This is a preprint of an article accepted for publication in the Journal of Combinatorial Designs © 1999 (copyright owner as specified in the journal).

Some new perfect Steiner triple systems

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

J. P. Murphy
International Computer Engineering
Styal Road, Wythenshawe
Manchester M22 5WB
UNITED KINGDOM

Abstract

In a Steiner triple system STS(v)=(V, B), for each pair $\{a, b\} \subset V$, the cycle graph $G_{a,b}$ can be defined as follows. The vertices of $G_{a,b}$ are $V \setminus \{a, b, c\}$ where $\{a, b, c\} \in B$. $\{x, y\}$ is an edge if either $\{a, x, y\}$ or $\{b, x, y\} \in B$. The Steiner triple system is said to be perfect if the cycle graph of every pair is a single $(v-3)$-cycle. Perfect STS(v) are known only for $v = 7$, 9, 25 and 33. We construct perfect STS(v) for $v = 79$, 139, 367, 811, 1531, 25771, 50923, 61339 and 69991.

1 Introduction

A Steiner triple system, STS(v), is a pair (V, B) where V is a set of cardinality v and B is a family of 3-element subsets of V with the property that every 2-element subset of V occurs precisely once as a subset of a member of B. The set V is called the *point* set and the members of the set B are called *blocks* or *lines*. Steiner triple systems exist if and only if $v \equiv 1$ or 3 (mod 6). In a Steiner triple system STS(v)=(V,B), for each pair $\{a, b\} \subset V$, we may define the *cycle graph* $G_{a,b}$ as follows. The vertices of $G_{a,b}$ are the points in $V \setminus \{a, b, c\}$ where $\{a, b, c\} \in B$. The pair $\{x, y\}$ is an edge of $G_{a,b}$ if and only if either $\{a, x, y\}$ or $\{b, x, y\} \in B$. Clearly $G_{a,b}$ is a union of disjoint cycles. If these cycles have lengths l_i then the *type* of $G_{a,b}$ is the multiset $\{l_i\}$. Note that $\sum_i l_i = v - 3$. If every $G_{a,b}$, for $a, b \in V$, is of the same type then the Steiner triple system is said to be *uniform*. If, in addition, the common type is $\{v - 3\}$, i.e. every $G_{a,b}$ comprises a single $(v - 3)$-cycle, then the Steiner triple system is said to be *perfect*. Further information about uniform and perfect systems can be found in [1].

Perfect STS(v) were previously known only for $v = 7$, 9, 25 and 33. That the unique STS(7) and the unique STS(9) are perfect is trivial. A perfect STS(25) is ♯3 of the three systems invariant under the group $C_5 \times C_5$ found by Tonchev [5]. A perfect STS(33) is the cyclic system ♯80 given in the listing of Colbourn and Mathon [2] with full automorphism group of order 165. For completeness the two systems are given.

Perfect STS(25)
Let $V = Z_5 \times Z_5$.
The blocks are constructed from the following base blocks of triples of V:
{(0,0),(0,1),(1,0)}, {(0,0),(0,2),(2,1)}, {(0,0),(1,1),(2,3)}, {(0,0),(1,3),(3,3)}
under the action of the mappings $(x, y) \mapsto (x + 1, y)$ and $(x, y) \mapsto (x, y + 1)$, with addition modulo 5.

Perfect STS(33)
Let $V = Z_{33}$. The blocks are constructed from the following base blocks of triples of V: {0,1,7}, {0,2,21}, {0,3,20}, {0,4,28}, {0,8,18}, {0,11,22}
under the action of the mapping $x \mapsto x + 1$ (mod 33).

The main result of this paper is the construction of perfect STS(v) for nine additional values of v, specifically $v = 79$, 139, 367, 811, 1531, 25771, 50923, 61339 and 69991, all of which are prime and satisfy $v \equiv 7 \pmod{12}$. In addition we construct uniform (but not perfect) STS(v) for $v = 31$, 43, 13063 and 34303. The system for $v = 31$ is $PG(4, 2)$ and that for $v = 43$ was previously obtained by C. J. Colbourn (unpublished). The central idea is to produce STS(v)s with a "large" automorphism group, G, so that these systems are realized as a single block-orbit under G. The group G then has at most three orbits on the pairs of points. If $\{a, b\}$ and $\{c, d\}$ lie in the same orbit of pairs then the cycle graphs $G_{a,b}$ and $G_{c,d}$ are isomorphic. Hence the cycle graphs of such an STS(v) are of at most three different types. In those cases where these types reduce to one single type, the system will be uniform and amongst such cases we may find perfect STS(v)s.

