\},\{0,x_1,x_5\},\{x_2,x_3,x_4\}\},\\
\mathcal{G}_{12} &= \{\{0,1,\alpha\},\{\alpha,x_1,x_2\},\{\alpha,x_3,x_5\},\{0,x_1,x_4\},\{1,x_1,x_5\},\{x_2,x_3,x_4\}\},\\
\mathcal{G}_{13} &= \{\{0,1,\alpha\},\{\alpha,x_1,x_2\},\{\alpha,x_3,x_5\},\{1,x_1,x_4\},\{0,x_1,x_5\},\{x_2,x_3,x_4\}\}.
\end{aligned}$$

Then there is a $\mathcal{G} \in \Gamma$ such that $\mathcal{G} \subset \mathcal{B}$ for some $x_1, x_2, \ldots, x_n \in V$, where $n = |\mathcal{G}| - 1$.

Proof. By Theorem 4, $v = 3p$, p prime, $p \equiv 3 \pmod 4$, and S is generated by blocks $\{0, 1, \alpha\}$ and $\{0, p, 2p\}$. Let $\mathcal{X}$ be one of the configurations Pasch, mitre, 6-cycle, crown. Suppose $\mathcal{X} \subset \mathcal{B}$.

Observe that $\mathcal{G}_1$ is a Pasch configuration, $\mathcal{G}_2$, $\mathcal{G}_3$ and $\mathcal{G}_4$ are mitres, $\mathcal{G}_5$, $\mathcal{G}_6$ and $\mathcal{G}_7$ are 6-cycles, $\mathcal{G}_8$, $\mathcal{G}_9$, …, $\mathcal{G}_{13}$ are crowns and the block of $\mathcal{G} \in \Gamma$ labelled $\{0, 1, \alpha\}$ is one of two intersecting blocks which map to each other under an automorphism of $\mathcal{G}$. Since $\mathcal{X}$ cannot contain two intersecting blocks belonging to the orbit of $\{0, p, 2p\}$, it is straightforward to verify (perhaps by drawing diagrams) that there exists an automorphism of S which maps $\mathcal{X}$ to some $\mathcal{G} \in \Gamma$ for some $x_1, x_2, \ldots, x_{|\mathcal{G}|-1} \in V$. □

Lemma 3. *Let p be prime and suppose that the polynomial $f(x)$ is not a constant multiple of a square over $GF(p)$. Then*

$$\left| \sum_{x \in GF(p)} \theta(f(x)) \right| = O(\sqrt{p}).$$

Proof. This is a special case of the theorem on page 43 of [11]. □

In the next lemma we introduce a set of polynomials, Λ. In Lemma 5 we investigate certain sets of linear congruences. The coefficients of these congruences involve a parameter, α. We wish to show that there exists an α such that either the congruences have no solution, or the solution satisfies certain conditions that can be expressed in the form $\theta(\rho(\alpha)) = 1$ for certain rational functions $\rho(x)$. We then find that there is a set of polynomials Λ with the property that if $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$, then $\theta(\rho(\alpha)) = -1$ for at least one of the functions $\rho(x)$. Actually, to deal with questions of existence and uniqueness of solutions, slightly more than this is required, and the key property of Λ is that given in Lemma 4. The set Λ given in this lemma was obtained by considering the numerators and denominators of the functions $\rho(x)$. It is not feasible to explain why each individual polynomial is included in Λ. However, we give below, following the proof of Lemma 5, several examples to illustrate the method. In particular, Example 1 explains why $-x^3 + 5x^2 - 6x + 3 \in \Lambda$.

Lemma 4. *Let*

$$\begin{aligned}\Lambda = \{&x, x-1, x+1, -2x+1, 2x-3, -x+3, x^2+1, -x^2-2,\\ &-x^2-x+1, x^2-x+1, -x^2+x+1, -x^2+2x-2,\\ &-x^2+3x-3, -2x^2+3x-2, 3x^2-4x+2, 2x^2-4x+3,\\ &-2x^2+3x-3, 3x^2-5x+3, x^2-2x+3, x^2-3x+1,\\ &-x^3+x^2-1, -x^3+2x^2-x-1, -x^3+3x^2-2x+1,\\ &x^3-2x^2+3x-3, x^3-3x^2+6x-3, x^3-3x+3,\\ &-x^3+5x^2-6x+3, -x^3+3x^2-4x+1\}.\end{aligned}$$

Given any positive number N, for all sufficiently large prime p, there exist at least N numbers α, distinct modulo p, such that $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$.

