BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(80), 2016, Pages 118–124
ISSN 1024–7696

On cosets in Steiner loops

Aleš Drápal, Terry S. Griggs

Abstract. We give a complete answer to the question of when the cosets of a Steiner subloop $\bar{W}$ of a Steiner loop $\bar{V}$ form a partition of $\bar{V}$. We also determine when $\bar{W}$ is a normal subloop of $\bar{V}$.

Mathematics subject classification: 05B07, 20N05.
Keywords and phrases: Steiner triple system, Steiner loop, coset, normal subloop.

1 Introduction

Let L be a loop and M be a subloop of L. For all $x \in L$, the set xM (resp. Mx) is a left (resp. right) coset of M. If $L = G$ is a group and $M = H$ is a subgroup then, as is very well known, the cosets form a partition of G, i.e. for $x, y \in G$, either $xH = yH$ (resp. $Hx = Hy$) or $xH \cap yH = \emptyset$ (resp. $Hx \cap Hy = \emptyset$). However the same is not true for loops in general and leads to the following definition (see I.2.10 of [8]).

Definition The loop L has a left (resp. right) coset decomposition modulo M if the set of all left (resp. right) cosets modulo M is a partition of L. We call this the *decomposition property*.

Properties of cosets in loops were studied in [6] where on page 180 the authors remark that "the article should be viewed as a point of departure for a more systematic study". In this paper we will be interested in Steiner loops, a variety of loops not studied in [6]. Again the decomposition property does not generally hold and the aim of this paper is to study those situations where it does. We are able to give a complete description of the structure of such Steiner loops and subloops including normality.

We recall the basic definitions and results which are appropriate for our purposes. A *Steiner triple system* of order v, STS(v), is a pair $(V, \mathcal{B})$ where V is a set of *points* of cardinality v and $\mathcal{B}$ is a set of triples of V, called *blocks*, such that every pair of distinct points is contained in precisely one block. Such systems exist if and only if $v \equiv 1$ or $3 \pmod 6$ [7], see also [2]. Given an STS(v), a *Steiner loop* is defined on the set $\bar{V} = V \cup \{e\}$ by the rules $ex = xe = x$, $xx = e$, for all $x \in \bar{V}$, $xy = z$ if $\{x, y, z\} \in \mathcal{B}$. We say that the Steiner loop is *associated* with the Steiner triple system. The process is reversible. Thus there is a one-one correspondence between all Steiner triple systems and all Steiner loops and the existence spectrum of the latter is $v + 1 \equiv 2$ or $4 \pmod 6$. Note that in this formulation, a Steiner loop of order 2 is associated with the STS(1) having no blocks and a Steiner loop of order 4 is associated with the STS(3) having one block and containing all three points. The latter Steiner loop is isomorphic to the Klein group $\mathbb{K}_4$. Algebraically a Steiner loop can be characterized as a totally symmetric loop. The variety of such loops is described by the identities $xy = yx$ and $x \cdot yx = y$. In every such loop $xx = e$, where e is the identity element.

In addition we will need the concept of a 3-*group divisible design*, 3-GDD. This is an ordered triple $(V, \mathcal{G}, \mathcal{B})$ where V is a set of *points* of cardinality v, $\mathcal{G}$ is a partition of V into *groups* and $\mathcal{B}$ is a set of triples of V, called *blocks*, such that every pair of distinct points is contained in either precisely one group or one block, but not both. We will only be interested in 3-GDDs which are *uniform*, i.e. $v = gu$ and V is partitioned into u groups all of cardinality g. The 3-GDD is said to be of type g^u. Necessary and sufficient conditions for the existence of 3-GDDs of type g^u were determined in [4], see also [3].