2 Basic Theory

The fundamental theory upon which the computations are based is described in the following Theorem. We state, and use, the Theorem for v a prime but we note that it also holds, with minor and obvious changes to the wording, when v is a prime power.

Theorem
Suppose that v is a prime congruent to 7 modulo 12 and that ω is a primitive root of v. Suppose also that α and $1 - \alpha$ are residues modulo v having the forms $\alpha \equiv \omega^{3i+k}$ and $1 - \alpha \equiv \omega^{3j+l} \pmod{v}$, where i and j are integers and $\{k, l\} = \{1, 2\}$. Let G denote the group comprising all the mappings of the form $x \mapsto \omega^{6n}x + m \pmod{v}$ for $0 \leq n < (v-1)/6$ and $0 \leq m < v$. Then the orbit generated by the block $\{0, 1, \alpha\}$ under the action of G forms an STS(v).

Proof
Since $|G| = v(v - 1)/6$ is the number of blocks in an STS(v), it suffices to prove that every pair of points $\{\gamma, \beta\} \subset Z_v$ appears in some block of the orbit. Because of the transitivity of the cyclic subgroup of G generated by $x \mapsto x + 1 \pmod{v}$ it suffices to prove that this is true for all pairs of the form $\{0, \beta\}$. We may write $\beta \equiv \omega^{6q+r} \pmod{v}$, where $0 \leq q < (v - 1)/6$ and $r \in \{0, 1, 2, 3, 4, 5\}$. We may write v in the form $v = 12s + 7$ for some

integer s and then $\omega^{6s+3} \equiv -1 \pmod{v}$. The orbit generated by $\{0, 1, \alpha\}$ will contain all blocks of the form $\{0, \omega^{6n}, \alpha\omega^{6n}\}$, $\{-\omega^{6n}, 0, (\alpha-1)\omega^{6n}\}$ and $\{-\alpha\omega^{6n}, (1-\alpha)\omega^{6n}, 0\}$ for $0 \leq n < (v-1)/6$.

However, $\{\omega^{6n}, \alpha\omega^{6n}, -\omega^{6n}, (\alpha-1)\omega^{6n}, -\alpha\omega^{6n}, (1-\alpha)\omega^{6n}\} = \{\omega^{6n}, \omega^{6n+3i+k}, \omega^{6n+6s+3}, \omega^{6n+6s+3j+l+3}, \omega^{6n+6s+3i+k+3}, \omega^{6n+3j+l}\}$ and the exponents in this set take all six of the values 0, 1, 2, 3, 4, 5 modulo 6. Consequently, for an appropriate choice of n, precisely one of the six powers of ω will give $\omega^{6q+r} \equiv \beta \pmod{v}$. □

As an immediate corollary of the above Theorem suppose that α is taken to be a primitive sixth root of unity modulo v. Then $\alpha^6 - 1 = (\alpha^3+1)(\alpha^3-1) \equiv 0$. Since $\alpha^3 \not\equiv 1$ we have $\alpha^3 + 1 = (\alpha+1)(\alpha^2 - \alpha + 1) \equiv 0$. Since $\alpha \not\equiv -1$ it follows that $\alpha^2 - \alpha + 1 \equiv 0$ and so $1 - \alpha \equiv 1/\alpha$. Thus if $v = 36s + 7$ we have $\omega^{36s+6} \equiv 1$, and if we put $\alpha \equiv \omega^{6s+1}$ then from the previous observation $1 - \alpha \equiv \omega^{30s+5}$, so that $\{\alpha, 1-\alpha\}$ satisfies the conditions of the Theorem. Similarly if $v = 36s + 31$ so that $\omega^{36s+30} \equiv 1$, and if we put $\alpha \equiv \omega^{6s+5}$ then $1 - \alpha \equiv \omega^{30s+25}$, so that $\{\alpha, 1-\alpha\}$ again satisfies the conditions of the Theorem. These choices for α correspond to the well-known Netto systems [3]. However the Netto systems for $v = 36s + 19$ are not obtained because $\{\alpha, 1-\alpha\}$ does not satisfy the conditions of the Theorem when $\alpha \equiv \omega^{6s+3}$.

