SOME RESULTS USED BY THE GAP PACKAGE RIGHTQUASIGROUPS

GÁBOR P. NAGY AND PETR VOJTĚCHOVSKÝ

1. Congruences

Let $Q = (Q, \cdot, /)$ be a right quasigroup. Then an equivalence relation $\sim$ on Q is a *right quasigroup congruence* if for every $x, y, u, v \in Q$, if $x \sim y$ and $u \sim v$ then $xu \sim yv$ and $x/u \sim y/v$.

Proposition 1.1. *Let $Q = (Q, \cdot, /)$ be a right quasigroup and $\sim$ an equivalence relation on Q. Then:*

(i) *$\sim$ is a right quasigroup congruence iff for every $x, y, u \in Q$, if $x \sim y$ then $xu \sim yu$, $x/u \sim y/u$, $ux \sim uy$ and $u/x \sim u/y$.*
(ii) *If Q is finite then $\sim$ is a right quasigroup congruence iff for every $x, y, u \in Q$, if $x \sim y$ then $xu \sim yu$ and $ux \sim uy$.*

Proof. If $\sim$ is a right quasigroup congruence then certainly the conditions of (i) and (ii) hold. Conversely, suppose that the condition of (i) holds and let $x, y, u, v \in Q$ be such that $x \sim y$ and $u \sim v$. Then $xu \sim yu \sim yv$ and $x/u \sim y/u \sim y/v$ shows that $\sim$ is a right quasigroup congruence.

Finally suppose that Q is finite and the condition of (ii) holds. We will verify the condition of (i). Suppose that $x, y, u \in Q$ and $x \sim y$. We then have $xu \sim yu$ and $ux \sim uy$ by assumption. Since Q is finite, there is n such that $R_u^n = 1$ and thus $R_u^{-1} = R_u^{n-1}$. It follows by an easy induction on n that $x/u = R_u^{-1}(x) = R_u^{n-1}(x) \sim R_u^{n-1}(y) = R_u^{-1}(y) = y/u$. Using finiteness again, let s and t be such that $R_x^s = 1 = R_y^t$. Consider $m = st - 1$. Then $R_x^m = R_x^{st-1} = R_x^{-1}$ and $R_y^m = R_y^{ts-1} = R_y^{-1}$. We then again have $u/x = R_x^{-1}(u) = R_x^m(u) \sim R_y^m(u) = R_y^{-1}(u) = u/y$ by induction on m. The condition of (i) therefore holds and $\sim$ is a congruence. □

Let $Q = (Q, \cdot, /, \backslash)$ be a right quasigroup. Then an equivalence relation $\sim$ on Q is a *quasigroup congruence* if for every $x, y, u, v \in Q$, if $x \sim y$ and $u \sim v$ then $xu \sim yv$, $x/u \sim y/v$ and $x\backslash u \sim y\backslash v$.

Proposition 1.2. *Let $Q = (Q, \cdot, /, \backslash)$ be a quasigroup and $\sim$ an equivalence relation on Q. Then:*

(i) *$\sim$ is a quasigroup congruence iff for every $x, y, u \in Q$, if $x \sim y$ then $xu \sim yu$, $ux \sim uy$, $x/u \sim y/u$ and $u\backslash x \sim u\backslash y$.*
(ii) *If Q is finite then $\sim$ is a quasigroup congruence iff for every $x, y, u \in Q$, if $x \sim y$ then $xu \sim yu$ and $ux \sim uy$.*

Proof. If $\sim$ is a quasigroup congruence then the certainly the conditions of (i) and (ii) holds. Conversely, suppose that the condition of (i) holds and let $x, y, u, v \in Q$ be such that $x \sim y$ and $u \sim v$. Since $u \sim v$, we have $x = (x/u \cdot u) \sim (x/u \cdot v)$ and therefore $x/v \sim ((x/u \cdot v)/v) = x/u$. Also, from $x \sim y$ we get $x/v \sim y/v$. Therefore $x/u \sim x/v \sim y/v$. Dually, $x\backslash u \sim y\backslash v$. Hence $\sim$ is a quasigroup congruence.

