Representation of finite nilpotent squags

Andreas J. Guelzow*

Department of Mathematics, Concordia University, College of Alberta, 7128 Ada Blvd, Edmonton, AB, Canada T5B 4E4

Received 14 January 1992; revised 4 August 1994

Abstract

Squags arise from the co-ordinatization of Steiner triple systems. We will present a strengthened version of the representation theorem given by S. Klossek for finite distributive squags and generalize this theorem to the class of all finite nilpotent squags.

1. Introduction

Klossek, in [12], presented representation and construction theorems for finite distributive squags. Unfortunately, the representation obtained by her representation theorem is too weak to be used in connection with her powerful construction theorems. In Section 4, we will strengthen her theorem and generalize it to all finite nilpotent squags. (We are using the universal algebraic concept of nilpotence as given in [2].) We will see our representation theorem to be indeed a generalization of Klossek’s result: every distributive squag is nilpotent in the squag theoretic sense — this has been proven in [1, 12] — and in Section 5 we see that the universal algebraic and squag theoretic concepts of nilpotence coincide. In Section 6, we will briefly discuss the interaction of the improved representation theorem with Klossek’s construction theorems.

In this paper we use commutator theory and universal algebra in general as presented in [2, 6]. We endeavour to provide as much detail as possible to allow the reader inexperienced in these fields to understand the concepts and methods.

A squag is an algebra \( \langle S; \cdot \rangle \) of type (2) satisfying the equations:

\[
\begin{align*}
\mathbf{A} & \quad x \cdot x = x \\
\mathbf{B} & \quad x \cdot y = y \cdot x \\
\mathbf{C} & \quad x \cdot (x \cdot y) = y
\end{align*}
\]

\* Author’s research was in part supported by NSERC grant 0121310.

* Alternative address: Department of Mathematics, University of Alberta, Edmonton, AB, Canada T6G 2E9 E-mail: aguelzow@vega.math.ualberta.ca

0012-365X/96/$15.00 © 1996—Elsevier Science B.V. All rights reserved

SSDI 0012-365X(94)00312-2
Squags arise from the co-ordinatization of Steiner triple systems (see [5]) and have been well studied. Two interesting subvarieties are the class of all distributive squags, i.e. squags satisfying the additional equation:

\[(x \cdot y) \cdot (x \cdot z) = x \cdot (y \cdot z)\]

and the class of all medial squags, i.e. squags satisfying the additional equation:

\[(w \cdot x) \cdot (y \cdot x) = (w \cdot y) \cdot (x \cdot z).\]

Distributive squags are also called commutative reflection spaces (kommutative Spiegelungsräume) and symmetric distributive quasigroups. The finite members of each variety can be nicely characterized via their corresponding Steiner triple systems: finite distributive squags are exactly those squags that correspond to Hall triple systems, i.e. to Steiner triple systems whose subplanes are the affine (9-element) plane over GF(3), and finite medial squags are those corresponding to affine geometries over GF(3). Clearly every medial squag is distributive.

2. Notation

To further simplify the presentation of our — rather technical — proofs we will use the following notation: Given a vector \(x \in A^n\), \(x_i\) denotes the \(i\)th component of \(x\). Similarly, if \(p : A^n \times A^n \to A^n\), then we say \(p\) is a polynomial in \(x\) and \(y\) if every \((p(x, y))_i\) is a polynomial in \(x_1, \ldots, x_n, y_1, \ldots, y_n\). Since we will frequently consider projections, we will denote the image of \(x \in A^n\) under the projection onto the components \(i\) to \(j\) with \(x_{[i,j]}\), i.e. \(x_{[i,j]} = (x_i, x_{i+1}, \ldots, x_j)\). We will also use the abbreviation \(x_{[i,j]} = x_{(1,j)}\). Note that \(x_{[i,i]} = x_i\); but, in general, \(x_{[i,j]} \neq x_i\). Moreover, \(0_{[n]}\) is the vector \((0, \ldots, 0) \in GF(3)^n\).

We will omit the subscript \([n]\) if the number of components in \(0\) is obvious from the context. Vectors with small numbers of non-zero entries will also be used frequently. If \(a \in GF(3)\) then \(a_{[i]}\) denotes the vector in \(GF(3)^n\) given by

\[a_{[i]} = \begin{cases} a & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}\]

