International Journal of Algebra and Computation
Vol. 17, No. 8 (2007) 1577–1592

World Scientific
www.worldscientific.com

EVANS' NORMAL FORM THEOREM REVISITED

JONATHAN D. H. SMITH
Department of Mathematics, Iowa State University
Ames, Iowa 50011-2064, USA
jdhsmith@math.iastate.edu

Received 4 February 2006
Revised 18 April 2007

Communicated by R. McKenzie

Evans defined quasigroups equationally, and proved a Normal Form Theorem solving the word problem for free extensions of partial Latin squares. In this paper, quasigroups are redefined as algebras with six basic operations related by triality, manifested as coupled right and left regular actions of the symmetric group on three symbols. Triality leads to considerable simplifications in the proof of Evans' Normal Form Theorem, and makes it directly applicable to each of the six major varieties of quasigroups defined by subgroups of the symmetric group. Normal form theorems for the corresponding varieties of idempotent quasigroups are obtained as immediate corollaries.

Keywords: Quasigroup; triality; normal form theorem; confluent rewriting; word problem; semisymmetric; totally symmetric; Steiner triple system; partial Latin square.

1. Introduction

Quasigroups were originally defined as algebras $(Q, \cdot)$ equipped with a single binary operation $\cdot$ of *multiplication*, such that in the equation

$$x_1 \cdot x_2 = x_3 \,, \tag{1}$$

knowledge of any two of the arguments x_1, x_2, x_3 specifies the third uniquely. It is convenient to speak of *combinatorial quasigroups* in this context. Evans [5] redefined quasigroups as *equational quasigroups*, algebras $(Q, \cdot, /, \backslash)$ equipped with three binary operations, including a *right division* $/$ and *left division* $\backslash$, such that the identities

$$\begin{array}{ll} \text{(IL)}\ \ y\backslash(y \cdot x) = x \,, & \text{(IR)}\ \ x = (x \cdot y)/y \,, \\ \text{(SL)}\ \ y \cdot (y\backslash x) = x \,, & \text{(SR)}\ \ x = (x/y) \cdot y \end{array} \tag{2}$$

are satisfied. These identities yield

$$\text{(DL)}\ \ y/(x\backslash y) = x \,, \quad \text{(DR)}\ \ x = (y/x)\backslash y \tag{3}$$

as immediate consequences. The symmetry of the theory of equational quasigroups is duality: reversing products, interchanging left and right divisions, and switching

the identities (XL), (XR) for X = I, S, D. Working in the language of equational quasigroups, Evans proved his Normal Form Theorem [6] solving the word problem for free extensions of partial Latin squares. Beyond its fundamental importance within the theory of quasigroups, the theorem was remarkable for being one of the first instances of a confluent rewriting system. Evans' proof used the duality of equational quasigroups, but still had to consider dozens of separate cases, sometimes implicitly.

The aim of the current paper is to take Evans' program one step further. We now redefine equational quasigroups as so-called *hyperquasigroups*, algebras equipped with six basic binary operations subject to a stronger symmetry known as *triality* (Sec. 2). This symmetry consists of two coupled left and right actions of the symmetric group S_3 on three symbols. The left action, *syntactic triality*, governs the behavior of the quasigroup operations in identities. The right action, *semantic triality*, determines six major varieties of quasigroups, the varieties of *H-symmetric* quasigroups for each subgroup H of S_3 (Sec. 3). The correspondingly symmetric partial Latin squares (X, U) on a set X are described in Sec. 4. (This group-theoretical treatment contrasts with the approach of [10] using partial satisfaction of identities.) In Sec. 5, the full triality symmetry allows Evans' Normal Form Theorem to be stated explicitly in a single version that immediately covers all six H-symmetric varieties (Theorem 13), at the same time allowing for a considerable simplification of the proof. Two reduction rules (13), (14) suffice in place of the nine used by Evans [6, Sec. 1.3(ii)/Sec. 2.1(vii), Sec. 2.1 (iva)–(vib)]. The number of external cases to be considered in the proof of the Diamond Lemma is cut by a factor of three (Sec. 6). With minor changes — one extra reduction rule (24) and three further cases in the proof of the Diamond Lemma — Evans' Normal Form Theorem applies explicitly to each of the six corresponding varieties of idempotent quasigroups (Sec. 8). In particular, idempotent S_3-symmetric quasigroups are Steiner triple systems, so Evans' Normal Form Theorem in that case subsumes known results about free extensions of partial Steiner triple systems (compare [19, Sec. 4], for example).

Some additional remarks are in order. It should first be recalled that the original statement of the Normal Form Theorem was explicitly given for loops, although Evans pointed out that his proof "can easily be adapted to apply to quasigroups" [6, Sec. 2.4] — in fact just by deleting all the relations and reductions involving the identity element and its consequences. In [2, pp. 14–15], Evans discussed the adaptation of his Normal Form Theorem to "commutative quasigroups[,] ... totally symmetric quasigroups[,] ... Steiner quasigroups ... and many other related varieties" using equivalence classes of words along the lines followed below. From that standpoint, the current paper has little to add. Rather, its three key features are:

(1) Introduction of the new language of hyperquasigroups, endowed with the full triality symmetry.

(2) Use of the hyperquasigroup language to produce a single Normal Form Theorem covering all six H-symmetric cases directly, with a slight adaptation for all the six idempotent cases.
(3) Elimination of redundancy in the analysis.

