ON GROUPS OF HYPERSUBSTITUTIONS

JONATHAN D.H. SMITH

Abstract. Groups of (proper) hypersubstitutions are symmetries of algebraic theories. Symmetry at this abstract level is broken at the level of concrete algebras, because the complexity of operations may vary over the orbits of a hypersubstitution group.

This is a preprint version. Please cite the published version as: J.D.H. Smith, On groups of hypersubstitutions, *Algebra Univers.* **64** (2010), 39–48.

1. Introduction

Consider a finitary type $\tau : \Omega \to \mathbb{N}$, with derived type $\tau' : P\Omega \to \mathbb{N}$ [7, §IV.1.3]. A *hypersubstitution* of type τ is a morphism $\sigma : \tau \to \tau'$ in the slice category $\underline{\underline{\mathrm{Set}}}/\mathbb{N}$, a function $\sigma : \Omega \to P\Omega$ such that the diagram

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma} & P\Omega \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau'} \\ \mathbb{N} & = & \mathbb{N} \end{array}$$

commutes. Each hypersubstitution $\sigma : \Omega \to P\Omega$ induces a corresponding function $\widehat{\sigma} : P\Omega \to P\Omega$ with $x^{\widehat{\sigma}} = x$ for x in P, and $v^{\widehat{\sigma}} = (u_1^{\widehat{\sigma}}, \ldots, u_n^{\widehat{\sigma}})\omega^{\sigma}$ for a derived operator $v = (u_1, \ldots, u_n)\omega$ with ω in Ω [1, 2]. If $\mathcal{V}$ is a variety of algebras of type τ, a ($\mathcal{V}$-)*proper hypersubstitution* is a hypersubstitution σ such that $u^{\widehat{\sigma}} = v^{\widehat{\sigma}}$ for all identities $u = v$ of $\mathcal{V}$ [2, 5]. Of course, general hypersubstitutions of a given type τ are proper hypersubstitutions of the full variety of all algebras of that type.

The main concern of this paper is with the invertible proper hypersubstitutions

$$\sigma : \Omega \to \Omega$$

of a variety $\mathcal{V}$. (The codomain is restricted to Ω, so that the inverse σ^{-1} is also a hypersubstitution.) Such hypersubstitutions are

2000 *Mathematics Subject Classification.* 08A40, 20B25, 20M30, 20N05.

Key words and phrases. hypersubstitution, lattice, one-way function, quasigroup, hyperquasigroup, loop transversal, Catalan loop.

important, because they embody the symmetries of the algebraic theory represented by $\mathcal{V}$. It is convenient to refer to the invertible $\mathcal{V}$-proper hypersubstitutions as *hyperequivalences*, or more precisely as *$\mathcal{V}$-hyperequivalences*. Two derived operators u and v are said to be *hyperequivalent* (in $\mathcal{V}$) if there is a $\mathcal{V}$-hyperequivalence σ such that $u^{\widehat{\sigma}} = v$.

Perhaps the simplest example of hyperequivalence is lattice duality (Section 3): The meet and join operations of a lattice are hyperequivalent. However, although there is symmetry between the meet and join of a lattice at the abstract algebraic level, the symmetry may be broken when one actually considers the complexity of computing meets and joins of specified elements in a particular lattice. This symmetry-breaking phenomenon appears to be quite widespread, and is the second topic addressed in the paper.

The paper begins by examining which monoids are represented as monoids of hypersubstitutions, and which groups appear as groups of hyperequivalences. In Theorem 2.2, it is observed that each monoid (and indeed each faithful monoid action) may be realized as a monoid of hypersubstitutions. Theorem 2.2 answers Problem 6 of Denecke and Wismath [2, p. 288], formulated as Problem 2.1 below. Corollary 2.6 shows that if a group is the automorphism group of a monoid, then it is the group of hyperequivalences of a certain variety, while Theorem 2.7 shows that each finite group is the hyperequivalence group of some variety. Symmetric groups reappear as the groups of hyperequivalences of n-quasigroups in Section 4.