Proof. Let

$$\pi(x) = \prod_{\lambda(x)\in\Lambda} (1 + \theta(\lambda(x)))$$

and

$$\Delta = \sum_{x\in \mathrm{GF}(p)} \pi(x).$$

Then

$$\Delta = p + \sum_{f(x)} \sum_{x\in \mathrm{GF}(p)} \theta(f(x)),$$

where $f(x)$ in the outer sum runs through all $2^{|\Lambda|} - 1$ non-empty products of polynomials $\lambda(x) \in \Lambda$. It is easily checked that over the rationals the polynomial $\prod_{\lambda(x)\in\Lambda} \lambda(x)$ has non-zero discriminant. Hence, assuming that p is sufficiently large, $f(x)$ is never a constant multiple of a square over GF(p). So by Lemma 3 we have $\Delta = p - O(\sqrt{p})$.

Since both $\pi(x)$ and the number of factors of $\pi(x)$ which are equal to 1 are bounded as $p \to \infty$, it follows that for each fixed N and for p sufficiently large, there exist N distinct values of α modulo p such that $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$. □

Lemma 5. *Let $v = 3p$, p prime, $p \equiv 3 \pmod 4$. Let Λ be the set of polynomials in Lemma 4. Then there exists a polynomial $Q(x)$ such that if $\alpha \equiv 0 \pmod 3$, if $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$ and if $Q(\alpha) \not\equiv 0 \pmod p$, then there exists a 6-sparse two-generator Steiner triple system with parameters v and α.*

Proof. Let $v = 3p$, p prime, $p \equiv 3 \pmod 4$ and suppose α satisfies the conditions of the lemma with $Q(x)$ to be chosen later. Observe that $x - 1 \in \Lambda$; therefore $\theta(\alpha - 1) = 1$, as required by Theorem 4, and hence there exists a two-generator Steiner triple system $S = (V, \mathcal{B})$ with parameters v and α. We show that with a suitable choice of $Q(x)$ S is 6-sparse.

Let $\Gamma = \{\mathcal{G}_1, \mathcal{G}_2, \ldots, \mathcal{G}_{13}\}$ be the set of configurations in Lemma 2. Let $\mathcal{G} \in \Gamma$ and let $\mathcal{G}$ have $n+1$ blocks. For $d = 1, 2, \ldots, n$, let (a_d, b_d, c_d) be the dth block of $\mathcal{G} \setminus \{\{0, 1, \alpha\}\}$ in some ordering. Then if $\mathcal{G} \subset \mathcal{B}$, we have the following set of $3n$ linear congruences modulo $3p$ in variables $x_1, x_2, \ldots, x_n$, $m_1, m_2, \ldots, m_n$ and the variables ω_d for those d where the corresponding congruences have the first alternative on the right:

$$\begin{aligned}
(a_1, b_1, c_1) &\equiv \begin{cases} (m_1, m_1 + \omega_1, m_1 + \alpha\omega_1) \\ \text{or } (m_1, m_1 + p, m_1 + 2p), \end{cases} \\
(a_2, b_2, c_2) &\equiv \begin{cases} (m_2, m_2 + \omega_2, m_2 + \alpha\omega_2) \\ \text{or } (m_2, m_2 + p, m_2 + 2p), \end{cases} \\
&\ldots, \\
(a_n, b_n, c_n) &\equiv \begin{cases} (m_n, m_n + \omega_n, m_n + \alpha\omega_n) \\ \text{or } (m_n, m_n + p, m_n + 2p). \end{cases}
\end{aligned}$$

On eliminating the m_d we have $2n$ congruences modulo $3p$:

$$(b_i - a_i,\ c_i - a_i) \equiv (\omega_i,\ \alpha\omega_i) \text{ or } (p,\ 2p), \quad i = 1, 2, \ldots, n. \tag{3}$$

Since there are six permutations of (a_i, b_i, c_i) and two possible congruences for each, there are 12^n possible sets of congruences represented by (3). (Although this number can be reduced somewhat, we prefer, for simplicity, to present the results of our original computations, which do not exploit additional symmetries in (3).) Thus by Lemma 2, if S contains a Pasch, mitre, 6-cycle or crown configuration, there exists a $\mathcal{G} \in \Gamma$ and a corresponding set of congruences (3) which has, for some orderings of the blocks of $\mathcal{G}$ and some choice of the alternatives on the right of (3), a solution modulo 3 in which all the ω_d present satisfy $\omega_d \equiv 1 \pmod 3$ and a solution modulo p in which all the ω_d present satisfy $\theta(\omega_d) = 1$. To show that this cannot happen, we examine each of the 12^n possible sets of congruences (3) for each configuration $\mathcal{G} \in \Gamma$. Denote this collection of congruence sets by Φ_0. Thus $|\Phi_0| = 12^3 + 3 \cdot 12^4 + 9 \cdot 12^5 = 2303424$.