Note that \(0_{[n]} = 0_{[n]}\). For a set \(X \subseteq GF(3)^n\), the support of \(X\) is given by \(sup(X) = \{i \mid \exists x \in X : x_i \neq 0\}\). We abbreviate \(sup(x) = sup(\{x\})\) if \(x \in GF(3)^n\). The cardinality of the support is called the weight \(w(X)\), i.e. \(w(X) = |sup(X)|\). Again we abbreviate \(w(x) = w(\{x\})\) if \(x \in GF(3)^n\). Note that \(w(x)\) is commonly called the Hamming-weight of \(x\). If \(z = ((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)) \in (A \times B)^n\) then \(z_A\) and \(z_B\) denote the elements \(z_A = (x_1, x_2, \ldots, x_n) \in A^n\) and \(z_B = (y_1, y_2, \ldots, y_n) \in B^n\). \(\omega_\Delta\) and \(\omega_{\Omega}\) are the maximal and minimal congruences on an algebra \(\mathcal{A} = \langle A; \Omega \rangle\), i.e. \(\omega_\Delta = A^2\) and \(\omega_{\Omega} = \{(x, x) : x \in A\}\). If \(\alpha\) and \(\beta\) are any congruences on the algebra \(\mathcal{A} = \langle A; \Omega \rangle\) in a congruence modular variety, then \([\alpha, \beta] = \text{the commutator of } \alpha\text{ and } \beta\) is the commutator of \(\alpha\) and \(\beta\). A complete definition of the commutator can be found in [2]. Another congruence of importance in this paper is the center \(\zeta(\mathcal{A})\) of an algebra \(\mathcal{A} = \langle A; \Omega \rangle\). It is the maximal
congruence $\alpha$ on $\mathcal{A}$ such that $[1_{\mathcal{A}}, \alpha] = \omega_{\mathcal{A}}$. If $\alpha$ is any congruence on an algebra $\langle A; \Omega \rangle$ and $x \in A$, then $[x] \alpha$ is the congruence class of $\alpha$ containing $x$. Moreover, given a set $M \subseteq A$, $\Theta^\alpha(M)$ denotes the smallest congruence on $\mathcal{A}$ containing $M \times M$.

3. A universal algebraic tool

Some (universal) algebras contain a group structure. These algebras are called **affine**:

**Definition 3.1.** Let $\mathcal{A} = \langle A; \Omega \rangle$ be any algebra. $\mathcal{A}$ is called **affine** if and only if there exists an abelian group $\mathcal{A}' = \langle A; +, -, 0 \rangle$ and a ternary term function $\tau(x, y, z)$ of $\mathcal{A}$ such that

$$\tau(x, y, z) = x - y + z \quad \text{for all } x, y, z \in A$$

and

$$\{(x, y, z, u) \mid x + y = z + u\}$$

is a subalgebra of $\mathcal{A}'$. If this abelian group exists it is called the **group associated with $\mathcal{A}$** and the term function $\tau$ is called a **difference function for $\mathcal{A}$**.

A related concept is nilpotence — a generalization of the group theoretic concept to congruence modular varieties:

**Definition 3.2.** Let $\mathcal{A} = \langle A; \Omega \rangle$ be an algebra in a congruence modular variety. Let $\{\phi_i\}_{i=1}^{\infty}$ be the sequence of congruences on $\mathcal{A}$ given by:

$$\phi_0 = \{1_{\mathcal{A}}\}$$  
$$\phi_i = \begin{cases} 1_{\mathcal{A}} & \text{if } i = 0, \\ \phi_{i-1} \cdot 1_{\mathcal{A}} & \text{otherwise.} \end{cases}$$

$\mathcal{A}$ is said to be of **nilpotence class $k$** if $\phi_k = \omega_{\mathcal{A}}$ but $\phi_{k-1} \neq \omega_{\mathcal{A}}$. An algebra of nilpotence class 1 is also called **abelian**.

It is well known that an algebra $\mathcal{A} = \langle A; \Omega \rangle$ with $|A| > 1$ is nilpotent of class $k$ if and only if $\mathcal{A}/\zeta(\mathcal{A})$ is nilpotent of class $k - 1$. Christian Herrmann has shown in [10] that the affine algebras in modular varieties are exactly the abelian algebras. The main tool in the proof of our representation theorem is the description of the structure of the non-affine algebras in a congruence modular variety given by Freese and McKenzie in [2]. This description uses the following concept of a product of two algebras:

**Definition 3.3** (Freese and McKenzie [2]). Let $\mathcal{A} = \langle A; \Omega \rangle$ and $\mathcal{B} = \langle B; F^i : i \in I \rangle$ be algebras in a modular variety. Let $\mathcal{T}$ be a system of maps $T_i : B^{n_i} \to Q$, ($i \in I$) where $n_i$ is the arity of $F^i$. 
Then \( \mathcal{A} = \mathcal{B} \otimes^T \mathcal{Q} \) is defined to be the algebra with:

\[
F'(a) = (F'(a_B), F'(a_Q) + T_1(a_B))
\]

where \( a \in (B \times Q)^k \).

Heuristically \( \mathcal{B} \otimes^S \mathcal{Q} \) is the direct product of \( \mathcal{B} \) and \( \mathcal{Q} \) with a twist (given by \( T \)) in the second component. Note that in [2] \( \mathcal{B} \) and \( \mathcal{Q} \) are exchanged. The notation has been modified to match the use in [12].

The finite abelian squags, i.e. the finite squags of nilpotence class 1, are the finite medial squags, the squags corresponding to affine geometries over \( \text{GF}(3) \). Applied to the theory of squags the description in [2] becomes therefore:

**Theorem 3.4** (Freese and McKenzie [2]). Let \( \mathcal{S} \) be a squag. Let \( \mathcal{R} = \mathcal{S}/\zeta(\mathcal{S}) \) where \( \zeta(\mathcal{S}) \) denotes the center of \( \mathcal{S} \). Then there exists an affine squag \( \mathcal{A} \) and a system \( T \) of maps as described above such that \( \mathcal{S} \cong \mathcal{R} \otimes^T \mathcal{A} \) and the centre of \( \mathcal{R} \otimes^T \mathcal{A} \) is the kernel of the projection onto \( \mathcal{R} \).