In connection with the third point, Evans merely said that the various cases "can be systematically listed" when summarizing the proof of the Diamond Lemma in [2, Lemma I.3.1].

Semantic triality (in more or less explicit form) is well known within the theory of quasigroups — compare [17, (II.9)], for example. Note that the theory of loops does not satisfy triality symmetry: if $(Q, \cdot)$ is a loop, the conjugate $(Q, /)$ does not generally possess an identity element. Within the theory of inverse property loops, however, and more especially for Moufang loops, there is a slightly different version of semantic triality, related to triality in the group Spin_8 [3, Chaps. 7, 8]. Full triality as presented in Sec. 2 below, with the coupling of the syntactic and semantic triality, appears to be new. It amounts to an action of the multiplication group $\mathrm{Mlt}\, S_3 \cong S_3 \times S_3$ of S_3. Just as triality has simplified the proof of Evans' Normal Form Theorem, one might well expect it to streamline algorithms for automated reasoning about quasigroups used in work such as [18].

2. Triality

Writing σ and τ for the respective transpositions (12) and (23), the symmetric group S_3 on the three-element set $\{1, 2, 3\}$ is presented as

$$\langle \sigma, \tau \mid \sigma^2 = \tau^2 = (\sigma\tau)^3 = 1 \rangle \,.$$

The Cayley diagram of the presentation becomes

$$\begin{array}{ccccc} 1 & \Longleftrightarrow & \tau & \longleftrightarrow & \tau\sigma \\ \updownarrow & & & & \Updownarrow \\ \sigma & \Longleftrightarrow & \sigma\tau & \longleftrightarrow & \sigma\tau\sigma \end{array} \tag{4}$$

using $\leftrightarrow$ for right multiplication by σ and $\Leftrightarrow$ for right multiplication by τ. Note that the third transposition (13) or $\sigma\tau\sigma$ is also equal to the product $\tau\sigma\tau$. Write

$$x \circ y = y \cdot x \,, \quad x//y = y/x \,, \quad x\backslash\backslash y = y\backslash x$$

for the respective opposites of the basic equational quasigroup operations. Members of the set

$$\{\cdot, \backslash, //, /, \backslash\backslash, \circ\} \tag{5}$$

of binary operations are variously known as *conjugate*, "parastrophic" [17, p. 43; 20] or "derived" [9] quasigroup operations. It is convenient to use postfix notation for binary operations, setting $x \cdot y = xy\,\mu$ and rewriting (1) in the form

$$x_1 x_2\, \mu = x_3 \,. \tag{6}$$

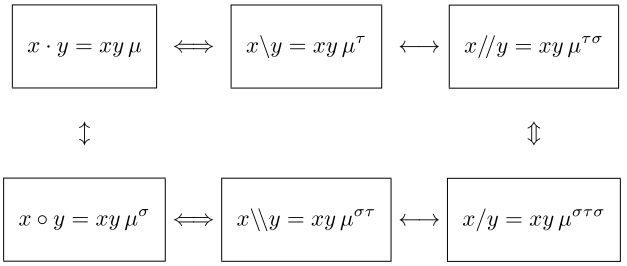

Fig. 1. Triality symmetry of the quasigroup operations.

The set (5) will now be construed as the homogeneous space

$$\mu^{S_3} = \{\mu^g \mid g \in S_3\} \tag{7}$$

for a regular right permutation action of the symmetric group S_3, such that (6) is equivalent to

$$x_{1g}x_{2g}\mu^g = x_{3g} \tag{8}$$

for each g in S_3. Figure 1 displays the six binary operations in their positions corresponding to the Cayley diagram (4).

The opposite of each operation μ^g in Fig. 1 is given by $\mu^{\sigma g}$. Thus passage to the opposite operation corresponds to left multiplication by the transposition σ. The pairs of opposite operations lie in the three respective columns of Fig. 1.

Left multiplication by τ also has a simple interpretation. Let M be the full set of derived binary operations on a quasigroup. Formally, this set may be considered as the free algebra on two generators x, y in the variety $\mathbf{Q}$ of quasigroups. Define a multiplication $*$ on M by

$$xy(\alpha * \beta) = x\,xy\alpha\,\beta\,. \tag{9}$$

Define the binary operation ϵ as the right projection $xy\epsilon = y$.

Lemma 1. *The set M of all derived binary quasigroup operations forms a monoid $(M, *, \epsilon)$ under the multiplication* (9)*, with identity element ϵ.*

Proof. First note that

$$(\alpha * \epsilon) = x\,xy\alpha\,\epsilon = xy\alpha$$

and

$$xy(\epsilon * \alpha) = x\,xy\epsilon\,\alpha = xy\alpha$$

for α in M, so that ϵ is an identity element. Now consider α, β, γ in M. Then

$$\begin{aligned} xy\big((\alpha * \beta) * \gamma\big) &= x\,xy(\alpha * \beta)\,\gamma \\ &= xxxy\alpha\beta\gamma \\ &= x\,xy\alpha(\beta * \gamma) = xy\big(\alpha * (\beta * \gamma)\big)\,, \end{aligned}$$

verifying the associativity of the multiplication (9). □

The significance of the left multiplication by τ then follows.

Proposition 2. *For each element g of S_3, the binary operation μ^g is an invertible element of the monoid M, with inverse $\mu^{\tau g}$. Thus the quasigroup operations generate a subgroup of M.*

Proof. The identity (IL), namely $x\backslash(x\cdot y) = y$, becomes $x\,xy\mu\,\mu^\tau = y$ or $\mu * \mu^\tau = \epsilon$. Similarly (SL), namely $x \cdot (x\backslash y) = y$, becomes $x\,xy\mu^\tau\,\mu = x$ or $\mu^\tau * \mu = \epsilon$. Thus μ and μ^τ are mutual inverses.