If Q is finite, the condition of (i) reduces to the condition of (ii) by the usual trick: $R_u^{-1} = R_u^{n-1}$ and $L_u^{-1} = L_u^{m-1}$ for suitable n and m. $\square$

2. Simplicity

Let G be a group acting on X. Then $B \subseteq X$ is a *block* of the action if for every $g \in G$ either $g(B) = B$ or $g(B) \cap B = \emptyset$. Given a partition $\mathcal{P}$ of X, we say that the action of G *preserves* $\mathcal{P}$ if for every $B \in \mathcal{P}$ and every $g \in G$ we have $g(B) \in \mathcal{P}$. The partitions $\{\{x\} : x \in X\}$ and $\{X\}$ are *trivial*. A transitive permutation group G acts *primitively* on X if it preserves no nontrivial partition of X, else it acts *imprimitively*. (The requirement that G be transitive is only needed if $|X| = 2$.)

For a right quasigroup Q let $\mathrm{Mlt}_r(Q) = \langle R_x : x \in Q\rangle$ be the *right multiplication group* of Q. For a quasigroup Q let $\mathrm{Mlt}(Q) = \langle R_x, L_x : x \in Q\rangle$ be the *multiplication group* of Q.

Theorem 2.1 (Albert)**.** *A quasigroup Q is simple if and only if $\mathrm{Mlt}(Q)$ acts primitively on Q.*

Proof. Well known. $\square$

Example 2.2. Consider the right quasigroup Q with multiplication table

	1	2	3	4
1	2	1	1	1
2	3	2	2	2
3	4	3	3	3
4	1	4	4	4

Then $G = \mathrm{Mlt}_r(Q) = \langle g\rangle$, where $g = (1, 2, 3, 4)$. Note that G acts transitively but imprimitively on Q, with $\{\{1, 3\}, \{2, 4\}\}$ being a nontrivial partition of Q preserved by G. However, an inspection of all possible partitions of Q reveals that Q has no nontrivial congruences and hence is simple. For instance, the above partition is not a right quasigroup congruence since $1 \sim 3$ but $1 \cdot 1 = 2 \not\sim 1 = 1 \cdot 3$.

Proposition 2.3. *Let Q be a right quasigroup. If $\mathrm{Mlt}_r(Q)$ acts primitively on Q then Q is simple. (The converse does not hold, as shown by the above example.)*

Proof. Suppose that Q is not simple and let $\sim$ be a nontrivial congruence on Q. Let B be an equivalence class of $\sim$. If $y \sim z$ then $R_x(y) \sim R_x(z)$ and $R_x^{-1}(y) \sim R_x^{-1}(z)$ since $\sim$ is a congruence. In particular, $R_x(B)$ is contained in some equivalence class C of $\sim$. Write $B = [b]$ and $C = [bx]$. If $c \in C$ then $c \sim bx$ and thus $c/x \sim (bx)/x = b$, so $c/x \in B$, but then $R_x(c/x) = (c/x)x = c$ shows that $R_x(B) = C$. Similarly, $R_x^{-1}(B)$ is an equivalence class of $\sim$. This shows that $\mathrm{Mlt}_r(Q)$ preserves the partition induced by $\sim$ and hence $\mathrm{Mlt}_r(Q)$ acts imprimitively on Q. $\square$

Lemma 2.4. *Let Q be a right quasigroup. The orbits of $\mathrm{Mlt}_r(Q)$ form a right quasigroup congruence of Q.*

Proof. Let $\sim$ be the equivalence relation induced by the orbits of $G = \mathrm{Mlt}_r(Q)$. Suppose that $x \sim y$ and $u \in Q$. Then $ux = R_x(u) \sim R_y(u) = uy$ and $u/x = R_x^{-1}(u) \sim R_y^{-1}(u) = u/y$. Let $g \in G$ be such that $g(x) = y$. Then $xu = R_u(x) \sim R_u(g(x)) = R_u(y) = yu$ and $x/u = R_u^{-1}(x) \sim R_u^{-1}(g(x)) = R_u^{-1}(y) = y/u$. By Proposition 1.1, $\sim$ is a right quasigroup congruence. $\square$

Corollary 2.5. *Let Q be a right quasigroup and suppose that $\mathrm{Mlt}_r(Q) \neq 1$ does not act transitively on Q. Then Q is not simple.*

Note that a right quasigroup Q satisfies $\mathrm{Mlt}_r(Q) = 1$ if and only if it is a projection right quasigroup, that is, a right quasigroup with multiplication and right division given by $xy = x$, $x/y = x$.