As an immediate first step, we eliminate from Φ_0 all sets where there are two intersecting blocks in the orbit of $\{0, p, 2p\}$, for such configurations cannot occur in S. This leaves a collection Φ_1 of 584064 sets: 864 for $\mathcal{G}_1$, 7776 each for $\mathcal{G}_2, \mathcal{G}_3$ and $\mathcal{G}_4$, 62208 each for $\mathcal{G}_5, \mathcal{G}_6, \ldots, \mathcal{G}_{13}$. For example, take the crown configuration $\mathcal{G}_8$. Denote the blocks other than $\{0, 1, \alpha\}$, by A, B, C, D and E, where $\{A, B\}$ and $\{C, D\}$ are pairs of parallel blocks. Then we have the following possibilities for blocks in the orbit of $\{0, p, 2p\}$: none, 6^5; block E, 6^5; one or both of $\{A, B\}$, $2 \cdot 6^5 + 6^5$; one or both of $\{C, D\}$, $2 \cdot 6^5 + 6^5$. So the total number of legitimate congruence sets that arise from $\mathcal{G}_8$ is $8 \cdot 6^5 = 62208$.

Next, we eliminate from Φ_1 all cases where (3) has no solution modulo 3. We assume that $\alpha = 0$ and that $\omega_d = 1$ for all multipliers ω_d present. We also assume that $p = 1$. For if a set of congruences (3) has a solution modulo 3 with $p = 2$ and includes the pairs $\{b_j - a_j \equiv p,\ c_j - a_j \equiv 2p\}$ for those $j \in \{1, 2, \ldots, n\}$ where the block $\{a_j, b_j, c_j\}$ is in the orbit of $\{0, p, 2p\}$, then the set of congruences obtained by interchanging b_j and c_j has the same solution with $p = 1$, and, of course, both sets of congruences are identical modulo p. After performing the computations we are left with the collection Φ_2 of 3320 congruence sets, partitioned as follows: $\mathcal{G}_1$, 32; $\mathcal{G}_2, \mathcal{G}_3, \mathcal{G}_4$, 168 each; $\mathcal{G}_5, \mathcal{G}_6, \mathcal{G}_7$, 384 each; $\mathcal{G}_8, \mathcal{G}_{13}$, 344 each; $\mathcal{G}_9, \mathcal{G}_{12}$, 224 each; $\mathcal{G}_{10}, \mathcal{G}_{11}$, 248 each. In all cases the solution modulo 3 is unique.

We deal with Φ_2 by examining each congruence set modulo p. For a given congruence set, let t be the number of blocks in the orbit of $\{0, p, 2p\}$ and note that $0 \leq t \leq 2$. Recall that the configuration has $n + 1$ blocks. So there are $2n$ congruences, n point variables, $x_1, x_2, ..., x_n$, and $n - t$ multiplier variables, ω_d. We select $2n - t$ congruences by excluding t (possibly none) of the $2t$ congruences that involve p.

Suppose $t = 0$. With the congruences (3) written in matrix form $\mathbf{Dx} = \mathbf{e}$, we find that in every case $|\mathbf{D}|$ is a polynomial in α, $d(\alpha)$, say, which is not identically zero. Assuming that p is sufficiently large and α is chosen such that $d(\alpha) \not\equiv 0 \pmod{p}$, we can obtain the unique solution $\mathbf{x} = \mathbf{D}^{-1}\mathbf{e}$ (modulo p), where $\mathbf{x} = (x_1, x_2, \ldots, x_n, \omega_1, \omega_2, \ldots, \omega_n)$ and the elements of $\mathbf{D}^{-1}\mathbf{e}$ are rational functions of α. Next we attempt to compute the quadratic characters of the multipliers ω_j and the ratios ω_j/ω_k on the assumption that $\theta(\lambda(\alpha)) = 1$ for each $\lambda(x) \in \Lambda$. In all except four cases we find that at least one multiplier or ratio of multipliers is not a quadratic residue modulo p, and hence $\mathcal{G}$ cannot occur in S. Example 1 illustrates this point. The remaining four cases correspond to a Pasch configuration and three 6-cycles, where in the solution of the congruences (3) the x_i are such that every block is of the form $\{a, b, c\}$ with $(a, b, c) \equiv (0, 1, \alpha) \pmod{p}$ and the ω_i are all $\equiv 1 \pmod{p}$. Since each ω_i is also congruent to 1 modulo 3, it follows that each ω_i is equal to 1. This in turn implies that the configuration contains repeated blocks. See Example 2 below.