The identity (IR), namely $(y \cdot x)/x = y$, is $x//(x \circ y) = y$. This becomes $x\,xy\mu^\sigma\,\mu^{\tau\sigma} = y$ or $\mu^\tau * \mu^{\tau\sigma} = \epsilon$. Similarly (SR), namely $(y/x) \cdot x = y$, may be written as $x \circ (x//y) = y$. This becomes $x\,xy\mu^{\tau\sigma}\,\mu^\sigma = y$ or $\mu^{\tau\sigma} * \mu^\tau = \epsilon$. Thus μ^σ and $\mu^{\tau\sigma}$ are mutual inverses.

The identity (DR), namely $(x/y)\backslash x = y$, is $x\backslash\backslash(x/y) = y$. This becomes $x\,xy\mu^{\tau\sigma\tau}\,\mu^{\sigma\tau} = y$ or $\mu^{\tau\sigma\tau} * \mu^{\sigma\tau} = \epsilon$. Finally (DL), namely $x/(y\backslash x) = y$, is $x/(x\backslash\backslash y) = y$. This becomes $x\,xy\mu^{\sigma\tau}\,\mu^{\tau\sigma\tau} = y$ or $\mu^{\sigma\tau} * \mu^{\tau\sigma\tau} = \epsilon$. Thus $\mu^{\sigma\tau}$ and $\mu^{\tau\sigma\tau}$ are mutual inverses. □

Remark 3. A general result of Movsisyan [15, Proposition 1.1] implies that the various quasigroup operations generate a subgroup of the monoid M. However, this result does not address the specific description of the inverses given by Proposition 2 in terms of the syntactic action.

Corollary 4. *A quasigroup may be defined as an algebra Q equipped with a binary operation μ^g for each element g of the group S_3, such that the* hypercommutative law

$$xy\,\mu^g = yx\,\mu^{\sigma g}$$

and the hypercancellation *law*

$$x\,xy\mu^g\,\mu^{\tau g} = y$$

are satisfied for each element g of S_3.

Definition 5. An algebra (Q, μ^{S_3}) with a set (7) of binary operations, satisfying the hypercommutative and hypercancellation laws, is formally described as a *hyperquasigroup.*

3. Symmetric Quasigroups

Let H be a subgroup of S_3. A quasigroup is said to be *H-symmetric* if it satisfies the identity

$$xy\,\mu^g = xy\,\mu^{gh} \tag{10}$$

for each g in S_3 and h in H. In considering H-symmetry, the following lemma is very useful.

Lemma 6. *A sufficient condition for the H-symmetry of a quasigroup Q is the existence of a single element g of S_3 such that Q satisfies the identity* (10) *for each h in H.*

Proof. Suppose that Q satisfies the identity (10) for each h in H and for each element g of a subset K of S_3. It will be shown that the identity (10) also holds for each h in H and for each element g of the subsets σK and τK of S_3. Since S_3 is generated by σ and τ, the required statement follows.

The identity (10) implies $yx\,\mu^g = yx\,\mu^{gh}$ or $xy\,\mu^{\sigma g} = xy\,\mu^{\sigma gh}$, so that (10) holds for each h in H and for each element g of the subset σK of S_3. Moreover, for each g in K and h in H, one has

$$x\,xy\,\mu^{\tau g}\,\mu^g = y = x\,xy\,\mu^{\tau gh}\,\mu^{gh} = x\,xy\,\mu^{\tau gh}\,\mu^g$$

by hypercancellativity and (10). Since (Q, μ^g) is a (combinatorial) quasigroup, it follows that $xy\,\mu^{\tau g} = xy\,\mu^{\tau gh}$. Thus (10) holds for each h in H and for each element g of the subset τK of S_3. □

Example 7. For $H = S_3$, H-symmetry is just *total symmetry*, the equality of all six conjugate operations. In particular, an idempotent totally symmetric quasigroup Q is equivalent to a Steiner triple system structure on Q, with

$$\big\{\{x, y, xy\} \;\big|\; x \neq y \in Q\big\}$$

as the set of blocks [19].

Example 8. Commutativity is $\langle\sigma\rangle$-symmetry, since the commutative law $xy = yx$ becomes $xy\,\mu = xy\,\mu^\sigma$.

Example 9. Semisymmetry is $\langle\sigma\tau\rangle$-symmetry, the equality of x/y, yx, and $x\backslash y$. Semisymmetric quasigroups have also been described as "3-cyclic". They have been studied by various authors, including Osborn [16], Sade [21–24], Mendelsohn [12, 13], Grätzer and Padmanabhan [7], Mitschke and Werner [14], DiPaola and Nemeth [4], and Lindner [10]. There is a construction known as *semisymmetrization* which associates a semisymmetric quasigroup Q^Δ with each quasigroup Q. Then two quasigroups are isotopic if and only if their semisymmetrizations are isomorphic [25].

The remaining nontrivial cases are covered by the following proposition.