### 4. Representation of finite nilpotent squags

The theorem of Klossek in [12] that we will generalize is:

**Theorem 4.1** (Klossek [12]). Let \( \mathcal{S} = \langle S; \star \rangle \) be a finite distributive squag generated by the set \( A = \{a_0, a_1, \ldots, a_{n-1}\} \) and not by any proper subset of \( A \). Let \( \left| [a_0] \zeta(\mathcal{S}) \right| = 3^r \) and \( \zeta(\mathcal{S}) \subseteq \mathcal{F}(\mathcal{S}) \) where \( \mathcal{F}(\mathcal{S}) \) is the Fratini congruence of \( \mathcal{S} \), i.e. the intersection of the maximal congruences on \( \mathcal{S} \). Then there exists an \( m \)-dimensional vector space \( V \) with \( m \geq n - 1 \) and a polynomial \( p: V^2 \rightarrow V \) over \( \text{GF}(3) \) such that

1. \( p(0, 0) = 0 \), i.e. the polynomials \( p_i \) have no constant terms.
2. \( p(x, y)|_{y = 0} = 0 \) for any \( x, y \in V \).
3. \( p(x, 0) = 0 = p(0, x) \) for all \( x \in V \), i.e. all monomials of every \( p_i(x, y) \) contain elements of both sets \( \{x_1, \ldots, x_m\} \) and \( \{y_1, \ldots, y_m\} \).
4. For \( n \leq i \leq m - r \) the polynomial \( p_i(x, y) \) does not depend on the variables \( x_{m-r+1}, \ldots, x_m \) and \( y_{m-r+1}, \ldots, y_m \).
5. \( \mathcal{S} \) is isomorphic to \( \mathcal{V} = \langle V; \star \rangle \) where

\[
x \star y = -x - y + p(x, y).
\]

6. The Fratini congruence \( \mathcal{F}(\mathcal{S}) \) is the kernel of the projection onto the first \( (n - 1) \) components. This projection is a squag homomorphism.
7. \( \zeta(\mathcal{S}) \) is the kernel of the projection onto the first \( (m - r) \) components, this projection is also a squag homomorphism.
8. \( \phi: \mathcal{S} \overset{1:1}{\longrightarrow} \mathcal{V} \) can be chosen such that \( \phi(a_i) = 1_{[m]} \) for all \( i \) with \( 0 < i < n \) and \( \phi(a_0) = 0 \).
Since every abelian (i.e. medial) squag is isomorphic to an \((\text{GF}(3))^n; * \) with \(x \cdot y = -x - y\), Theorem 3.4 can be used to prove the following representation theorem by induction over the class of nilpotence:

**Theorem 4.2.** Let \( \mathcal{S} = \langle S; \circ \rangle \) be a finite squag of nilpotence class \( k \). Then there exists an \( m \)-dimensional vector space \( V \), a polynomial \( p: V^2 \to V \) over \( \text{GF}(3) \), and a sequence \( 1 \leq n_1 < \cdots < n_k = m \) of integers such that

1. If \( 1 \leq s < n \) and \( n_s < i \leq n_{s+1} \), then the polynomial \( p_s(x, y) \) does not depend on the variables \( x_{n_s+1}, \ldots, x_m \) and \( y_{n_s+1}, \ldots, y_m \).
2. \( (p(x, y))_{|n_1} = 0 \) for all \( x, y \in V \).
3. \( \mathcal{S} = \langle V; \circ \rangle \) is isomorphic to \( \mathcal{S} \) where \( x \circ y = -x - y + p(x, y) \).
4. The center \( \zeta(\mathcal{S}) \) corresponds to the kernel of the projection onto the first \( n_{k-1} \) components of \( \mathcal{S} \), this projection is a squag homomorphism.
5. If \( \omega_{ij} = \zeta_0 \leq \zeta_1 \leq \zeta_2 \leq \cdots \leq \zeta_k = 1 \) is the upper central series of \( \mathcal{S} \) then for any \( 1 \leq i \leq k \) the congruence \( \zeta_j \) corresponds to the kernel of the projection onto the first \( n_{k-j} \) components of \( \mathcal{S} \).

The polynomial \( p \) in this theorem will have in fact several further properties, that are simple consequences of the defining equations (A) of a squag:

**Lemma 4.3.** Let \( V \) be an \( m \)-dimensional vector space over \( \text{GF}(3) \), \( \langle V; \circ \rangle \) be a squag and \( p: V^2 \to V \) a polynomial over \( \text{GF}(3) \) such that \( x \circ y = -x - y + p(x, y) \).

Then for all \( x, y \in V \):

- (B) \( p(x, x) = 0 \),
- (C) \( p(x, y) = p(y, x) \),
- (D) \( p(x, y) = p(x, x \circ y) \)

Equation (B) implies that the polynomials \( p_i \) have no constant terms. Equations (C) and (D) say that \( p \) is constant on pairs from the same block, i.e. 2-generated subsquag.

It is clear that for any given finite nilpotent squag \( \mathcal{S} \) there may be different representations satisfying the conditions of Theorem 4.2. These representations can only differ in the choice of the polynomial \( p \). In the following, we will denote the set of all possible polynomials \( p \) satisfying 4.2 for a given finite nilpotent squag \( \mathcal{S} \) with \( \Psi(\mathcal{S}) \). We will show now that this polynomial \( p \) can always be chosen such that all monomials of each \( p_i \) must contain at least one of \( x_1, x_2, \ldots, x_{i-1} \) and one of \( y_1, y_2, \ldots, y_{i-1} \).

