All the Shortest Single Axioms for Boolean SQS-Skeins

Nick C. Fiala

Department of Mathematics
St. Cloud State University
St. Cloud, MN 56301
ncfiala@stcloudstate.edu

Abstract

In this note, we show that the variety of Boolean SQS-skeins can be defined by a single axiom and, in the process, we find all of the shortest single axioms for said variety. Our investigations were aided by the automated theorem-prover Prover9 and the finite model-finder Mace4.

1 Introduction

A *Steiner triple* (*quadruple*) *system*, or STS (SQS), is a pair $(X, \mathcal{B})$ where X is a set, the elements of which are called *points*, and $\mathcal{B}$ is a set of 3-subsets (4-subsets) of X, the elements of which are called *blocks*, such that every 2-subset (3-subset) of points is contained in exactly one block.

Given an SQS $(X, \mathcal{B})$, we can construct an algebra $(X; q)$ of type (3) as follows: define $q(y, x, x) = q(x, y, x) = q(x, x, y) = y$ for all $x, y \in X$ and also define $q(x, y, z)$ to be the fourth point in the unique block containing $\{x, y, z\}$ for all distinct $x, y, z \in X$. Clearly, this algebra satisfies the four identities below.

$$q(x, x, y) = y \tag{1}$$

$$q(x, y, z) = q(x, z, y) \tag{2}$$

$$q(x, y, z) = q(y, z, x) \tag{3}$$

$$q(x, y, q(x, y, z)) = z \tag{4}$$

Conversely, given an algebra $(X; q)$ of type (3) that satisfies (1), (2), (3), and (4), we can construct an SQS whose points are the elements of X and whose blocks are the 4-subsets of X of the form $\{x, y, z, q(x, y, z)\}$, x,

y, and z distinct. Therefore, there is a one-to-one correspondence between SQS's and type (3) algebras satisfying (1), (2), (3), and (4) [7], just as there is a one-to-one correspondence between STS's and idempotent totally symmetric quasigroups (squags). For this reason, type (3) algebras $(X; q)$ satisfying (1), (2), (3), and (4) are known as SQS-*skeins.*

The smallest non-trivial subvariety of SQS-skeins is the variety of SQS-skeins $(X; q)$ such that there exists a Boolean group $(X; +)$ such that $q(x, y, z) = x + y + z$. These are known as *Boolean* SQS-*skeins*, or BSQS-*skeins.* It is known that the BSQS-skeins are precisely the SQS-skeins that satisfy the additional identity below [3].

$$q(x, u, q(y, u, z)) = q(x, y, z) \tag{5}$$

Remark 1.1. It can be shown that BSQS-skeins can be axiomatized by $q(x, y, x) = y$ and (5). However, we will only work with the more familiar axiomatization of BSQS-skeins by (1), (2), (3), (4), and (5) in this paper.

We will call an identity in a single ternary operation q a *single axiom for* BSQS-*skeins* if and only if the identity is valid in all BSQS-skeins and all models of the identity are BSQS-skeins. Single axioms for several varieties of algebras arising from combinatorial designs are known. For instance, in [2], it was shown that

$$x((w(w(((yy)z)y)))x) = z$$

is a single axiom for squags and, in [1], it was shown that

$$y((yy)(w((xw)((xz)w)))) = z$$

is a single axiom for the subvariety of squags corresponding to the Hall triple systems (distributive squags) and

$$y((yy)((wy)((xw)((xz)y)))) = z$$

is a single axiom for the subvariety of squags corresponding to the affine spaces over $GF(3)$ (medial squags). Also, in [8], it was shown that

$$q(q(x, y, q(z, q(u, u, q(v, w, q(q(s, t, t), w, v))), z)), x, y) = s$$

is a single axiom for SQS-skeins. Therefore, it is natural to ask if there exists a single axiom for BSQS-skeins and, if so, what is the shortest such identity (in terms of the number of variable occurrences) and what is the smallest number of distinct variables among such identities.