Now suppose $t > 0$. We find that it is always possible to choose $2n - t$ congruences from (3) such that when they are written in matrix form $\mathbf{Dx} = \mathbf{e}$, $|\mathbf{D}| = d(\alpha)$ is not identically zero. So if α is chosen such that $d(\alpha) \not\equiv 0 \pmod{p}$, then we get a unique solution for the $2n - t$ variables, $\mathbf{x} = \mathbf{D}^{-1}\mathbf{e}$. The excluded $t = 1$ or 2 congruences have the form $b_i - a_i \equiv 0 \pmod{p}$ or $c_i - a_i \equiv 0 \pmod{p}$ for some i. So suppose for these i that the solution $\mathbf{x} = \mathbf{D}^{-1}\mathbf{e}$ gives $a_i = a_i(\alpha)$, $b_i = b_i(\alpha)$ and $c_i = c_i(\alpha)$ for rational functions $a_i(\alpha)$, $b_i(\alpha)$ and $c_i(\alpha)$. We either have: (i) for all t excluded congruences, $b_i(\alpha) - a_i(\alpha)$ or $c_i(\alpha) - a_i(\alpha)$ is identically zero for all α; or (ii) for one of the excluded congruences there exists α such that $b_i(\alpha) - a_i(\alpha) \not\equiv 0 \pmod{p}$ or $c_i(\alpha) - a_i(\alpha) \not\equiv 0 \pmod{p}$.

In case (i), the excluded congruences may be ignored and we proceed as for $t = 0$, where it turns out always that, assuming $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$, either $\theta(\omega_j) = -1$ for some multiplier ω_j or $\theta(\omega_j/\omega_k) = -1$ for some ratio ω_j/ω_k of multipliers. Hence $\mathcal{G}$ does not occur in S. Example 3 illustrates this case.

In case (ii), by clearing the denominator we obtain an additional constraint, which takes the form $q(\alpha) \equiv 0 \pmod{p}$ for some polynomial $q(x)$. Then if α is chosen such that $q(\alpha) \not\equiv 0 \pmod{p}$, the congruences (3) will be inconsistent and hence $\mathcal{G}$ will not occur in S. See Example 4.

To complete the proof we set $Q(x)$ equal to the least common multiple of all the determinant polynomials $d(x)$ and constraint polynomials $q(x)$ encountered in the preceding analysis. Observe that if p is sufficiently large, none of the functions $d(x)$ and $q(x)$ depend

on p, and hence $Q(x)$ is independent of p. □

Whilst it is not feasible within the space limitations of this paper to give details of all the cases that occur in the proof of Lemma 5, the main features of the method can be illustrated by a few examples.

Example 1.

Let $\mathcal{G}$ be the 6-cycle configuration $\mathcal{G}_5$ with the blocks ordered as written:

$$\{\{0,1,\alpha\},\{0,x_1,x_2\},\{x_5,\alpha,x_3\},\{x_3,0,x_4\},\{x_1,x_5,1\},\{x_4,x_2,x_5\}\}.$$

Suppose all these blocks belong to the orbit of $\{0,1,\alpha\}$. The congruences to be solved modulo $3p$ are

$$\begin{aligned}(0,\ x_1,\ x_2) &\equiv (m_1,\ m_1+\omega_1,\ m_1+\alpha\omega_1),\\ (x_5,\ \alpha,\ x_3) &\equiv (m_2,\ m_2+\omega_2,\ m_2+\alpha\omega_2),\\ (x_3,\ 0,\ x_4) &\equiv (m_3,\ m_3+\omega_3,\ m_3+\alpha\omega_3),\\ (x_1,\ x_5,\ 1) &\equiv (m_4,\ m_4+\omega_4,\ m_4+\alpha\omega_4),\\ (x_4,\ x_2,\ x_5) &\equiv (m_5,\ m_5+\omega_5,\ m_5+\alpha\omega_5),\end{aligned}$$