First we observe that if $\bar{W}$ is a subloop of a Steiner loop $\bar{V}$, then it does not follow that the order of $\bar{W}$ divides the order of $\bar{V}$. For example there are 86 701 547 non-isomorphic STS(19)s containing a subsystem STS(7), equivalently Steiner loops of order 20 containing a subloop of order 8,[5]. An example of a situation where the order of the subloop does divide the order of the Steiner loop but the decomposition property does not hold is given by the STS(19) with base set $V = \{0, 1, \dots, 18\}$ and block set $\mathcal{B}$ generated by the triples $\{0, 1, 8\}$, $\{0, 2, 5\}$, $\{0, 4, 13\}$, under the action of the mapping $i \mapsto i + 1 \pmod{19}$. A subloop of order 4 is $\bar{W} = \{e, 0, 1, 8\}$ and two cosets are $2\bar{W} = \{2, 5, 9, 12\}$ and $5\bar{W} = \{5, 2, 14, 3\}$.

In Section 2, given a Steiner loop $\bar{W}$ of order $w + 1$ we give an exhaustive construction of Steiner loops of order $v + 1$ for which $\bar{W}$ is a subloop with the decomposition property and in Section 3 we determine when $\bar{W}$ is normal. Finally in Section 4, we show that if all subloops of order 2 are normal or if all subloops of order 4 have the decomposition property then the Steiner loop is the elementary Abelian 2-group associated with a projective Steiner triple system.

2 Cosets

Let $S = (V, \mathcal{B})$ be an STS(v) and $\bar{V}$ be its associated Steiner loop. Further let $T = (W, \mathcal{C})$ with $W \subset V$ and $\mathcal{C} \subset \mathcal{B}$ be a proper subsystem STS(w) of S and $\bar{W}$ be its associated Steiner loop. Let $s = (v + 1)/(w + 1)$. We require s to be integral, called the *index* of $\bar{W}$ in $\bar{V}$. Since both $v + 1 \equiv 2$ or $4 \pmod 6$ and $w + 1 \equiv 2$ or 4 (mod 6) it follows that $s \equiv 1$ or $2 \pmod 3$. Further $2 \le s \le (v + 1)/2$. It will be more instructive to deal first with the two cases: (i) $s = 2$ and (ii) $s = (v + 1)/4$. This will then make it easier to describe the more general case (iii) $2 \le s \le (v+1)/4$. Finally we consider the case (iv) $s = (v + 1)/2$.

Case (i): $s = 2$.
Thus $v = 2w + 1$ and the structure of the STS(v) is given by the following well known doubling construction (see Lemma 8.1.2 of [1]). Let $W = \{x_1, x_2, \dots, x_w\}$

and $V = W \cup \{y_1, y_2, \ldots, y_{w+1}\}$ where the x_i's and y_i's are distinct. Consider a one-factorization of the complete graph K_{w+1} on vertices $V \setminus W$ and let $\mathcal{F}_1, \mathcal{F}_2, \ldots, \mathcal{F}_w$ be the one factors. The STS(v) consists of the blocks of the STS(w) on the set W together with all of the blocks $x_i\mathcal{F}_i$, $1 \leq i \leq w$. In the Steiner loop $\bar{V}$, the subloop $\bar{W} = W \cup \{e\}$ and there is one further coset $V \setminus W$.

Case (ii): $s = (v+1)/4$.
Here $w = 3$ and the subloop $\bar{W} = \{e, a, b, c\}$ where the triple $\{a, b, c\} \in \mathcal{B}$. Choose $y \in V$. Then $y\bar{W} = \{y, p, q, r\}$ is a coset where the triples $\{a, y, p\}, \{b, y, q\}, \{c, y, r\} \in \mathcal{B}$. It then follows that $p\bar{W} = q\bar{W} = r\bar{W} = y\bar{W}$ which implies that further triples $\{a, q, r\}, \{b, p, r\}, \{c, p, q\} \in \mathcal{B}$, i.e. the points $\{a, b, c, y, p, q, r\}$ form an STS(7). The structure of the STS(v) is now clear. We must have that $v \equiv 3$ or $7 \pmod{12}$. Put $u = (v-3)/4$. Let $Y_0 = \{a, b, c\}$ and $Y_i = \{y_i, p_i, q_i, r_i\}$, $1 \leq i \leq u$. Then $V = \bigcup_{i=0}^{u} Y_i$. Triples $\{a, b, c\}$, $\{a_i, y_i, p_i\}, \{b_i, y_i, q_i\}, \{c_i, y_i, r_i\}, \{a_i, q_i, r_i\}, \{b_i, p_i, r_i\}, \{c_i, p_i, q_i\} \in \mathcal{B}$. The remaining blocks are the blocks of a 3-GDD of type 4^u on the set $V \setminus \{a, b, c\}$ where the sets Y_i, $1 \leq i \leq u$, form both the groups of the group divisible design and the cosets of the subloop $\bar{W}$. Such 3-GDDs always exist, see [3].