The remainder of the paper is devoted to the phenomenon of symmetry-breaking. Section 3 considers lattice duality from this point of view: Theorem 3.1 exhibits a concrete lattice, and a specification procedure for its elements, such that the complexity of joins is negligible in comparison with the complexity of meets. A general discussion of hyperequivalence in n-quasigroups, for each positive integer n, is given in Section 4. Section 5 then casts the problem of one-way functions as a symmetry-breaking for unary quasigroups, while Section 6 looks at (binary) quasigroups, presenting a ring-theoretic example where hyperequivalent operations vary from rational to algebraic in complexity.

For algebraic concepts and notations used in the paper that are not otherwise explained, readers are referred to [7].

2. Representing monoids and groups

The first result gives a simple solution to the following problem of Denecke and Wismath:

Problem 2.1. [2, Problem 8.2(6)] Which monoids are isomorphic ro a monoid of hypersubstitutions of some type τ?

Theorem 2.2. *Let (Q, G) be a faithful monoid action. Then there is a variety $\mathcal{V}$ such that (Q, G) is similar to a monoid of hypersubstitutions on $\mathcal{V}$.*

Proof. Consider the type $\tau : Q \to \{0\}$. Let $\mathcal{V}$ be the variety of all algebras (A, Q) of type τ. Thus a $\mathcal{V}$-algebra (A, Q) corresponds to a function $Q \to A$. Note that the free $\mathcal{V}$-algebra on a set X is the insertion $Q \to Q + X$ of Q in the disjoint union $Q + X$. In particular, the free $\mathcal{V}$-algebra on the empty set is just (Q, Q), corresponding to the identity function $1_Q : Q \to Q$. For each element g of G, define a $\mathcal{V}$-proper hypersubstitution directly by the action of G on Q. Then (Q, G) becomes (similar to) a monoid of hypersubstitutions on $\mathcal{V}$. □

Algebras in the variety $\mathcal{V}$ of the proof of Theorem 2.2 are known as *Q-pointed sets*. Specializing Theorem 2.2 to the case where the monoid G is a group yields the following.

Corollary 2.3. *Let (Q, G) be a permutation group. Then there is a variety $\mathcal{V}$ such that (Q, G) is similar to a group of invertible hypersubstitutions on $\mathcal{V}$.*

Problem 2.1 merely asked which abstract monoids are isomorphic to a monoid of hypersubstitutions. Theorem 2.2 already answers a stronger question, since it deals with concrete monoid actions.

In the construction of Theorem 2.2, the monoid Q^Q of all self-maps on Q is the full monoid of all (proper) hypersubstitutions on $\mathcal{V}$. The given monoid G may well be a proper submonoid of Q^Q. Again, in Corollary 2.3, the symmetric group $Q!$ of all permutations of the set Q is the full group of all hyperequivalences of $\mathcal{V}$, and the given permutation group G may well be a proper subgroup of $Q!$. One is led to refine Problem 2.1, and its group analogue, as follows.

Problem 2.4. (a) Which abstract monoids are isomorphic to the monoid of all proper hypersubstitutions of a variety $\mathcal{V}$?
(b) Which abstract groups are isomorphic to the group of all proper invertible hypersubstitutions of a variety $\mathcal{V}$?

Theorem 2.5 below gives a partial answer to Problem 2.4(a), while Corollary 2.6 and Theorem 2.7 give partial answers to Problem 2.4(b).

Theorem 2.5. *Let M be the endomorphism monoid of a monoid S. Then there is a variety $\mathcal{V}$ such that M is isomorphic, as an abstract monoid, to the monoid of all proper hypersubstitutions on $\mathcal{V}$.*

Proof. Let $\mathcal{V}$ be the variety of right S-actions, algebras (A, S) of type $\tau : S \to \{1\}$ satisfying the unital law $a1 = a$ and the mixed associative law $(as_1)s_2 = a(s_1s_2)$ for s_1, s_2 in S. Let $\sigma : S \to S$ be a proper hypersubstitution on $\mathcal{V}$. Then for a in a $\mathcal{V}$-algebra A and s_1, s_2 in S, one has

$$a(s_1^\sigma s_2^\sigma) = (as_1^\sigma)s_2^\sigma = a(s_1s_2)^\sigma \,. \tag{2.1}$$

