# HOMOTOPIES OF CENTRAL QUASIGROUPS

JONATHAN D. H. SMITH

Abstract. The paper analyzes homotopies between central quasigroups, and their groups of autotopies. In particular, the cycle types of autotopies of central quasigroups and other group isotopes of prime order are identified.

## 1. Introduction

A quasigroup $Q$ or $(Q, \cdot)$ is a set $Q$ with a binary multiplication $x \cdot y$ or $xy$ such that in the equation $xy = z$, knowledge of any two of $x, y, z$ specifies the third uniquely. Thus the body of the multiplication table of a quasigroup is a Latin square, and each Latin square equipped with left and top borders is the multiplication table of a quasigroup. Quasigroups are equivalently axiomatized as algebras $(Q, \cdot, /, \backslash)$ with three binary operations satisfying the identities

$$x = (x \cdot y)/y = (x/y) \cdot y = y\backslash(y \cdot x) = y \cdot (y\backslash x)\,.$$

For $x$ in $Q$, the square is defined as $x^2 = x \cdot x$.

Given quasigroups $Q'$ and $Q$, a triple $(f_1, f_2, f_3)$ of maps from $Q'$ to $Q$ is a *homotopy* if

$$xf_1 \cdot yf_2 = (xy)f_3$$

for all $x, y$ in $Q'$. A homotopy is an *isotopy* if its components biject. An isotopy $(f_1, f_2, f_3) : Q' \to Q$ is said to be an *autotopy* (of $Q$) if $Q = Q'$. (Certain authors, feeling that "autotopy" sounds like the morbid word "autopsy," use "autotopism" instead.) Note that quasigroup homomorphisms, isomorphisms, and automorphisms are respectively just homotopies, isotopies, and autotopies in which all three components coincide.

A quasigroup is *abelian* if it is commutative and associative, so that nonempty abelian quasigroups are just abelian groups. A quasigroup is *central* if the diagonal subquasigroup $\widehat{Q} = \{(q, q) \mid q \in Q\}$ is a normal subquasigroup of the direct square $Q^2$, i.e., if there is a congruence on

2010 *Mathematics Subject Classification.* 20N05, 05B15.

*Key words and phrases.* Latin square, quasigroup, central, homotopy, autotopy, cycle type.

$Q^2$ with $\widehat{Q}$ as a congruence class. If $Q$ is a nonempty central quasigroup, then there is at least one abelian group structure $(Q,+,0)$ on $Q$, together with a pair $a,b$ of automorphisms of $(Q,+,0)$, such that $x\cdot y = xa+yb+0^2$ for $x,y$ in $Q$ [1, Ch. III] [5, Ch. 3]. (For each choice of 0, central quasigroups are thus coordinatized as *$T$-quasigroups* in the sense of [3, 4]. Conversely, each $T$-quasigroup is central.) In particular, the triple

$$(x\mapsto xa, y\mapsto yb, z\mapsto z-0^2)$$

is an isotopy from $(Q,\cdot)$ to $(Q,+)$.

The aim of this paper is to identify all homotopies between a given pair of central quasigroups (Section 2). In Section 3, the results of Section 2 are applied to recover a specification of the autotopy and automorphism groups of a central quasigroup. (Other approaches have appeared at various times in the literature.) Motivated by a question of D.S. Stones [7, Question 5.0.46], [8], discussed in Section 4, Section 5 then specifies the cycle-type multisets of autotopies of a quasigroup of prime order that is central, or (more generally) isotopic to a group.

For conventions and concepts not otherwise outlined explicitly in this paper, readers are referred to [5, 6].

## 2. Homotopies of central quasigroups

The following proposition gives a construction of homotopies between nonempty central quasigroups.

**Proposition 2.1.** *Let $Q'$ and $Q$ be nonempty central quasigroups, with respective multiplications $x\cdot y = xa'+yb'+0^2$ and $x\cdot y = xa+yb+0^2$. Let $f:(Q',+)\to(Q,+)$ be an abelian quasigroup homomorphism. Let $m_1$ and $m_2$ be elements of $Q$. Working in $(Q,+)^3$, define maps $f_i: Q'\to Q$ by*

$$(xf_1, yf_2, zf_3) = \big(xa'fa^{-1}, yb'fb^{-1}, zf\big) + (m_1,m_2,m_3) \tag{2.1}$$

*for all $x,y,z$ in $Q'$, with $m_3 = m_1\cdot m_2 - 0^2f$. Then $(f_1,f_2,f_3): Q'\to Q$ is a homotopy.*