Proposition 10. *Let Q be a quasigroup.*

(a) *The following are equivalent*:

(i) *Q is $\langle\tau\rangle$-symmetric*;
(ii) *$(Q, /)$ is commutative*;
(iii) *$(Q, \cdot)$ satisfies the* left symmetric identity

$$x \cdot (x \cdot y) = y\,. \tag{11}$$

(b) *The following are equivalent*:

(i) Q *is* $\langle\sigma\tau\sigma\rangle$*-symmetric*;
(ii) $(Q, \backslash)$ *is commutative*;
(iii) $(Q, \cdot)$ *satisfies the* right symmetric identity

$$(y \cdot x) \cdot x = y\,. \tag{12}$$

Proof. Part (a) will be proved: Part (b) is similar. Statement (ii) means that $x/y = x//y$, so $xy\,\mu^{\tau\sigma\tau} = xy\,\mu^{\tau\sigma}$. By Lemma 6, this is equivalent to (i). Statement (iii) means that $x \cdot y = x\backslash y$, so $xy\,\mu = xy\,\mu^{\tau}$. By Lemma 6 again, this is also equivalent to (i). □

Together, (11) and (12) are known as *symmetric identities*. With a parity that depends on the conventions used for mappings, they appear — along with the two identities of idempotence and (self-)distributivity — in Loos' axiomatization of symmetric spaces [11].

4. Partial Latin Squares

A ternary relation $U \subseteq X^3$ on a set X is said to have the *Latin square property* when

$$\big|\{1 \le i \le 3 \mid x_i = y_i\}\big| \neq 2$$

for any two elements (x_i, x_2, x_3), (y_1, y_2, y_3) of U. A quasigroup Q determines a ternary relation T or

$$T(Q) = \{(x_1, x_2, x_3) \in Q^3 \mid x_1 \cdot x_2 = x_3\}$$

known as the (*ternary*) *multiplication table* of Q. By the combinatorial property (1) defining quasigroup multiplications, the ternary multiplication table has the Latin square property. Now let X be a set. A *partial Latin square* (X, U) on X consists of a ternary relation U on X that has the Latin square property.

When considering H-symmetric quasigroups for a subgroup H of S_3, it becomes necessary to specify the corresponding partial Latin squares. For each subgroup H of S_3, define a partial Latin square (X, U) to be H*-symmetric* if

$$(x_1, x_2, x_3) \in U \;\Rightarrow\; (x_{1h}, x_{2h}, x_{3h}) \in U$$

for all h in H. Before relating H-symmetry of quasigroups to ternary multiplication tables, it is helpful to reformulate the equivalence of (6) and (8).

Lemma 11. *Let* x_1, x_2, x_3 *be elements of a quasigroup* Q*, and let* g*,* h *be elements of* S_3*.*

(a) $x_1 x_2\,\mu^{g^{-1}} = x_3$ *implies* $x_{1g^{-1}hg} x_{2g^{-1}hg}\,\mu^{g^{-1}h} = x_{3g^{-1}hg}$*.*
(b) $x_{1g} x_{2g}\,\mu = x_{3g}$ *implies* $x_{1hg} x_{2hg}\,\mu^{h} = x_{3hg}$*.*

Proof. Set $y_i = x_{ig}$ for $1 \leq i \leq 3$, so that $x_i = y_{ig^{-1}}$.
(a): The hypothesis of (a) becomes $y_{1g^{-1}} y_{2g^{-1}} \, \mu^{g^{-1}} = y_{3g^{-1}}$. As an instance of (8), this is equivalent to (6) as $y_1 y_2 \, \mu = y_3$. The latter yields (8) in the form $y_{1g^{-1}h} y_{2g^{-1}h} \, \mu^{g^{-1}h} = y_{3g^{-1}h}$. Rewriting in terms of the x_i, this becomes $x_{1g^{-1}hg} x_{2g^{-1}hg} \, \mu^{g^{-1}h} = x_{3g^{-1}hg}$ as required.
(b): The hypothesis of (b) becomes $y_1 y_2 \, \mu = y_3$, so $y_{1h} y_{2h} \, \mu^h = y_{3h}$. The result follows on rewriting in terms of the x_i. □

Proposition 12. *Let H be a subgroup of S_3. Then a quasigroup Q is H-symmetric if and only if its ternary multiplication table $T(Q)$ is H-symmetric.*

Proof. First suppose that Q is H-symmetric. Then $(x_1, x_2, x_3) \in T(Q)$ implies $x_1 x_2 \, \mu = x_3$. Since Q is H-symmetric, one has $x_1 x_2 \, \mu^{h^{-1}} = x_3$ for each h in H. Lemma 11(a) with $g = h$ yields $x_{1h} x_{2h} \, \mu = x_{3h}$, whence $(x_{1h}, x_{2h}, x_{3h}) \in T(Q)$ as required.

Conversely, suppose that $T(Q)$ is H-symmetric. If $x_1 x_2 \, \mu = x_3$, then $(x_1, x_2, x_3) \in T(Q)$. For h in H, the symmetry of $T(Q)$ implies $(x_{1h^{-1}}, x_{2h^{-1}}, x_{3h^{-1}}) \in T(Q)$. This means that $x_{1h^{-1}} x_{2h^{-1}} \, \mu = x_{3h^{-1}}$. Lemma 11(b) with $g = h^{-1}$ yields $x_1 x_2 \mu^h = x_3 = x_1 x_2 \, \mu$. Lemma 6 then gives the H-symmetry of Q. □

5. Normal Forms

Let H be a subgroup of S_3. Let (X, U) be an H-symmetric partial Latin square. An H-symmetric quasigroup Q is said to *extend* (X, U) if X is a subset of Q and U is a subset of $T(Q)$. Such an extension Q is said to be *free* if the embedding of X in any H-symmetric extension Q' extends to a unique quasigroup homomorphism from Q to Q'. Evans' Normal Form Theorem shows that (X, U) possesses a free H-symmetric extension $Q^H_{(X,U)}$, and gives an explicit description of the extension.