Case (iii): $2 \leq s \leq (v+1)/4$.
We are now able to describe this more general case with reference to the two cases considered above. Let $W = Y_0 = \{x_1, x_2, \ldots, x_w\}$ and $Y_i = \{y_{i,1}, y_{i,2}, \ldots, y_{i,w+1}\}$, $1 \leq i \leq s-1$. Let $V = \bigcup_{i=0}^{s-1} Y_i$. For each i, $1 \leq i \leq s-1$, let $\mathcal{F}_{i,1}, \mathcal{F}_{i,2}, \ldots, \mathcal{F}_{i,w}$ be the one factors of a one-factorization of the complete graph K_{w+1} on vertex set Y_i. The blocks of the STS(v) are of three types: (i) the blocks of the STS(w), (ii) the triples $x_j\mathcal{F}_{i,j}$, $1 \leq i \leq s-1$, $1 \leq j \leq w$, (iii) the blocks of a 3-GDD of type $(w+1)^{s-1}$ on the set $\bigcup_{i=1}^{s-1} Y_i$ where the sets Y_i form the groups of the 3-GDD. Such 3-GDDs always exist, see [3]. The subloop $\bar{W} = W \cup \{e\}$ and the sets Y_i are the other cosets.

Case (iv): $s = (v+1)/2$.
This is the simplest case to describe. The subloop $\bar{W}$ is of order 2 and comprises the set $\{e, x\}$ for any $x \in V$. The other cosets are the pairs of points which occur in blocks of the STS(v) which contain the point x. Probably more conveniently, this case can also be regarded as a special case of the general Case (iii) where $w = 1$.

We can express all of the above by the following theorem.

Theorem 2.1. *Let $S = (V, \mathcal{B})$ be a Steiner triple system of order v and $T = (W, \mathcal{C})$ be a proper subsystem of order w. Then the Steiner loop $\bar{V}$ associated with S has a coset decomposition modulo $\bar{W}$, the Steiner loop associated with T, if and only if*
(i) $s = (v+1)/(w+1)$ is an integer, and
(ii) S contains $s-1$ subsystems $S_i = (V_i, \mathcal{B}_i)$, $1 \leq i \leq s-1$, of order $2w+1$ where $V_i \cap V_j = W$ and $\mathcal{B}_i \cap \mathcal{B}_j = \mathcal{C}$, $1 \leq i < j \leq s-1$.

The above theorem has an elegant algebraic formulation.

Corollary 2.2. *Let M be a subloop of a finite Steiner loop L. Then L has a coset decomposition modulo M if and only if L can be covered by subloops of order $2|M|$, any two of which intersect in M.*

3 Normality

We begin with a definition.

Definition Let L be a commutative loop and M be a subloop of L. Then M is *normal* if its cosets $xM = Mx$ form a partition of L and induce a factor loop.

This means that for any two cosets xM and yM there exists a coset zM such that for all $a \in xM$ and $b \in yM$, $ab \in zM$. The fact that this does not hold in general for a Steiner loop can be shown by the following easy example.

Example 3.1. Let S be the STS(9) with base set $V = \{0, 1, \ldots, 8\}$ and block set $\mathcal{B}$ consisting of the triples $\{0,1,2\}$, $\{3,4,5\}$, $\{6,7,8\}$, $\{0,3,6\}$, $\{1,4,7\}$, $\{2,5,8\}$, $\{0,4,8\}$, $\{1,5,6\}$, $\{2,3,7\}$, $\{0,5,7\}$, $\{1,3,8\}$, $\{2,4,6\}$. This gives the Steiner loop with the following Cayley table.

	e	0	1	2	3	4	5	6	7	8
e	e	0	1	2	3	4	5	6	7	8
0	0	e	2	1	6	8	7	3	5	4
1	1	2	e	0	8	7	6	5	4	3
2	2	1	0	e	7	6	8	4	3	5
3	3	6	8	7	e	5	4	0	2	1
4	4	8	7	6	5	e	3	2	1	0
5	5	7	6	8	4	3	e	1	0	2
6	6	3	5	4	0	2	1	e	8	7
7	7	5	4	3	2	1	0	8	e	6
8	8	4	3	5	1	0	2	7	6	e

Then $2(3\{e,0\}) \neq 7\{e,0\}$.