*Proof.* For elements $x$ and $y$ of $Q'$, one has

$$\begin{aligned} xf_1\cdot yf_2 &= xf_1a + yf_2b + 0^2 \\ &= \big(xa'fa^{-1}+m_1\big)\,a + \big(yb'fb^{-1}+m_2\big)\,b + 0^2 \\ &= xa'f + yb'f + m_1a + m_2b + 0^2 \\ &= \big(xa'+yb'+0^2\big)\,f - 0^2f + m_1\cdot m_2 \\ &= (x\cdot y)f + m_3 = (x\cdot y)f_3\,. \end{aligned}$$

Thus (2.1) gives a homotopy. □

As a converse of Proposition 2.1, the following theorem classifies all homotopies between central quasigroups.

**Theorem 2.2.** *Consider nonempty central quasigroups $Q'$ and $Q$, with respective multiplications $x \cdot y = xa' + yb' + 0^2$ and $x \cdot y = xa + yb + 0^2$. Suppose that $(f_1, f_2, f_3) : Q' \to Q$ is a homotopy. Then there is an abelian group homomorphism $f : (Q', +) \to (Q, +)$ such that*

$$(xf_1, yf_2, zf_3) = \big(xa'fa^{-1}, yb'fb^{-1}, zf\big) + (0f_1, 0f_2, 0f_3) \tag{2.2}$$

*in $(Q, +)^3$ for all $x, y, z$ in $Q'$, and the condition*

$$0f_1 \cdot 0f_2 - 0^2 f = 0f_3 \tag{2.3}$$

*holds.*

*Proof.* Since $(f_1, f_2, f_3) : Q' \to Q$ is a homotopy,

$$xf_1a + yf_2b + 0^2 = \big(xa' + yb' + 0^2\big)\, f_3 \tag{2.4}$$

for $x$ and $y$ in $Q'$. In particular, $x = y = 0$ gives

$$0f_1a + 0f_2b + 0^2 = 0^2 f_3\,. \tag{2.5}$$

Setting $y = 0$ in (2.4) gives

$$xf_1a = \big(xa' + 0^2\big)\, f_3 - 0f_2b - 0^2\,. \tag{2.6}$$

Setting $x = 0$ in (2.4) gives

$$yf_2b = \big(yb' + 0^2\big)\, f_3 - 0f_1a - 0^2\,. \tag{2.7}$$

Substituting back into (2.4) from (2.6) and (2.7) gives

$$\big[(xa' + 0^2)f_3 - 0f_2b - 0^2\big] + \big[(yb' + 0^2)f_3 - 0f_1a - 0^2\big] + 0^2 = (xa' + yb' + 0^2)f_3\,.$$

With $x$ replaced by $(x - 0^2)a'^{-1}$ and $y$ replaced by $(y - 0^2)b'^{-1}$, this becomes

$$xf_3 - 0f_2b - 0^2 + yf_3 - 0f_1a = (x + y - 0^2)f_3\,.$$

In view of (2.5), a further reduction to

$$xf_3 + yf_3 - 0^2 f_3 = (x + y - 0^2)f_3 \tag{2.8}$$

takes place. Now define

$$f : Q' \to Q; x \mapsto (x + 0^2)f_3 - 0^2 f_3\,, \tag{2.9}$$

so that $xf_3 = (x - 0^2)f + 0^2 f_3$. In terms of $f$, (2.8) assumes the form

$$(x - 0^2)f + 0^2 f_3 + (y - 0^2)f + 0^2 f_3 - 0^2 f_3 = (x - 0^2 + y - 0^2)f + 0^2 f_3$$

or

$$(x-0^2)f+(y-0^2)f=\left[(x-0^2)+(y-0^2)\right]f\,,$$

so that (2.9) becomes a homomorphism $f:(Q',+)\to(Q,+)$ of abelian groups. Thus $0f_3=0^2f_3-0^2f$.

For $z$ in $Q'$, one has

$$zf_3=(z-0^2)f+c'f_3=(z-0^2)f+0f_3+0^2f=zf+0f_3\,,$$

verifying the third component of (2.2). By (2.5), one has

$$0f_2b=0^2f_3-0f_1a-0^2=0^2f+0f_3-0f_1a-0^2\,.$$

For $y$ in $Q$, (2.7) then gives

$$yf_2=\left[yb'f+0^2f+0f_3-0f_1a-0^2\right]b^{-1}=yb'fb^{-1}+0f_2\,,$$

verifying the second component of (2.2). Similarly, (2.5) yields

$$0f_1a=0^2f_3-0f_2b-0^2=0^2f+0f_3-0f_2b-0^2\,.$$

For $x$ in $Q$, (2.6) then gives

$$xf_1=\left[xa'f+0^2f+0f_3-0f_2b-0^2\right]a^{-1}=xa'fa^{-1}+0f_1\,,$$

verifying the first component of (2.2). Finally, since $(f_1,f_2,f_3)$ is a homotopy, one has $0f_1\cdot 0f_2=0^2f_3=0^2f+0f_3$, verifying (2.3). □