Lemma 2.6. *Let Q be a projection right quasigroup. Then any partition of Q is a right quasigroup congruence of Q. In particular, Q is simple if and only if $|Q| > 2$.*

Proof. Let $\sim$ be the equivalence relation induced by a given partition of Q. Suppose that $x \sim y$ and $u \in Q$. Then $xu = x \sim y = yu$, $x/u = x \sim y = y/u$, $ux = u \sim u = uy$ and $u/x = u \sim u = u/y$. By Proposition 1.1, $\sim$ is a right quasigroup congruence. $\square$

3. Nuclei and center

Proposition 3.1. *A nonempty subset S of a finite (right) quasigroup Q is a sub(right)quasigroup of Q iff it is closed under multiplication.*

Proof. In the case of right quasigroups, it suffices to show that S is closed under right division. For $x, y \in S$, consider $R_x \in \mathrm{Sym}(Q)$. Since Q is finite, there is n such that $R_x^n = \mathrm{id}_Q$, so $R_x^{-1} = R_x^{n-1}$. Then $y/x = R_x^{-1}(y) = R_x^{n-1}(y) \in S$ by induction on n. The argument for left divisions is dual in the case of quasigroups. $\square$

Proposition 3.2. *Let Q be a finite (right) quasigroup. Then each of the four nuclei is either a sub(right)quasigroup of Q or the empty set.*

Proof. Let $S = \mathrm{Nuc}_\ell(Q) \neq \emptyset$. Then for every $x, y \in S$ and every $u, v \in Q$ we have $(xy)(uv) = x(y(uv)) = x((yu)v) = (x(yu))v = ((xy)u)v$, so $xy \in S$ and we are done by Proposition 3.1. Dually, if $\mathrm{Nuc}_r(Q) \neq \emptyset$ then it is a sub(right)quasigroup of Q. Now suppose that $S = \mathrm{Nuc}_m(Q) \neq \emptyset$. Then for all $x, y \in S$ and $u, v \in Q$ we have $(u(xy))v = ((ux)y)v = (ux)(yv) = u(x(yv)) = u((xy)v)$, so $xy \in S$ and we are done by Proposition 3.1. The intersection of sub(right)quasigroups is a sub(right)quasigroup. $\square$

Proposition 3.3. *Let Q be a finite (right) quasigroup. Then the center of Q is either a sub(right)quasigroup of Q or the empty set. (Do we need finiteness here?)*

Proof. It remains to prove that if $x, y \in Z(Q)$ and $u \in Q$ then $(xy)u = u(xy)$. We have $(xy)u = x(yu) = (yu)x = (uy)x = u(yx) = u(xy)$. $\square$

4. Lower central series for loops

The lower central series for a loop Q is defined by $Q_{(0)} = Q$, $Q_{(i+1)} = [Q_{(i)}, Q]_Q$, using the congruence commutator of normal subloops. Here we are only using the commutator of the form $[A, Q]_Q$ for $A \trianglelefteq Q$. It's easy to see that $[A, Q]_Q = D$ iff D is the smallest normal subloop of Q such that $A/D \leq Z(Q/D)$.

Lemma 4.1. *Let $A \trianglelefteq Q$. Then $[A, Q]_Q$ is the smallest normal subloop of Q containing $\{\theta(a)/a : a \in A,\ \theta \in \mathrm{Inn}(Q)\}$.*

Proof. Let $D \trianglelefteq Q$. The following conditions are equivalent:

- $A/D \leq Z(Q/D)$
- $\theta(aD) = aD$ for all $a \in A$, $\theta \in \mathrm{Inn}(Q/D)$

- $L_{xD,yD}(aD) = aD$, $R_{xD,yD}(aD) = aD$, $T_{xD}(aD) = aD$ for all $x, y \in Q$, $a \in A$
- $L_{x,y}(a)D = aD$, $R_{x,y}(a)(D) = aD$, $T_x(a)D = aD$ for all $x, y \in Q$, $a \in A$,
- $\theta(a)D = aD$ for all $a \in A$, $\theta \in \mathrm{Inn}(Q)$
- $\theta(a)/a \in D$ for all $a \in A$, $\theta \in \mathrm{Inn}(Q)$.