The first equality is a direct application of the mixed associative law, while the second equality follows since σ is a proper hypersubstitution. Similarly, one has

$$a1 = a = a^{\widehat{\sigma}} = a1^{\widehat{\sigma}} = a1^\sigma \,. \tag{2.2}$$

Now consider a faithful S-action (A, S), for example the right regular representation (S, S) of the monoid S. Applying (2.1) and (2.2) to such a case yields

$$s_1^\sigma s_2^\sigma = (s_1s_2)^\sigma \quad \text{and} \quad 1 = 1^\sigma$$

for s_1, s_2 in S, so that σ is an element of the endomorphism monoid M of S. □

The technique of the proof of Theorem 2.5 yields the following.

Corollary 2.6. *Suppose that G is the automorphism group of a monoid S. Then there is a variety $\mathcal{V}$ such that G is isomorphic to the hyperequivalence group of $\mathcal{V}$.*

The final result of this section shows that each finite group is isomorphic to the hyperequivalence group of a certain variety.

Theorem 2.7. *Let G be a finite group. Then there is a variety $\mathcal{V}$ such that G is isomorphic to the hyperequivalence group of $\mathcal{V}$.*

Proof. Suppose $|G| = n$. Without loss of generality, identify G with $\{1, \ldots, n\}$, and take a group structure $\big(\{1, \ldots, n\}, \cdot, 1\big)$ isomorphic to G. Define the operator domain $\Omega = \{\omega_i \mid 1 \leq i \leq n\}$. Consider the type $\tau : \Omega \to \{n\}$. Let $\mathcal{V}$ be the variety of algebras of type τ satisfying the identities

$$x_1x_2 \ldots x_n\omega_{l\cdot m} = x_lx_{l\cdot 2} \ldots x_{l\cdot n}\omega_m \tag{2.3}$$

for $1 \leq l, m \leq n$. In particular, the projections

$$\omega_m : G^n \to G; (x_1, \ldots, x_m, \ldots, n) \mapsto x_m$$

for $1 \leq m \leq n$ yield a $\mathcal{V}$-algebra (G, Ω) in which

$$x_1x_2 \ldots x_n\omega_l = x_1x_2 \ldots x_n\omega_m$$

for $1 \leq l, m \leq n$ if and only if $l = m$.

Now consider a $\mathcal{V}$-proper hypersubstitution with $\widehat{\sigma} : \Omega \to \Omega; \omega_m \mapsto \omega_{m\sigma}$. The properness of $\widehat{\sigma}$ and (2.3) together imply

$$x_1 x_2 \dots x_n \omega_{(l\cdot m)\sigma} = x_l x_{l\cdot 2} \dots x_{l\cdot n} \omega_{m\sigma} = x_1 x_2 \dots x_n \omega_{l\cdot(m\sigma)} \,,$$

so that $(l \cdot m)\sigma = l \cdot (m\sigma)$ for all l, m in G. There is then an element s of G, namely $s = 1\sigma$, such that $m\sigma = m \cdot s$ for all m in G (compare [7, §IV.3.1]). Conversely, for each element s of G, consider the hypersubstitution $\sigma : \Omega \to \Omega; \omega_m \mapsto \omega_{m\cdot s}$. Then the associative law in G and (2.3) yield

$$\begin{aligned} x_1 x_2 \dots x_n \omega^{\sigma}_{l\cdot m} &= x_1 x_2 \dots x_n \omega_{(l\cdot m)\cdot s} \\ &= x_1 x_2 \dots x_n \omega_{l\cdot(m\cdot s)} \\ &= x_l x_{l\cdot 2} \dots x_{l\cdot n} \omega_{m\cdot s} \\ &= x_l x_{l\cdot 2} \dots x_{l\cdot n} \omega^{\sigma}_{m} \,, \end{aligned}$$

so the hypersubstitution σ is proper. □

3. Lattice duality

Consider lattices $(L, \vee, \wedge)$ in the usual form, as algebras of type $\{\vee, \wedge\} \times \{2\}$, with semilattices $(L, \vee)$, $(L, \wedge)$, and the absorption laws