## 3. Autotopy groups

Let $Q$ be a nonempty central quasigroup, with multiplication given by $x\cdot y=xa+yb+0^2$. An element $f$ of the automorphism group $\mathrm{Aut}(Q,+,0)$ of the abelian group $(Q,+,0)$ acts on the direct square $(Q,+,0)^2$ by

$$f:(x,y)\mapsto(xafa^{-1},ybfb^{-1})\,.$$

The following theorem identifies the autotopy group $\mathrm{Atp}(Q)$ of $Q$ as the split extension $(Q,+,0)^2\rtimes\mathrm{Aut}(Q,+,0)$, parametrizing autotopies by triples $(m_1,m_2,f)$ with $m_1,m_2$ in $Q$ and $f$ in $\mathrm{Aut}(Q,+,0)$.

**Theorem 3.1.** *Suppose that $Q$ is a nonempty central quasigroup, with multiplication $x\cdot y=xa+yb+0^2$ for automorphisms $a$ and $b$ of the abelian group $(Q,+,0)$. Then up to isomorphism, the autotopy group $\mathrm{Atp}(Q)$ of $Q$ is built on the set $Q^2\times\mathrm{Aut}(Q,+,0)$, with multiplication given by*

$$(m_1,m_2,f)(n_1,n_2,g)=(m_1aga^{-1}+n_1,m_2bgb^{-1}+n_2,fg) \tag{3.1}$$

*for $m_1,m_2,n_1,n_2$ in $Q$ and $f,g$ in $\mathrm{Aut}(Q,+,0)$.*

*Proof.* By the results of Section 2, each element $(n_1, n_2, g)$ of the set $Q^2 \times \mathrm{Aut}(Q, +, 0)$ determines an autotopy $(g_1, g_2, g_3)$ of $Q$, with

$$\begin{cases} xg_1 = xaga^{-1} + n_1 \,, \\ yg_2 = ybgb^{-1} + n_2 \,, \text{ and} \\ zg_3 = zg + n_1 \cdot n_2 - 0^2 f \end{cases}$$

for $x, y, z$ in $Q$. Equivalently, the element $(m_1, m_2, f)$ lying in the set $Q^2 \times \mathrm{Aut}(Q, +, 0)$ determines the autotopy (2.1), with $a' = a$. Then for $x$ in $Q$, one has

$$\begin{aligned} xf_1g_1 &= \left(xafa^{-1} + m_1\right) g_1 \\ &= \left(xafa^{-1} + m_1\right) aga^{-1} + n_1 \\ &= xa(fg)a^{-1} + \left(m_1aga^{-1} + n_1\right) \end{aligned}$$

and similarly $xf_2g_2 = xb(fg)b^{-1} + (m_2bgb^{-1} + n_2)$. Thus the first two components $(fg)_1$ and $(fg)_2$ of the composite autotopy $fg$ are given by the right hand side of (3.1). □

**Corollary 3.2.** *Automorphisms of $Q$ are parametrized by those triples $(m, m, f)$ for which $f$ lies in the centralizer $C_{\mathrm{Aut}(Q,+,0)}\langle a, b\rangle$ of $a$ and $b$ in $\mathrm{Aut}(Q, +, 0)$. Thus the automorphism group $\mathrm{Aut}(Q)$ of $Q$ is the split extension $(Q, +, 0) \rtimes C_{\mathrm{Aut}(Q,+,0)}\langle a, b\rangle$ given by the restriction to $C_{\mathrm{Aut}(Q,+,0)}\langle a, b\rangle$ of the natural action of $\mathrm{Aut}(Q, +, 0)$ on $(Q, +, 0)$.*

## 4. Quasigroups of prime order

In his Ph.D. thesis, D.S. Stones observed that for each prime $p$ that does not exceed 23, the multiset of cycle types of the components of an autotopy of a quasigroup of order $p$ is either $\langle\lambda, \lambda, \lambda\rangle$ for some partition $\lambda$ of $p$, or else $\langle p^1, p^1, 1^p\rangle$. He then asked whether this pattern holds for all primes [7, Question 5.0.46], [8].

In his own Ph.D. thesis, the author gave the following classification of quasigroups of prime order, reproduced as [1, Th.III.5.10], [5, Th.3.10].