In order to determine which Steiner subloops are normal we return to the structure of the STS(v) as described in Case (iii). First note that if $x = e$, the equation $x(yM) = (xy)M$ is satisfied trivially. The other cosets are the sets Y_i, $1 \le i \le s-1$, which form the groups of a 3-GDD of type $(w+1)^{s-1}$. Thus normality is equivalent to the 3-GDD having the property that if Y_i and Y_j, $i \neq j$, are groups of the 3-GDD then all of the $(w+1)^2$ products xy, where $x \in Y_i$ and $y \in Y_j$ must lie in the same group. Thus the set of groups themselves define a Steiner triple system and so $s - 1 \equiv 1$ or $3 \pmod 6$. The construction of a 3-GDD which ensures normality is now clear and can be obtained by a standard design-theoretic technique. Let $Z = (Y, \mathcal{D})$ be an STS($s-1$). Now inflate each point $y \in Y$ by a factor $w+1$, i.e. replace each point by a set of $w+1$ points. Then replace each block $D \in \mathcal{D}$ by a

3-GDD of type $(w+1)^3$, equivalently a Latin square of side $w+1$, on the inflated points.

This is perhaps better illustrated by an example.

Example 3.2. Let $v = 31$ and $w = 3$, so $s = 8$.
Then $T = (W, \mathcal{C})$ is an STS(3). Let $W = \{a, b, c\}$ and $\mathcal{C} = \{abc\}$. Here and throughout the example, for simplicity, we will represent blocks by the concatenation of three points.
Further $S = (V, \mathcal{B})$ is an STS(31) and contains 7 subsystems $(V_i, \mathcal{B}_i)$, $1 \le i \le 7$, whose intersection is T. Let $V_i \backslash W = \{x_i, y_i, z_i, w_i\}$ and $\mathcal{B}_i = \{abc, ax_iy_i, az_iw_i, bx_iz_i, by_iw_i, cx_iw_i, cy_iz_i\}$.
To complete the STS(31) choose an STS(7) on base set $\{1, 2, 3, 4, 5, 6, 7\}$ with block set say $\{123, 145, 167, 246, 257, 347, 356\}$ and a Latin square on set {x,y,z,w}, say

	x	y	z	w
x	x	y	z	w
y	w	x	y	z
z	z	w	x	y
w	y	z	w	x

Now for each block of the STS(7) proceed as follows. We will illustrate using the block 246. Choose one element, say 2, to be the row, a second element, say 4, to be the column and the third element, say 6, to be the entry and assign these to the Latin square to obtain further triples of the STS(31), i.e. $x_2x_4x_6$, $x_2y_4y_6$, $x_2z_4z_6$, $x_2w_4w_6$, $y_2x_4w_6$, $y_2y_4x_6$, $y_2z_4y_6$, $y_2w_4z_6$, $z_2x_4z_6$, $z_2y_4w_6$, $z_2z_4x_6$, $z_2w_4y_6$, $w_2x_4y_6$, $w_2y_4z_6$, $w_2z_4w_6$, $w_2w_4x_6$.
Note that it is permissible to use different Latin squares for each triple but this just complicates the process.

Again we can express all of the above by a theorem.