$$(x \wedge y) \vee y = (x \vee y) \wedge y = y \,.$$

Lattice duality is the involutary hyperequivalence

$$\delta = (\wedge\ \vee)$$

(written as a 2-cycle) between the join $\vee$ and meet $\wedge$ operations. The following theorem exhibits a concrete lattice $(L, \vee, \wedge)$, including a determined procedure for specifying the elements of L, such that the abstract symmetry of lattice duality is broken: The complexity of the join is negligible in comparison with the complexity of the meet. In the statement of the theorem, a typical value for the index α would be $\log_2 7$ for the Strassen algorithm [9].

Theorem 3.1. *Let V be a vector space of finite dimension n. Let $(L, \wedge, \vee)$ be the lattice of subspaces of V. Suppose that subspaces are specified as spans of (not necessarily independent) subsets. Suppose further that a pair of $n \times n$ matrices may be multiplied by a program of complexity $\mathrm{O}(n^\alpha)$, for some index α. Then the complexity of the meet operation $\wedge$ is*

$$\mathrm{O}(n^\alpha + n \log n) \,, \tag{3.1}$$

while the complexity of the join operation $\vee$ is negligible.

Proof. Consider subspaces

$$X = \mathrm{Span}\{x_1, x_2, \dots\} \quad \text{and} \quad Y = \mathrm{Span}\{y_1, y_2, \dots\}\,. \tag{3.2}$$

Then

$$X \vee Y = \mathrm{Span}\{x_1, x_2, \dots, y_1, y_2, \dots\}\,. \tag{3.3}$$

To determine a spanning set for $X \wedge Y$, consider an inner product $u \cdot v$ on V. The respective orthogonal complements of the subspaces (3.2) are

$$X^\perp = \mathrm{Span}\{x'_1, x'_2, \dots\} \quad \text{and} \quad Y^\perp = \mathrm{Span}\{y'_1, y'_2, \dots\}\,. \tag{3.4}$$

The spanning vectors $x'_1, x'_2, \dots$ for $X^\perp$ are determined by the solution to the system $x_! \cdot z' = 0$, $x_2 \cdot z' = 0, \dots$ of linear equations in the n unknown components of a vector z' in $X^\perp$. A comparable system determines the spanning set for $Y^\perp$. One then obtains

$$X \wedge Y = \mathrm{Span}\{\mathrm{z}_1, \mathrm{z}_2, \dots\} \tag{3.5}$$

as the solution set to the system $z{\cdot}x'_1 = 0$, $z{\cdot}x'_2 = 0, \dots, z{\cdot}y'_1 = 0$, $z{\cdot}y'_2 = 0, \dots$ of linear equations (in the n unknown components of a vector z in $X \wedge Y$) with coefficient vectors from (3.4). Overall, determination of the specification (3.5) for $X \wedge Y$ has required the solution of three systems of $\mathrm{O}(n)$ linear equations in n unknowns. Under the assumptions of the theorem, the complexity of each of these solution procedures, and thus for their totality, is (3.1) [8]. □

Remark 3.2. The extreme symmetry-breaking exhibited in Theorem 3.1 depends critically on the chosen method of identification for the elements of the subspace lattice L. For example, suppose that the subspaces were instead required to be specified as spans of *linearly independent* subsets. Each of the spanning sets (3.3) and (3.5) would then have to be pruned to delete redundant vectors. In that case, the complexity of the lattice join would no longer be negligible in comparison to the complexity of the meet. Note also that in both this specification procedure for subspaces, and in the procedure adopted for Theorem 3.1, it is nontrvial to determine whether two given spans represent the same subspace.

4. Hyperquasigroups

For each positive integer n, this section exhibits the symmetric group S_{n+1} on $n+1$ symbols as the hyperequivalence group of the variety of n-ary quasigroups. The two following sections discuss how this symmetry may be broken in the unary and binary cases. Recall that S_{n+1} has

already appeared as the hyperequivalence group of the variety of Q-pointed sets, according to Corollary 2.3, with (Q, S_{n+1}) as the natural action of S_{n+1} on an $(n+1)$-element set Q.