□

5. Displacement groups

For a right quasigroup $(Q, \cdot)$, define the *right positive displacement group*, the *right negative displacement group* and the *right displacement group* by

$$\begin{aligned}\mathrm{Dis}_r^+(Q) &= \langle R_x R_y^{-1} : x, y \in Q\rangle,\\ \mathrm{Dis}_r^-(Q) &= \langle R_x^{-1} R_y : x, y \in Q\rangle,\\ \mathrm{Dis}_r(Q) &= \langle R_x R_y^{-1}, R_x^{-1} R_y : x, y \in Q\rangle,\end{aligned}$$

respectively.

Fix $e \in Q$. Since $R_x R_y^{-1} = (R_e R_x^{-1})^{-1}(R_e R_y^{-1}) = (R_x R_e^{-1})(R_y R_e^{-1})^{-1}$ and $R_x^{-1} R_y = (R_x^{-1} R_e)(R_y^{-1} R_e)^{-1} = (R_e^{-1} R_x)^{-1}(R_e^{-1} R_y)$, we have

$$\begin{aligned}\mathrm{Dis}_r^+(Q) &= \langle R_e R_x^{-1} : x \in Q\rangle = \langle R_x R_e^{-1} : x \in Q\rangle,\\ \mathrm{Dis}_r^-(Q) &= \langle R_x^{-1} R_e : x \in Q\rangle = \langle R_e^{-1} R_x : x \in Q\rangle.\end{aligned}$$

The left displacement groups are defined analogously for a left quasigroup $(Q, \cdot)$ by

$$\begin{aligned}\mathrm{Dis}_\ell^+(Q) &= \langle L_x L_y^{-1} : x, y \in Q\rangle,\\ \mathrm{Dis}_\ell^-(Q) &= \langle L_x^{-1} L_y : x, y \in Q\rangle,\\ \mathrm{Dis}_\ell(Q) &= \langle L_x L_y^{-1}, L_x^{-1} L_y : x, y \in Q\rangle,\end{aligned}$$

and we once again have

$$\begin{aligned}\mathrm{Dis}_\ell^+(Q) &= \langle L_e L_x^{-1} : x \in Q\rangle = \langle L_x L_e^{-1} : x \in Q\rangle,\\ \mathrm{Dis}_\ell^-(Q) &= \langle L_x^{-1} L_e : x \in Q\rangle = \langle L_e^{-1} L_x : x \in Q\rangle\end{aligned}$$

for a fixed $e \in Q$.

Proposition 5.1. *Let $(Q, \cdot)$ be a quasigroup. Then $(Q, \cdot)$ is isotopic to a group if and only if the left positive displacement group $\mathrm{Dis}_\ell^+(Q, \cdot)$ acts regularly on Q. In that case, $(Q, \cdot)$ is isotopic to $\mathrm{Dis}_\ell^+(Q, \cdot)$.*

Proof. Let $D = \mathrm{Dis}_\ell^+(Q, \cdot)$. Given $y, z \in Q$, there exists a unique $x \in Q$ such that $L_x L_e^{-1}(y) = z$, namely $x = z/(e\backslash y)$. Suppose that D acts regularly on Q. Then $D = \{L_x L_e^{-1} : x \in Q\}$ and for every $x, y \in Q$ there is $z \in Q$ such that $L_x L_e^{-1} L_y L_e^{-1} = L_z L_e^{-1}$. Thus $L_x L_e^{-1} L_y = L_z$ and, applying this to e, we get $x(e\backslash(ye)) = ze$ and $z = x(e\backslash ye)/e$. Define $(Q, *)$ by $x * y = x(e\backslash ye)/e$. Then $f : D \to (Q, *)$, $L_x L_e^{-1} \mapsto x$ is an isomorphism, so $(Q, *)$ is a group. Since $(x * y)e = x(e\backslash ye)$, the triple $(\mathrm{id}, L_e^{-1} R_e, R_e)$ is an isotopism $(Q, *) \to (Q, \cdot)$.

Conversely, suppose that $(Q, *)$ is a group and (α, β, γ) is an isotopism $(Q, *) \to (Q, \cdot)$, so $\alpha(x) \cdot \beta(y) = \gamma(x * y)$, or $x \cdot y = \gamma(\alpha^{-1}(x) * \beta^{-1}(y))$ for all $x, y \in Q$. This shows that the left translation by x in $(Q,\cdot)$ is equal to $L_x = \gamma L^*_{\alpha^{-1}(x)}\beta^{-1}$. Then