**Lemma 4.4.** For every finite nilpotent squag \( \mathcal{S} \) there exists \( p \in \Psi(\mathcal{S}) \) such that for all \( x \in V \)

\[
p(x, 0) = 0.
\]
The major tool in the proof of Lemma 4.4 is the use of appropriately defined isomorphisms. Lemma 4.5 provides this tool:

**Lemma 4.5.** Let $V$ be an $m$-dimensional vector space over $\text{GF}(3)$, $\mathcal{V} = \langle V; \cdot \rangle$ be a squag and $p: V^2 \to V$ a polynomial over $\text{GF}(3)$ such that

$$x \cdot y = -x - y + p(x, y)$$

and $p_i(x, y)$ does not depend on the variables $x_1, \ldots, x_m$ and $y_1, \ldots, y_m$. Let $k \in \{2, \ldots, m\}$ and let $\Pi(x): \text{GF}(3)^{k-1} \to \text{GF}(3)$ be a polynomial over $\text{GF}(3)$. Let $\phi: V \to V$ be the function

$$\phi(x) = \begin{cases} x_i & \text{if } i \neq k, \\ x_i + \Pi(x_{[k-1]}) & \text{if } i = k. \end{cases}$$

Let $\circ$ be the binary operation on $V$ defined by $x \circ y = -x - y + q(x, y)$ where $q: V^2 \to V$ is the polynomial over $\text{GF}(3)$ given by

$$(E) \quad q_i(x, y) = \begin{cases} p_i(x, y) & \text{if } 1 \leq i < k, \\ p_k(x, y) + \Pi(x_{[k-1]}) + \Pi(y_{[k-1]} + \Pi((x \cdot y)_{[k-1]}) & \text{if } i = k, \\ p_i(\phi(x), \phi(y)) & \text{if } i < k \leq m. \end{cases}$$

Then the mapping $\phi: \langle V; \cdot \rangle \to \langle V; \circ \rangle$ is an isomorphism with $\phi^{-1}$ given by

$$\phi^{-1}(x) = \begin{cases} x_i & \text{if } i \neq k, \\ x_i - \Pi(x_{[k-1]}) & \text{if } i = k. \end{cases}$$

Moreover, if $p \in \mathfrak{P}(\mathcal{V})$ then $q \in \mathfrak{P}(\mathcal{V})$.

Since the proof of Lemma 4.5 is completely straightforward, it has been omitted. The following proof of Lemma 4.4 is due to R.W. Quackenbush:

**Proof of Lemma 4.4.** Suppose there is no such $p$ and that $V$ is $m$-dimensional. Then let $p \in \mathfrak{P}(\mathcal{V})$ be a polynomial with maximal $k$ such that

$$(p(x, 0))_{[k-1]} = 0 \quad \text{for all } x \in V.$$ 

Clearly $1 < k \leq m$. Let $\cdot$ be the squag operation corresponding to $p$ and let $\Pi: \text{GF}(3)^{k-1} \to \text{GF}(3)$ be the polynomial over $\text{GF}(3)$ with $\Pi(x) = p_k(x, 0)$. Consider the polynomial $q$ given by Lemma 4.5. Clearly

$$(q(x, 0))_{[k-1]} = (p(x, 0))_{[k-1]} = 0 \quad \text{for all } x \in V.$$ 

Moreover, for $x \in V$

$$q(x, 0)_k = p_k(x, 0) + \Pi(x_{[k-1]}) + \Pi(0_{[k-1]}) + \Pi((x \cdot 0)_{[k-1]})$$

$$= p_k(x, 0) + p_k(x, 0) + p_k(0, 0) + p_k(x \cdot 0, 0)$$
and by equations (B) and (D) we obtain
\[ q(x, 0)_k = p_k(x, 0) + p_k(x, 0) + 0 + p_k(x, 0) = 3p_k(x, 0) = 0, \]
Since by Lemma 4.5 \( q \in \Psi(\mathcal{V}) \) this contradicts the maximality of \( k \).

Before we specify the polynomials for distributive squags even more closely, we will examine some additional properties of the polynomials described in Lemma 4.4. The following Lemmas 4.6 and 4.8 are due to R.W. Quackenbush.

**Lemma 4.6** (Quackenbush). Let \( \mathcal{V} = \langle V; \cdot \rangle \) be a squag, where \( V \) is an \( m \)-dimensional vector space over \( \text{GF}(3) \), and \( p: V^2 \to V \) a polynomial over \( \text{GF}(3) \) such that
\[ x \cdot y = -x - y + p(x, y) \]
and \( p_i(x, y) \) does not depend on the variables \( x_1, \ldots, x_m \) and \( y_1, \ldots, y_m \). Let \( 1 \leq k < m \), \( S \subseteq \{1, \ldots, k\} \) and let \( \langle Q; \cdot \rangle \) be a subsquag of \( \mathcal{V} \). Then
\[ \sup(Q) \subseteq S \Rightarrow \forall x, y \in Q: (p(x, y))_{[k+1,m]} = 0. \]
Since the proof of this lemma is utterly trivial we omit it. An immediate consequence of Lemma 4.6 is the following corollary:

**Corollary 4.7.** Let \( V \) be an \( m \)-dimensional vector space over \( \text{GF}(3) \), let \( \mathcal{V} = \langle V; \cdot \rangle \) be a squag, and let \( p: V^2 \to V \) be a polynomial over \( \text{GF}(3) \) such that
\[ x \cdot y = -x - y + p(x, y) \]
and \( p_i(x, y) \) does not depend on the variables \( x_1, \ldots, x_m \) and \( y_1, \ldots, y_m \) and
\[ p(0, x) = 0 \]
for all \( x \in V \). Then for all \( x, y \in V \)
\[ (w(x, y))^1 \leq 1 \Rightarrow p(x, y) = 0 \quad \text{and} \quad (p(x, y))_{[2]} = 0 \]
**Proof.** Since \( p(0, x) = 0 \) for all \( x \in V \), \( 0 \cdot x = -x \). Therefore, for every \( x \in V \) the set \( \{0, x, -x\} \) forms a subsquag of \( \mathcal{V} \). If \( \sup(\{x, y\}) \subseteq \{j\} \) then
\[ (p(x, y))_{[1,j]} = (p(0, 0))_{[1,j]} = 0 \]
\[ (p(x, y))_{[j+1,m]} = 0 \quad \text{by Lemma 4.6} \]
which establishes the implication. Since \( p_2(x, y) \) depends only on \( x_1 \) and \( y_1 \),
\[ (p(x, y))_{[2]} = (p((x_1)_{[m]}, (y_1)_{[m]}))_{[2]} = 0 \]
verifies the second statement. \( \square \)
The next result permits us to describe the polynomials for finite distributive squags even better.

**Lemma 4.8 (Quackenbush).** For every finite nilpotent squag \( \mathcal{S} \) there exists \( p \in \mathfrak{P}(\mathcal{S}) \) such that the following conditions hold (where \( \mathcal{V} = \langle V; \circ \rangle \) is the corresponding squag described in Theorem 4.2):

1. For all \( x \in V \),
   \[ p(x, 0) = 0. \]
2. Let \( m \) be the dimension of \( V \). If
   \[ S \subseteq \{1_{[m]}^{[1]}, \ldots, 1_{[m]}^{[m]}\} \]
   and the subsquag \( \langle Q; \circ \rangle \) of \( \mathcal{V} \) generated by \( S \cup \{0_{[m]}\} \) is medial, then
   \[ p(x, y) = 0 \]
   for all \( x, y \in Q \),
   i.e. \( x \circ y = -x - y \) for all \( x, y \in Q \).

**Proof.** By Lemma 4.4 we know there are polynomials in \( \mathfrak{P}(\mathcal{S}) \) satisfying condition (1). We have to show that among those polynomials we can find a polynomial \( p \) also satisfying condition (2). Suppose this is not possible. Then let \( \mathcal{S} \) be a counterexample with minimal \( m \). Choose \( p \in \mathfrak{P}(\mathcal{S}) \) such that the number of medial subsquags \( \mathcal{S} = \langle Q; \circ \rangle \) of \( \mathcal{V} \) for which condition (2) fails is also minimal. From among these \( \mathcal{S} \) pick a subsquag \( \mathcal{S}' \) generated by

\[ \{0, 1_{[m]}^{[i]}, \ldots, 1_{[m]}^{[i]}\} \quad \text{with} \quad i_s < i_t \quad \text{whenever} \quad s < t \]

such that \( j \) is minimal. By Corollary 4.7 \( m \geq 3 \) and \( j \geq 2 \). Since Lemma 4.8 obviously holds for medial squags \( \mathcal{S} \) we have \( m > j \geq 2 \). Since \( m \) is minimal, we also know that \( (p(x, y))_{[m-1]} = 0 \) for all \( x, y \in Q \). Therefore, by the minimality of \( j \), \( x_i = 0 \) for all \( x \in Q \) and \( i \notin \{i_1, \ldots, i_j, m\} \). Since the components in \( \{1, \ldots, m\}\backslash\{i_1, \ldots, i_j, m\} \) would be unnecessary for this counterexample, by the minimality of \( m \) in fact \( \{1, \ldots, m\} = \{i_1, \ldots, i_j, m\} \), i.e. \( j = m - 1 \) and \( i_k = k \) for all \( k = 1, \ldots, m - 1 \). Let

\[ \mathcal{Z} = \langle 0, 1_{[m]}^{[1]}, 2_{[m]}^{[2]}; \circ \rangle. \]

By Corollary 4.7 \( |Q| = 3^{m-1} \). Therefore \( \mathcal{S} \cong \mathcal{Z} \times \mathcal{Z} \). Since both \( \mathcal{Z} \) and \( \mathcal{Z} \) are medial, so is \( \mathcal{S} \) and for medial squags we know Lemma 4.8 to hold. \( \square \)

Since every 3-generated distributive squag is medial, we obtain immediately the following corollary:

**Corollary 4.9.** If \( \mathcal{S} = \langle S; \circ \rangle \) is a finite distributive squag then there exist a \( p \in \mathfrak{P}(\mathcal{S}) \) such that for all \( x, y \in V \)

\[ p(x, 0) = 0 \]
\[ w(\{x, y\}) \leq 2 \Rightarrow p(x, y) = 0 \]
and
\[(p(x, y))(0) = 0\]
(where \(\mathcal{V} = \langle V; \circ \rangle\) is the corresponding squag described in Theorem 4.2).