For the purposes of the section, it is most convenient to define n-quasigroups using the language of hyperquasigroups [6]. An *n-ary space* (G, σ, τ) is a set G that is equipped with unary operations $\sigma : G \to G; g \mapsto \sigma g$ (known as the *shift*) and $\tau : G \to G; g \mapsto \tau g$ (the *inversion*) satisfying $\sigma^n = \tau^2 = 1$. An *n-hyperquasigroup* (Q, G) is a set Q equipped with an n-ary operation ω_g for each element g of the n-ary space G, such that the *hypercommutative law*

$$x_n \dots x_2 x_1 \omega_g = x_{n-1} \dots x_1 x_n \omega_{\sigma g}$$

and *hypercancelation law*

$$x_n \dots x_2 (x_n \dots x_1 \omega_g) \omega_{\tau g} = x_1$$

are satisfied for all $x_1, \dots, x_n$ in Q and g in G.

Consider the symmetric group S_{n+1} as the group of permutations of the set $\{0, 1, \dots, n\}$. Define the permutations

$$s = (n \; n-1 \; \dots \; 2 \; 1) \quad \text{and} \quad t = (0 \; 1) \, .$$

Note that S_{n+1} is generated by the set $\{s, t\}$. Construe S_{n+1} as an n-ary space with the left multiplications

$$\sigma : S_{n+1} \to S_{n+1}; g \mapsto sg \quad \text{and} \quad \tau : S_{n+1} \to S_{n+1}; g \mapsto tg \, .$$

Defining $\Omega = \{\omega_g \mid g \in S_{n+1}\}$, each n-hyperquasigroup (Q, S_{n+1}) corresponds to an n-quasigroup (Q, Ω) [6, Remark 6.3]. Let $\mathcal{V}_n$ denote the variety of algebras of type $\Omega \times \{n\}$ satisfying the hypercommutative and hypercancelation laws.

Theorem 4.1. *Let n be a positive integer. Then the symmetric group S_{n+1} is the hyperequivalence group of the variety $\mathcal{V}_n$ of n-quasigroups.*

Proof. Let π be an element of S_{n+1}. Construe π as a hypersubstitution of type $\Omega \times \{n\}$ by means of the right multiplication

$$S_{n+1} \to S_{n+1}; g \mapsto g\pi \, .$$

For each element g of S_{n+1}, hypercommutativity and the associative law in S_{n+1} yield

$$x_n \dots x_2 x_1 \omega_{g\pi} = x_{n-1} \dots x_1 x_n \omega_{\sigma(g\pi)} = x_{n-1} \dots x_1 x_n \omega_{(\sigma g)\pi} \, .$$

Similarly, hypercancelation and the associative law in S_{n+1} yield

$$x_1 = x_n \dots x_2 (x_n \dots x_1 \omega_{g\pi}) \omega_{\tau(g\pi)} = x_n \dots x_2 (x_n \dots x_1 \omega_{g\pi}) \omega_{(\tau g)\pi} \, .$$

Thus π is a $\mathcal{V}_n$-proper hypersubstitution.

Conversely, let $\pi : S_{n+1} \to S_{n+1}$ be a $\mathcal{V}_n$-proper hypersubstitution. For each element g of S_{n+1}, the properness of π and hypercommutativity yield

$$x_n \dots x_2 x_1 \omega_{(sg)\pi} = x_{n-1} \dots x_1 x_n \omega_{g\pi} = x_n \dots x_2 x_1 \omega_{s(g\pi)} \,. \tag{4.1}$$

Similarly, the properness of π and hypercancelation yield

$$x_n \dots x_2 (x_n \dots x_1 \omega_{(tg)\pi}) \omega_{g\pi} = x_1 = x_n \dots x_2 (x_n \dots x_1 \omega_{t(g\pi)}) \omega_{g\pi} \,,$$

so that

$$x_n \dots x_1 \omega_{(tg)\pi} = x_n \dots x_1 \omega_{t(g\pi)} \,. \tag{4.2}$$