$$\begin{aligned} L_x L_e^{-1} &= (\gamma L^*_{\alpha^{-1}(x)}\beta^{-1})(\gamma L^*_{\alpha^{-1}(e)}\beta^{-1})^{-1} \\ &= \gamma L^*_{\alpha^{-1}(x)}(L^*_{\alpha^{-1}(e)})^{-1}\gamma^{-1} = \gamma L_{\alpha^{-1}(x)*(\alpha^{-1}(e))^{-1}}\gamma^{-1} \end{aligned}$$

because $(Q,*)$ is a group. Hence D is a conjugate of $\langle L_{\alpha^{-1}(x)*(\alpha^{-1}(e))^{-1}} : x \in Q\rangle = \langle L^*_x : x \in Q\rangle = \{L^*_x : x \in Q\}$, which certainly acts regularly on Q. □

Corollary 5.2. *A quasigroup Q is isotopic to a group iff $|\mathrm{Dis}^+_\ell(Q)| = |Q|$.*

6. Twists of right quasigroups

Given a magma Q and three mappings $f, g, h : Q \to Q$, the *twist* $\mathrm{Tw}(Q, f, g, h)$ of Q via (f, g, h) is defined to be the magma $(Q,*)$ with multiplication $x * y = h(f(x)g(y))$.

If Q is a right quasigroup, the twist $\mathrm{Tw}(Q, f, g, h)$ is a right quasigroup iff both f and h are bijections of Q. Moreover, the twist $\mathrm{Tw}(Q, f, g, h)$ is a quasigroup iff all three f, g and h are bijections of Q. Finally, if $\mathrm{Tw}(Q, f, g, h)$ is a quasigroup then it is a loop iff $g^{-1}(f(x)\backslash h^{-1}(x))$ is equal to $f^{-1}(h^{-1}(x)/g(x))$ and independent of x.

Isotopes and affine constructions can be realized as twists.

7. Affine right quasigroups

Given a loop $(Q,\cdot)$, its automorphism f, endomorphism g and two elements u, v, define $\mathrm{Aff}(Q,\cdot,f,u,g,v) = (Q,*)$ by $x * y = (f(x)u)(g(y)v)$. (We also allow variations with $uf(x)$, $vg(y)$ and any combinations. For instance, $\mathrm{Aff}(Q,\cdot,u,f,g,v)$ has multiplication $x * y = (uf(x))(g(y)v)$.) Then $(Q,*)$ is *affine* over $(Q,\cdot)$ and $(Q,\cdot,f,u,g,v)$ is the *arithmetic form* of $(Q,*)$.

Lemma 7.1. *$(Q,*)$ is a right quasigroup. $(Q,*)$ is a quasigroup iff g is an automorphism.*

Proof. Solving $x * y = (f(x)u)(g(y)v) = z$ for x yields $x = f^{-1}((z/(g(y)v))/u)$ and similarly in the other three cases. Solving $x * y = (f(x)u)(g(y)v) = z$ for y is equivalent to solving $g(y) = ((f(x)u)\backslash z)/v$. □

If $(Q,\cdot)$ is an abelian group, the formula $x*y = (f(x)u)(g(y)v)$ becomes $f(x)g(y)uv$ and it therefore suffices to consider only arithmetic forms $(Q,\cdot,f,g,c)$ with automorphism f, endomorphism g and central element c, and define the multiplication by $x * y = f(x)g(y)c$. In general this is a special case of the affine construction. From now on we assume that we are dealing with the special case (Q, f, g, c).

Lemma 7.2. *$(Q,*)$ is a rack iff $g(c) = 1$, $fg = gf$, $g(x) = fg(x)g^2(x)$ and $xfg(y)\cdot g(z) = xfg(z)\cdot fg(y)g^2(z)$ for all $x, y, z \in Q$.*

Proof. We have $(x*y)*z = (f(x)g(y)c)*z = f^2(x)fg(y)f(c)\cdot g(z)\cdot c$, while $(x*z)*(y*z) = (f(x)g(z)c)*(f(y)g(z)c) = f^2(x)fg(z)f(c)\cdot gf(y)g^2(z)g(c)\cdot c$. Since c, $f(c)$ and $g(c)$ are central, we see that $(Q,*)$ is a rack iff $f^2(x)fg(y)\cdot g(z) = f^2(x)fg(z)\cdot gf(y)g^2(z)\cdot g(c)$. Substituting $x = y = z = 1$ then yields $g(c) = 1$ as a necessary condition. Assuming this, we need to verify $f^2(x)fg(y)\cdot g(z) = f^2(x)fg(z)\cdot gf(y)g^2(z)$. With $x = z = 1$ we obtain $fg(y) = gf(y)$ as a necessary condition. Assuming this, we need to verify $f^2(x)fg(y)\cdot g(z) = f^2(x)fg(z)\cdot fg(y)g^2(z)$. With $x = y = 1$ we get $g(z) = fg(z)g^2(z)$ as a necessary condition. Assuming this and substituting x for $f^2(x)$ yields the last condition. □