Consider the free monoid $(X + \mu^{S_3})^*$, the set of words with letters taken from the disjoint union $X + \mu^{S_3}$ of X with the set (7). The set (7) — or more precisely its image in the disjoint union — acts as a set of binary operations on $(X + \mu^{S_3})^*$, with

$$\mu^g : (w, w') \mapsto w w' \mu^g$$

for w, w' in $(X + \mu^{S_3})^*$ and g in S_3. Let W_X or W be the subalgebra of

$$\big((X + \mu^{S_3})^*, \mu^{S_3}\big)$$

generated by X. An equivalence relation V will be defined on the set W of words, such that the set W^V of equivalence classes will carry the structure of the free extension $Q^H_{(X,U)}$. Each V-equivalence class will be represented by a unique word, of minimal length among all the words in the class. This representative is the *normal form* of the words in the class. Formally, Evans' Normal Form Theorem may be stated as follows.

Theorem 13. *Let H be a subgroup of the symmetric group S_3. Let (X, U) be an H-symmetric partial Latin square. Then $Q^H_{(X,U)}$, the free H-symmetric extension of (X, U), is obtained as the quotient W^V. There is an algorithm to determine the normal form $\overline{w}$ of each word w from W. Two words w_1, w_2 from W are related by V if and only if their normal forms $\overline{w_1}$, $\overline{w_2}$ coincide.*

Given a word w in W, its normal form is obtained by the iterative process of *rewriting*. The steps in the process are the *rewriting rules*. First, each instance of $uv\mu^g$ in w with u, v in W may be replaced by $vu\mu^{\sigma g}$, to obtain a new word w', of the same length as w. Two words are said to be σ-*equivalent* if they are related by a (possibly empty) sequence of such replacements. Second, each instance of $uv\mu^g$ in w with u, v in W may be replaced by $uv\mu^{gh}$ for any h in H, to obtain a new word w', of the same length as w. Two words are said to be H-*equivalent* if they are related by a (possibly empty) sequence of such replacements. Two words w, w' are said to be (σ, H)-*equivalent* if they are related by a concatenation of σ-equivalence and H-equivalence.

Lemma 14. *Let H be a subgroup of S_3, of order l. Let w be an element of W containing r letters from μ^{S_3}.*

(a) *The relations of σ-equivalence and H-equivalence commute.*
(b) *The word w has 2^r σ-equivalent forms.*
(c) *The word w has l^r H-equivalent forms.*
(d) *The word w has $(2l)^r$ (σ, H)-equivalent forms.*

A word w from W is said to be *basic* if it does not include the letters μ^σ, $\mu^{\tau\sigma}$, or $\mu^{\sigma\tau}$ (i.e. the opposites of the respective basic quasigroup operations $\cdot$, $/$, $\backslash$). Each of the σ-equivalence classes has a unique basic representative, which is a word in the alphabet $X + \{\mu, \mu^{\tau\sigma\tau}, \mu^\tau\}$. Now order the set of basic operations as $\{\mu < \mu^{\tau\sigma\tau} < \mu^\tau\}$ or $\{\cdot < / < \backslash\}$. A basic word is said to be *primary* if its H-equivalence class does not contain a word using lesser basic operations in any location. For example, the primary words for commutative quasigroups will only involve the basic operations of multiplication and right division ($+$ and $-$ in additive notation), while primary words for right symmetric quasigroups will only involve the multiplication and left division. The normal form is chosen as the primary representative of its (σ, H)-equivalence class.

The remaining rewriting rules are of two kinds, each reducing the length of words. They are the so-called *reduction rules*. The first kind of reduction rule will implement hypercancellation. If some (σ, H)-equivalent of w contains an instance of $u\,uv\mu^g\,\mu^{\tau g}$ with u, v in W, the subword $u\,uv\mu^g\,\mu^{\tau g}$ may be replaced by v to yield an equivalent but shorter word w'. A rewriting step of this kind is denoted by $w \to w'$, or more explicitly by

$$w \xrightarrow{g} w'\,. \tag{13}$$

In practice, rather than potentially searching the (σ, H)-equivalence class of w, for instances, of $u\,uv\mu^g\,\mu^{\tau g}$ at each step, it is better to regard (13) as representative of $4 \cdot |H|^2$ different reductions.

The second reduction rule depends on an element $x = (x_1, x_2, x_3)$ of the partial Latin square U. Note that such a triple represents an equation

$$x_{1g}x_{2g}\mu^g = x_{3g}$$

for each element g of S_3. Now if a word w involves $x_{1g}x_{2g}\mu^g$ as a subword, this subword may be replaced by x_{3g} to yield an equivalent but shorter word w'. A rewriting step of this kind is denoted by $w \to w'$, or more explicitly by

$$w \xrightarrow{x_g} w'\,. \tag{14}$$

The equivalence relation V is defined as the smallest equivalence relation on W that contains the set of pairs (w, w') for which either w and w' are (σ, H)-equivalent, or for which one of (13) or (14) holds.