Interpreting (4.1) and (4.2) in the free n-quasigroup on n generators yields

$$(sg)\pi = s(g\pi) \quad \text{and} \quad (tg)\pi = t(g\pi)$$

for all g in S_{n+1}. Since s and t generate S_{n+1}, one has

$$(hg)\pi = h(g\pi)$$

for all g, h in S_{n+1}. Thus there is an element p of S_{n+1}, namely $p = 1\pi$, such that $g\pi = gp$ for all g in S_{n+1} (compare [7, §IV.3.1]). □

5. One-way functions

A *unary quasigroup* is an algebra (A, T, U) of type $\{T, U\} \times \{1\}$, satisfying the identities

$$xTU = x \quad \text{and} \quad xUT = x$$

that establish the invertibility of the function $T : A \to A$. A unary quasigroup (A, T, U) is sometimes construed as a *reversible dynamical system* (A, T), with A as the state space and T as the reversible evolution operator (whose effect is undone by U). The involutary hyperequivalence

$$\rho = (T\ U)$$

of unary quasigroups (written with the same cycle notation used for lattice duality in §3) corresponds to a time reversal in the dynamical system interpretation. Now suppose that this abstract symmetry is broken by a concrete unary quasigroup (A, T, U), say with the invertible function $T : A \to A$ being easy, while its inverse $U : A \to A$ is hard. The symmetry-breaking is then equivalent to $T : A \to A$ being a one-way function. (Compare [3] for a recent survey of one-way functions.)

6. Binary quasigroups

A (*binary*) *quasigroup* is an algebra $(Q, \cdot, /, \backslash)$ of type $\{\cdot, /, \backslash\} \times \{2\}$ satisfying the identities

$$(x/y) \cdot y = (x \cdot y)/y = x = y\backslash(y \cdot x) = y \cdot (y\backslash x)\,. \tag{6.1}$$

Defining the opposite operations

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

quasigroups will be construed as algebras of binary type $\{\cdot, \circ, /, //, \backslash, \backslash\backslash\} \times \{2\}$. The symmetric group S_3 is generated by the transpositions (0 1) and (1 2). According to the case $n = 2$ of Theorem 4.1, the group S_3 acts as the group of hypersubstitutions of the theory of binary quasigroups. The action may be displayed by the following version of the Cayley diagram of S_3 as generated by (0 1) and (1 2):

$$\begin{array}{ccccc} (Q, \cdot, /, \backslash) & \Longleftrightarrow & (Q, \backslash, //, \cdot) & \longleftrightarrow & (Q, //, \backslash, \circ) \\ \updownarrow & & & & \Updownarrow \\ (Q, \circ, \backslash\backslash, //) & \Longleftrightarrow & (Q, \backslash\backslash, \circ, /) & \longleftrightarrow & (Q, /, \cdot, \backslash\backslash) \end{array} \tag{6.2}$$

The quasigroups appearing in (6.2) are known as mutual *conjugates* (or possibly "parastrophes" according to some authors).

A *right quasigroup* is an algebra $(Q, \cdot, /)$ of type $\{\cdot, /\} \times \{2\}$, satisfying the first two identities of (6.1). Right quasigroups arise when one takes the quotient of a group G by a subgroup H which is not necessarily normal. Let Q be a right transversal to H in G, so that G is expressed as the disjoint union $G = \sum_{t \in Q} Ht$ of cosets. Define an algebra $(Q, \cdot, /)$ of type $\{\cdot, /\} \times \{2\}$ by

$$t \cdot u \in H(tu), \qquad t/u \in H(tu^{-1}) \tag{6.3}$$

for t, u in Q. Then $(Q, \cdot, /)$ is a right quasigroup. If H is normal in G, then Q is isomorphic to (the right quasigroup reduct of) the usual group quotient G/H. There are other cases, with H not normal, in which the operations (6.3) complete to a quasigroup $(Q, \cdot, /, \backslash)$. However, it often then happens that the complexity of the left division $\backslash$ (and its opposite) is higher than the complexity of the right quasigroup operations, breaking the S_3-symmetry (6.2). In the following ring-theoretic example (summarizing results from [4]), the right quasigroup operations are rational, while the left division is algebraic.