Theorem 3.3. *Let $S = (V, \mathcal{B})$ be a Steiner triple system of order v and $T = (W, \mathcal{C})$ be a subsystem of order w. Then the Steiner loop $\bar{W}$ associated with T is normal in $\bar{V}$, the Steiner loop associated with S, if and only if*
(i) $s = (v+1)/(w+1) \equiv 2$ or $4 \pmod 6$,
(ii) S contains $s-1$ subsystems $S_i = (V_i, \mathcal{B}_i)$, $1 \le i \le s-1$, of order $2w+1$ where $V_i \cap V_j = W$ and $\mathcal{B}_i \cap \mathcal{B}_j = \mathcal{C}$, $1 \le i < j \le s-1$, and
(iii) for each $i, j : 1 \le i < j \le s-1$, there exists $k : 1 \le k \le s-1$ such that for all blocks $\{x, y, z\} \in \mathcal{B}$ if $x \in V_i \setminus W$ and $y \in V_j \setminus W$ then $z \in V_k \setminus W$.

Finally in this section, it may be worth noting that normality depends critically on the value of s, the index of the subloop $\bar{W}$ in the Steiner loop $\bar{V}$. We have already observed that $s \equiv 1$ or $2 \pmod 3$. Comparing the statements of Theorem 2.1 and Theorem 3.3 it follows that if $s \equiv 1$ or $5 \pmod 6$, then the subloop $\bar{W}$ cannot be normal. If $s = 2$, condition (iii) in Theorem 3.3 does not apply and so the subloop $\bar{W}$ is always normal. We have the situation described in Case (i) of

Section 2. If $s = 4$, condition (iii) in Theorem 3.3 is automatically satisfied and so in this case too, the subloop $\bar{W}$ must be normal. For other values of $s \equiv 2$ or $4 \pmod 6$, both situations can occur; the subloop $\bar{W}$ is normal depending on whether or not condition (iii) holds. Nevertheless, as indicated, we can always construct a Steiner system $S = (V, \mathcal{B})$ so that condition (iii) is satisfied and thus the subloop $\bar{W}$ is normal.

4 Small subloops

In this section we will be interested in Steiner subloops of order 2 or 4, i.e. subloops which contain respectively either a single point or three points of a block of the associated Steiner triple system. First consider subloops of order 2. It is immediate from Theorem 2.1 that in every Steiner loop, every subloop of order 2 has the decomposition property. But the subloops need not be normal as was shown in Example 3.1. This naturally raises the question of when all the subloops of order 2 of a Steiner loop are normal. The answer is easy. A normal subloop of order 2 is always central. Thus the Steiner loop must be the elementary Abelian 2-group of order 2^n associated with the projective $\mathrm{STS}(2^n - 1) = \mathrm{PG}(n-1, 2)$, $n \geq 2$. This result can also be proved combinatorially and this we now do since it will be relevant to when we consider subloops of order 4.

Let $S = (V, \mathcal{B})$ be an $\mathrm{STS}(v)$ where $v \equiv 3$ or $7 \pmod{12}$. Choose $x \in V$ so $\{e, x\}$ is a Steiner subloop of order 2. Let $w = (v-1)/2$, then $w \equiv 1$ or $3 \pmod 6$. The cosets are the pairs $Y_1 = \{y_1, z_1\}, Y_2 = \{y_2, z_2\}, \ldots, Y_w = \{y_w, z_w\}$ where $\{x, y_i, z_i\} \in \mathcal{B}$, $i = 1, 2, \ldots, w$. If $\{e, x\}$ is normal then the system S is completed by choosing an $\mathrm{STS}(w)$ on base set $\{Y_1, Y_2, \ldots, Y_w\}$ and replacing each block $\{Y_i, Y_j, Y_k\}$ by the triples $\{y_i, y_j, y_k\}, \{y_i, z_j, z_k\}, \{z_i, y_j, z_k\}, \{z_i, z_j, y_k\}$. These four triples on six points are known as a *quadrilateral* or *Pasch configuration*. There are $w(w-1)/6 = (v-1)(v-3)/24$ blocks in the $\mathrm{STS}(w)$ and thus also the same number of Pasch configurations. So in total, by considering all v points there will be $v(v-1)(v-3)/24$ Pasch configurations in S. This is the maximum number possible and only occurs in the projective systems [9].