Using the preceding lemmas and some further arguments we can now formulate a stronger version of Theorem 4.2.

**Theorem 4.10** (Main representation theorem). Let \(\mathcal{S} = \langle S; \cdot \rangle\) be a finite squag of nilpotence class \(k\). Then there exists an \(m\)-dimensional vector space \(V\), a polynomial \(p : V^2 \to V\) over \(GF(3)\), and a sequence \(1 \leq n_1 < \cdots < n_k = m\) of integers such that

1. If \(1 \leq s < n\) and \(n_s < i \leq n_{s+1}\), then the polynomial \(p_i(x, y)\) does not depend on the variables \(x_{n_s+1}, \ldots, x_m\) and \(y_{n_s+1}, \ldots, y_m\).
2. For all \(x, y \in V\)
\[(p(x, y))(0) = 0.\]
3. \(\mathcal{V} = \langle V; \circ \rangle\) is isomorphic to \(\mathcal{S}\) where
\[x \circ y = -x - y + p(x, y).\]
4. The center \(\zeta(\mathcal{S})\) corresponds to the kernel of the projection onto the first \(n_k-1\) components of \(\mathcal{V}\), this projection is a squag homomorphism.
5. If \(\omega_{\mathcal{S}} = \xi_0 < \xi_1 < \xi_2 < \cdots < \xi_k = 1_{\mathcal{S}}\) is the upper central series of \(\mathcal{S}\) then for any \(1 \leq j \leq k\) the congruence \(\xi_j\) corresponds to the kernel of the projection onto the first \(n_k-j\) components of \(\mathcal{V}\).
6. For all \(x, y \in V\)
\[p(x, y) = p(y, x).\]
7. For all \(x \in V\)
\[p(x, 0) = 0,\]
i.e. no \(p_i\) has a constant term and all monomials in each \(p_i(x, y)\) contain variables from both sets \(\{x_1, \ldots, x_i-1\}\) and \(\{y_1, \ldots, y_i-1\}\).
8. For all \(x, y \in V\)
\[w(\{x, y\}) \leq 1 \implies p(x, y) = 0.\]
9. If \(k > 1\) then \(n_1 \geq 2\).
If \(\mathcal{S}\) is even distributive, the polynomial \(p\) also satisfies:
10. For all \(x, y \in V\)
\[w(\{x, y\}) \leq 2 \implies p(x, y) = 0.\]
11. If \(k > 1\) then \(n_1 \geq 3\).
12. For any \(1 \leq i \leq j \leq m\), the set \(\{0, 1^{(i)}_{[m]}, 1^{(j)}_{[m]}\}\) generates a medial subsquag \(\mathcal{Q} = \langle Q; \circ \rangle\) such that \(\text{sup}(Q) = \{i, j\}\) and for all \(x, y \in Q\):
\[x \circ y = -x - y.\]
For all $x, y \in V$
\[ p(-x, -y) = -p(x, y), \]
i.e. all monomials in each $p_i(x, y)$ have an odd number of factors.

**Proof.** All parts but (13) follow immediately from earlier theorems and lemmas. To verify part (13) consider
\[ x + y - p(x, y) = (-x \cdot y) \]
\[ = 0 \cdot (x \cdot y) \]
\[ - (0 \cdot x) \cdot (0 \cdot y) \]
\[ = (-x) \cdot (-y) \]
\[ = x + y + p(-x, -y) \]
Therefore
\[ -p(x, y) = p(-x, -y). \]

The nilpotence of the squags considered was essential in our proofs of the preceding theorems. The following theorem of the author — proven in [9] — shows that the nilpotence is even necessary to obtain these representation theorems:

**Theorem 4.11.** Let $\mathcal{V} = \langle V; \cdot \rangle$ be a squag with the following properties:
1. $V$ is an $m\text{-dimensional}$ vector space over $\text{GF}(3)$.
2. There exists a positive integer $k$ and an increasing sequence $0 = n_0 < n_1 < \cdots < n_k = m$ of integers such that the binary operation $\cdot$ is given by
\[ x \cdot y = -x - y + p(x, y), \]
where $p : V^2 \to V$ is a polynomial over $\text{GF}(3)$ such that for all $0 \leq t < k$ and $n_i < i \leq n_{i+1}$ the polynomial $p_t(x, y)$ does not depend on $x_{n_i+1}, \ldots, x_m$ and $y_{n_i+1}, \ldots, y_m$. Then $\mathcal{V}$ is nilpotent of class at most $k$.

Note that a weakened version with $k = m$ is an immediate consequence of [11, Lemma 4.36 and Theorem 13.9].