Example 6.1. Let R be a commutative, unital ring with a topologically nilpotent element e, for example 2 in the ring $\mathbb{Z}/2^n\mathbb{Z}$ of integers modulo 2^n for some positive integer n, or the indeterminate X in the

power series ring $R = S[[X]]$ over some commutative, unital ring S. Note that $1 + eR$ is a subset of the group R^* of units of R. Consider the torus

$$T = \left\{ \begin{bmatrix} d & 0 \\ 0 & d^{-1} \end{bmatrix} \;\middle|\; d \in R^* \right\}$$

in $\mathrm{SL}(2, R)$, and the subset

$$Q = \left\{ \begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix} \;\middle|\; x, x' \in R \right\}$$

of $\mathrm{SL}(2, R)$. Define $G = TQ$. Then G is a subgroup of $\mathrm{SL}(2, R)$, and Q is a transversal to H in R.

Let E be the annihilator of e in R. It is convenient to write

$$\begin{bmatrix} 1 & ex \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ ex' & 1 \end{bmatrix}$$

in Q as $\langle x, x' \rangle$ in the square of R/E. Then Q forms a quasigroup $(Q, /, \backslash)$. Writing $\lambda_m = 1 + e^2 yx'$, the multiplication is rational, with

$$\langle x, x' \rangle \cdot \langle y, y' \rangle = \langle x\lambda_m^2 + y\lambda_m, x'\lambda_m^{-1} + y' \rangle \,.$$

Similarly, the right division is rational, namely

$$\langle z, z' \rangle / \langle y, y' \rangle = \langle z\lambda_r^2 - y\lambda_r, z'\lambda_r^{-1} - y'\lambda_r^{-1} \rangle$$

with $\lambda_r = 1 - e^2 y(z' - y')$. On the other hand, the left division is algebraic, with a quadratic irrationality. Setting

$$d = \frac{-1 + \sqrt{1 + 4(1 + e^2 x'x)(e^2 x'z)}}{2e^2 x'z} \,,$$

one has

$$\langle x, x' \rangle \backslash \langle z, z' \rangle = \left\langle dz - d^{-1}x, (d^{-1}z' - dx') - e^2 x'z'(dz - d^{-1}x) \right\rangle .$$

In particular,

$$\langle 0, -1 \rangle \backslash \langle 1, 0 \rangle = \langle d, d \rangle$$

with

$$d = 1 + e^2 + 2e^4 + 5e^6 + 14e^8 + \ldots$$

as the generating function for the Catalan numbers.

References

[1] K. Denecke, D. Lau, R. Pöschel and D. Schwiegert, *Hyperidentities, hyperequational classes, and clone congruences*, Contributions to General Algebra **7** (1991), 97–118.

[2] K. Denecke and S.L. Wismath, *Hyperidentities and Clones*, Gordon and Breach, Amsterdam, 2000.

[3] L.A. Levin, *The tale of one-way functions*, `arXiv:cs/0012023v5` [cs.CR], 17 Aug 2003. English version of *One-way functions* (Russian), Problemy Peredachi Informatsii **39** (1), 2003.

[4] L. Long and J.D.H. Smith, *Catalan loops*, Math. Proc. Camb. Phil. Soc. **149** (2010), 445–453.

[5] J. Płonka, *Proper and inner hypersubstitutions of algebras*, Proceedings of the International Conference Summer School on General Algebra and Ordered Sets, Olomouc 1994, pp. 106–116.

[6] J.D.H. Smith, *Ternary quasigroups and the modular group*, Comment. Math. Univ. Carol. **49** (2008), 309–317

[7] J.D.H. Smith and A.B. Romanowska, *Post-Modern Algebra*, Wiley, New York, NY, 1999.

[8] V.I. Solodovnikov, *Upper bounds on the complexity of solving systems of linear equations* (Russian), Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), AN SSSR **118** (1982), 159–187.

[9] V. Strassen, *Gaussian elimination is not optimal*, Numer. Math. **13** (1969), 354–356.

Department of Mathematics, Iowa State University, Ames, Iowa 50011, U.S.A.

Email address: `jdhsmith@iastate.edu`

URL: `https://jdhsmith.math.iastate.edu/`