Substituting $fg(z)g^2(z)$ for $g(z)$ into the left hand side of the last condition of Lemma 7.2 yields $xfg(y) \cdot fg(z)g^2(z) = xfg(z) \cdot fg(y)g^2(z)$. This condition is certainly satisfied when $(Q, \cdot)$ is a medial loop. Recall that a loop is medial iff it is an abelian group. Indeed, from $(xu)(vy) = (xv)(uy)$ we obtain commutativity with $x = y = 1$ and associativity with $v = 1$.

Lemma 7.3. *$(Q, *)$ is a quandle iff $c = 1$, $g(x) = f(x)\backslash x$ and $xfg(y) \cdot g(z) = xfg(z) \cdot fg(y)g^2(z)$ for all $x, y, z \in Q$.*

Proof. We have $x * x = x$ iff $f(x)g(x)c = x$. Substituting $x = 1$ yields $c = 1$. Using this, we have $x * x = x$ iff $f(x)g(x) = x$, that is, $g(x) = f(x)\backslash x$. If $g(x) = f(x)\backslash x$ then both $fg = gf$ and $g(x) = fg(x)g^2(x)$ hold. We are done by Lemma 7.2. □

Note that the conditions of Lemma 7.3 do not impose any restrictions on the loop $(Q, \cdot)$. Indeed, if $(Q, \cdot)$ is any loop, $f(x) = x$, $g(x) = 1$ and $c = 1$ then $x * y = f(x) = x$ and $(Q, *)$ is a projection quandle.

Also note that a latin rack is a quandle. Indeed, substituting $z = y$ into $(xy)z = (xz)(yz)$ yields $(xy)y = (xy)(yy)$ and canceling xy on the left then yields $y = yy$.

Lemma 7.4. *$(Q, *)$ is a latin rack (i.e., latin quandle) iff $c = 1$, $g(x) = f(x)\backslash x$ and $xy \cdot z = xf(z) \cdot y(f(z)\backslash z)$ for all $x, y, z \in Q$.*

Proof. Replace $g(z)$ with z and $fg(y)$ with y in the last condition of Lemma 7.3. □

Corollary 7.5. *Suppose that $(Q, \cdot)$ is an abelian group. Then $(Q, *)$ is a rack iff $g(c) = 1$, $fg = gf$ and $g(x) = fg(x)g^2(x)$ for all $x \in Q$.*

Proof. Suppose that $g(x) = fg(x)g^2(x)$ for all $x \in Q$. Then $xfg(y) \cdot g(z) = xfg(y) \cdot fg(z)g^2(z) = xfg(z) \cdot fg(y)g^2(z)$, where we have used mediality in the last step. □

Corollary 7.6. *Suppose that $(Q, \cdot)$ is an abelian group. Then $(Q, *)$ is a quandle iff $c = 1$ and $g(x) = f(x)\backslash x = xf(x)^{-1}$.*

8. Calculating isotopisms and autotopisms

Let $Q_1 = (Q_1, \cdot, \backslash, /)$, $Q_2 = (Q_2, *, \backslash^*, /^*)$ be quasigroups. The triple (f, g, h) of mappings $Q_1 \to Q_2$ is a homotopism if $f(x) * g(y) = h(x \cdot y)$ for all $x, y \in Q_1$.

8.1. **Method via perfect matchings with invariants.** Let (f, g, h) be an isotopism of right quasigroups $(Q_1, \cdot) \to (Q_2, *)$. In principle, no information about g can be deduced from f and h. For instance, if both $(Q1, \cdot)$, $(Q_2, *)$ are projection right quasigroups (that is, $x \cdot yy = x$ and $x * y = x$) then the identity $f(x) * g(y) = h(xy)$ becomes $f(x) = h(x)$.