or, after eliminating m_1, m_2, m_3, m_4, m_5,

$$\begin{aligned}(x_1,\ x_2) &\equiv (\omega_1,\ \alpha\omega_1),\\ (\alpha-x_5,\ x_3-x_5) &\equiv (\omega_2,\ \alpha\omega_2),\\ (-x_3,\ x_4-x_3) &\equiv (\omega_3,\ \alpha\omega_3),\\ (x_5-x_1,\ 1-x_1) &\equiv (\omega_4,\ \alpha\omega_4),\\ (x_2-x_4,\ x_5-x_4) &\equiv (\omega_5,\ \alpha\omega_5).\end{aligned} \tag{4}$$

Setting $\alpha = 0$ and $\omega_1 = \omega_2 = \omega_3 = \omega_4 = \omega_5 = 1$, we solve this set of congruences modulo 3 to obtain the unique solution:

$$x_1 = 1, \quad x_2 = 0, \quad x_3 = x_4 = x_5 = 2.$$

Therefore we consider the congruences (4) modulo p, and for this purpose we put them into matrix form:

$$\begin{bmatrix} -1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0\\ 0 & -1 & 0 & 0 & 0 & \alpha & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0\\ 0 & 0 & -1 & 0 & 1 & 0 & \alpha & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & \alpha & 0 & 0\\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0\\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \alpha & 0\\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 & \alpha \end{bmatrix} \begin{bmatrix} x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ \omega_1\\ \omega_2\\ \omega_3\\ \omega_4\\ \omega_5 \end{bmatrix} \equiv \begin{bmatrix} 0\\ 0\\ \alpha\\ 0\\ 0\\ 0\\ 0\\ 1\\ 0\\ 0 \end{bmatrix} \pmod{p}.$$

There are ten congruences and ten variables, the determinant of the system is $-\alpha(\alpha^3 - 5\alpha^2 + 6\alpha - 3)$, and we assume that $x(x^3 - 5x^2 + 6x - 3)$ is a factor of $Q(x)$. Hence there is a unique solution modulo p:

$$x_1 = \frac{\alpha^4 - 2\alpha^3 + 3\alpha - 3}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ x_2 = \frac{\alpha^5 - 2\alpha^4 + 3\alpha^2 - 3\alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ x_3 = \frac{-\alpha^4 + 2\alpha^2 - 2\alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},$$

$$x_4 = \frac{\alpha^5 - \alpha^4 - 2\alpha^3 + 4\alpha^2 - 2\alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ x_5 = \frac{\alpha^4 - 3\alpha^3 + 3\alpha^2 - 2\alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},$$
$$\omega_1 = \frac{\alpha^4 - 2\alpha^3 + 3\alpha - 3}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ \omega_2 = \frac{-2\alpha^3 + 3\alpha^2 - \alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ \omega_3 = \frac{\alpha^4 - 2\alpha^2 + 2\alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},$$
$$\omega_4 = \frac{-\alpha^3 + 3\alpha^2 - 5\alpha + 3}{\alpha^3 - 5\alpha^2 + 6\alpha - 3},\ \omega_5 = \frac{-\alpha^4 + 2\alpha^3 - \alpha^2 - \alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3}.$$

Since x, $x-1$, $1-2x$ and $-x^3+5x^2-6x+3$ are in Λ, we can assume that

$$\theta(\alpha) = \theta(\alpha - 1) = \theta(1 - 2\alpha) = \theta(-\alpha^3 + 5\alpha^2 - 6\alpha + 3) = 1.$$

Hence we can compute the quadratic character of ω_2,

$$\theta(\omega_2) = \theta\left(\frac{-2\alpha^3 + 3\alpha^2 - \alpha}{\alpha^3 - 5\alpha^2 + 6\alpha - 3}\right) = \theta\left(\frac{\alpha(\alpha-1)(1-2\alpha)}{\alpha^3 - 5\alpha^2 + 6\alpha - 3}\right) = -1,$$

and deduce that the configuration does not occur in S.

Example 2.

