BULL. AUSTRAL. MATH. SOC. 20N05, 05B07
VOL. 42 (1990) [157–165]

SINGLE LAWS FOR TWO SUBVARIETIES OF SQUAGS

DIANE DONOVAN

We give single laws for two subvarieties of Steiner quasigroups (squags); the subvariety of squags whose underlying triple systems are the affine spaces over $GF[3]$, and the subvariety of squags whose underlying triple systems are the affine triple systems.

Let S be a set of size v. Then a *Steiner triple system*, $\mathcal{S}$, is a collection of 3-subsets chosen from S in such a way that each pair of distinct elements $x, y \in S$ occurs in precisely one 3-subset. The 3-subsets are called the blocks of $\mathcal{S}$. Any Steiner triple system can be co-ordinatised by a Steiner quasigroup, termed a squag.

DEFINITION: ([2], pp.3–4) Let $\mathcal{S}$ be a Steiner triple system defined on a set S. Define a binary operation $\circ$ on S by:

(i) if $x, y \in S$ and $x \neq y$, then $x \circ y = z$ where $\{x, y, z\} \in \mathcal{S}$;
(ii) if $x \in S$, then $x \circ x = x$.

Then $(S, \circ)$ is a commutative quasigroup, known as a *Steiner quasigroup* or *squag*.

The commutativity of $\circ$ follows naturally and it is easily shown that $x \circ (x \circ y) = y$ for all $x, y \in S$ and so we have the following basis for the variety of squags.

THEOREM 1. ([2], pp.3–4) *A basis for the variety of all squags is given by:*

(i) $x \circ x = x$,
(ii) $x \circ y = y \circ x$,
(iii) $x \circ (x \circ y) = y$,

where $x, y \in S$.

Donovan and Oates-Williams [1] gave a single law for the variety of squags.

THEOREM 2. [1] *The variety of all squags is defined by the law*

$$x \circ ((w \circ (w \circ (((y \circ y) \circ z) \circ y))) \circ x) = z,$$

Received 21st November, 1989.
I wish to thank Dr. Sheila Oates–Williams for her suggestions and for detecting an error in an earlier draft. I wish to acknowledge the support of a Special Grant from the University of Queensland.

where $w, x, y, z \in S$.

If we place further conditions on the variety of squags, we form subvarieties. We take two subvarieties and show that the basis for each subvariety can be expressed in terms of a single law.

Recall that the *medial law* for elements w, x, y, z of a quasigroup is given by:

$$(w \circ x) \circ (y \circ z) = (w \circ y) \circ (x \circ z).$$

THEOREM 3. ([2] p.19) *The subvariety of squags whose underlying Steiner triple systems are the affine spaces over* $GF[3]$, *is characterised among all squags by the law*

$$(w \circ x) \circ (y \circ z) = (w \circ y) \circ (x \circ z)$$

where $w, x, y, z \in S$.

In the next theorem we show that this subvariety can be defined by a single law.

THEOREM 4. *The subvariety of squags whose underlying triple systems are the affine spaces over* $GF[3]$ *is defined by the law*

$$y \circ ((y \circ y) \circ ((w \circ y) \circ ((x \circ w) \circ ((x \circ z) \circ y)))) = z,$$

where $x, y, z \in S$.

PROOF: First we show that the law

$$y \circ ((y \circ y) \circ ((w \circ y) \circ ((x \circ w) \circ ((x \circ z) \circ y)))) = z \tag{1}$$

is satisfied by the subvariety of squags given in Theorem 3. Using the medial law we obtain

$$y \circ ((y \circ y) \circ ((w \circ (x \circ w)) \circ (y \circ ((x \circ z) \circ y))))$$

for the left-hand side of the above equation. If we apply the identities given in Theorem 1, then we see that this simplifies to z, as required.

We now take the given law and show that the identities listed in Theorems 1 and 3 can be derived from it.

Equation 1 can be rewritten in terms of left and right multiplication as follows:

$$L(x)R(y)L(x \circ w)L(w \circ y)L(y \circ y)L(y) = I. \tag{2}$$

We see that left multiplication is one-to-one and onto and hence a permutation. So we can write:

$$R(y) = L^{-1}(x)L^{-1}(y)L^{-1}(y \circ y)L^{-1}(w \circ y)L^{-1}(x \circ w),$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

and it follows that right multiplication is a permutation. Since both left multiplication and right multiplication are permutations our groupoid is a quasigroup.