**Theorem 4.1.** *Let $Q$ be a quasigroup of prime order $p$. Let $G$ be the multiplication group $\mathrm{Mlt}\, Q$ of $Q$. Then one of the following holds:*

(a) *$Q$ is central;*
(b) *$G$ is the alternating or symmetric group on $Q$;*
(c) *$p = 11$ and $G$ is $\mathrm{PSL}_2(11)$ or $\mathrm{M}_{11}$;*
(d) *$p = 23$ and $G$ is $\mathrm{M}_{23}$;*
(e) *$p = (q^k - 1)/(q - 1)$ for a prime power $q$ and positive integer $k$, while $\mathrm{PSL}_k(q) \leq G \leq \mathrm{P\Gamma L}_k(q)$.*

Since Stones' question is already resolved positively in the cases (c) and (d) of this theorem [2, 7], the cases (a), (b), and (e) remain. The following section is motivated by consideration of Stones' question for the case (a). It gives an affirmative answer there, and also in many instances of (b) and (e). Nevertheless, in April 2010, Wanless announced an example of a quasigroup of order 41 having an autotopy with cycle-type multiset $\langle 1^6 2^1 3^1 6^5, 1^6 2^1 3^1 6^5, 2^4 3^3 6^4 \rangle$ [9]. Wanless' example is an instance of case (b). Stones' question may thus be refined as follows:

**Problem 4.2.** Let $q$ be a prime power. Let $k$ be a positive integer such that $(q^k - 1)/(q - 1) = p$ is prime. Let $Q$ be a quasigroup of order $p$, with $\mathrm{PSL}_k(q) \leq \mathrm{Mlt}\, Q \leq \mathrm{P\Gamma L}_k(q)$. Is the multiset of cycle types of the components of an autotopy of $Q$ either $\langle \lambda, \lambda, \lambda \rangle$ for some partition $\lambda$ of $p$, or else $\langle p^1, p^1, 1^p \rangle$?

## 5. Group isotopes of prime order

Up to isomorphism, each central quasigroup of prime order $p$ is given by the multiplication $x \cdot y = xa + yb + c$ on the additive group $(\mathbb{Z}/_p, +)$ of integers modulo $p$, with residues $a, b, c$ in $\mathbb{Z}/_p$ and $a, b$ nonzero. Thus each central quasigroup of prime order $p$ is isotopic to the additive group $(\mathbb{Z}/_p, +)$. It follows that each cycle-type multiset of an autotopy of a central quasigroup of order $p$ is the cycle-type multiset of an autotopy of the additive group $(\mathbb{Z}/_p, +)$ [7, Lemma 4.3.3(1)].

Each automorphism $f$ of $(\mathbb{Z}/_p, +)$ may be identified as multiplication by a nonzero residue $f$, the image of 1 under the automorphism $f$. By the results of Section 2, each autotopy of $(\mathbb{Z}/_p, +)$ is of the form

$$(f_1, f_2, f_3) : (x, y, z) \mapsto (xf + m_1, yf + m_2, zf + m_3)$$

with $m_3 = m_1 + m_2$ — corresponding to $0f_3 = (0 + 0)f_3 = 0f_1 + 0f_2$. As in Section 3, such an autotopy is parametrized by an arbitrary triple $(m_1, m_2, f)$ of integers modulo $p$, in which the last component is nonzero.

**Lemma 5.1.** *The cycle-type multiset of the autotopy*

$$(x, y, z) \mapsto (x + m_1, y + m_2, z + m_3)$$

*parametrized by a triple of the form* $(m_1, m_2, 1)$ *is either of the form* $\langle \lambda, \lambda, \lambda \rangle$ *for* $\lambda = p^1$ *or* $1^p$, *or else* $\langle p^1, p^1, 1^p \rangle$.

*Proof.* In the relation $m_3 = m_1 + m_2$, it is impossible for just two of $m_1, m_2, m_3$ to be zero. If all three are either zero or nonzero, the cycle-type multiset is $\langle \lambda, \lambda, \lambda \rangle$ for $\lambda = 1^p$ or $\lambda = p^1$ respectively. If just one of $m_1, m_2, m_3$ is zero, then the cycle-type multiset is $\langle p^1, p^1, 1^p \rangle$. □

For what follows, suppose that $f$ is an element of order $r > 1$ in the multiplicative group $\mathbb{Z}/_p^*$ of nonzero residues, while $m$ is an arbitrary element of $\mathbb{Z}/_p$. Consider the permutation $\theta : x \mapsto xf + m$ of $\mathbb{Z}/_p$.