Turning now to subloops of order 4, observe that any such subloop which has the decomposition property, tightly controls the structure of the associated Steiner triple system S. From Theorem 2.1, S must contain $(v-3)/4$ subsystems of order 7, all of which intersect in the block associated with the subloop. From [5], of the 86 701 547 non-isomorphic STS(19)s containing a subsystem STS(7), a mere 2 557 contain 4 or more subsystems of order 7. So the vast majority of Steiner loops obtained from these systems will not contain a subloop of order 4 with the decomposition property.

Example 4.1. Consider the STS(9) in Example 3.1. Let $V' = \{x' : x \in V\}$. Construct an STS(19) on base set $V \cup V' \cup \{\infty\}$ as follows. For each block $\{x, y, z\}$ which is a block of the STS(9), let triples $\{x, y, z\}$, $\{x, y', z'\}$, $\{x', y, z'\}$, $\{x', y', z\}$ be blocks of the STS(19). Complete the system with blocks $\{\infty, x, x'\}$ for each $x \in V$.

On the other hand, consider the STS(19) constructed in the above example. It contains 12 STS(7)s. Each of the blocks $\{\infty, x, x'\}, x \in V$, is contained in 4 of these STS(7)s and the subloops $\{e, \infty, x, x'\}, x \in V$, have the decomposition property. All other blocks are contained in just a single STS(7). Thus we might ask whether there exist Steiner loops, all of whose subloops of order 4 have the decomposition property. Again the answer is easy and can be proved both algebraically and combinatorially. Choose $x, y, z \in \bar{V}$. If $e \in \{x, y, z\}$ or $\{x, y, z\} \in \mathcal{B}$, then $x(yz) = (xy)z$ trivially. Otherwise $\bar{W} = \{x, y, xy, e\}$ is a subloop of order 4 and $\bar{W} \cup z\bar{W}$ is a subloop of order 8. This latter subloop is associative and so is a group, i.e. induced by a projective Steiner triple system. Combinatorially we can argue as follows. Consider any block of the associated Steiner triple system. It must be contained in $(v-3)/4$ STS(7)s. Since there are $v(v-1)/6$ blocks this gives $v(v-1)(v-3)/(24 \times 7)$ different STS(7)s. Finally each STS(7) contains 7 Pasch configurations so there are $v(v-1)(v-3)/24$ of these again the maximum possible and the Steiner loops are the elementary Abelian groups associated with the projective Steiner triple systems.

References

[1] I. Anderson, Combinatorial Designs: Construction Methods, Ellis Horwood, New York, 1990.

[2] C. J. Colbourn and A. Rosa, Triple Systems, Oxford University Press, Oxford, 1999.

[3] G. Ge, Group divisible designs, Handbook of Combinatorial Designs, second edition (ed. C. J. Colbourn and J. H. Dinitz), Chapman and Hall/CRC Press, 255–260, 2007.

[4] H. Hanani, Balanced incomplete block designs and related designs, *Discrete Math.* **11** (1975), 255–369.

[5] P. Kaski, P. R. J. Östergård, S. Topolova and R. Zlatarski, Steiner triple systems of order 19 and 21 with subsystems of order 7, *Discrete Math.* **308** (2008), 2732–2741.

[6] M. Kinyon, K. Pula and P. Vojtěchovský, Incidence properties of cosets in loops, *J. Combin. Designs* **20** (2012), 179–197.

[7] T. P. Kirkman, On a problem in combinations, *Cambridge and Dublin Math. J.* **2** (1847), 191–204.

[8] H. O. Pflugfelder, Quasigroups and Loops: Introduction, Heldermann Verlag, Berlin, 1990.

[9] D. R. Stinson and Y. J. Wei, Some results on quadrilaterals in Steiner triple systems, *Discrete Math.* **105** (1992), 207–219.

Received February 2, 2016

Aleš Drápal
Department of Algebra
Charles University
Sokolovská 83
186 75 Praha 8, CZECH REPUBLIC
E-mail: *drapal@karlin.mff.cuni.cz*

Terry S. Griggs
Department of Mathematics and Statistics
The Open University
Walton Hall
Milton Keynes MK7 6AA, UNITED KINGDOM
E-mail: *t.s.griggs@open.ac.uk*