We now rewrite Equation 2 as $L(x)R(y)L(x\circ w) = L^{-1}(y)L^{-1}(y\circ y)L^{-1}(w\circ y)$, which is independent of x and so:

$$(x\circ w)\circ((x\circ z)\circ y) = (v\circ w)\circ((v\circ z)\circ y) \tag{3}$$

for all v, w, x, y, z. Similarly we obtain $L(s\circ t)L(t\circ r) = R^{-1}(r)L^{-1}(s)L^{-1}(r)L^{-1}(r\circ r)$, which is independent of t and so:

$$(t\circ r)\circ((s\circ t)\circ z') = (u\circ r)\circ((s\circ u)\circ z') \tag{4}$$

for all r, s, t, u, z'. Let $x = t = s = z$, $r = w$ and $z' = y$. Then the left-hand sides of Equations 3 and 4 are equal, implying:

$$(v\circ w)\circ((v\circ z)\circ y) = (u\circ w)((z\circ u)\circ y).$$

Let $u = v$, then:

$$(v\circ w)\circ((v\circ z)\circ y) = (v\circ w)\circ((z\circ v)\circ y).$$

Thus $v\circ z = z\circ v$ for all v, z, and the quasigroup is commutative.

Return to Equation 4 and choose $r = t = s = z' = z$ and $u = z\circ z$. Then:

$$(z\circ z)\circ((z\circ z)\circ z) = ((z\circ z)\circ z)\circ((z\circ(z\circ z))\circ z).$$

Using the fact that the quasigroup is commutative we obtain:

$$z\circ z = (z\circ(z\circ z))\circ z;$$

implying:

$$z = z\circ(z\circ z)$$

for all z. Now return to Equation 4 again and choose $r = t = s = z' = z$. This gives:

$$(z\circ z)\circ((z\circ z)\circ z) = (u\circ z)\circ((z\circ u)\circ z).$$

Let $x = u\circ z$ then, by commutativity, we obtain:

$$z = x\circ(x\circ z). \tag{5}$$

Let u range over the quasigroup. This equation is then true for all x, z.

We return to Equation 4 again, and use this to verify the medial law. Choose $s = t\circ q$, for some q, or equivalently $s\circ t = (t\circ q)\circ t$, implying $q = s\circ t$. Also choose $u = s\circ r$ or equivalently $u\circ r = s$ or $s\circ u = r$. Then:

$$(t\circ r)\circ((s\circ t)\circ z) = (u\circ r)\circ((s\circ u)\circ z),$$

or:

$$(t\circ r)\circ(q\circ z) = s\circ(r\circ z);$$

but $s = t\circ q$ and so:

$$(t\circ r)\circ(q\circ z) = (t\circ q)\circ(r\circ z),$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

for all r, z, t, q. The medial law is satisfied.

If we replace y by x in Equation 1 we see that:

$$x\circ((x\circ x)\circ((w\circ x)\circ((x\circ w)\circ((x\circ z)\circ x)))) = z.$$

Since $x\circ(x\circ z) = (x\circ z)\circ x = z$,

$$x\circ((x\circ x)\circ((w\circ x)\circ((x\circ w)\circ z))) = z.$$

Using commutativity and Equation 5 again:

$$x\circ((x\circ x)\circ z) = z.$$

Choosing $x = z$, we can write:

$$z\circ((z\circ z)\circ z) = z,$$

or

$$z\circ z = z,$$

for all z.

The result now follows. □

Next we give a single law for the subvariety of squags which is characterised by the distributive law. In the variety of all squags the distributive law is obtained from the medial law by letting $w = x$. However the identity given in Theorem 6 implies the distributive law directly. Further, this identity yields the required properties, but has a smaller word length than that given in Theorem 4; that is, it has word length 9 instead of 10. We include the proof of this result as it uses slightly different techniques than those given in Theorem 4.

An *affine triple system* is a triple system where every three points generate an affine plane of order 9. Young [4] characterised the subvariety of squags whose underlying triple systems are the affine triple systems in terms of the distributive law. For elements x, y, z of a quasigroup the *distributive law* is given by

$$x\circ(y\circ z) = (x\circ y)\circ(x\circ z).$$

THEOREM 5. [4] *The subvariety of squags whose underlying triple systems are the affine triple systems is characterised among all squags by the law*

$$x\circ(y\circ z) = (x\circ y)\circ(x\circ z),$$

where $x, y, z \in S$.