**Lemma 5.2.** *For each positive integer $k$, one has*

$$x\theta^k = xf^k + m\left(f^k - 1\right)/(f-1) \tag{5.1}$$

*for an element $x$ of $\mathbb{Z}/_p$.*

*Proof.* Induction on $k$ shows that

$$x\theta^k = xf^k + m(f^{k-1} + f^{k-2} + \ldots + f + 1)\,.$$

Now $f^k - 1 = (f-1)\left(f^{k-1} + f^{k-2} + \ldots + f + 1\right)$. Division by $(f-1)$ yields the coefficient of $m$ in (5.1). □

**Lemma 5.3.** *If $x = x\theta^s$ for $0 < s < r$, then $x = m/(1-f)$.*

*Proof.* By Lemma 5.2, $x\theta^s = xf^s + m(f^s-1)/(f-1)$. Then $x = x\theta^s$ gives $x(1-f^s) = m(f^s-1)/(f-1)$, from which the result follows on canceling the nonzero residue $(1-f^s)$. □

**Lemma 5.4.** *For each element $x$ of $\mathbb{Z}/_p$, one has $x = x\theta^r$.*

*Proof.* By Lemma 5.2, $x\theta^r = xf^r + m(f^r-1)/(f-1) = x$. □

**Proposition 5.5.** *Suppose that $f$ is an element of order $r > 1$ in the multiplicative group $\mathbb{Z}/_p^*$ of nonzero residues. Then for each element $m$ of $\mathbb{Z}/_p$, the cycle type of the permutation $\theta : x \mapsto xf + m$ is $r^{(p-1)/r}1^1$.*

*Proof.* By Lemma 5.2, $x = m/(1-f)$ is a fixed point of $\theta$. Lemmas 5.3 and 5.4 then show that the remaining elements of $\mathbb{Z}/_p$ all lie in $\theta$-orbits of length $r$. □

**Lemma 5.6.** *Let $f$ be an element of order $r > 1$ in the multiplicative group $\mathbb{Z}/_p^*$ of nonzero residues. Then for elements $m_1$ and $m_2$ of $\mathbb{Z}/_p$, the cycle-type multiset of the autotopy*

$$(x, y, z) \mapsto (xf + m_1, yf + m_2, zf + m_3) \tag{5.2}$$

*parametrized by the triple $(m_1, m_2, f)$ is $\langle\lambda, \lambda, \lambda\rangle$ for $\lambda = r^{(p-1)/r}1^1$.*

*Proof.* Apply Proposition 5.5 to each component of (5.2). □

Lemmas 5.1 and 5.6 together yield the following theorem, which offers an affirmative answer to Stones' question for central quasigroups, and indeed all group isotopes, of prime order.

**Theorem 5.7.** *Let $p$ be a prime number. Let $Q$ be a quasigroup of order $p$. Suppose that $Q$ is central, or more generally just some group isotope. Then the cycle-type multiset of an autotopy of $Q$ is either $\langle p^1, p^1, 1^p\rangle$, or else $\langle\lambda, \lambda, \lambda\rangle$ for $\lambda = p^1$ or $r^{(p-1)/r}1^1$ with $r\big|(p-1)$.*

## References

[1] O. Chein et al., *Quasigroups and Loops: Theory and Applications*, Heldermann, Berlin, 1990.

[2] R.M. Falcón, *Cycle structures of autotopisms of the Latin squares of order up to* 11, `arXiv:0709.2973v2 [math.CO]`, 2009. To appear in Ars Combinatoria.

[3] T. Kepka and P. Němec, *$T$-quasigroups I*, Acta Univ. Carolinae Math. et Phys. **12**, No. 1, (1971), 39–49.

[4] T. Kepka and P. Němec, *$T$-quasigroups II*, Acta Univ. Carolinae Math. et Phys. **12**, No. 2 (1971), 31–49.

[5] J.D.H. Smith, *An Introduction to Quasigroups and Their Representations*, Chapman and Hall/CRC, Boca Raton, FL, 2007.

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

[7] D.S. Stones, *On the number of Latin rectangles*, Ph.D. thesis, Monash University, 2010. Available online at `http://arrow.monash.edu.au/hdl/1959.1/167114`

[8] D.S. Stones, P. Vojtěchovský, and I.M. Wanless, *Cycle structure of autotopisms of quasigroups and Latin squares*, preprint, 2011.

[9] I.M. Wanless, private communication, 2010.

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

*E-mail address*: `jdhsmith@iastate.edu`

*URL*: `http://www.math.iastate.edu/jdhsmith/`