The Netto systems are, in fact, invariant under the group of mappings $x \mapsto \omega^{2n}x + m \pmod{v}$ for $0 \leq n < (v-1)/2$ and $0 \leq m < v$. This larger group is doubly homogeneous and consequently there is just one orbit of pairs. Thus the graphs $G_{a,b}$ are all of a single type and the Netto systems are uniform. The structure of the cycle graph has been investigated by Robinson [4]. Define the character $\chi(a)$ to have the value 1, 0 or -1 according as a is a non-zero square, 0 or a nonsquare. Robinson shows that the cycle graph contains a unique cycle of length 4 when $\chi(2) = 1$, i.e. when $v \equiv 7 \pmod{24}$ but no such cycle when $\chi(2) = -1$, i.e. when $v \equiv 19 \pmod{24}$. He also gives the conditions for the graph to contain a 6-cycle, namely that there exists a such that $\chi(a) = 1$, $\chi(a-1) = 1$, $\chi(a+\mu) = -1$ and $\chi(a+\mu^2) = -1$ where μ and μ^2 are the solutions of $x^3 \equiv 1 \pmod{v}$, other than 1. As is easily verified, in the case where $v \equiv 19 \pmod{24}$ the conditions are satisfied by choosing $a = \mu$ if $\chi(\mu - 1) = 1$ and $a = \mu^2$ if $\chi(\mu - 1) = -1$. So, apart from when $v = 7$, the Netto systems are never perfect.

3 Computational Results

As a prelude, suppose that $\{\alpha, 1-\alpha\}$ satisfies the conditions of the Theorem. Then the six STS(v)s generated by the blocks $\{0, 1, \beta\}$ for $\beta \in \{\alpha, 1-\alpha, 1/(1-\alpha), \alpha/(\alpha-1), 1-1/\alpha, 1/\alpha\}$ are all isomorphic. The reader may easily check this by applying, in turn, the mappings $x \mapsto 1-x$, $x \mapsto (x-1)/(\alpha-1)$, $x \mapsto (\alpha - x)/(\alpha - 1)$, $x \mapsto 1 - x/\alpha$ and $x \mapsto x/\alpha$ (mod v) to the block $\{0, 1, \alpha\}$. We may therefore limit the scope of an exhaustive search firstly to the case when α has the form ω^{3i+1} (mod v). Furthermore, for each such value of α we may eliminate from consideration the values $1/(1-\alpha)$ and $1 - 1/\alpha$ which will have the same form. We also note that the choice of the primitive ω is immaterial.

Armed with these observations we have examined all prime numbers v of the form $v = 12s + 7$ up to and including $v = 75079$. In each case we firstly determine a primitive root ω and next examine all potential values of α. When $\{\alpha, 1-\alpha\}$ satisfies the conditions of the Theorem we examine $G_{0,1}$, $G_{0,\alpha}$ and $G_{1,\alpha}$ to determine if each of these three graphs comprise a single $(v-3)$-cycle. The perfect STS(v)s obtained by this method are given below. In each case we quote the least primitive root ω and the lowest possible value of α (not necessarily of the form ω^{3i+1}). In no case do we find a perfect system arising from more than one set of six equivalent values of α.

v	7	79	139	367	811	1531	25771	50923	61339	69991
ω	3	3	2	6	3	2	2	2	2	3
α	3	29	25	112	18	84	4525	12999	630	7175

For prime numbers of the same form up to and including $v = 50383$ we have also searched for uniform systems which are not perfect. In addition to the Netto systems which occur for primes of the form $v = 36s + 7$ and $v = 36s + 31$ and which were described in Section 2, four further systems were found and these are as follows.

1. $v = 31$, $\omega = 3$, $\alpha = 12$.
   This is PG(4,2).

2. $v = 43$, $\omega = 3$, $\alpha = 10$.
   The cycle type of this system is $\{4, 36\}$.

3. $v = 13063, \quad \omega = 5, \quad \alpha = 2174.$
   The cycle type of this system is $\{4, 13056\}$.

4. $v = 34303, \quad \omega = 17, \quad \alpha = 5386.$
   The cycle type of this system is $\{4, 34296\}$.

Despite the above computations we are unable to identify a general method which permits the construction of any new infinite families of uniform Steiner triple systems. A possible first step might be to characterize those values of v for which uniform or perfect systems can be constructed by the method described in this paper.

References

[1] C. J. Colbourn and A. Rosa, *Leaves, excesses and neighbourhoods in triple systems*, Australas. J. Combin. **4** (1991), 143-178.

[2] M. J. Colbourn and R. A. Mathon, *On cyclic Steiner 2-designs*, Annals of Discrete Math. **7** (1980), 215-253.

[3] A. Delandtsheer, J. Doyen, J. Siemons and C. Tamburini, *Doubly homogeneous 2-(v,k,1) designs*, J. Combin. Theory A **43** (1986), 140-145.

[4] R. M. Robinson, *The structure of certain triple systems*, Math. of Comput. **29** (1975), 223-241.

[5] V. D. Tonchev, *Transitive Steiner triple systems of order 25*, Discrete Math. **67** (1987), 211-214.