Lemma 8.1. *Let $(Q_1, \cdot)$, $(Q_2, *)$ be right quasigroups and let $e \in Q_1$.*

(i) *If $f : Q_1 \to Q_2$ is a bijection and $g(e)$ is given then there is a unique $h : Q_1 \to Q_2$ such that (f, g, h) is an isotopism (note that g might not be unique).*

(ii) *Suppose that two bijections $f, h : Q_1 \to Q_2$ are given. Then (f, g, h) is an isotopism iff g is a bijection such that $g(y) \in S(y)$ for every $x \in Q$, where*

$$S(y) = \bigcap_{x \in X} \{z \in Q_1 : f(x) * g(z) = h(x \cdot z)\}.$$

Hence an isotopism (f, g, h) with given components f and h exists if and only if there is a perfect matching in the bipartite graph (V, E) with $V = Q_1 \cup Q_2$ and $E = \{(x, y) : y \in S(x)\}$.

Proof. (i) We have $h(y) = f(x/e) * g(e)$.
Part (ii) is obvious. □

If $(Q, \cdot)$ is a groupoid and $x \in Q$, let $m_x = m_x(Q)$ be the sorted list $(m_{x,y} : y \in Q)$, where $m_{x,y} = |\{z \in Q : xy = z\}|$, that is, $m_{x,y}$ counts the number of occurrences of y in the row indexed by x. Since the effect of an isotopism $(f, g, h) : (Q_1, \cdot) \to (Q_2, *)$ on a multplication table is to rename rows by f, rename columns by g and re rename entries by h, we must have $m_x(Q_1) = m_{f(x)}(Q_2)$.

The sorted list $(m_x : x \in Q)$ is therefore an isotopism invariant. Moreover, while searching for an isotopism $(f, g, h) : Q_1 \to Q_2$, we must select $f(x) \in \{y \in Q_2 : m_y(Q_2) = m_x(Q_1)\}$. This severely restricts f for random Q_1. The above lemma then allows us to calculate h from a single entry $g(e)$, and the we can easily decide if a suitable g exists by solving the perfect matching problem.

8.2. **Method via perfect matchings with automorphisms groups.** The invariant $(m_x : x \in X)$ is useless for quasigroups. The perfect matching idea still applies but it is not practical to check all possible permutations f. It suffices to work modulo $\mathrm{Aut}(Q_1)$, which sometimes helps.

8.3. **Method via domain extension.** The following works reasonably well for quasigroups and loops.

Lemma 8.2. *Let Q_1, Q_2 be quasigroups. Let c be a fixed element of Q_1. A homotopism (f, g, h) from Q_1 to Q_2 is determined by the values of one of the three mappings on Q_1 and by the value on c of one of the two remaining mappings.*

Proof. We will give a proof when $h(x)$ is known for all $x \in Q_1$ and $f(c)$ is known. The remaining five cases are similar. We have $f(c) * g(c\backslash x) = h(c(c\backslash x)) = h(x)$ and hence $g(c\backslash x) = g(c)\backslash^* h(x)$. This shows that $g(x)$ is determined for all $x \in Q_1$. We also have $f(x/c) * g(c) = h((x/c)c) = h(x)$ and hence $f(x/c) = h(x)/^* g(c)$. This shows that $f(x)$ is determined for all $x \in Q_1$. □

The following result shows how the domain of a partially defined homotopism of quasigroups must be extended (iteratively) whenever a new image of f, g or h has been chosen. The domain of a mapping f is denoted by $D(f)$.

Lemma 8.3. *Let $(f, g, h) : Q_1 \to Q_2$ be a partial homotopism of quasigroups.*

(i) *If $x \in D(f)$ then $g(x\backslash y) = f(x)\backslash^* h(y)$ for all $y \in D(h)$ and $h(xy) = f(x) * g(y)$ for all $y \in D(g)$.*
(ii) *If $x \in D(g)$ then $f(y/x) = h(y)/^* g(x)$ for all $y \in D(h)$ and $h(yx) = f(y) * g(x)$ for all $y \in D(f)$.*
(iii) *If $x \in D(h)$ then $g(y\backslash x) = f(y)\backslash^* h(x)$ for all $y \in D(f)$ and $f(x/y) = h(x)/^* g(y)$ for all $y \in D(g)$.*

8.4. **Method via principal loop isotopes.** To find an isotopism of loops $Q \to Q'$, it suffices to check whether there is an isomorphism $Q_{a,b} \to Q'$, for all $a, b \in Q_1$. In both coordinates it suffices to work modulo some nucleus.