Let $\mathcal{G}$ be the Pasch configuration $\mathcal{G}_1$ with the blocks ordered as written:

$$\{\{0, 1, \alpha\}, \{0, x_1, x_2\}, \{x_3, 1, x_2\}, \{x_3, x_1, \alpha\}\}.$$

Suppose all these blocks belong to the orbit of $\{0, 1, \alpha\}$. The congruences to be solved modulo $3p$ are

$$\begin{aligned}(0,\ x_1,\ x_2) &\equiv (m_1,\ m_1 + \omega_1,\ m_1 + \alpha\omega_1),\\ (x_3,\ 1,\ x_2) &\equiv (m_2,\ m_2 + \omega_2,\ m_2 + \alpha\omega_2),\\ (x_3,\ x_1,\ \alpha) &\equiv (m_3,\ m_3 + \omega_3,\ m_3 + \alpha\omega_3),\end{aligned}$$

or, after eliminating m_1, m_2, m_3,

$$\begin{aligned}(x_1,\ x_2) &\equiv (\omega_1,\ \alpha\omega_1),\\ (1 - x_3,\ x_2 - x_3) &\equiv (\omega_2,\ \alpha\omega_2),\\ (x_1 - x_3,\ \alpha - x_3) &\equiv (\omega_3,\ \alpha\omega_3).\end{aligned} \tag{5}$$

Setting $\alpha = 0$ and $\omega_1 = \omega_2 = \omega_3 = 1$, we solve this set of congruences modulo 3 to obtain the unique solution $x_1 = 1$, $x_2 = x_3 = 0$. Therefore we consider the congruences (5) modulo p, and for this purpose we put them into matrix form:

$$\begin{bmatrix} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & -1 & 0 & \alpha & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & 1 & 0 & \alpha & 0 \\ -1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & \alpha \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \omega_1 \\ \omega_2 \\ \omega_3 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ \alpha \end{bmatrix} \pmod{p}.$$

The determinant of the system is $2\alpha(\alpha-1)$, and we assume that $x(x-1)$ is a factor of $Q(x)$. Hence there is a unique solution modulo p: $x_1 = 1$, $x_2 = \alpha$, $x_3 = 0$, $\omega_1 = \omega_2 = \omega_3 = 1$.

In fact, this is one of the four configurations where the system of congruences (3) has a legitimate solution and, as previously explained, it does not exist in S.

The other three configurations where the congruences have legitimate solutions modulo $3p$ are the 6-cycles $\mathcal{G}_5$, $\mathcal{G}_6$ and $\mathcal{G}_7$, with the blocks, all in the orbit of $\{0,1,\alpha\}$, ordered as written:

$$\begin{aligned}
&\mathcal{G}_5 : \{\{0,1,\alpha\},\{0,x_3,x_4\},\{x_5,1,x_1\},\{x_5,x_2,x_4\},\{0,x_2,x_1\},\{x_5,x_3,\alpha\}\},\\
&\mathcal{G}_6 : \{\{0,1,\alpha\},\{0,x_5,x_1\},\{x_2,x_5,x_4\},\{x_3,1,x_4\},\{x_2,1,x_1\},\{x_3,x_5,\alpha\}\},\\
&\mathcal{G}_7 : \{\{0,1,\alpha\},\{0,x_1,x_5\},\{x_2,x_4,x_5\},\{x_3,x_4,\alpha\},\{x_2,x_1,\alpha\},\{x_3,1,x_5\}\}.
\end{aligned}$$

Example 3.

Let $\mathcal{G}$ be the mitre configuration $\mathcal{G}_2$ with the blocks ordered as written:

$$\{\{0,1,\alpha\},\{0,x_1,x_2\},\{x_1,x_3,1\},\{x_2,x_4,\alpha\},\{0,x_4,x_3\}\}.$$

Suppose the second, third and fourth blocks belong to the orbit of $\{0,1,\alpha\}$ and the fifth belongs to the orbit of $\{0,p,2p\}$. The congruences to be solved modulo $3p$ are

$$\begin{aligned}
(0,\ x_1,\ x_2) &\equiv (m_1,\ m_1+\omega_1,\ m_1+\alpha\omega_1),\\
(x_1,\ x_3,\ 1) &\equiv (m_2,\ m_2+\omega_2,\ m_2+\alpha\omega_2),\\
(x_2,\ x_4,\ \alpha) &\equiv (m_3,\ m_3+\omega_3,\ m_3+\alpha\omega_3),\\
(0,\ x_4,\ x_3) &\equiv (m_4,\ m_4+p,\ m_4+2p),
\end{aligned}$$

or, after eliminating m_1, m_2, m_3, m_4,

$$\begin{aligned}
(x_1,\ x_2) &\equiv (\omega_1,\ \alpha\omega_1),\\
(x_3-x_1,\ 1-x_1) &\equiv (\omega_2,\ \alpha\omega_2),\\
(x_4-x_2,\ \alpha-x_2) &\equiv (\omega_3,\ \alpha\omega_3),\\
(x_4,\ x_3) &\equiv (p,\ 2p).
\end{aligned} \tag{6}$$