6. The Diamond Lemma

A given word w of W initiates a maximal chain

$$w \to w_1 \to w_2 \to \cdots \to \overline{w} \tag{15}$$

of reductions of types (13) or (14), with implicit (σ, H)-equivalences at the tail of each arrow. The final node $\overline{w}$, representing the normal form of w, is taken to be in primary form. Note that w and $\overline{w}$ are related by V. There is a unique normal form $\overline{w}$ terminating a reduction chain starting at the given word w.

Lemma 15 (Diamond Lemma). *Let w be a word in W. If w has two maximal reduction chains of type* (15)*, namely*

$$w \to w_1 \to w_2 \to \cdots \to \overline{w}_k \tag{16}$$

and

$$w \to w'_1 \to w'_2 \to \cdots \to \overline{w}'_l\,, \tag{17}$$

then $\overline{w}_k = \overline{w}'_l$, so that w reduces to a unique normal form $\overline{w}$.

Proof. The proof proceeds by induction on the length of the word w in the alphabet $X + \mu^{S_3}$. If the length is 1, then w is just an element x of the set X. Now assume that the normal forms are unique for all words shorter than w. If w cannot be reduced further, then the normal form $\overline{w}$ is taken as the chosen representative within the (σ, H)-equivalence class of w. If w_1 and w'_1 are (σ, H)-equivalent, then $\overline{w} = \overline{w_1} = \overline{w'_1}$ by the induction hypothesis, since w_1 is shorter than w. For example, if

$$w = u\,u\,ut\mu^g\,\mu^{\tau g}\,\mu^g \tag{18}$$

for words t, u in W, then $w \to w_1$ may take the form

$$w = u\,u\,(ut\mu^g)\,\mu^{\tau g}\,\mu^g \xrightarrow{\tau g} ut\mu^g\,,$$

with $w \to w_1'$ as

$$w = u\,(u\,ut\mu^g\,\mu^{\tau g})\,\mu^g \xrightarrow{\ g\ } ut\mu^g\,.$$

Otherwise, w_1 and w_1' are (σ, H)-inequivalent, and the reduction chains (16), (17) begin as

$$\begin{array}{ccc} & & w_1 \\ & \nearrow & \\ w & & \\ & \searrow & \\ & & w_1' \end{array} \tag{19}$$

with diverging paths. It will be shown that one of the following occurs:

Triangle. There is a chain of reductions from one of w_1, w_1' to the other, without loss of generality from w_1' to w_1:

$$w_1' \to \cdots \to w_1\,.$$

In this case $\overline{w} = \overline{w_1}$.

Diamond. There is a word w_0 in W that lies on reduction chains

$$w_1 \to \cdots \to w_0$$

from w_1 and

$$w_1' \to \cdots \to w_0$$

from w_1'. In this case $\overline{w} = \overline{w_0}$.

Suppose that $w = uv\mu^g$ for words u, v in W. A reduction $w \to w_1$ is said to be *internal* if it is of the form $uv\mu^g \to u_1v\mu^g$ for a reduction $u \to u_1$ of u, or else of the form $uv\mu^g \to uv_1\mu^g$ for a reduction $v \to v_1$ of v. There are two possible cases for (19): *internal* and *external*.

Internal case. Here the initial reductions $w \to w_1$ and $w \to w_1'$ are both internal. If (19) takes the form

$$\begin{array}{ccc} & & u_1v\mu^g \\ & \nearrow & \\ w = uv\mu^g & & \\ & \searrow & \\ & & u_1'v\mu^g \end{array}$$

with reduction chains $u \to u_1 \to \cdots$ and $u \to u_1' \to \cdots$ for u, then the diamond pattern occurs with $w_0 = \overline{u}v\mu^g$. Similarly, if (19) takes the form

$$\begin{array}{ccc} & & uv_1\mu^g \\ & \nearrow & \\ w = uv\mu^g & & \\ & \searrow & \\ & & uv_1'\mu^g \end{array}$$

with reduction chains $v \to v_1 \to \cdots$ and $v \to v_1' \to \cdots$ for v, the diamond pattern occurs with $w_0 = u\overline{v}\,\mu^g$. Finally, if (19) takes the form of the left-hand side of the diagram

$$\begin{array}{ccccc} & & u_1 v \mu^g & & \\ & \nearrow & & \searrow & \\ w = uv\mu^g & & & & u_1 v_1 \mu^g\,, \\ & \searrow & & \nearrow & \\ & & uv_1\mu^g & & \end{array}$$

then the diamond pattern occurs once again, as illustrated by the full diagram.

External case. Here at least one of the initial reductions $w \to w_1$ and $w \to w_1'$ is not internal. If (19) takes the form of the left-hand side of the diagram

$$\begin{array}{ccc} & & t \\ & g \nearrow & \uparrow g \\ w = u\,ut\mu^g\,\mu^{\tau g} & & u_1\,u_1 t\mu^g\,\mu^{\tau g} \\ & \searrow & \uparrow \\ & & u_1\,ut\mu^g\,\mu^{\tau g} \end{array}$$

for some word t in W, then the triangle pattern occurs, as illustrated by the full diagram.

Similarly, if (19) takes the form of the left-hand side of the diagram

$$\begin{array}{ccc} & & t \\ & g \nearrow & \uparrow g \\ w = u\,ut\mu^g\,\mu^{\tau g} & & u_1\,u_1 t\mu^g\,\mu^{\tau g} \\ & \searrow & \uparrow \\ & & u\,u_1 t\mu^g\,\mu^{\tau g} \end{array}$$

then the triangle pattern occurs again, as illustrated by the full diagram.