In this note, we show that the variety of BSQS-skeins admits a single axiom (or is *one-based*) and, in the process, we find all of the shortest single axioms for said variety. Our investigations were aided by the automated theorem-prover Prover9 [6] and the finite model-finder Mace4 [5]. Prover9 searches for proofs by contradiction of first-order statements while Mace4 searches for finite models of first-order statements. Their combination can be a powerful tool in investigations of this kind. We also used the scripting language Perl to further automate our search. For another example of automated reasoning being used to find all of the shortest single axioms for a variety of algebras, see [4], where it was shown that

$$y((y((yy)(xz)))(z(zz))) = x \quad ((yy)y)(((y(xz))(zz))z) = x$$
$$(y((((yy)y)(xz))z))(zz) = x$$

are all of the shortest single axioms for groups of exponent 4 (up to renaming, mirroring, and symmetry).

2 Single Axioms for BSQS-Skeins

In this section, we describe our search for the shortest single axioms for BSQS-skeins.

We began by generating all identities (up to renaming and symmetry) in a single ternary operation q with at most eight variable occurrences and with the following properties. One side consists of a single variable (otherwise it would be valid in any model of $q(x,y,z) = q(u,v,w)$) that is not the left-most (right-most) variable on the other side (otherwise it would be valid in any model of $q(x,y,z) = x$ ($q(x,y,z) = z$)) where each occurring variable occurs at least twice (otherwise it would imply $x = y$ in a BSQS-skein). This resulted in 4381 identities.

We then sent the negation of each identity (stored in the Perl variable `$negated_identity`) to Mace4 and ran

```
assign(domain_size, 2).  % model of size two
clauses(theory).
q(x,x,y) = y.  q(x,y,z) = q(x,z,y).  q(x,y,z) = q(y,z,x).
q(x,y,q(x,y,z)) = z.  q(x,u,q(y,u,z)) = q(x,y,z).  % BSQS-skein
$negated_identity.
end_of_list.
```

to search for a 2-element BSQS-skein that does not satisfy the identity and then removed the identities for which a model was found. This resulted in 2392 identities. For example, the identity $q(x, q(x,y,y), q(z,z,z)) = y$ was eliminated at this stage in 0.06 seconds (the maximum amount of time it took to eliminate an identity at this stage).

Next, we sent the negation of each of these identities to Prover9 and ran

```
set(auto).  % autonomous mode
clauses(sos).  % set of support
q(x,x,y) = y.  q(x,y,z) = q(x,z,y).  q(x,y,z) = q(y,z,x).
q(x,y,q(x,y,z)) = z.  q(x,u,q(y,u,z)) = q(x,y,z).  % BSQS-skein
$negated_identity.
end_of_list.
```

to search for a proof that the identity is implied by (1), (2), (3), (4), and (5) and is therefore valid in the variety of BSQS-skeins. A proof was found for all of these identities. For example, a proof of length 13 (the longest proof found at this stage) was found for the identity $q(x, q(y, q(z, u, x), u), z) = y$ and a proof was found in 0.05 seconds (the maximum amount of time it took to find a proof at this stage) for the identity $q(x, q(y, q(z, u, u), y), x) = z$.

We then sent each of these identities (stored in the variable `$identity`) to Mace4 and ran

```
assign(iterate_up_to, 200).  % model of size at most 200
assign(max_seconds, 3600).  % one hour time limit per identity
clauses(theory).
$identity.
q(0,0,a) != a | q(0,a,b) != q(0,b,a) | q(0,a,b) != q(a,b,0) |
 q(0,a,q(0,a,b)) != b | q(0,c,q(a,c,b)) != q(0,a,b).  % not
                                                        BSQS-skein
end_of_list.
```

to search for a model of the identity that does not satisfy at least one of (1), (2), (3), (4), and (5), and therefore is not a BSQS-skein, and then removed the identities for which a model was found. This resulted in 80 identities. For example, the identity $q(x, q(y, z, u), q(z, u, x)) = y$ was eliminated at this stage by an 8-element model (the largest model that eliminated an identity at this stage) and the identity $q(x, y, q(q(z, u, u), y, x)) = z$ was eliminated at this stage in 316.2 seconds (the maximum amount of time it took to eliminate an identity at this stage).

Next, we sent each of these identities to Prover9 and ran

```
set(auto).  % autonomous mode
assign(max_seconds, 60).  % one minute time limit per identity
clauses(sos).  % set of support
$identity.
q(a,a,b) != b | q(a,b,c) != q(a,c,b) | q(a,b,c) != q(b,c,a) |
 q(a,b,q(a,b,c)) != c | q(a,d,q(b,d,c)) != q(a,b,c).  % not
                                                        BSQS-skein
end_of_list.
```

to search for a proof that the identity implies (1), (2), (3), (4), and (5), and is therefore a single axiom for BSQS-skeins. A proof was found for 78 identities. For example, a proof of length 43 (the longest proof found at this stage) was found for the identity $q(x, q(q(y, z, u), x, y), y) = z$ and a proof was found in 0.27 seconds (the maximum amount of time it took to find a proof at this stage) for the identity $q(x, y, q(z, u, q(y, u, x))) = z$.

Finally, the two remaining identities for which a proof was not found were each shown to be valid in a non-Boolean 10-element SQS-skein (using Mace4). Therefore, we have the following result.

Theorem 2.1. *The variety of* BSQS*-skeins is one-based. A shortest single axiom for* BSQS*-skeins has exactly eight variable occurrences (and exactly four distinct variables). There are exactly* 78 *shortest single axioms for* BSQS*-skeins (up to renaming and symmetry). They can all be obtained by uniformly permuting the three arguments of* q *in one of the* 13(= 78/6) *identities below.*

$$q(q(q(x,y,z),x,u),y,u) = z \qquad q(q(q(x,y,z),x,u),z,u) = y$$
$$q(q(q(x,y,z),y,u),x,z) = u \qquad q(q(q(x,y,z),y,u),z,x) = u$$
$$q(q(x,q(x,y,z),u),y,u) = z \qquad q(q(x,q(x,y,z),u),z,u) = y$$
$$q(q(x,q(y,x,z),u),y,z) = u \qquad q(q(x,q(y,z,u),z),x,u) = y$$
$$q(q(x,q(y,z,u),u),y,x) = z \qquad q(q(x,q(y,z,u),u),z,x) = y$$
$$q(q(x,y,z),q(x,z,u),u) = y \qquad q(q(x,y,z),q(x,u,y),u) = z$$
$$q(q(x,y,z),q(z,x,u),u) = y$$

References

[1] D. Donovan, *Single laws for two subvarieties of squags*, Bull. Austral. Math. Soc. **42** (1990), 157–165.

[2] D. Donovan and Sheila Oates-Williams, *Single laws for sloops and squags*, Discrete Math. **92** (1991), 79–83.

[3] A. J. Guelzow, *Semi-Boolean* SQS*-skeins*, J. Algebraic Combin. **2** (1993), 147–153.

[4] K. Kunen, *The shortest single axioms for groups of exponent* 4, Computers and Math. with Appl. **29** (1995), 1–12.

[5] W. McCune, *Mace4* (http://www.cs.unm.edu/~mccune/prover9/).

[6] W. McCune, *Prover9* (http://www.cs.unm.edu/~mccune/prover9/).

[7] R. W. Quackenbush, *Algebraic aspects of Steiner quadruple systems*, in: Proc. Conf. Algebraic Aspects of Combinatorics, Univ. of Toronto, 1973, 265-268.

[8] Z. Stojaković, *Single identities for Mendelsohn and Steiner 3-quasigroups*, Bull. Austral. Math. Soc. **53** (1996), 419–424.