Setting $\alpha = 0$ and $\omega_1 = \omega_2 = \omega_3 = p = 1$, we solve this set of congruences modulo 3 to obtain this unique solution:

$$x_1 = 1, \quad x_2 = 0, \quad x_3 = 2, \quad x_4 = 1.$$

Therefore we consider the congruences (6) modulo p, and for this purpose we put them into matrix form:

$$\begin{bmatrix}
-1 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & -1 & 0 & 0 & \alpha & 0 & 0\\
1 & 0 & -1 & 0 & 0 & 1 & 0\\
1 & 0 & 0 & 0 & 0 & \alpha & 0\\
0 & 1 & 0 & -1 & 0 & 0 & 1\\
0 & 1 & 0 & 0 & 0 & 0 & \alpha\\
0 & 0 & 0 & -1 & 0 & 0 & 0\\
0 & 0 & -1 & 0 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix} x_1\\ x_2\\ x_3\\ x_4\\ \omega_1\\ \omega_2\\ \omega_3 \end{bmatrix}
\equiv
\begin{bmatrix} 0\\ 0\\ 0\\ 1\\ 0\\ \alpha\\ 0\\ 0 \end{bmatrix} \pmod{p}.$$

There are eight congruences but only seven variables. So we exclude the last congruence and work with just the first seven. The determinant of the reduced system is $\alpha^2(\alpha-1)$,

and we assume that $x(x-1)$ is a factor of $Q(x)$. Hence there is a unique solution modulo p:

$$x_1 = \frac{1}{1-\alpha},\ x_2 = \frac{\alpha}{1-\alpha},\ x_3 = x_4 = 0,\ \omega_1 = \frac{1}{1-\alpha},\ \omega_2 = \frac{1}{\alpha-1},\ \omega_3 = \frac{\alpha}{\alpha-1}$$

and, furthermore, this solution is consistent with the excluded congruence, $x_3 \equiv 0 \pmod p$. However, we can compute the quadratic character of ω_1:

$$\theta(\omega_1) = \theta(1-\alpha) = -1,$$

since $x - 1 \in \Lambda$, and therefore deduce that this configuration does not occur in S.

Example 4.

Let $\mathcal{G}$ be the crown configuration $\mathcal{G}_8$ with the blocks ordered as written:

$$\{\{0,1,\alpha\},\{1,x_1,x_4\},\{x_2,x_3,x_4\},\{x_1,\alpha,x_5\},\{x_3,0,x_5\},\{0,x_2,x_1\}\},$$

and suppose only the last block belongs to the orbit of $\{0,p,2p\}$. The congruences to be solved modulo $3p$ are

$$\begin{aligned}
(1,\ x_1,\ x_4) &\equiv (m_1,\ m_1+\omega_1,\ m_1+\alpha\omega_1),\\
(x_2,\ x_3,\ x_4) &\equiv (m_2,\ m_2+\omega_2,\ m_2+\alpha\omega_2),\\
(x_1,\ \alpha,\ x_5) &\equiv (m_3,\ m_3+\omega_3,\ m_3+\alpha\omega_3),\\
(x_3,\ 0,\ x_5) &\equiv (m_4,\ m_4+\omega_4,\ m_4+\alpha\omega_4),\\
(0,\ x_2,\ x_1) &\equiv (m_5,\ m_5+p,\ m_5+2p),
\end{aligned}$$

or, after eliminating m_1, m_2, m_3, m_4, m_5,

$$\begin{aligned}
(x_1-1,\ x_4-1) &\equiv (\omega_1,\ \alpha\omega_1),\\
(x_3-x_2,\ x_4-x_2) &\equiv (\omega_2,\ \alpha\omega_2),\\
(\alpha-x_1,\ x_5-x_1) &\equiv (\omega_3,\ \alpha\omega_3),\\
(-x_3,\ x_5-x_3) &\equiv (\omega_4,\ \alpha\omega_4),\\
(x_2,\ x_1) &\equiv (p,\ 2p).
\end{aligned} \tag{7}$$