If (19) takes the form of the left-hand side of

$$\begin{array}{ccccc} & & t & & \\ & g \nearrow & & \searrow & \\ w = u\,ut\mu^g\,\mu^{\tau g} & & & & t_1\,. \\ & \searrow & & \nearrow g & \\ & & u\,ut_1\mu^g\,\mu^{\tau g} & & \end{array}$$

with a reduction $t \to t_1$ for t, then the diamond pattern occurs as given by the full diagram.

If (19) takes the form of the left-hand side of

$$\begin{array}{ccc} & & s \\ & g \nearrow & \\ st\mu^{\tau\sigma g}\, st\mu^{\tau\sigma g}\, s\mu^{g}\, \mu^{\tau g} & & \uparrow \sigma\tau\sigma g \\ \| & & \\ st\mu^{\tau\sigma g}\, s\, st\mu^{\tau\sigma g}\, \mu^{\sigma g}\, \mu^{\tau g} & & t\, ts\mu^{\sigma\tau\sigma g}\, \mu^{\sigma\tau g} \\ & \tau\sigma g \searrow & \| \\ & & st\mu^{\tau\sigma g}\, t\mu^{\tau g} \end{array} \tag{20}$$

for words s, t in W, then the triangle pattern occurs, as presented by the full diagram. Note the use of the σ-equivalences denoted by $\|$. Finally, suppose that $x = (x_1, x_2, x_3)$ is an element of the partial Latin square U. If (19) takes the form of the left-hand side of

$$\begin{array}{ccc} & & x_{2g} \\ & g \nearrow & \uparrow x_{\tau g} \\ w = x_{1g}\, x_{1g} x_{2g} \mu^{g}\, \mu^{\tau g} & & x_{1\tau g} x_{2\tau g} \mu^{\tau g} \\ & x_g \searrow & \| \\ & & x_{1g} x_{3g} \mu^{\tau g} \end{array} \tag{21}$$

then the triangle pattern occurs again, as given by the full diagram. This time $\|$ denotes true equality. □

Remark 16. The presentation has been chosen to follow Evans' original [6] as closely as possible. Using the modern language of term rewriting systems, it may be noted that the *critical pairs* correspond to (18), (20), and (21) [1, Sec. 6.2] [8, Sec. 3.2].

7. The Normal Form Theorem

Following the proof of the Diamond Lemma 15, this section completes the proof of the Normal Form Theorem 13.

Proposition 17. *Two words u and v of W are related by V if and only if the normal forms $\overline{u}$ and $\overline{v}$ coincide.*

Proof. The "if" statement is immediate, since $(u, \overline{u})$ and $(\overline{v}, v)$ both lie in the transitive relation V. Conversely, suppose that u and v are related by V. Then there is a chain

$$u = w_0 \sim w_1 \sim \cdots \sim w_{n-1} \sim w_n = v \tag{22}$$

of some finite length n such that successive elements w_i, w_{i+1} of W (for $0 \leq i < n$) are either (σ, H)-equivalent, or else related by a reduction $w_i \to w_{i+1}$ or $w_{i+1} \to w_i$. The desired equality of the normal forms will be proved by induction on n. If $n = 1$, then the equality is immediate if u and v are (σ, H)-equivalent. Otherwise, suppose without loss of generality that there is a reduction $u \to v$. Suppose that u and v reduce to their normal forms by respective chains

$$u \to u_1 \to \cdots \to \overline{u} \tag{23}$$

and

$$v \to v_1 \to \cdots \to \overline{v}.$$

Applying the Diamond Lemma 15 to the reduction chains (23) and

$$u \to v \to v_1 \to \cdots \to \overline{v}$$

for u then shows that $\overline{u} = \overline{v}$.

Now suppose that the desired equality holds for all pairs u', v' of words connected by chains of length less than n. Consider the chain (22). Then $\overline{u} = \overline{w_1}$ and $\overline{w_1} = \overline{v}$ by induction, so $\overline{u} = \overline{v}$ as required. □

The free H-symmetric extension $Q^H_{(X,U)}$ of (X, U) is now obtained abstractly as the quotient (W^V_X, μ^{S_3}). More concretely, it is realized as the quasigroup

$$\overline{W} = \{\overline{w} \mid w \in W\}$$

of normal forms, with

$$\overline{u}\,\overline{v}\,\mu^g = \overline{\overline{u}\,\overline{v}\,\mu^g}$$

for u, v in W and g in S_3. In particular, the free H-symmetric quasigroup generated by a set X is the free extension $Q^H_{(X,\varnothing)}$ of the empty partial Latin square $(X, \varnothing)$ on the set X.

8. Idempotent Quasigroups

A partial Latin square (X, U) is said to be *idempotent* if $(x, x, x) \in U$ for all x in X. Of course, a quasigroup Q is idempotent if and only if its ternary multiplication table is idempotent as a partial Latin square.

Let H be a subgroup of S_3. Let (X, U) be an H-symmetric, idempotent partial Latin square. An H-symmetric idempotent quasigroup Q is said to *extend* (X, U) if X is a subset of Q and U is a subset of $T(Q)$. Such an extension Q is *free* if the embedding of X in any H-symmetric idempotent extension Q' extends to a unique

quasigroup homomorphism from Q to Q'. Evans' Normal Form Theorem adapts to show that (X, U) possesses a free H-symmetric idempotent extension $Q^{H,I}_{(X,U)}$, again giving an explicit description of the extension.

One additional reduction is needed for the Diamond Lemma 15. If a word w from W contains an instance of $uu\mu^g$ for a word u from W, the subword $uu\mu^g$ is replaced by u. The new reduction rule $w \to w'$ is written explicitly as

$$w \xrightarrow{I_g} w' . \tag{24}$$

There are three additional external cases in the proof of the Diamond Lemma 15. For the instance of (19) given by the left-hand side of the diagram

$$\begin{array}{ccccc} & & u & & \\ & I_g \nearrow & & \searrow & \\ w = uu\,\mu^g & & & & u_1 \\ & \searrow & & & \uparrow I_g \\ & & u_1 u \mu^g & \to & u_1 u_1 \mu^g \end{array}$$

for some word u in W, a diamond pattern is obtained as shown by the full diagram. The second case has the reduction $w = uu\mu^g \longrightarrow uu_1\mu^g$ down its southwest side, but the diagram is identical otherwise. Finally, if (19) takes the form of the left-hand side of the diagram

$$\begin{array}{ccc} & u & \\ g \nearrow & & \\ & \uparrow & \\ w = u\,uu\mu^g\,\mu^{\tau g} & \Big| & I_{\tau g} \\ & & \\ I_g \searrow & & \\ & uu\mu^{\tau g} & \end{array}$$

for some word u in W, then the triangle pattern occurs, as illustrated by the full diagram.

Acknowledgment

Thanks are due to an anonymous referee for valuable comments on an earlier version of this paper.

References

[1] F. Baader and T. Nipkow, *Term Rewriting and All That* (CUP, Cambridge, 1998).
[2] O. Chein *et al.*, *Quasigroups and Loops: Theory and Applications* (Heldermann, Berlin, 1990).
[3] J. H. Conway and D. A. Smith, *On Quaternions and Octonions* (Peters, Natick, MA, 2002).

[4] J. W. DiPaola and E. Nemeth, Generalized triple systems and medial quasigroups, in *Proc. Seventh Southeastern Conf. Combinatorics, Graph Theory and Computing, 1976*, Congressus Numerantium, No. XVII (Utilitas Math., Winnipeg, Manitoba, 1976), pp. 289–306.
[5] T. Evans, Homomorphisms of non-associative systems, *J. London Math. Soc.* **24** (1949) 254–260.
[6] T. Evans, On multiplicative systems defined by generators and relations, *Proc. Camb. Phil. Soc.* **47** (1951) 637–649.
[7] G. Grätzer and R. Padmanabhan, On idempotent commutative and nonassociative groupoids, *Proc. Amer. Math. Soc.* **29** (1973) 249–264.
[8] G. Huet, Confluent reductions: Abstract properties and applications to term rewriting systems, *J. ACM* **27** (1980) 797–821.
[9] I. M. James, Quasigroups and topology, *Math. Zeitschr.* **84** (1964) 329–342.
[10] C. C. Lindner and T. Evans, *Finite Enbedding Theorems for Partial Designs and Algebras* (Université de Montréal, Montreal, 1977).
[11] O. Loos, *Symmetric Spaces I: General Theory* (Benjamin, New York, NY, 1969).
[12] N. S. Mendelsohn, Orthogonal Steiner systems, *Aequationes Math.* **5** (1979) 268–272.
[13] N. S. Mendelsohn, A natural generalization of Steiner triple systems, in *Proc. Sci. Res. Council Atlas Sympos.* No. 2, Oxford, 1969 (Academic Press, London, 1971), pp. 323–338.
[14] A. Mitschke and H. Werner, On groupoids representable by vector spaces over finite fields, *Arch. Math.* **24** (1973) 14–20.
[15] Yu. M. Movsisyan, Hyperidentities in algebras and varieties, *Uspekhi Mat. Nauk* **53** (1998) 61–114 (in Russian).
[16] J. M. Osborn, New loops from old geometries, *Amer. Math. Monthly* **68** (1961) 103–107.
[17] H. O. Pflugfelder, *Quasigroups and Loops: Introduction* (Heldermann, Berlin, 1990).
[18] J. D. Phillips and P. Vojtechovsky, The varieties of quasigroups of Bol-Moufang type: An equational reasoning approach, *J. Algebra* **293** (2005) 17–33.
[19] D. Pigozzi and J. Sichler, Homomorphisms of partial and of complete Steiner triple systems and quasigroups, in *Universal Algebra and Lattice Theory*, ed. S. D. Comer (Springer, Berlin, 1985), pp. 224–237.
[20] A. Sade, Quasigroupes obéissant à certaines lois, *Rev. Fac. Sci. Univ. Istanbul, Ser. A* **22** (1957) 151–184.
[21] A. Sade, Quasigroupes demi-symétriques, *Ann. Soc. Sci. Bruxelles Ser. I* **79** (1965) 133–143.
[22] A. Sade, Quasigroupes demi-symétriques II. Autotopies gauches, *Ann. Soc. Sci. Bruxelles Ser. I* **79** (1965) 223–232.
[23] A. Sade, Quasigroupes demi-symétriques III. Constructions linéaires, A-maps, *Ann. Soc. Sci. Bruxelles Ser. I* **81** (1967) 5–17.
[24] A. Sade, Quasigroupes demi-symétriques. Isotopies préservant la demi-symétrie, *Math. Nach.* **33** (1967) 177–188.
[25] J. D. H. Smith, Homotopy and semisymmetry of quasigroups, *Algebra Univ.* **38** (1997) 175–184.