THEOREM 6. *The subvariety of squags whose underlying triple systems are the affine triple systems, is defined by the law*

$$y\circ((y\circ y)\circ(w\circ((x\circ w)\circ((x\circ z)\circ w)))) = z,$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

where $w, x, y, z \in S$.

PROOF: Clearly this law holds for squags which satisfy the distributive law. We must show that the three laws given in Theorem 1 and the distributive law can be derived from this law. We let z range over the whole groupoid and express the law

$$y\circ((y\circ y)\circ(w\circ((x\circ w)\circ((x\circ z)\circ w)))) = z \tag{6}$$

in terms of left and right multiplication as follows:

$$L(x)R(w)L(x\circ w)L(w)L(y\circ y)L(y) = I. \tag{7}$$

We see that left multiplication is one-to-one and onto and hence is a permutation. So we can write:

$$R(w) = L^{-1}(x)L^{-1}(y)L^{-1}(y\circ y)L^{-1}(w)L^{-1}(x\circ w),$$

and it follows that right multiplication is also a permutation. Since both left and right multiplication are permutations, our groupoid is a quasigroup.

We can rewrite Equation 7 as $R(w)L(x\circ w)L(w) = L^{-1}(x)L^{-1}(y)L^{-1}(y\circ y)$, which is independent of w and so:

$$w\circ((x\circ w)\circ(z\circ w)) = u\circ((x\circ u)\circ(z\circ u)), \tag{8}$$

for all u, w, x, z. Similarly, $L(r)L(s\circ s)L(s) = L^{-1}(x\circ r)R^{-1}(r)L^{-1}(x)$, and this is independent of s so:

$$s\circ((s\circ s)\circ(r\circ z')) = t\circ((t\circ t)\circ(r\circ z')), \tag{9}$$

for all r, s, t, z'. Let $w = s = z' = x$ and $r = z$. Then the left-hand sides of Equations 8 and 9 are equal, so:

$$u\circ((x\circ u)\circ(z\circ u)) = t\circ((t\circ t)\circ(z\circ x)).$$

Letting $t = u$ yields:

$$(x\circ u)\circ(z\circ u) = (u\circ u)\circ(z\circ x), \tag{10}$$

for all u, x, z. Equation 7 also gives $L(x)R(w)L(x\circ w) = L^{-1}(y)L^{-1}(y\circ y)L^{-1}(w)$. This equation is independent of x and so:

$$(x\circ w)\circ((x\circ z)\circ w) = (v\circ w)\circ((v\circ z)\circ w),$$

for all v, w, x, z. If we let $w = x$ in this equation we have:

$$(x\circ x)\circ((x\circ z)\circ x) = (v\circ x)\circ((v\circ z)\circ x),$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

and by applying Equation 10 to the right-hand side of this we obtain:

$$(x \circ x) \circ ((x \circ z) \circ x) = (x \circ x) \circ ((v \circ z) \circ v).$$

This now implies that

$$(x \circ z) \circ x = (v \circ z) \circ v \tag{11}$$

for all v, x, z. If we let $x = z$ and $v = z \circ z$ in this last equation, then:

$$(z \circ z) \circ z = ((z \circ z) \circ z) \circ (z \circ z),$$

and by applying Equation 10 to the right-hand side of this we obtain:

$$(z \circ z) \circ z = (z \circ z) \circ (z \circ (z \circ z)).$$

Cancelling $z \circ z$ gives:

$$z = z \circ (z \circ z), \tag{12}$$

for all z. Take Equation 11 again and let $z = v \circ v$ so:

$$(x \circ (v \circ v)) \circ x = (v \circ (v \circ v)) \circ v,$$

or by Equation 12:

$$(x \circ (v \circ v)) \circ x = v \circ v, \tag{13}$$

for all v, x. Rewrite Equation 7 in the form $L(y \circ y)L(y) = L^{-1}(w)L^{-1}(x \circ w)R^{-1}(w)L^{-1}(x)$. This is independent of y and so:

$$y \circ ((y \circ y) \circ z) = v \circ ((v \circ v) \circ z), \tag{14}$$

for all v, y, z. Now let $z = y \circ y$, implying:

$$y \circ ((y \circ y) \circ (y \circ y)) = v \circ ((v \circ v) \circ (y \circ y)).$$

If we apply Equation 10 to the right-hand side of this we obtain:

$$y \circ ((y \circ y) \circ (y \circ y)) = v \circ ((y \circ v) \circ (y \circ v)).$$

Now let $v = y \circ y$ and so:

$$y \circ ((y \circ y) \circ (y \circ y)) = (y \circ y) \circ ((y \circ (y \circ y)) \circ (y \circ (y \circ y))),$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

which, using Equation 12, reduces to:

$$y\circ((y\circ y)\circ(y\circ y)) = (y\circ y)\circ(y\circ y).$$

We go on to use this equation and Equations 12 and 13 to show that the original identity does in fact imply that the system is idempotent. Recall Equation 6:

$$y\circ((y\circ y)\circ(w\circ((x\circ w)\circ((x\circ z)\circ w)))) = z.$$

Let $x = w$ and $z = w\circ w$ as follows:

$$y\circ((y\circ y)\circ(w\circ((w\circ w)\circ((w\circ(w\circ w))\circ w)))) = w\circ w.$$

Using Equation 13 this can be rewritten as

$$y\circ((y\circ y)\circ(w\circ((w\circ w)\circ(w\circ w)))) = w\circ w.$$

But earlier we noted that $y\circ((y\circ y)\circ(y\circ y)) = (y\circ y)\circ(y\circ y)$, and so:

$$y\circ((y\circ y)\circ((w\circ w)\circ(w\circ w))) = w\circ w.$$

Now let $y = w$ implying:

$$w\circ((w\circ w)\circ((w\circ w)\circ(w\circ w))) = w\circ w,$$

or by Equation 12:

$$w\circ(w\circ w) = w\circ w.$$

But Equation 12 states that $w\circ(w\circ w) = w$, therefore $w\circ w = w$ and the system is idempotent.

Using the fact that the system is idempotent in Equation 13 gives:

$$(x\circ v)\circ x = v,$$

for all v, x.

Next we prove commutativity. The quasigroup is idempotent so we can rewrite Equation 14 as:

$$y\circ(y\circ z) = v\circ(v\circ z).$$

Let $y = z$ and by Equation 12 we obtain:

$$z = v\circ(v\circ z).$$

https://doi.org/10.1017/S0004972700028276 Published online by Cambridge University Press

But we have just stated that $(u \circ z) \circ u = z$, and so:

$$v \circ (v \circ z) = (u \circ z) \circ u.$$

So if we let $u = v$ and $u \circ z = t$, then:

$$t \circ u = u \circ t.$$

Let z range over the quasigroup; then the equation is true for all t, u. Hence our quasigroup is commutative.

Finally we show that the distributive law is satisfied. Take Equation 10:

$$(x \circ u) \circ (z \circ u) = (u \circ u) \circ (z \circ x),$$

and since $u \circ u = u$ and our system is commutative we can write:

$$u \circ (z \circ x) = (u \circ z) \circ (u \circ x)$$

for all u, x, z.

The result now follows. □

We conclude this paper by considering an alternate characterisation for the subvariety of squags whose underlying triple systems are the affine triple systems. If we take the distributive law, on this variety of squags, we see that:

$$x \circ (y \circ z) = (x \circ y) \circ (x \circ z);$$

distributing once again gives

$$= ((x \circ y) \circ x) \circ ((x \circ y) \circ z),$$

and since $(x \circ y) \circ x = y$:

$$= y \circ ((x \circ y) \circ z),$$

and finally:

$$= ((x \circ y) \circ z) \circ y.$$

Hence the subvariety of squags given in Theorem 5 could have been characterised by the law $x \circ (y \circ z) = ((x \circ y) \circ z) \circ y$. We say that the element y is an associator. In fact Macdonald [3] showed precisely this. Macdonald considered the affine triple systems in terms of their associated sloops (see [2] p.4, for a definition). She showed that if x, y, z, where $x \circ y \neq z$, are all distinct non-identity elements of a sloop, with underlying triple systems the affine triple systems, then $x \circ (y \circ z) = ((x \circ y) \circ z) \circ y$. This corresponds to showing the property is satisfied by the given subvariety of squags.

References

[1] Diane Donovan and Sheila Oates-Williams, 'Single laws for sloops and squags', *Discrete Math.* (to appear).

[2] B. Ganter and H. Werner, 'Co-ordinatizing Steiner systems', *Ann. Discrete Math.* **7** (1980), 3–24.

[3] Sheila Oates Macdonald, 'A characterisation of affine triple systems', *Ars Combin.* **2** (1976), 23–24.

[4] H. Peyton Young, 'Affine triple systems and Matroid Designs', *Math. Z.* **132** (1973), 343–359.

Department of Mathematics
The University of Queensland
Queensland 4072 Australia