5. Concepts of nilpotence

A comparison between Klossek's representation theorem (Theorem 4.1 in this paper) and Theorem 4.10 shows clearly that the latter improves and generalizes the former with the exception of its parts (6) and (8), provided that every distributive squag is nilpotent. It is well known that every distributive squag is squag-nilpotent. (We recall the definition of squag-nilpotence below.) We will see that — for distributive squags — squag-nilpotence coincides with nilpotence.
In [1] Bruck defines and discusses the concept of an associator subloop for Moufang loops of exponent three. He uses this concept to introduce the idea of nilpotence to the theory of such algebras. In [12] Klossek translated these concepts of commutator and nilpotence into the theory of distributive squags. (Distributive squags are functionally equivalent to Moufang loops of exponent 3.) Definitions 5.1 and 5.4 are essentially her definitions expressed in terms of congruences rather than normal subalgebras:

**Definition 5.1** (Bruck and Klossek). Let \( \mathcal{S} = \langle S; \cdot \rangle \) be a distributive squag and \( e \in S \). Let \( \alpha \) and \( \beta \) be congruences on \( \mathcal{S} \). Then the squag theoretic commutator of \( \alpha \) and \( \beta \) will be denoted as \( \mathcal{C}(\alpha, \beta) \) and is defined as

\[
\mathcal{C}(\alpha, \beta) = \Theta^\mathcal{S}(\{\{(e, f_\alpha(a, b, c))\mid a \alpha b \in S \& \ c \beta e\}\})
\]

where \( f_\alpha(a, b, c) = ((e \cdot a) \cdot (b \cdot c)) \cdot (((e \cdot c) \cdot (b \cdot a)) \cdot e) \).

Since \( f_\alpha(a, b, c) \) can easily be shown to be a commutator term in the sense of Vaughan–Lee (see [2, 13]), we immediately obtain the following theorem.

**Theorem 5.2.** Let \( \alpha \) and \( \beta \) be congruences on the distributive squag \( \mathcal{S} \). Then

\[
[\alpha, \beta] \supseteq \mathcal{C}(\alpha, \beta).
\]

It has been shown in [7] that the two commutators coincide if one of the two congruences is \( \iota_\mathcal{S} \):

**Theorem 5.3.** Let \( \alpha \) be a congruence on the distributive squag \( \mathcal{S} \). Then

\[
[\alpha, \iota_\mathcal{S}] = \mathcal{C}(\alpha, \iota_\mathcal{S}).
\]

**Proof.** Let \( \mathcal{S} = \langle S; \cdot \rangle \), \( \pi \) be the canonical homomorphism \( \pi: \mathcal{S} \to \mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S}) \). For every congruence \( \gamma \) on \( \mathcal{S} \) let \( \pi(\alpha) \) denote the congruence on \( \mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S}) \) generated by \( \{\{(\alpha(a), \alpha(b))\mid a \alpha b \in S\}\} \). If \( e \in S \), then \( N_e = \{(x, x) \mid x \in \pi([e]_\alpha)\} \) is a normal subalgebra of \( \mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2 \). Since the variety of squags is congruence regular (see [3, 4]) there exists a unique congruence \( \beta_e \) on \( \mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2 \) with class \( N_e \), i.e. \( N_e = \{(\pi(e), \pi(e))\} \beta_e \). For \( u, v \in \mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S}) \) it can be shown that \( (u, u) \beta_e (v, v) \). Therefore

\[
(F) \quad \beta \supseteq \Theta^{\mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2}(\{(u, (u, (v, v)\mid (u, v) \in \pi(\alpha)\}) = A_{\mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2}^{\pi(\alpha)}(a, b),
\]

where \( A_{\mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2}^{\pi(\alpha)} \) is defined as in [2]. If \( a[\pi(\alpha), \pi(\iota_\mathcal{S})]b \), then

\[
(a, b) \in A_{\mathcal{S}/\mathcal{C}(\alpha, \iota_\mathcal{S})^2}^{\pi(\alpha)}(a, b),
\]

and therefore by inclusion (F), \( \alpha \beta b \). This implies \( a = b \), i.e. \( [\pi(\alpha), \pi(\iota_\mathcal{S})] = \omega_\mathcal{S} \). We have shown that \( [\alpha, \beta] \subseteq \mathcal{C}(\alpha, \beta) \). Together with Theorem 5.2, this completes the proof. □
Definition 5.4 (Bruck and Klossek). Let $\mathcal{S} = \langle S; \cdot \rangle$ be any distributive squag. Then let $\mathcal{S}_0 = \mathcal{S}$ and $\mathcal{S}_{n+1} = \langle S_{n+1}; \cdot \rangle$ be the subalgebra generated by

$$f_e(S_n, S, S) = \{ (e, f_e(a, b, c)) | a \in S_{n+1} \& b \in S \& c \in e \},$$

where $f_e$ is the polynomial given in Definition 5.1. If $S_k = \{ e \}$ and $S_{k-1} \neq \{ e \}$ then $\mathcal{S}$ is said to be of squag-nilpotence class $k$. Moreover, we will consider the trivial (i.e. 1-element) squag also to be of squag-nilpotence class 1.

Theorem 5.3 clearly implies:

**Corollary 5.5.** In the theory of distributive squags, the universal algebraic and the squag-theoretic concepts of nilpotence coincide.

6. Construction of finite nilpotent squages

In this section we will give an example of the usefulness of the improved representation Theorem 4.10. In [12] Klossek presents the following powerful recursive construction theorems for distributive squags:

**Theorem 6.1** (Klossek [12]). Let $V$ be an $n$-dimensional vector space over $\text{GF}(3)$ and let $\langle V; \cdot \rangle$ be a subdirectly irreducible distributive squag of nilpotence class $k$ such that there exist a polynomial $p: V^2 \rightarrow V$ over $\text{GF}(3)$ with the following properties:

1. $x \circ y = -x - y + p(x, y)$ for all $x, y \in V$.
2. $p(x, y) = 0$ for all $x, y \in V$.
3. $p(0, 0) = 0$.
4. For all $x, y \in V$

$$\sup \{ (x, y) \} \subset \{ 1 \} \Rightarrow p(x, y) = 0.$$ (5) The center $\zeta(\langle V; \cdot \rangle)$ is the kernel of the projection onto the first $n - 1$ components.

6. The polynomials $p_i(x, y)$ do not depend on $x_i$ and $y_i$.

Then the $n + 2$ dimensional vector space $W$ over $\text{GF}(3)$ with the operation $\cdot$ defined by

$$\begin{align*}
(x \circ y)_{i} &= \begin{cases} 
-x_i - y_i & \text{if } i \leq 2 \\
(x_{[3, n+2]} \circ y_{[3, n+2]})_{i-2} & \text{if } 3 \leq i \leq n + 1 \\
(x_{[3, n+2]} \circ y_{[3, n+2]})_n + (x_3 - y_3) & \text{if } i = n + 2
\end{cases}
\end{align*}$$

is a subdirectly irreducible distributive squag of nilpotence class $k$ and the center $\zeta(\langle W; \cdot \rangle)$ is the kernel of the projection onto the first $n + 1$ components of $W$.

**Theorem 6.2** (Klossek [12]). Let $V$ be an $n$-dimensional vector space over $\text{GF}(3)$ and let $\langle V; \cdot \rangle$ be a subdirectly irreducible distributive squag of nilpotence class $k$ such that there
exists a polynomial $p: V^2 \rightarrow V$ over $\mathbb{GF}(3)$ with the following properties:

1. $x \cdot y = -x - y + p(x, y)$ for all $x, y \in V$.
2. $p(0, y) = 0$ for all $y \in V$.
3. The center $\zeta(\langle V; \cdot \rangle)$ is the kernel of the projection onto the first $n - 1$ components of $V$.
4. The polynomials $p_i(x, y)$ do not depend on $x_n$ and $y_n$.

Let $W$ be an $m$-dimensional vector space over $\mathbb{GF}(3)$ and let $\langle W; \circ \rangle$ be a subdirectly irreducible distributive squag of nilpotence class $j$ such that there exists a polynomial $q: W^2 \rightarrow W$ over $\mathbb{GF}(3)$ with the following properties:

1. $(x \circ y) = -x - y + q(x, y)$ for all $x, y \in W$.
2. $q(0, y) = 0$ for all $y \in W$.
3. The center $\zeta(\langle W; \circ \rangle)$ is the kernel of the projection onto the first $m - 1$ components of $W$.
4. The polynomials $q_i(x, y)$ do not depend on $x_m$ and $y_m$.

Then the $(n + m - 1)$-dimensional vector space $U$ over $\mathbb{GF}(3)$ with the operation $\ast$ defined by

\[
\begin{align*}
\text{if } & 1 \leq i < n, \\
(x \ast y) &= \begin{cases} 
(x_{[n]} \cdot y_{[n]}), & \text{if } 1 \leq i < n, \\
(x_{[n, n+m-1]} \circ y_{[n, n+m-1]}), & \text{if } n \leq i < n + m - 1, \\
(x_{[n, n+m-1]} \circ y_{[n, n+m-1]}) + p_n(x_{[n]}, y_{[n]}), & \text{if } i = n + m - 1
\end{cases}
\end{align*}
\]

is a subdirectly irreducible distributive squag of nilpotence class $\max(k, j)$.

Note that in the third case of equation (G) the polynomial $p_n$ does not depend on $x_n$ or $y_n$.

It is clear that Klossek’s own representation theorem (Theorem 4.1 in this paper) is too weak to be used with these construction theorems, but the new Theorem 4.10 is applicable. Since every nilpotence class of distributive squags has to contain at least one subdirectly irreducible squag and this squag can be represented as described in Theorem 4.10, we obtain the following corollary:

**Corollary 6.3.** For every $k \geq 2$ there are infinitely many finite subdirectly irreducible distributive squags of nilpotence class $k$.

Corollary 6.3 is also a consequence of [2, Proposition 7.8].

7. **Open questions**

While the representation Theorem 4.10 provides some properties of the polynomials $p_i$, it does not limit the size of the monomials. The known examples use large sums of small monomials as they would be created by both the construction theorems. It would be interesting to determine whether there are examples of distributive squags
whose representations require large monomials, or whether monomials of a length 3 or 4 always suffice. The author suspects that the answer depends on whether the squags are distributive or not. The representation theorems in this paper do not increase the nilpotence class of any squags. Are there any recursive constructions for nilpotent squags that raise the nilpotence class? Are there any such constructions for distributive squags? Finally, it is still open whether for distributive squags the squag-commutator as defined in Definition 5.1 coincides with the universal algebraic commutator.

Some of the results presented in this paper are also included in the PhD thesis [8] and Diplom thesis [7] of the author. The remaining results originated from the research conducted by the author during his stay at Brandon University.

The author would like to thank the referees for their constructive criticism and their helpful suggestions.

References