Setting $\alpha = 0$ and $\omega_1 = \omega_2 = \omega_3 = \omega_4 = p = 1$, this set of congruences has a unique solution modulo 3:

$$x_1 = x_3 = x_5 = 2,\quad x_2 = x_4 = 1.$$

For solving modulo p, we put (7) in matrix form:

$$\begin{bmatrix}
-1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & -1 & 0 & \alpha & 0 & 0 & 0\\
0 & 1 & -1 & 0 & 0 & 0 & 1 & 0 & 0\\
0 & 1 & 0 & -1 & 0 & 0 & \alpha & 0 & 0\\
1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0\\
1 & 0 & 0 & 0 & -1 & 0 & 0 & \alpha & 0\\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1\\
0 & 0 & 1 & 0 & -1 & 0 & 0 & 0 & \alpha\\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\
-1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\begin{bmatrix} x_1\\ x_2\\ x_3\\ x_4\\ x_5\\ \omega_1\\ \omega_2\\ \omega_3\\ \omega_4 \end{bmatrix}
\equiv
\begin{bmatrix} -1\\ -1\\ 0\\ 0\\ \alpha\\ 0\\ 0\\ 0\\ 0\\ 0 \end{bmatrix}
\pmod p.$$

There are ten congruences but only nine variables. We temporarily remove the last congruence and consider only the first nine. However, the determinant of this reduced system is identically zero. So we take instead the first eight and the tenth congruences, omitting the ninth. This system has determinant $d(\alpha) = (\alpha - 1)^2$, which is not zero modulo p provided $x - 1$ is a factor of $Q(x)$. The unique solution modulo p of this system is then

$$x_1 = 0,\ x_2 = \frac{1 - 2\alpha + \alpha^2 - \alpha^3}{(\alpha - 1)^2},\ x_3 = \frac{-\alpha^2}{\alpha - 1},\ x_4 = 1 - \alpha,\ x_5 = \alpha^2,$$

$$\omega_1 = -1,\ \omega_2 = \frac{2\alpha - 1}{(\alpha - 1)^2},\ \omega_3 = \alpha,\ \omega_4 = \frac{\alpha^2}{\alpha - 1},$$

which is inconsistent with the omitted congruence, $x_2 \equiv 0 \pmod{p}$, unless $q(\alpha) \equiv 0 \pmod{p}$, where $q(x) = 1 - 2x + x^2 - x^3$. Since we can assume that $x - 1$ and $q(x)$ are factors of $Q(x)$, this configuration does not occur in S.

Proof of Theorem 5. The result follows from Lemma 4 and Lemma 5. Choose N greater than the degree of $Q(x)$. Take p so large that it does not divide any of the coefficients of $Q(x)$ and is sufficiently large for Lemma 4 to apply. Then by Lemma 4 we select an α which is not a root of $Q(x)$ modulo p and is such that $\theta(\lambda(\alpha)) = 1$ for all $\lambda(x) \in \Lambda$. If necessary we add a multiple of p to α to obtain a value that is congruent to 0 modulo 3. Now apply Lemma 5. □

Finally, we briefly address a question which naturally arises. Can Theorem 4 be used to create 7-sparse Steiner triple systems? We suspect not. In our research we have been unable to find any 6-sparse system which avoids the 7-block, 9-point configuration {012, 034, 135, 246, 257, 168, 078}, obtained by adding a diagonal to the 'window frame'.

References

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

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

3. 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.

4. A. D. Forbes, M. J. Grannell and T. S. Griggs, On 6-sparse Steiner triple systems, J. Combin. Theory Ser. A **114**, 235–252 (2007).

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

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

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

8. T. S. Griggs, J. P. Murphy and J. S. Phelan, Anti-Pasch Steiner triple systems, J. Combin. Inform. System Sci. **15**, 79–84 (1990).

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

10. 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**, 641–657 (2000).

11. W. M. Schmidt, Equations over Finite Fields, Lecture Notes in Mathematics **536**, Berlin Heidelberg New York: Springer 1976.

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

13. A. Wolfe, Private communication (2006).

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

15. A. Wolfe, The existence of 5-sparse Steiner triple systems of order $n \equiv 3 \pmod 6, n \notin \{9, 15\}$, J. Combin. Theory Ser. A, to appear (2008).

Received:
Final version received: