Aleš Drápal; Viktor Alekseevich Shcherbakov

Identities and the group of isostrophisms

Commentationes Mathematicae Universitatis Carolinae, Vol. 53 (2012), No. 3, 347--374

Persistent URL: http://dml.cz/dmlcz/142929

Identities and the group of isostrophisms

Aleš Drápal, Victor Shcherbacov

Abstract. In this paper we reexamine the concept of isostrophy. We connect it to the notion of term equivalence, and describe the action of dihedral groups that are associated with loops by means of isostrophy. We also use it to prove and present in a new way some well known facts on m-inverse loops and middle Bol loops.

Keywords: isostrophe, isostrophism, paratope, paratopism, middle Bol

Classification: Primary 20N05; Secondary 15A30

Let $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ be pencils of a 3-net. If α, β and γ biject a set Q upon $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$, respectively, then there exists a (unique) quasigroup on $Q(\cdot)$ such that $xy = z$ if and only if $\alpha(x)$, $\beta(y)$ and $\gamma(z)$ meet in a common point. It is well known that if Q is one of the lines of the 3-net, then α, β and γ can be defined naturally in such a way that a distinguished element of Q (say 1) becomes the unit of Q. This construction will serve as the departing point of the paper.

Suppose thus that $Q \in \mathcal{A}$ and that $1 \in Q$. Define β and γ in such a way that both $\beta(a) \in \mathcal{B}$ and $\gamma(a) \in \mathcal{C}$ are incident to a, for every $a \in Q$. If $Q(\cdot)$ is to be a loop with unit 1, then there must be $a \cdot 1 = a$, and hence $\alpha(a) \in \mathcal{A}$ has to be the line that is incident to the intersection of $\beta(1)$ and $\gamma(a)$. With this definition of α we get $\alpha(1) = Q$ since $\beta(1)$ and $\gamma(1)$ meet in 1. Now, $\alpha(1) = Q$ implies $1 \cdot a = a$ for every $a \in Q$, by the definition of β and γ. We have obtained a loop $Q(\cdot, 1)$.

Consider now a loop $\overline{Q} = Q(\circ, 1)$ that is obtained by this method when rôles of $\mathcal{B}$ and $\mathcal{C}$ are exchanged. Then $x \circ y = z$ if and only $\overline{\alpha}(x)$, $\gamma(y)$ and $\beta(z)$ meet in a point. In particular, $\overline{\alpha}(a)$, $\gamma(1)$ and $\beta(a)$ have a common point, and that defines $\overline{\alpha}$. The existence of the common point means that $\alpha^{-1}(\overline{\alpha}(a)) \cdot a = 1$ for every $a \in Q$. Thus $\alpha^{-1}(\overline{\alpha}(a)) = 1/a$, and therefore $\overline{\alpha}(a) = \alpha(1/a)$. We see that $x \circ y = z \Leftrightarrow \alpha(1/x)$, $\gamma(y)$ and $\beta(z)$ meet in a common point $\Leftrightarrow (1/x) \cdot z = y \Leftrightarrow z = (1/x)\backslash y$.

We have described the geometrical meaning of operation $(1/x)\backslash y$. The operation is induced by the transposition $(\mathcal{B}\ \mathcal{C})$ of the set $\{\mathcal{A}, \mathcal{B}, \mathcal{C}\}$. In fact, every of the six permutations can be used to induce a loop. Artzy [3] seems to have been the first who systematically investigated these transformations of loops. He called them *isostrophisms*. The concept is reexamined in this paper. Our approach is purely algebraic.

The first author (Aleš Drápal) was supported by grant VF20102015006.

For a loop Q denote by $\mathbf{l}(Q)$ the loop with operation $(1/x)\backslash y$ and by $\mathbf{o}(Q)$ the loop with operation yx (the *opposite* loop — it corresponds to the transposition of $\mathcal{A}$ and $\mathcal{B}$). It is easy to verify that $\mathbf{l}(\mathbf{l}(Q)) = Q = \mathbf{o}(\mathbf{o}(Q))$. Nevertheless, alternating applications of $\mathbf{l}$ and $\mathbf{o}$ produce a set of loops $\mathcal{I}(Q)$ that can be infinite (however, it contains at most six isomorphism classes). Operators $\mathbf{l}$ and $\mathbf{o}$ act upon $\mathcal{I}(Q)$ as involutions and generate a permutation group $\mathbf{I}(Q)$. This group is either dihedral, or cyclic of orders 1 or 2. (The Klein four-group is regarded as a dihedral group.)

We shall observe that $\mathbf{I}(Q)$ acts nearly always regularly. There are only three exceptional situations, two of which can be considered as related to Bol loops (and that is why we shall discuss the middle Bol identity as well). In these exceptional cases $|\mathcal{I}(Q)| \in \{3, 6\}$.

Our main aim is to present the concept of isostrophy in a coherent and compact way. There are some new results and there are many new proofs of old results.

However, it should be stressed that no ideas in this paper are principally new. Furthermore, many statements that are new might have been present in some form in minds of those who coined and studied the concepts of this paper in the sixties. We hope that this paper will succeed in illustrating that these concepts are relevant to contemporary loop theory and can motivate further research.

Very important among the objects of our study are the *m-inverse loops* defined by Karkliňš and Karkliň [14]. They arise in a natural way as a generalization of cross inverse [1], [2] and weak inverse properties [21]. It was observed already by Artzy in [3] that CI and WI properties can be obtained via identifications of certain isostrophes. We shall see that such an approach can be extended to all m-inverse loops. In fact, our description has a parallel in the work of Karkliňš and Karkliň [14] and can be regarded as an interpretation of their Section 2.

The *isostrophes* of Q (i.e. the elements of $\mathcal{I}(Q)$) have been called *inverse loops* (of Q) by Belousov [7]. He also mentions them in his book [6, p. 19]. Using the terminology of Belousov as inspiration, we suggest to call $\mathbf{l}(Q)$ the *left inverse* of Q (we shall define the *right inverse* $\mathbf{r}(Q)$ as a mirror image).

A thorough geometrical treatment of isostrophy can be found in Chapter II of Pflugfelder's book [22]. (In the Preface to [22] Pflugfelder writes "To Rafael Artzy I am grateful for his encouragement and advice and for writing the original text of Chapter II.") Artzy himself offered in [4, Section 2] a more structured approach to the material of [3]. In Section 3 of the same paper he defined *net motions*. The algebraic expression of net motions is paratopy, which is, together with loop terms, a main tool of this paper.

Note that m-inverse loops have been recently studied with respect to a possible application in cryptography [17] and that Buchsteiner loops were discovered [8] to be 1-inverse (synonymously, *doubly weak inverse*).

Problems that involve the structure of $\mathcal{I}(Q)$ might be of interest in the future since this is an area where the algebraic structure (loops) gets mixed with the combinatorial structure (normalized latin squares). Hence a future application to cryptography cannot be excluded, while its guiding principle may be different than that expressed by Keedwell in [16] (which motivated [17] and the subsequent papers [18] and [19]).

Section 1 describes endomorphisms of a monogenerated free loop. Section 2 shows that isostrophies can be viewed as paratopies that yield term equivalent loops. In Section 3 we define the group of isostrophisms $\mathbf{I}(Q)$ and discuss its structural properties. The impact upon nuclei is presented in Section 4. The number of isostrophic isomorphism classes is studied in Section 5. In that section we also define loops of *odd type* as loops that are either commutative or have an automorphism I^r for an odd r. We show how such loops can be described via $\mathbf{I}(Q)$. Section 6 presents the concept of isostrophic varieties and employs it to interpret several standard results on LIP, RIP, AAIP and Bol loops.

In this paper the mappings are composed from right to left.

1. Free loops in one generator

This section is of an auxiliary character. It proves in an elementary way that all automorphisms of a free loop generated by a single element x (denote it by $F(x)$) are those substitutions that map x to one of its iterated inverses. This result was published already in 1953 by Evans [10, Theorem 1]. We shall use it in Corollary 2.9.

The proof of Evans is short and elegant. It depends upon the theory of loops that are relatively free with respect to a set of (defining) relations that are in a closed form. This theory was developed by Evans in [9]. A special case is the case of the void set of relations, that is the case of a free loop. The associated set of rewriting rules (cf. Table 1) became part of a folklore knowledge. In fact it is one of few results of loop and quasigroup theory that is well known by many non-specialists. However, the general theory of relations in a closed form is not nearly as well-known. That is why we offer a proof that uses nothing else but the well understood structure of a free loop. As a bonus we prove that every nontrivial endomorphism of $F(x)$ is injective — a fact that seems to be evident, but for which we do not know a reference.

For a set of variables X consider the totally free algebra of terms $W(X)$ over the binary operations $\cdot$, $/$, $\backslash$ and the nullary operation 1. An element $w \in W(X)$ is said to be *reduced* if none of its subterms can be subjected to one of the rewriting rules that appear in Table 1.

$t_1 \cdot (t_1 \backslash t_2) \to t_2$	$t_1 \backslash (t_1 \cdot t_2) \to t_2$	$t_1/(t_2 \backslash t_1) \to t_2$	$t_1 \cdot 1 \to t_1$	$t_1/1 \to t_1$
$(t_2/t_1) \cdot t_1 \to t_2$	$(t_2 \cdot t_1)/t_1 \to t_2$	$(t_1/t_2) \backslash t_1 \to t_2$	$1 \cdot t_1 \to t_1$	$1 \backslash t_1 \to t_1$

Table 1. The rewriting rules for loop terms

It is clear that each term $w \in W(X)$ can be transformed by a sequence of rewriting rules to a reduced term. There may be many such sequences. However, because the above system of rewriting rules is known to be confluent [9], a terminal element of such a sequence will always be the same reduced term (in other words the terminal term is independent of the chosen path). We shall denote the (terminal) reduced term by $\rho(w)$. The set of all reduced terms will be denoted $F(X)$ alluring thus to the fact that the reduced terms yield a model of a free loop for which X is the free base (cf. [9], [10] for details).

If u and v are reduced, then their term product $u \cdot v$ need not be reduced. Hence the product in $F(X)$ is defined as $\rho(u \cdot v)$. Left and right division are treated similarly.

As a synonym for $t\backslash 1$ write $I(t)$. Similarly interpret $I^{-1}(t)$ as $1/t$. Note that $\rho(II^{-1}(t)) = \rho(t) = \rho(I^{-1}I(t))$ since $1/(t\backslash 1) \to t$ and $(1/t)\backslash 1 \to t$. Thus $\rho(I^rI^s(t)) = \rho(I^{r+s}(t))$ for any $r, s \in \mathbb{Z}$.

We shall write $F(x)$ and $W(x)$ in place of $F(X)$ and $W(X)$ when $X = \{x\}$.

For $t \in F(x)$ define a mapping $\sigma_t : F(x) \to F(x)$ so that it expresses the substitution $x \mapsto t$. Thus for $s = s(x) \in F(x)$ we set $\sigma_t(s) = \rho(s(t))$. For example $\sigma_{x^2}(x\backslash(1/x)) = x^2\backslash(1/x^2)$ and $\sigma_{I(x)}(x\backslash(1/x)) = (x\backslash 1)\backslash x$.

It is easy to see that for every $t \in F(x)$ there exist unique $k \in \mathbb{Z}$ and $t_0 \in W(x)$ such that

$$t = I^k(t_0) \quad \text{and} \quad t_0 \neq I^{\pm 1}(s) \quad \text{for all} \quad s \in W(x). \tag{1.1}$$

For example, if $t = 1/(1/x^2)$, then $k = -2$ and $t_0 = x^2$.

Call t_0 the *I-core* of t and k the *I-depth* of t. For the next three statements let us assume that $t \neq 1$ is reduced and that t_0 and k are the I-core and I-depth of t, respectively.

Lemma 1.1. *$I^j(t_0) \in F(x)$ for every $j \in \mathbb{Z}$.*

Proof: Any subterm of a reduced term has to be reduced, and thus $t_0 \in F(x)$. We can proceed by induction on j since the mirror symmetry allows us to assume $j \geq 1$. Note that $t_0\backslash 1$ is reduced unless $t_0 = 1$ or $t_0 = 1/s$ for some $s \in W(x)$. The latter situation is excluded by the definition of the I-core, while $t_0 = 1$ would imply $t = 1$. The statement thus holds for $j = 1$. Assume $j \geq 2$ and set $s = I^{j-2}(t_0)$. Then $I^{j-1}(t_0) = s\backslash 1 \in F(x)$, and hence $I^j(t_0) = (s\backslash 1)\backslash 1 \in F(x)$ as well. □

Corollary 1.2. *$\sigma_t(I^j(x)) = I^{j+k}(t_0)$ for every $j \in \mathbb{Z}$.*

Proof: We have $\sigma_t(I^j(x)) = \rho(I^j(t)) = \rho(I^j(I^k(t_0))) = \rho(I^{j+k}(t_0))$. However, $I^{j+k}(t_0)$ is reduced, by Lemma 1.1. □

For $s \in W(x)$ define the *weight* $|s|$ as $2i+j$, where i is the number of occurrences of x and j is the number of occurrences of 1. For example, $|1/(1/x^2)| = 6$.

Let $a, b \in W(x)$. Then $a * b$ can mean any of $a \cdot b$, a/b and $a\backslash b$. If more than one operation is involved, we shall also use $a \circ b$.

Lemma 1.3. *Let s_0 be the I-core of $s \in F(x)$ and let j be its I-depth. Then*

$$\sigma_t(s) = \begin{cases} 1 & \textit{if } \ s = 1, \\ I^{j+k}(t_0) & \textit{if } \ s_0 = x, \\ I^j(\sigma_t(a) * \sigma_t(b)) & \textit{if } \ s_0 = a * b. \end{cases}$$

Furthermore, the mapping $\sigma_t : F(x) \to F(x)$ is injective.

Proof: It is obvious that $\sigma_t(1) = 1$. Corollary 1.2 gives the formula for $s = I^j(x)$. For the rest we shall proceed by induction on $|s|$. The induction step consists of showing that

(a) $\sigma_t(s) = I^j(\sigma_t(a) * \sigma_t(b))$ where $a * b$ is the I-core of s and j is the I-depth of s; and that

(b) $\sigma_t(s) = \sigma_t(s')$ implies $s = s'$ if $s, s' \in F(x)$ and $|s| \geq |s'|$.

If $|s| \leq 2$, then $s = 1$ or $s = x$. Part (a) is voidly true since (a) assumes $s = a * b$. Part (b) is obvious.

To prove (a) for $|s| \geq 3$ we need to show that $I^j(\sigma_t(a) * \sigma_t(b))$ is reduced. Note that $\sigma_t(a) = 1$ implies $a = 1$ by part (b) and the induction assumption. However, if $a = 1$, then either $a * b$ is not reduced, or j is not the I-depth of s. Hence $a \neq 1$ and $\sigma_t(a) \neq 1$. Similarly $b \neq 1$ and $\sigma_t(b) \neq 1$. Therefore $I^j(\sigma_t(a) * \sigma_t(b)) \in F(x)$ if $\sigma_t(a) * \sigma_t(b) \in F(x)$. That follows by induction if $j \neq 0$. Assume $j = 0$ and suppose that there is a rule in Table 1 that applies to $\sigma_t(a) * \sigma_t(b)$. We have observed that it can be none of the four rules that involve 1. In view of the left-right (mirror) symmetry we can assume that $\sigma_t(b) = u \circ v$ and that the rewriting rule matches $\sigma_t(a) * (u \circ v)$. (Hence the rewriting rule must be one of $t_1 \backslash (t_1 \cdot t_2) \to t_2$, $t_1/(t_2 \backslash t_1) \to t_2$ and $t_1 \cdot (t_1 \backslash t_2) \to t_2$.) Let b_0 be the I-core of b. We know that $b_0 \neq 1$. Assume $b_0 \neq x$. By the induction assumption the structure of $\sigma_t(b)$ copies the structure of b. Hence $b = c \circ d$ where $u = \sigma_t(c)$ and $v = \sigma_t(d)$. From part (b) we know that if $\sigma_t(a) = \sigma_t(c)$ then $a = c$, and if $\sigma_t(a) = \sigma_t(d)$ then $a = d$. The rewriting rule that matches $\sigma_t(a) * (\sigma_t(c) \circ \sigma_t(d))$ thus applies to $s = a * (c \circ d)$ as well. That is a contradiction since s is assumed to be reduced.

To finish the proof of (a) it remains to treat the case of $b_0 = x$. Then $b = I^r(x)$ for some $r \in \mathbb{Z}$ and $u \circ v = \sigma_t(b) = I^{r+k}(t_0)$, by Corollary 1.2. From part (a) of the induction assumption and from Corollary 1.2 we see that $|\sigma_t(a)| \geq |t_0|$. Both u and v are subterms of t_0 if $r + k = 0$. In such a case $|u| < |\sigma_t(a)|$, $|v| < |\sigma_t(a)|$, and none of the above mentioned three rewriting rules matches $\sigma_t(a) * (u \circ v)$. Thus $r + k \neq 0$ and the operation $\circ$ is equal to $\backslash$ or $/$. None of the three rules allows the alternative of $/$, and so $\circ$ equals $\backslash$. That means $r + k > 0$ and $v = 1$. Since $\sigma_t(a) \neq 1$, the only possibility for simplification is that of $u \cdot (u \backslash 1) \to 1$. From $u \backslash 1 = \sigma_t(b)$ we see that the weight of the I-core of u is equal to $|t_0|$. If the I-core of a is different from x, then the I-core of $u = \sigma_t(a)$ is of weight at least $2|t_0|$, by part (a) of the induction argument. Hence $a = I^q(x)$ for some $q \in \mathbb{Z}$. Then $\sigma_t(a) = I^{q+k}(t_0) = u$ which yields $r = q + 1$ and $s = I^q(x) \cdot I^{q+1}(x)$. This is a reducible term both for $q \geq 0$ and $q < 0$.

To prove (b) first note that $|\sigma_t(s')| > 1$ if $s' \neq 1$. Hence $s' \neq 1$ can be assumed. By considering again the weights of I-cores, this time with respect to $\sigma_t(s)$ and $\sigma_t(s')$, we easily distinguish the case when the I-core of s is equal to x and the I-core of s' is not equal to x (or vice versa). Now, Corollary 1.2 can be employed if both I-cores are equal to x. Suppose that none of the I-cores equals x. Then the I-depth of $\sigma_t(s)$ agrees with the I-depth of s, and hence (b) follows from (a) by a direct induction argument. □

Theorem 1.4. *A mapping $\varphi : F(x) \to F(x)$ is an endomorphism of the free loop $F(x)$ if and only if there exists $t \in F(x)$ such that $\varphi = \sigma_t$. The endomorphism σ_t is injective if and only if $t \neq 1$. It is an automorphism if and only if $t = I^k(x)$ for some $k \in \mathbb{Z}$.*

Proof: Because $\{x\}$ is the free base of $F(x)$ there exists for every $t \in F(x)$ a unique endomorphism φ with $\varphi(x) = t$. This endomorphism fulfils $\varphi(s(x)) = \rho(s(t))$ for any $s \in F(x)$ and hence it agrees with σ_t. If $t \neq 1$, then σ_t is injective by Lemma 1.3. Of course, σ_1 maps every element of $F(x)$ to 1. Let us assume $t \neq 1$ and let t_0 be the I-core of t. From Lemma 1.3 we see that $|\sigma_t(s)| \geq |t_0|$ for every $s \neq 1$. Note that the endomorphism σ_t is an automorphism if and only if $x \in \operatorname{Im}(\sigma_t)$. Since this cannot happen if $|t_0| > 2$ there must be $t_0 = x$ and $t = I^k(x)$, where k is the I-depth of t. In such a case $x = \sigma_t(I^{-k}(x))$, by Lemma 1.3. □

Corollary 1.5 (Evans). $\operatorname{Aut}(F(x))$ *is an infinite cyclic group that is generated by the substitution $x \mapsto 1/x$.*

2. Paratopisms, isostrophisms and terms

Quasigroups can be seen as sets of triples (a_1, a_2, a_3) such that two elements of the triple can be chosen freely from the given set Q while the third element is determined uniquely by this choice. It is usual to set $a_3 = a_1 \cdot a_2$, $a_2 = a_1 \backslash a_3$ and $a_1 = a_3 / a_2$. Put also $a_3 = a_2 \circ a_1$, $a_2 = a_3 \backslash\backslash a_1$ and $a_1 = a_2 // a_3$. In this way we get six quasigroup operations that are called *parastrophes*. They are related by permutations $\sigma \in S_3$. Say that $Q(*)$ is a σ *parastrophe* of $Q = Q(\cdot)$ if $a_1 * a_2 = a_3$ is equivalent to $a_{\sigma(1)} \cdot a_{\sigma(2)} = a_{\sigma(3)}$. In other words, if we start from triples (a_1, a_2, a_3) where $a_3 = a_1 \cdot a_2$, then the new triples are obtained by sending a_i from the position i to the position $\sigma(i)$. It follows that the τ parastrophe of a σ parastrophe is the $\tau\sigma$ parastrophe.

If Q_1 and Q_2 are quasigroups, then $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ is an *isotopism* $Q_1 \to Q_2$ if all α_i are bijections $Q_1 \to Q_2$ and $\alpha_1(x) \cdot \alpha_2(y) = \alpha_3(xy)$ for all $x, y \in Q_1$.

By combining the notions of *para*strophy and iso*topy* we get the notion of *paratopy*. This term was coined by Sade [24]. It provides an algebraic framework for the combinatorial notion of main classes. (The alternative *isostrophy* = *iso*topy + para*strophy* has a different meaning in this paper. Admittedly, there may exist authors who use it as a synonym for paratopy.)

Let Q_1 and Q_2 be quasigroups. The pair $(\sigma, \alpha) = (\sigma, (\alpha_1, \alpha_2, \alpha_3))$ is said to be a *paratopism* from Q_1 to Q_2 if $\alpha_i : Q_1 \to Q_2$ is a bijection for all $i \in \{1, 2, 3\}$, if

$\sigma \in S_3$ and if

$$\alpha_{\sigma^{-1}(1)}(a_{\sigma^{-1}(1)}) \cdot \alpha_{\sigma^{-1}(2)}(a_{\sigma^{-1}(2)}) = \alpha_{\sigma^{-1}(3)}(a_{\sigma^{-1}(3)})$$

whenever $a_1 a_2 = a_3$ holds in Q_1. It is not difficult to deduce that α is an isotopism from Q_1 to the σ^{-1} parastrophe of Q_2, and that by composing paratopisms $(\sigma, \alpha) : Q_1 \to Q_2$ and $(\tau, \beta) : Q_2 \to Q_3$ we obtain a paratopism $Q_1 \to Q_3$. The composition follows the rule

$$(\tau, \beta)(\sigma, \alpha) = (\tau\sigma, \beta^{\sigma}\alpha), \quad \text{where} \quad (\beta_1, \beta_2, \beta_3)^{\sigma} = (\beta_{\sigma(1)}, \beta_{\sigma(2)}, \beta_{\sigma(3)}).$$

Hence $(\sigma, \alpha)^{-1} = (\sigma^{-1}, (\alpha^{-1})^{\sigma^{-1}})$. Therefore

$$b_1 \cdot b_2 = b_3 \text{ in } Q_2 \;\Leftrightarrow\; \alpha_1^{-1}(b_{\sigma(1)}) \cdot \alpha_2^{-1}(b_{\sigma(2)}) = \alpha_3^{-1}(b_{\sigma(3)}) \text{ in } Q_1.$$

For a quasigroup Q, a set S, a permutation $\sigma \in S_3$ and bijections $\alpha_i : Q \to S$, $i \in \{1, 2, 3\}$, there exists a unique quasigroup structure on S such that (σ, α) is a paratopism $Q \to S$. It is called the quasigroup *paratopically induced* by (σ, α). The multiplication and the left and right divisions of such quasigroups are explicitly shown in Table 2 for each $\sigma \in S_3$.

$\sigma \in S_3$	multiplication	left division	right division
id	$\alpha_3(\alpha_1^{-1}(x) \cdot \alpha_2^{-1}(y))$	$\alpha_2(\alpha_1^{-1}(x) \backslash \alpha_3^{-1}(y))$	$\alpha_1(\alpha_3^{-1}(x) / \alpha_2^{-1}(y))$
(1 2 3)	$\alpha_2(\alpha_1^{-1}(y) \backslash \alpha_3^{-1}(x))$	$\alpha_1(\alpha_3^{-1}(x) / \alpha_2^{-1}(y))$	$\alpha_3(\alpha_1^{-1}(y) \cdot \alpha_2^{-1}(x))$
(1 3 2)	$\alpha_1(\alpha_3^{-1}(y) / \alpha_2^{-1}(x))$	$\alpha_3(\alpha_1^{-1}(y) \cdot \alpha_2^{-1}(x))$	$\alpha_2(\alpha_1^{-1}(x) \backslash \alpha_3^{-1}(y))$
(1 2)	$\alpha_3(\alpha_1^{-1}(y) \cdot \alpha_2^{-1}(x))$	$\alpha_1(\alpha_3^{-1}(y) / \alpha_2^{-1}(x))$	$\alpha_2(\alpha_1^{-1}(y) \backslash \alpha_3^{-1}(x))$
(2 3)	$\alpha_2(\alpha_1^{-1}(x) \backslash \alpha_3^{-1}(y))$	$\alpha_3(\alpha_1^{-1}(x) \cdot \alpha_2^{-1}(y))$	$\alpha_1(\alpha_3^{-1}(y) / \alpha_2^{-1}(x))$
(1 3)	$\alpha_1(\alpha_3^{-1}(x) / \alpha_2^{-1}(y))$	$\alpha_2(\alpha_1^{-1}(y) \backslash \alpha_3^{-1}(x))$	$\alpha_3(\alpha_1^{-1}(x) \cdot \alpha_2^{-1}(y))$

TABLE 2. Paratopic quasigroup operations induced by (σ, α)

Let Q be a loop. Put $I(x) = x \backslash 1$ and $J(x) = 1/x$ for every $x \in Q$. Then both $I_Q = I$ and $J_Q = J$ permute Q, and $J = I^{-1}$. Further permutations of Q are the *left translations* $L_a : x \mapsto ax$ and the *right translations* $R_a : x \mapsto xa$, for every $a \in Q$.

An isotopism of loops $(\alpha_1, \alpha_2, \alpha_3) : Q \to \bar{Q}$ is called *principal* if $\alpha_3 = \mathrm{id}_Q$. In such a case there exist $e, f \in Q$ such that $\alpha_1 = R_f$ and $\alpha_2 = L_e$. Furthermore, $\bar{Q} = Q(\circ)$ where $x \circ y = (x/f)(e \backslash y)$ for all $x, y \in Q$. Loops $Q(\circ)$ are known as the *principal isotopes* of Q.

Every isotopism of loops $\alpha : Q \to \bar{Q}$ can be written as $(\gamma R_f, \gamma L_e, \gamma)$ where $e, f \in Q$. Thus it can be expressed as a composition of an isomorphism $\gamma : Q(\circ) \to \bar{Q}$ with a principal isotopism $(R_f, L_e, \mathrm{id}_Q) : Q \to Q(\circ)$.

A paratopims $(\sigma, (\alpha_1, \alpha_2, \alpha_3)) : Q_1 \to Q_2$ of loops Q_1 and Q_2 will be called *unital* if $\alpha_1(1) = \alpha_2(1) = \alpha_3(1) = 1$.

Lemma 2.1. *Let $(\sigma,\alpha) : Q_1 \to Q_2$ be a paratopism of loops. Then there exists a unital paratopism $(\sigma,\beta) : Q_1 \to Q_3$ and a principal isotopism $\rho : Q_3 \to Q_2$ such that $(\sigma,\alpha) = (\mathrm{id},\rho)(\sigma,\beta)$.*

Proof: The inverse of a principal isotopism is a principal isotopism. Therefore it suffices to find a principal isotopism $\rho : Q_2 \to Q_3$ such that $(\mathrm{id},\rho)(\sigma,\alpha) = (\sigma,\beta)$ is a unital paratopism of loops.

The isotopism ρ will be of the form $(R_f, L_e, \mathrm{id}_{Q_2})$ for some $e, f \in Q_2$. Then $\beta_{\sigma^{-1}(1)} = R_f\alpha_{\sigma^{-1}(1)}$, $\beta_{\sigma^{-1}(2)} = L_e\alpha_{\sigma^{-1}(2)}$ and $\beta_{\sigma^{-1}(3)} = \alpha_{\sigma^{-1}(3)}$. Put $e = \alpha_{\sigma^{-1}(1)}(1)$ and $f = \alpha_{\sigma^{-1}(2)}(1)$. In every loop $1 \cdot 1 = 1$. Thus $ef = \alpha_{\sigma^{-1}(3)}(1) = \beta_{\sigma^{-1}(3)}(1) = \beta_{\sigma^{-1}(2)}(1) = \beta_{\sigma^{-1}(1)}(1)$. The element ef serves as the unit of Q_3. □

Lemma 2.2. *Let Q be a loop, S a quasigroup, and (σ,α) a paratopism $Q \to S$ such that $\alpha_i(1) = 1$ for every $i \in \{1,2,3\}$. Then S is a loop if and only if there exists a bijection $\theta : Q \to S$, $\theta(1) = 1$, such that*

(a) *$\alpha = (\theta,\theta,\theta)$ if $\sigma = \mathrm{id}$ or $\sigma = (1\ 2)$;*
(b) *$\alpha = (\theta I,\theta,\theta)$ if $\sigma = (1\ 2\ 3)$ or $\sigma = (2\ 3)$; and*
(c) *$\alpha = (\theta,\theta J,\theta)$ if $\sigma = (1\ 3\ 2)$ and $\sigma = (1\ 3)$.*

Proof: Assume, for example, that $\sigma = (1\ 2\ 3)$. By Table 2 the operation in S can be expressed as $\alpha_2(\alpha_1^{-1}(y)\backslash\alpha_3^{-1}(x))$. Setting $y = 1$ yields $\alpha_2 = \alpha_3$. Denote this mapping by θ. Setting $x = 1$ yields $y = \theta I\alpha_1^{-1}(y)$ for all $y \in Q$. Thus $\alpha_1 = \theta I$. Other cases are similar. □

For each unital paratopism (σ,α) of loops there thus exists a (unique) bijection θ such that there are at least two distinct $i, j \in \{1,2,3\}$ with $\alpha_i = \alpha_j = \theta$. A unital paratopism is fully described by the pair (σ,θ). We shall say that it is *carried* by (σ,θ). In Table 3 we record explicitly the multiplication in S when $Q \to S$ is a unital paratopism carried by (σ,θ). The table can be obtained by applying Lemma 2.2 to Table 2. For every loop Q these are the loops *paratopically induced* by (σ,θ).

id	$\theta(\theta^{-1}(x)\cdot\theta^{-1}(y))$
(1 2 3)	$\theta(J\theta^{-1}(y)\backslash\theta^{-1}(x))$
(1 3 2)	$\theta(\theta^{-1}(y)/I\theta^{-1}(x))$

(1 2)	$\theta(\theta^{-1}(y)\cdot\theta^{-1}(x))$
(2 3)	$\theta(J\theta^{-1}(x)\backslash\theta^{-1}(y))$
(1 3)	$\theta(\theta^{-1}(x)/I\theta^{-1}(y))$

Table 3. Paratopically induced loop operations

Let Q be a loop. The loop paratopically induced by $((1\ 2),\mathrm{id}_Q)$ is the opposite loop Q^{op}, while $((2\ 3),\mathrm{id}_Q)$ and $(1\ 3),\mathrm{id}_Q)$ induce the *left inverse loop* and the *right inverse loop* of Q, respectively.

Left and right inverse loops and the opposite loop are special cases of isostrophes of Q. A loop is said to be an *isostrophe* of Q if it is paratopically induced by (σ, I^m), for some $m \in \mathbb{Z}$ and $\sigma \in S_3$. A (unital) paratopism $Q \to S$ is called an *isostrophism* if it is carried by (σ, I^m) for some $m \in \mathbb{Z}$ and $\sigma \in S_3$.

Lemma 2.3. *Let $Q_1 \to Q_2$ be a unital paratopism that is carried by (σ, ϑ). If $\varphi : Q_0 \to Q_1$ and $\psi : Q_2 \to Q_3$ are isomorphisms of loops, then $(\sigma, \psi\vartheta\varphi)$ carries a unital paratopism $Q_0 \to Q_3$.*

Proof: This follows directly from the rule for composition of paratopisms. □

Corollary 2.4. *Every unital paratopism can be expressed as a composition of an isomorphism and of an isostrophism that is carried by (σ, id_Q), where Q is a loop and $\sigma \in S_3$.*

Proof: Combine Lemmas 2.2 and 2.3. □

The set of all isostrophes of Q will be denoted by $\mathcal{I}(Q)$. We can thus say that $\mathcal{I}(Q)$ consists of all possible targets for isostrophisms starting from Q. Isostrophisms from Q to Q could be called *autostrophisms*. However, we shall not use this term in this paper. Autostrophisms of Q correspond to the elements in the point stabilizer of Q in the group $\mathbf{I}(Q)$ (the group is defined in Section 3).

For a permutation $\sigma \in S_3$ define the *sign* $\mathrm{sgn}(\sigma) = \varepsilon$ so that $\varepsilon = 1$ if σ is an even permutation and $\varepsilon = -1$ if σ is an odd permutation (a transposition).

Lemma 2.5. *Consider a unital paratopism of loops $Q \to S$ that is carried by (σ, θ). Put $I = I_Q$. Then $I_S = \theta I^{\mathrm{sgn}(\sigma)} \theta^{-1}$.*

Proof: Suppose that $x, y \in S$ are such that $xy = 1$. We shall use Table 3. If $\sigma = (1\ 2\ 3)$, then $J\theta^{-1}(y) = \theta^{-1}(x)$ and so $y = \theta I \theta^{-1}(x)$, as required. Other cases are similar. □

Lemma 2.6. *A composition of two isostrophisms is again an isostrophism. The inverse of an isostrophism is also an isostrophism.*

Proof: Let $(\sigma, \alpha) : Q_1 \to Q_2$ be a unital paratopism of loops. Put $I = I_{Q_1}$. From Lemma 2.2 we see immediately that this paratopism is an isostrophism if and only if there exist $k_i \in \mathbb{Z}$ such that $\alpha_i = I^{k_i}$ for all $i \in \{1, 2, 3\}$. Let $(\tau, \beta) : Q_2 \to Q_3$ be another paratopism of loops. If (σ, α) is an isostrophism, then $I_{Q_2} = I^{\pm 1}$ by Lemma 2.5. If both (σ, α) and (β, γ) are isostrophisms, then there exist ℓ_i such that $\beta_i = I^{\ell_i}$. Formulas for the composition and inverse of paratopisms yield the rest. □

Corollary 2.7. *Let Q_1 and Q_2 be loops. Then $Q_1 \in \mathcal{I}(Q_2)$ if and only if $Q_2 \in \mathcal{I}(Q_1)$.*

Proof: For loops A and B on a set S write $(A, B) \in \mu$ if and only if $B \in \mathcal{I}(A)$. The relation μ is symmetric and transitive by Lemma 2.6. Hence it is an equivalence. □

We shall now describe another approach to isostrophy. It is inspired by notions of universal algebra. A loop Q_2 is said to be a *term paratope* of a loop Q_1 if there exist terms $t_i \in F(x)$, $1 \leq i \leq 3$, and $\sigma \in S_3$ such that $(\sigma, \alpha) : Q_1 \to Q_2$ is a paratopism, where $\alpha_i(u) = t_i(u)$ for each $u \in Q_1$. (Loops Q_2 and Q_1 are assumed to have the same underlying set.)

Term paratopy is a special case of a more general concept: Let Q_1 be a loop with binary operations $x \cdot y$, $x\backslash y$ and x/y, the unit of which is equal to 1. Let Q_2 be a loop upon the same underlying set, and with the same unit 1. Suppose that the three binary operations of Q_2 can be expressed as $t_1(x,y)$, $t_2(x,y)$ and $t_3(x,y)$, where the terms $t_1, t_2, t_3 \in F(x,y)$ are evaluated in Q_1. If we can pass from Q_2 to Q_1 in a similar way, we call Q_1 and Q_2 *term equivalent.*

From Corollary 2.7 and from Tables 2 and 3 we see that every isostrophe of a loop Q is a term paratope of Q. Hence we have:

Corollary 2.8. *Let Q_1 and Q_2 be loops such that $Q_2 \in \mathcal{I}(Q_1)$. Then Q_1 and Q_2 are term equivalent. Furthermore, Q_1 is a term paratope of Q_2 and Q_2 is a term paratope of Q_1.*

Corollary 2.9. *A loop is a term paratope of the free loop $F(x)$ if and only if it is an isostrophe of $F(x)$.*

Proof: This follows from Theorem 1.4 since $u \mapsto t_i(u)$ does not permute $Q = F(x)$ if t_i is not of the form $I^m(x)$. □

Isostrophes are hence the only term paratopes that can be constructed without assuming some additional equational properties of the loop Q.

Term equivalence is a standard notion of universal algebra. Term equivalent algebras share subalgebras and congruences. This is easy to verify, and in the case of loops the proof is even easier. We can hence state:

Proposition 2.10. *Let Q_1 and Q_2 be term equivalent loops. Then S is a* (*normal*) *subloop of Q_1 if and only if it is a* (*normal*) *subloop of Q_2. In particular, this is true if Q_2 is an isostrophe of Q_1.*

A further discussion of connections between loop terms and isostrophy can be found in Sections 6 and 7.

3. Isostrophisms and their groups

Let us investigate what exactly happens when we compose two isostrophisms. As an example consider $\varphi \circ \psi$, where Q, R and S are loops with the same underlying set, and $\psi = ((1\ 3), (I, \mathrm{id}, I)) : Q \to R$ and $\varphi = ((1\ 2\ 3), (I, \mathrm{id}, \mathrm{id})) : R \to S$ are paratopisms. Note that I in ψ means I_Q, while I in φ means I_R. By Lemma 2.5, to base both paratopisms in Q we have to replace I in φ by $J = I^{-1}$. Using the formula for composing paratopisms we can express $\varphi \circ \psi$ as

$$((2\ 3), (I, \mathrm{id}, \mathrm{id})) = ((1\ 2\ 3), (I, \mathrm{id}, \mathrm{id})) \circ ((1\ 3), (I, \mathrm{id}, I)).$$

In this equality I means I_Q in the outer triples, and it means I_R in the middle triple. Loops Q, R and S share the same underlying set, and hence $\mathrm{id}_Q = \mathrm{id}_R = \mathrm{id}_S$. The choice of R is determined by ψ, while the choice of S is determined by φ. The equality can be thus seen as true relative to Q. Of course, it is true for any choice of a loop Q. Therefore we can view the equality as a rule that expresses the composition of φ and ψ as if they had been considered to be mappings that act upon the class of all loops. For set theoretical reasons we cannot define a mapping upon the class of all loops. However, we can define φ and ψ as mappings upon any set of loops that is closed under isostrophes.

Our next aim is to determine a general composition rule, i.e. to describe by a formula the isostrophism that is obtained when there is composed an isostrophism that is carried by (τ, I^n) with an isostrophism that is carried by (σ, I^m). In every given case the result can be computed similarly as above. Table 4 gives the results for situations when $m = n = 0$. The table uses an abbreviated form in which 0 represents id, and spaces, commas and outer parentheses are suppressed.

$0\ (000)$	$(123)(I00)$	$(132)(0J0)$	$(12)(000)$	$(23)(I00)$	$(13)(0J0)$
$(123)(I00)$	$(132)(I0I)$	$0\ (000)$	$(13)(0J0)$	$(12)(000)$	$(23)(0JJ)$
$(132)(0J0)$	$0\ (000)$	$(123)(0JJ)$	$(23)(I00)$	$(13)(I0I)$	$(12)(000)$
$(12)(000)$	$(23)(I00)$	$(13)(0J0)$	$0\ (000)$	$(123)(I00)$	$(132)(0J0)$
$(23)(I00)$	$(13)(I0I)$	$(12)(000)$	$(132)(0J0)$	$0\ (000)$	$(123)(0JJ)$
$(13)(0J0)$	$(12)(000)$	$(23)(0JJ)$	$(123)(I00)$	$(132)(I0I)$	$0\ (000)$

Table 4. Compositions of isostrophisms that are carried by the identity

Proposition 3.1. *Let $\psi : Q \to R$ and $\varphi : R \to S$ be isostrophisms such that ψ is carried by (σ, I_Q^m) and φ by (τ, I_R^n). Then $\varphi\psi$ is an isostrophism $Q \to S$ that is carried by $(\tau\sigma, I_Q^k)$ where $k = m + \operatorname{sgn}(\sigma)n + \mathrm{d}(\tau, \sigma)$ and where $\mathrm{d} : S_3 \times S_3 \to \{0, -1, 1\}$ is determined by the following table:*

	id	(1 2 3)	(1 3 2)	(1 2)	(2 3)	(1 3)
id	0	0	0	0	0	0
(1 2 3)	0	1	0	0	0	−1
(1 3 2)	0	0	−1	0	1	0
(1 2)	0	0	0	0	0	0
(2 3)	0	1	0	0	0	−1
(1 3)	0	0	−1	0	1	0

Proof: In this proof we shall denote by $\gamma_0(T)$ the isostrophism that is carried by (γ, id_T), for every $\gamma \in S_3$ and every loop T. We see (cf. Corollary 2.4) that $\psi = \sigma_0(\bar{Q})I_Q^m$, where $\bar{Q}$ is defined so that $I_Q^m : Q \to \bar{Q}$ is an isomorphism. Similarly $\varphi = \tau_0(\bar{R})I_R^n$. Put $n' = \operatorname{sgn}(\sigma)n$. We can express φ as $\tau_0(\bar{R})I_Q^{n'}$, by Lemma 2.5. Consider now the isostrophism $I_Q^{n'}\sigma_0(\bar{Q})$. It is carried by $(\sigma, I_Q^{n'})$ and so it equals $\sigma_0(T)I_Q^{n'}$, where T is the loop such that $I_Q^{n'} : \bar{Q} \to T$ is an isomorphism. Note that $I_T = I_{\bar{Q}} = I_Q$, by Lemma 2.5. We can express $\varphi\psi$ as $\tau_0(\bar{R})\sigma_0(T)I_Q^{m+n'}$. The fact that $\tau_0(\bar{R})\sigma_0(T)$ is carried by $(\tau\sigma, I_T^{\mathrm{d}(\tau,\sigma)})$ follows from Table 4. □

The composition rule for isostrophisms thus induces a group on $S_3 \times \mathbb{Z}$ in which

$$(\tau, n)(\sigma, m) = (\tau\sigma, \mathrm{sgn}(\sigma)n + m + \mathrm{d}(\tau, \sigma)).$$

The group will be denoted by $\mathbf{I}$. It acts in a natural way upon any set of loops that is closed under isostrophes. Writing $(\sigma, m)(Q) = R$ means that there exists a (unique) isostrophism $Q \to R$ that is carried by (σ, I_Q^m). If $(\tau, n)(R) = S$, then $((\tau, n)(\sigma, m))(Q) = S$.

It can be easily verified that $\mathbf{I}$ acts faithfully upon $\mathcal{I}(F)$ when F is a free loop. Before investigating possible kernels of the action upon $\mathcal{I}(Q)$ for other loops Q, we shall first study the abstract nature of $\mathbf{I}$. It is quite easy to see that $\mathbf{I}$ is an infinite dihedral group.

Indeed, put $\mathbf{s} = ((1\ 2\ 3), 0)$. From the definition of $\mathbf{I}$ we see that $\mathbf{s}^2 = ((1\ 3\ 2), 1)$ and $\mathbf{s}^3 = (\mathrm{id}, 1)$. Hence $\mathbf{s}^{3k} = (\mathrm{id}, k)$ for every $k \in \mathbb{Z}$ and so $\langle \mathbf{s} \rangle = \{(\sigma, i) \in \mathbf{I};\ \mathrm{sgn}(\sigma) = 1\}$. Put also $\mathbf{o} = ((1\ 2), 0)$, $\mathbf{l} = ((2\ 3), 0)$ and $\mathbf{r} = ((1\ 3), 0)$. Further computations in $\mathbf{I}$ yield the following results:

Proposition 3.2 (Artzy). *The group $\mathbf{I}$ satisfies defining relations $\langle \mathbf{o}, \mathbf{s};\ \mathbf{o}^2 = 1, \mathbf{oso} = \mathbf{s}^{-1} \rangle$. Furthermore, $\mathbf{l} = \mathbf{os}$, $\mathbf{r} = \mathbf{os}^{-1}$, $\mathbf{r} = \mathbf{s}^2\mathbf{l}$ and $\mathbf{I} = \langle \mathbf{o}, \mathbf{l} \rangle = \langle \mathbf{o}, \mathbf{r} \rangle$.*

In the rest of this paper we shall treat $\mathbf{I}$ as an (infinite dihedral) group that is determined by the defining relations of Proposition 3.2, and shall not use the identification of elements of $\mathbf{I}$ as pairs (σ, m).

Recall that identities $J(x)(xy) = y$, $(xy)I(y) = x$, $J(xy)x = y$, $J(x)(yx) = y$ and $J(xy) = J(y)J(x)$ define what is known as LIP, RIP, WIP, CIP and AAIP loops. The respective "Inverse Property" is thus Left or Right or Weak or Cross or Anti-Automorphic. Loops that are both LIP and RIP are called IP (inverse property) loops. Note that Q is commutative if and only if $\mathbf{o}(Q) = Q$.

Lemma 3.3 (Artzy). *Let Q be loop. Then Q is an LIP or RIP or AAIP loop if and only if $\mathbf{l}(Q) = Q$, $\mathbf{r}(Q) = Q$, or $\mathbf{os}^3(Q) = Q$, respectively. In each of these cases $I = J$.*

Proof: The case of LIP is immediate since LIP can be clearly expressed in a weaker form that for every $x \in Q$ there exists $x' \in Q$ such that $x'(xy) = y$ for all $x \in Q$. Using Tables 3 and 4 we see that $\mathbf{os}^3(Q) = Q$ if and only if $I(J(y) \cdot J(x)) = xy$ for all $x, y \in Q$. The equality $I = J$ is well known and easy (in case of LIP use $J(x) = J(x)(xI(x)) = I(x)$, for AAIP employ $1 = J(xI(x)) = xJ(x)$). □

We have observed that the isostrophism $\mathbf{s}^3$ equals $(\mathrm{id}, (I, I, I))$, and so it is in fact an isomorphism. This fact is recorded in the next lemma for the sake of reference. The inverses of loops Q and S coincide, say, by Lemma 2.5.

Lemma 3.4. *Let Q be a loop. Put $S = \mathbf{s}^3(Q)$. Then $I = I_Q = I_S$ is an isomorphism $Q \cong S$.*

Suppose that the set of all $\{k \in \mathbb{Z};\ \mathbf{s}^k(Q) = Q\}$ is nontrivial. Then there exists exactly one $t > 0$ such that $\mathbf{s}^k(Q) = Q$ if and only if t divides k. If t is not divisible by 3, then there exists a unique $m \in \mathbb{Z}$ such that $|3m+1| = t$. In such a case $\mathbf{s}^{3m+1}(Q) = Q$.

The isostrophism $\mathbf{s}^{3m+1}$ is carried by $((1\ 2\ 3), I^m)$. Table 3 implies that if $\mathbf{s}^{3m+1}(Q) = Q$, then $xy = I^m(JI^{-m}(y)\backslash I^{-m}(x))$ for all $x, y \in Q$. This is equivalent to $J^{m+1}(y)J^m(xy) = J^m(x)$. Every loop satisfying such an law is called *m-inverse* [14].

The m-inverse law can be equivalently expressed as $I^m(yx)I^{m+1}(y) = I^m(x)$ [14], [8]. A proof along the lines of this presentation can be obtained if we put $m' = -m-1$ and note that $\mathbf{s}^{3m'+2}$ is carried by $((1\ 3\ 2), I^{m'+1})$. We have $m'+1 = -m$ and $|3m'+2| = t$, and so Table 3 yields $xy = J^m(I^m(y)/I^{m+1}(x))$. That is the same as $I^m(xy)I^{m+1}(x) = I^m(y)$.

Note that 0-inverse loops are the CIP loops ($t=1$), and that (-1)-inverse loops are the WIP loops ($t=2$).

Proposition 3.5. *Let Q be a loop and let $t > 0$ be such that $\mathbf{s}^t(Q) = Q$ and that t is the least possible.*

(i) *If $t = 3k$, then $I^k \in \operatorname{Aut}(Q)$ and Q is not n-inverse for any $n \in \mathbb{Z}$. Furthermore, $I^\ell \in \operatorname{Aut}(Q)$ if and only if k divides ℓ.*

(ii) *If $t = 3k \pm 1$, put $m = \pm k$. Then $t = |3m+1|$. The loop Q is an n-inverse loop if and only if $3m+1$ divides $3n+1$. Furthermore, $I^\ell \in \operatorname{Aut}(Q)$ if and only if $3m+1$ divides ℓ.*

Proof: If Q is an n-inverse loop, then we can reverse the process described above to show that $\mathbf{s}^{3n+1}(Q) = Q$. This is possible if and only if $3n+1$ is divisible by t. For the rest use the fact that $I^k \in \operatorname{Aut} Q$ if and only of $\mathbf{s}^{3k}(Q) = Q$ (Lemma 3.4). □

The value of m in the definition of an m-inverse loop can be thus seen as a way of coding the positive integer $t = 3k \pm 1$. Up to now there is no evidence of an interesting algebraic theory that would involve m-inverse loops for higher values of $|m|$. Known connections to other classes of loops are restricted to situations when t is a small power of two. If $t = 2^k$, then $m = ((-2)^k - 1)/3$. In such cases an m-inverse loop is called [8] a W^{k}IP loop (it has the *k-fold weak inverse property*). Note that then $I^{2^k} \in \operatorname{Aut}(Q)$, by Proposition 3.5.

Note also that a CIP loop is m-inverse for any $m \in \mathbb{Z}$. In particular, the CI property implies the WI property.

The group $\mathbf{I}$ acts upon $\mathcal{I}(Q)$. The image of this action will be denoted by $\mathbf{I}(Q)$. Hence $\mathbf{I}(Q)$ is a permutation group that is either trivial, or cyclic of order two, or the Klein four-group or a noncommutative dihedral group. Thus $\mathbf{I}(Q)$ is commutative if and only if $|\mathbf{I}(Q)|$ is a divisor of 4.

Proposition 3.6. *Let Q be a loop such that $|\mathbf{I}(Q)|$ divides 4. Then exactly one of the following cases takes place:*

(1) *Q is a noncommutative WIP loop that is not IP; $|\mathcal{I}(Q)| = 4$.*

(2) *Q is a noncommutative IP loop; $|\mathcal{I}(Q)| = 2$.*

(3) *Q is a commutative WIP loop that is not IP; $|\mathcal{I}(Q)| = 2$.*

(4) *Q is a noncommutative CIP loop;* $|\mathcal{I}(Q)| = 2$.
(5) *Q is a commutative IP loop;* $|\mathcal{I}(Q)| = 1$.

Proof: Our assumption can be also expressed by saying that $\mathbf{s}^2$ acts trivially upon $\mathcal{I}(Q)$. Hence Q is a WIP loop. From $\mathbf{r} = \mathbf{s}^2\mathbf{l}$ we see that $\mathbf{l}(Q) = Q$ is equivalent to $\mathbf{r}(Q) = Q$. That happens exactly when Q is an IP loop. Each of $\mathbf{s}$, $\mathbf{o}$ and $\mathbf{l}$ acts upon $\mathcal{I}(Q)$ either trivially or as an involution. If none of them acts trivially, then we get case (1). Cases (2)–(4) describe situations when exactly one of them acts trivially (note that an IP CIP loop is commutative). □

A permutation group G on Ω is said to be *regular* if it is transitive and if $g = \mathrm{id}_\Omega$ whenever $g \in G$ is such that $g(\omega) = \omega$ for some $\omega \in \Omega$. If Q is a loop, then $\mathbf{I}(Q)$ is transitive, but not necessarily regular. We shall see that there are only few nonregular cases. A transitive commutative permutation group is always regular. Therefore a finite nonregular $\mathbf{I}(Q)$ has to be isomorphic to the dihedral group D_{2n} for some $n \geq 3$. We shall see that $n \in \{3, 6\}$. Note that $D_6 \cong S_3$.

A loop Q is said to have *automorphic inverse property* (AIP) if $I \in \mathrm{Aut}(Q)$ (i.e. $I(xy) = I(x)I(y)$ for all $x, y \in Q$. Equivalently $J(xy) = J(x)J(y)$.) For a loop to have the AI property it is not necessary that $I = J$. However, AIP loops occurring in Proposition 3.7 have $I = J$ (then $I(x) = J(x)$ is written as x^{-1}).

Note that if Q has the AIP, then every element of $\mathcal{I}(Q)$ has the AIP.

Note also that $I \in \mathrm{Aut}(Q)$ if and only if $\mathbf{s}^3(Q) = Q$, by Proposition 3.5.

Proposition 3.7. *Let Q be a loop such that $\mathbf{I}(Q)$ is not regular. Then one of the following cases takes place:*

(1) $\mathbf{I}(Q) \cong S_3$, $|\mathcal{I}(Q)| = 3$ *and there exists a unique commutative AIP loop $Q_1 \in \mathcal{I}(Q)$ such that $\mathcal{I}(Q) = \{Q_1, \mathbf{s}(Q_1), \mathbf{s}^{-1}(Q_1)\}$. Then $\mathbf{s}(Q_1)$ has the LIP and the AIP, and $\mathbf{s}^{-1}(Q_1)$ has the RIP and the AIP. On the other hand, $\mathbf{I}(Q) \cong S_3$ and $|\mathcal{I}(Q)| = 3$ whenever Q is an AIP loop that is not IP, and is commutative or RIP or LIP.*

(2) $\mathbf{I}(Q) \cong D_{12}$, $|\mathcal{I}(Q)| = 6$ *and there exist in $\mathcal{I}(Q)$ two different commutative loops Q_1 and Q_2 such that I: $Q_1 \cong Q_2$ and $\mathcal{I}(Q) = \{Q_i, \mathbf{l}(Q_i), \mathbf{r}(Q_i);$ $i \in \{1, 2\}\}$. On the other hand if Q is a commutative loop without the AIP, then $|\mathcal{I}(Q)| = 6$ and $\mathbf{I}(Q) \cong D_{12}$.*

(3) $\mathbf{I}(Q) \cong D_{12}$, $|\mathcal{I}(Q)| = 6$ *and $\mathcal{I}(Q)$ consists of two LIP loops, two RIP loops and two AAIP loops, none of which is commutative or an IP loop or an AIP loop. On the other hand, if Q is neither an IP loop nor an AIP loop, but it is an LIP loop or an RIP loop or an AAIP loop, then it is not commutative, $\mathbf{I}(Q) \cong D_{12}$ and $|\mathcal{I}(Q)| = 6$.*

Proof: Suppose that $\mathbf{I}(Q)$ is not regular. Then it is isomorphic to D_{2n} for some $n \geq 3$. If $I = J$, then $I^2 = \mathrm{id}_Q$, and hence $\mathbf{s}^6(Q) = Q$. Thus $n \in \{3, 6\}$ if $I = J$. If n is odd, then $\mathbf{I}(Q)$ contains only one conjugacy class of involutions. If n is even, then in $\mathbf{I}(Q)$ there are two classes of noncentral involutions. One of the classes contains the noncentral involutions that are fixed point free, while the other class contains the involutions that fix exactly two points. If n is even, then $\mathbf{l}$ and $\mathbf{o}$ yield involutions that are not conjugate. We can thus assume that Q fulfils $\mathbf{l}(Q) = Q$ or $\mathbf{o}(Q) = Q$. Both cases imply $I = J$ (cf. Lemma 3.3), and so $n \in \{3, 6\}$.

Suppose first that $n = 3$. Then all elements of $\mathcal{I}(Q)$ are AIP loops since $I = J \in \mathrm{Aut}(Q)$, by Lemma 3.4. There is only one class of involutions, and so we can assume that Q is commutative. Then $\mathbf{ls}(Q) = \mathbf{os}^2(Q) = \mathbf{os}^2\mathbf{o}(Q) = \mathbf{s}^{-2}(Q) = \mathbf{s}(Q)$ since $\mathbf{l} = \mathbf{os}$ and since $\mathbf{s}^3(Q) = Q$. Thus $\mathbf{l}$ fixes $\mathbf{s}(Q)$ and, similarly, $\mathbf{r}$ fixes $\mathbf{s}^{-1}(Q)$. This proves case (1), by Lemma 3.3.

Suppose now that $n = 6$. If $\mathbf{o}(Q) = Q$, then $\mathbf{os}^3(Q) = \mathbf{os}^3\mathbf{o}(Q) = \mathbf{s}^{-3}(Q) = \mathbf{s}^3(Q)$. We can thus put $Q_1 = Q$ and $Q_2 = \mathbf{s}^3(Q)$. Then I: $Q_1 \cong Q_2$, by Lemma 3.4, and the rest of case (2) follows from $\mathbf{l}(Q_i) = \mathbf{lo}(Q_i) = \mathbf{s}^{-1}(Q_i)$ and $\mathbf{r}(Q_i) = \mathbf{ro}(Q_i) = \mathbf{s}(Q_i)$, $i \in \{1, 2\}$.

It remains to consider the case when $n = 6$ and $\mathbf{l}(Q) = Q$. Then $\mathbf{ls}^3(Q) = \mathbf{ls}^{-3}\mathbf{l}(Q) = \mathbf{s}^3(Q)$. To prove (3) it thus suffices to verify that $\mathbf{rs}(Q) = \mathbf{s}(Q)$ and that $\mathbf{os}^3(\mathbf{s}^{-1}(Q)) = \mathbf{s}^{-1}(Q)$, by Lemma 3.3. From Proposition 3.2 we obtain that $\mathbf{rs}(Q) = \mathbf{s}^2\mathbf{lsl}(Q) = \mathbf{s}^2\mathbf{s}^{-1}(Q) = \mathbf{s}(Q)$ and that $\mathbf{os}^2(Q) = \mathbf{lsl}(Q) = \mathbf{s}^{-1}(Q)$. □

Let us investigate more closely case (2) of Proposition 3.7. It involves (a) commutative loops, (b) loops in which the left inverse is commutative and (c) loops in which the right inverse is commutative. Since $J_Q = I_Q$ when Q is commutative, there is $J_Q = I_Q$ in other cases as well.

Now, $\mathbf{l}(Q)$ is commutative if and only if $J(x)\backslash y = J(y)\backslash x$ for all $x, y \in Q$. The latter law can be equivalently expressed as $x\backslash y = J(y)\backslash I(x)$ or $y = J(xy)\backslash I(x)$ or $J(xy)y = I(x)$.

Proposition 3.8. *Let Q be a loop.*

(i) *If Q satisfies for some $\varepsilon, \eta \in \{-1, 1\}$ a law $x\backslash y = J^\varepsilon(y)\backslash J^\eta(x)$ or a law $J^\varepsilon(xy)y = J^\eta(x)$, then $I = J$, and Q satisfies all eight these laws. This takes place if and only if $\mathbf{l}(Q)$ is a commutative loop.*

(ii) *If Q satisfies for some $\varepsilon, \eta \in \{-1, 1\}$ a law $y/x = I^\eta(x)/I^\varepsilon(y)$ or a law $yI^\varepsilon(yx) = I^\eta(x)$, then $I = J$, and Q satisfies all eight these laws. This takes place if and only if $\mathbf{r}(Q)$ is a commutative loop.*

If both $\mathbf{l}(Q)$ and $\mathbf{r}(Q)$ are commutative loops, then Q is a commutative WIP loop and $\mathbf{l}(Q) = \mathbf{r}(Q)$. If $\mathbf{l}(Q)$ (or $\mathbf{r}(Q)$) is commutative and Q is not commutative, then $\mathbf{I}(Q) \cong D_{12/d}$ and $|\mathcal{I}(Q)| = 6/d$, where $d = 2$ if Q satisfies the AIP, and $d = 1$ otherwise.

Proof: If $x\backslash y = J^\varepsilon(y)\backslash J^\eta(x)$, then $y = J^\varepsilon(xy)\backslash J^\eta(x)$ and $J^\varepsilon(xy)y = J^\eta(x)$. If $J(xy)y = J(x)$, then $I(x) = J(xI(x))I(x) = J(x)$. If $J(xy)y = I(x)$ or $I(xy)y = J(x)$, then $I(x) = J(x)$ can be obtained by setting $y = 1$. If $I(xy)y = I(x)$, then $I(y)y = 1$, and so $I(y) = J(y)$. We have already observed above that $\mathbf{l}(Q)$ is commutative if and only if $x\backslash y = J(y)\backslash I(x)$ for all $x, y \in Q$. That proves point (i). Point (ii) follows by mirror symmetry.

Now, $\mathbf{l} = \mathbf{os}$ and $\mathbf{r} = \mathbf{os}^{-1}$, by Proposition 3.2. Hence $\mathbf{ol}(Q) = \mathbf{l}(Q) \Leftrightarrow \mathbf{s}(Q) = \mathbf{os}(Q) \Leftrightarrow Q = \mathbf{os}^2(Q)$, and $\mathbf{or}(Q) = \mathbf{r}(Q) \Leftrightarrow \mathbf{s}^{-1}(Q) = \mathbf{os}^{-1}(Q) \Leftrightarrow Q = \mathbf{os}^{-2}(Q)$.

If both $\mathbf{ol}(Q) = \mathbf{l}(Q)$ and $\mathbf{or}(Q) = \mathbf{r}(Q)$ are true, then $\mathbf{s}^3(Q) = \mathbf{s}^{-1}(Q)$ is commutative, and hence $Q \cong \mathbf{s}^3(Q)$ is commutative as well, by Lemma 3.4. In such a case $Q = \mathbf{s}^2(Q)$, Q is a commutative WIP loop and we can use Proposition 3.6.

If $\mathbf{l}(Q)$ is commutative and Q is not commutative, then no case of Proposition 3.6 applies, and hence one of cases of Proposition 3.7 has to be satisfied. □

Loops that satisfy the equality $J(xy)y = J(x)$ (i.e. loops in which the left inverse is commutative) were introduced by Johnson and Sharma [13] and recently studied by Greer and Kinyon [12]. They are known as *weak commutative inverse property* loops, or WCIP loops. In this paper we shall call them *left cross-commutative* loops. Loops in which the right inverse is commutative will be called *right cross-commutative*. By saying that Q is *cross-commutative* we mean that it is left cross-commutative or right cross-commutative.

Situations that are not covered by Proposition 3.7 and Proposition 3.6 are described in the following statement. The claims about the m-inversity follow from Proposition 3.5.

Proposition 3.9. *Suppose that Q is neither WIP nor LIP nor RIP nor AAIP loop, and that it is neither commutative nor cross-commutative. Then $\mathbf{I}(Q)$ is a regular permutation group that is isomorphic either to the infinite dihedral group, or to D_{2n}, $n \geq 3$. If $n = 3k + \varepsilon$, where $\varepsilon \in \{-1, 1\}$, then Q is εk-inverse. If $n = 3k$, then $I^k \in \operatorname{Aut} Q$ (and Q is m-inverse for no $m \in \mathbb{Z}$). On the other hand, if $\mathbf{I}(Q)$ is regular and noncommutative, then Q is neither commutative nor cross-commutative nor WIP nor LIP nor RIP nor AAIP loop.*

Lemma 3.4 implies that $\mathcal{I}(Q)$ contains at most six isomorphism classes. This is precised in detail in Section 5.

4. Paratopisms and nuclei

Let Q be a quasigroup. Isotopisms $Q \to Q$ are called *autotopisms*. They form a group that will be denoted by $\operatorname{Atp}(Q)$. An autotopism β can be seen as a paratopism $(\mathrm{id}, \beta) : Q \to Q$, and vice versa.

Hence each paratopism $f = (\sigma, \alpha) : Q \to R$ yields an isomorphism $f_* : \operatorname{Atp}(Q) \to \operatorname{Atp}(R)$ that sends $\beta \in \operatorname{Atp}(Q)$ to $(\alpha\beta\alpha)^{\sigma^{-1}} \in \operatorname{Atp}(R)$. Indeed,

$$(\sigma, \alpha)(\mathrm{id}, \beta)(\sigma, \alpha)^{-1} = (\sigma, \alpha\beta)(\sigma^{-1}, (\alpha^{-1})^{\sigma^{-1}}) = (\mathrm{id}, (\alpha\beta\alpha^{-1})^{\sigma^{-1}}).$$

For every $i \in \{1, 2, 3\}$ denote by $\operatorname{Atp}_i(Q)$ the group of all $(\alpha_1, \alpha_2, \alpha_3) \in \operatorname{Atp}(Q)$ with $\alpha_i = \mathrm{id}_Q$.

Lemma 4.1. *Let $f = (\sigma, \alpha) : Q \to R$ be a paratopism of quasigroups. Then $f_*(\operatorname{Atp}_i(Q)) = \operatorname{Atp}_{\sigma(i)}(R)$ for every $i \in \{1, 2, 3\}$.*

Proof: If $\beta \in \operatorname{Atp}(Q)$, then $\beta \in \operatorname{Atp}_i(Q)$ if and only if $\beta_i = \mathrm{id}_Q$. Now, the $\sigma(i)$th component of $(\alpha\beta\alpha^{-1})^{\sigma^{-1}}$ is equal to $\alpha_i\beta_i\alpha_i^{-1}$. Clearly $\alpha_i\beta_i\alpha_i^{-1} = \mathrm{id}_R$ if and only if $\beta_i = \mathrm{id}_Q$. □

We shall include a well known fact about nuclei of loops. The proof is simple enough to warrant omitting. Recall that $N_\lambda = N_\lambda(Q) = \{a \in Q;\ a(xy) = (ax)y$ for all $x, y \in Q\}$ is known as the *left nucleus*, while the *middle* and *right* nuclei N_μ and N_ρ are obtained by shifting to the right the position of a.

Lemma 4.2. *Let Q be a loop. Then $\mathrm{Atp}_1(Q)$ equals $\{(\mathrm{id}_Q, R_a, R_a);\ a \in N_\rho\}$, $\mathrm{Atp}_2(Q)$ equals $\{(L_a, \mathrm{id}_Q, L_a);\ a \in N_\lambda\}$, and $\mathrm{Atp}_3(Q)$ equals $\{(R_a^{-1}, L_a, \mathrm{id}_Q);\ a \in N_\mu\}$.*

The connection makes understandable why $\mathrm{Atp}_i(Q)$ is called an A_i-nucleus by some authors. Lemma 4.2 makes clear that for loops the construct of $\mathrm{Atp}_i(Q)$ is not needed, unless it can be employed with advantage in a proof. This is exactly what we shall do below. To make the connection direct, we dub $N_\rho(Q)$ as $N_1(Q)$, $N_\lambda(Q)$ as $N_2(Q)$ and $N_\mu(Q)$ as $N_3(Q)$.

Lemma 4.3. *Let $(\sigma, \alpha) : Q \to R$ be a paratopism of loops such that $\alpha_i(1) = 1$ for all $i \in \{1, 2, 3\}$. Then*

$$N_{\sigma(i)}(R) = \alpha_j(N_i(Q)) \ \text{ for all } \ i, j \in \{1, 2, 3\} \ \text{ such that } \ i \neq j.$$

PROOF: Let i and j be as assumed. By Lemma 4.2, elements of $N_i(Q)$ are exactly those that can be expressed as $\beta_j(1)$ for $\beta = (\beta_1, \beta_2, \beta_3) \in \mathrm{Atp}_i(Q)$. If $\beta \in \mathrm{Atp}_i(Q)$, then $(\alpha\beta\alpha^{-1})^{\sigma^{-1}} \in \mathrm{Atp}_{\sigma(i)}(R)$ by Lemma 4.1. Elements of $N_{\sigma(i)}(R)$ can be expressed as $\gamma_{\sigma(j)}(1)$, where $\gamma \in \mathrm{Atp}_{\sigma(i)}(R)$, by Lemma 4.2. If $\gamma = (\alpha\beta\alpha^{-1})^{\sigma^{-1}}$, $\beta \in \mathrm{Atp}_i(Q)$, then $\gamma_{\sigma(j)} = \alpha_j\beta_j\alpha_j^{-1}$. Thus $\gamma_{\sigma(j)}(1) = \alpha_j(\beta_j(1)) \in \alpha_j(N_i)$. We have proved that $\alpha_j(N_i(Q)) \subseteq N_{\sigma(i)}(R)$. By considering $(\sigma, \alpha)^{-1}$ we get $\alpha_j^{-1}(N_{\sigma(i)}(R)) \subseteq N_i(Q)$, and hence the required equality really takes place. □

If $(\sigma, \alpha) : Q \to R$ is an isostrophism, then $N_{\sigma(i)}(R) = N_i(Q)$ since α_j is a power of I. Table 5 shows the nuclei of the isostrophe that appears in the second column (say $\mathbf{s}^{3k+1}(Q)$). The value of σ is in the first column ((1 2 3) for $\mathbf{s}^{3k+1}$), and columns 3-5 show the sources for nuclei of the given loop in the order N_ρ, N_λ and N_μ. For example λ appears in the column 3 in the row of $\mathbf{s}^{3k+1}(Q)$, and that means that $N_\rho(\mathbf{s}^{3k+1}(Q)) = N_\lambda(Q)$.

id	$\mathbf{s}^{3k}(Q)$	ρ	λ	μ
(1 2 3)	$\mathbf{s}^{3k+1}(Q)$	λ	μ	ρ
(1 3 2)	$\mathbf{s}^{3k+2}(Q)$	μ	ρ	λ
(1 2)	$\mathbf{os}^{3k}(Q)$	λ	ρ	μ
(2 3)	$\mathbf{ls}^{3k}(Q)$	ρ	μ	λ
(1 3)	$\mathbf{rs}^{3k}(Q)$	μ	λ	ρ

TABLE 5. Isostrophies and the interdependence of nuclei

The fact that isostrophisms switch the nuclei was observed already by Artzy [3]. He also noted the consequences for LIP, RIP and AAIP loops.

In m-inverse loops $\mathbf{s}^{3m+1}(Q) = Q$, and so Table 5 shows that all three nuclei have to coincide. That was proved by Karkliňš and Karkliň [14] in a direct way.

We record these results in the next statement. The proof can be derived directly from Table 5.

Proposition 4.4. *If Q is an m-inverse loop, then $N_\lambda = N_\mu = N_\rho$. If Q has the LIP, then $N_\lambda = N_\mu$. If Q has the RIP, then $N_\rho = N_\mu$. If Q has the AAIP or is commutative, then $N_\lambda = N_\rho$.*

Karkliňš and Karkliň [14] also note that $N(Q) = Z(Q)$ if Q is $2k$-inverse. We shall explain this phenomenon in Corollary 4.8. As a preparatory step let us record the following easy facts:

Lemma 4.5. *Let Q be a loop. If $a \in N_\rho \cap N_\lambda$, then $I(ax) = I(x)a^{-1}$ and $J(xa) = a^{-1}J(x)$. If $a \in N_\mu$, then $I(xa) = a^{-1}I(x)$ and $J(ax) = J(x)a^{-1}$.*

Proof: Fulfilling $I(ax) = I(x)a$ means fulfilling $1 = (ax)(I(x)a)$. That clearly holds if $a \in N_\lambda \cap N_\rho$. The other cases can be proved similarly. □

Corollary 4.6. *Let Q be a loop. If $a \in N(Q)$, $x \in Q$ and $k \in \mathbb{Z}$, then*

$$I^{2k}(ax) = aI^{2k}(x), \qquad I^{2k}(xa) = I^{2k}(x)a,$$

$$I^{2k+1}(ax) = I^{2k+1}(x)a^{-1} \quad \text{and} \quad I^{2k+1}(xa) = a^{-1}I^{2k+1}(x).$$

Proof: Proceed by induction using Lemma 4.5. □

Theorem 4.7. *Let Q be a loop. Then $I^{2k+1} \in \mathrm{Aut}(Q)$ for some $k \in \mathbb{Z}$ if and only if $\mathbf{s}$ is of an odd order in $\mathbf{I}(Q)$. In such a case $N(Q) = Z(Q)$.*

Proof: By Lemma 3.4, $\mathbf{s}^{3r}(Q) = Q$ if and only if $I^r \in \mathrm{Aut}(Q)$. If this is true for an odd r, then $I^r(xa) = I^r(x)I^r(a) = I^r(x)a^{-1}$ for every $x \in Q$ and $a \in N(Q)$. However, by Corollary 4.6 we also have $I^r(xa) = a^{-1}I^r(x)$. □

Corollary 4.8 (Karkliňš and Karkliň). *If Q is a $2h$-inverse loop for some $h \in \mathbb{Z}$, then $N(Q) = Z(Q)$.*

Proof: If Q is $2h$-inverse, then $I^\ell \in \mathrm{Aut}(Q)$ for $\ell = 6h + 1$, by Proposition 3.5. □

5. Isomorphisms and the left and right inverses

Lemma 5.1. *Suppose that $\sigma \in S_3$, and that (σ, α_i) is a quasigroup paratopism $Q_i \to R_i$, $i \in \{1, 2\}$. Then Q_1 is isotopic to Q_2 if and only if R_1 is isotopic to R_2.*

Proof: An isotopism $R_1 \to R_2$ can be obtained from an isotopism $\beta : Q_1 \to Q_2$ as a composition $(\sigma, \alpha_2)(\mathrm{id}, \beta)(\sigma, \alpha_1)^{-1} = (\sigma, \alpha_2\beta)(\sigma^{-1}, (\alpha_1^{-1})^{\sigma^{-1}}) =$ $(\mathrm{id}, \alpha_2\beta(\alpha_1^{-1})^{\sigma^{-1}})$. □

Proposition 5.2. *Let Q_1 and Q_2 be loops and let $\mathbf{f} \in \mathbf{I}$ be an isostrophism. Then $Q_1 \cong Q_2$ if and only if $\mathbf{f}(Q_1) \cong \mathbf{f}(Q_2)$. Furthermore, Q_1 is isotopic to Q_2 if and only if $\mathbf{f}(Q_1)$ is isotopic to $\mathbf{f}(Q_2)$.*

Proof: The part about isotopy follows from Lemma 5.1. For the isomorphisms just note that if $\varphi : Q_1 \cong Q_2$, then $\varphi(t(x,y)) = t(\varphi(x), \varphi(y))$ for any $t \in F(x,y)$. □

Proposition 5.3. *Let Q be an m-inverse loop for some $m \in \mathbb{Z}$. Then every element of $\mathcal{I}(Q)$ is isomorphic to Q or to Q^{op}. If Q is commutative, then $Q = Q^{\mathrm{op}}$. If Q is an AAIP loop, then $Q \cong Q^{\mathrm{op}}$ as well.*

Proof: If $Q_1, Q_2 \in \mathcal{I}(Q)$ are in the same orbit of $\mathbf{s}$, then there exists $k \geq 1$ such that $\mathbf{s}^{3k}(Q_1) = Q_2$ since the length of the orbit is $|3m+1|$. By Lemma 3.4 this settles the case of m-inverse loops. The rest is obvious. □

Proposition 5.4. *Let Q be a loop that is not an IP loop. If Q is a LIP or RIP or AAIP or commutative loop, then $\mathcal{I}(Q)$ contains exactly three isomorphism types. They are represented by $\mathbf{s}^k(Q)$, $|k| \leq 1$.*

Proof: By Proposition 3.7 each element of $\mathcal{I}(Q)$ can be expressed as $\mathbf{s}^k(Q)$, $k \in \mathbb{Z}$. Hence we get all possible isomorphism types if k is restricted to -1, 0 and 1, by Lemma 3.4. We need to prove that no two of them may be isomorphic. For cases (1) and (3) of Proposition 3.7 this follows from the fact a loop is an IP loop if it satisfies at least two of the LI, RI and AAI properties. Suppose now that Q is commutative. Then $\mathbf{o}$ cannot fix $\mathbf{s}^k(Q)$ for $k \in \{-1, 1, 2\}$ since Q and $\mathbf{s}^3(Q)$ are the only points of $\mathcal{I}(Q)$ that are fixed by $\mathbf{o}$. If $\mathbf{s}^{-1}(Q) \cong \mathbf{s}(Q)$, then $Q \cong \mathbf{s}^2(Q)$ by Proposition 5.2. However, the commutative loop Q cannot be isomorphic to a noncommutative loop $\mathbf{s}^k(Q)$, $k \in \{-1, 1, 2\}$. □

By Proposition 3.9, the only cases not covered by Propositions 5.3 and 5.4 are those for which $\mathbf{I}(Q)$ is regular and, if finite, of order $6k$, $k \geq 1$. For such loops we can use the following general statement:

Theorem 5.5 (Artzy). *Let Q be a loop. Then $\mathcal{I}(Q)$ contains 1 or 2 or 3 or 6 isomorphism classes.*

Proof: By Proposition 5.2 isomorphic loops yield upon $\mathcal{I}(Q)$ a set of conjugate blocks. Consider the action of $\mathbf{I}(Q)$ upon this set. The kernel of the action contains $\mathbf{s}^3$, by Lemma 3.4. The image of the action is hence equivalent to a transitive action of S_3 since $\mathbf{I}/\langle \mathbf{s}^3 \rangle \cong S_3$. □

In the rest of this section we shall address the following question: Starting from Q iteratively construct left and right inverses. When do we get full $\mathcal{I}(Q)$?

Note first that by Proposition 3.2 the subgroup $\langle \mathbf{l}, \mathbf{r} \rangle \leq \mathbf{I}$ is of index 2, and equals $\langle \mathbf{l}, \mathbf{s}^2 \rangle = \langle \mathbf{os}, \mathbf{s}^2 \rangle = \{\mathbf{s}^{2k}, \mathbf{os}^{2k+1};\ k \in \mathbb{Z}\}$. Hence either $\langle \mathbf{l}, \mathbf{r} \rangle(Q) = \mathcal{I}(Q)$, or $\langle \mathbf{l}, \mathbf{r} \rangle$ halves $\mathcal{I}(Q)$ into two different orbits. In the former case we shall say that Q is of *odd type*, while in the latter case Q will be of *even type*.

It is clear that Q is of odd type if it is commutative or if it is a CIP loop. WIP loops are those loops Q for which $\mathbf{l}(Q) = \mathbf{r}(Q)$, and so noncommutative WIP loops are of even type, by Proposition 3.6.

The nonregular groups of Proposition 3.7 are of odd type in cases (1) and (2), and of even type in case (3).

Suppose that $\mathbf{I}(Q)$ is regular noncommutative (Proposition 3.9). If it is infinite, then it is of even type, and that is also true in the finite case if 4 divides $|\mathcal{I}(Q| = |\mathbf{I}(Q)|$. The remaining cases are of odd type.

We thus know when Q is of odd or even type in all cases. Using Proposition 3.5 it is easy to verify that our results can be formulated in the following compact way:

Theorem 5.6. *A loop Q is of odd type if $\mathcal{I}(Q)$ contains a commutative loop or if there exists $k \in \mathbb{Z}$ such that $I^{2k+1} \in \mathrm{Aut}(Q)$.*

We can thus restate Theorem 4.7 as: *If a loop is of odd type, then the centre and the nucleus coincide.*

Lemma 5.7. *A loop Q is of odd type if and only if the actions of $\mathbf{l}$ and $\mathbf{r}$ generate the group $\mathbf{I}(Q)$.*

Proof: If $\mathbf{I}(Q)$ is regular, then there is nothing to prove. So it suffices to verify that $\mathbf{l}$ and $\mathbf{r}$ generate $\mathbf{I}(Q)$ in cases (1) and (2) of Proposition 3.7. That is easy. □

The characterization of odd type loops in Theorem 5.6 gives immediately:

Corollary 5.8. *A subloop or a factorloop of an odd type loop is an odd type loop.*

Proposition 5.9. *Let Q be an odd type loop. Suppose that $V \leq U \leq Q$ are subloops such that $V \trianglelefteq U$ and that U/V is an IP loop. Then U/V is commutative.*

Proof: The loop U/V is of an odd type by Corollary 5.8. Hence $\mathbf{I}(U/V)$ is generated by $\mathbf{l}$ and $\mathbf{r}$, by Lemma 5.7. Since we are assuming $\mathbf{l}(U/V) = \mathbf{r}(U/V) = U/V$, the set $\mathcal{I}(U/V)$ has to contain only one element. Thus $\mathbf{o}(U/V) = U/V$. □

6. Isostrophical varieties

Sometimes it is useful to denote a quasigroup operation by a letter instead of by a binary operator. If $Q(A)$ is a quasigroup, then by A_π we shall denote the π parastrophe. (This is an ad hoc notation that will be used only in the first part of this section.) Thus $A = A_{\mathrm{id}}$, and if $A(x,y) = x \cdot y$, then $A_{(2\ 3)}(x,y) = x\backslash y$, $A_{(1\ 3)}(x,y) = x/y$ etc. We have $A_\pi(a_1,a_2) = a_3 \Leftrightarrow A(a_{\pi(1)}, a_{\pi(2)}) = a_{\pi(3)}$, which we record in the form

$$A_\pi(a_{\sigma(1)}, a_{\sigma(2)}) = a_{\sigma(3)} \ \Leftrightarrow\ A(a_{\sigma\pi(1)}, a_{\sigma\pi(2)}) = a_{\sigma\pi(3)}.$$

Lemma 6.1. *Suppose that $f = (\sigma, \alpha) : Q(A) \to S(B)$ is a paratopism. Then $B(x,y) = \alpha_{\sigma^{-1}(3)}(A_\sigma(\alpha^{-1}_{\sigma^{-1}(1)}(x), \alpha^{-1}_{\sigma^{-1}(2)}(y)))$. If $\tau \in S_3$, then*

$$B_\tau(x,y) = \alpha_{\sigma^{-1}\tau^{-1}(3)}(A_{\tau\sigma}(\alpha^{-1}_{\sigma^{-1}\tau^{-1}(1)}(x), \alpha^{-1}_{\sigma^{-1}\tau^{-1}(2)}(y))).$$

Proof: The fact that f is a paratopism can be expressed by

$$B_\tau(\alpha_{\sigma^{-1}\tau^{-1}(1)}(a_{\sigma^{-1}\tau^{-1}(1)}), \alpha_{\sigma^{-1}\tau^{-1}(2)}(a_{\sigma\tau^{-1}(2)})) = \alpha_{\sigma^{-1}\tau^{-1}(3)}(a_{\sigma^{-1}\tau^{-1}(3)})$$

as $(\sigma^{-1}\tau^{-1})\tau = \sigma$. Set $x = \alpha_{\sigma^{-1}\tau^{-1}(1)}(a_{\sigma^{-1}\tau^{-1}(1)})$ and $y = \alpha_{\sigma^{-1}\tau^{-1}(2)}(a_{\sigma^{-1}\tau^{-1}(2)})$. Our formula states that $B_\tau(x,y) = \alpha_{\sigma^{-1}\tau^{-1}(3)}(z)$, where $z = a_{\sigma^{-1}\tau^{-1}(3)}$ is equal to $A_{\tau\sigma}(a_{\sigma^{-1}\tau^{-1}(1)}, a_{\alpha^{-1}\sigma^{-1}\tau^{-1}(2)})$. By the choice of x, $a_{\sigma^{-1}\tau^{-1}(1)} = \alpha^{-1}_{\sigma^{-1}\tau^{-1}(1)}(x)$. The second argument depends upon y in a similar way, and that gives the required expression of $B_\tau(x,y)$. □

The above lemma is nothing else, but a formal verification that if $f = (\sigma, \alpha)$ is a paratopism, then α is an isotopism to the σ^{-1} parastrophe of the target quasigroup — a fact that has been mentioned in Section 2. Since the operation B depends fully upon f and A, we can denote it by $f(A)$. Note that Table 2 tabulates $f(A)$ for the all possible values of σ.

Lemma 6.2. *Suppose that $f : Q_1 \to Q_2$ and $g : Q_2 \to Q_3$ are paratopisms. Denote the quasigroup operation of Q_1 by A. Then the quasigroup operation of Q_3 can be expressed both as $g(f(A))$ and as $(gf)(A)$.*

Proof: Since gf is a paratopism $Q_1 \to Q_3$, the operation of Q_3 is equal to $(gf)(A)$. However, it is also equal to $g(B)$, where $B = f(A)$ is the operation of Q_2. □

Lemma 6.3. *Consider a free loop $F(X)$. Then $\mathbf{f}(F(X))$ is also a free loop with base X, for every $f \in \mathbf{I}$.*

Proof: Every loop can be expressed as $\mathbf{f}(Q)$, for some loop Q. A mapping $\varphi : X \to Q$ can be extended to a (unique) loop homomorphism $\psi : F(X) \to Q$. By term equivalence, a mapping $\psi : F(X) \to Q$ is a homomorphism if and only if it is a homomorphism $\mathbf{f}(F(X)) \to \mathbf{f}(Q)$. □

Suppose now that $X = \{x_1, x_2, \dots\}$. By Lemma 6.3 there exists a unique loop homomorphism $\mathbf{f}^* : F(X) \to \mathbf{f}(F(X))$ such that $\mathbf{f}^*(x_i) = x_i$ for every $i \geq 1$. To compute $\mathbf{f}^*(t)$ for a term t use either Lemma 6.1 or Table 2. Note that $\mathbf{f}^*$ is a mapping from $F(X)$ to $F(X)$, and hence it maps a reduced loop term upon a reduced loop term.

Lemma 6.4. *If $\mathbf{f}, \mathbf{g} \in \mathbf{I}$, then $\mathbf{g}^*\mathbf{f}^* = (\mathbf{fg})^*$. In particular, $(\mathbf{f}^*)^{-1} = (\mathbf{f}^{-1})^*$.*

Proof: Denote the operation of $F(X)$ by A. Then $\mathbf{f}^* : F(X)(A) \to F(X)(\mathbf{f}(A))$ and $\mathbf{g}^* : F(X)(A) \to F(X)(\mathbf{g}(A))$ are loop homomorphisms. Hence
$\mathbf{g}^* : F(X)(\mathbf{f}(A)) \to F(X)(\mathbf{fg}(A))$ is also a loop homomorphism, and $\mathbf{g}^*\mathbf{f}^*$:

$F(X) \to F(X)(\mathbf{fg}(A))$ is a loop homomomorphism as well. This homomorphism is identical upon X, and hence it has to agree with $(\mathbf{fg})^*$. □

Lemma 6.5. *Suppose that Q is a loop, $\mathbf{f} \in \mathbf{I}$, $s, t = F(x_1, \dots, x_m)$ and that $a_1, \dots, a_m \in Q$. Then $s(a_1, \dots, a_m)$ is equal to $t(a_1, \dots, a_m)$ in $\mathbf{f}(Q)$ if and only if $(\mathbf{f}^*(s))(a_1, \dots, a_m)$ is equal to $(\mathbf{f}^*(t))(a_1, \dots, a_m)$ in Q.*

Proof: Put $F = F(x_1, \dots, x_m)$ and denote by ψ the homomorphism $F \to \mathbf{f}(Q)$ that sends x_i to a_i. Furthermore, denote by φ the homomorphism $\mathbf{f}(F) \to \mathbf{f}(Q)$ that sends x_i to a_i. The homomorphisms ψ and $\varphi\mathbf{f}^*$ agree upon $x_1, \dots, x_m$, and hence they agree everywhere. Since φ can be also interpreted as a homomorphism $\varphi : F \to Q$ we can write the equality $(\mathbf{f}^*(s))(a_1, \dots, a_m) = (\mathbf{f}^*(t))(a_1, \dots, a_m)$ (which is assumed to be true in Q) as $\varphi(\mathbf{f}^*(s)) = \varphi(\mathbf{f}^*(t))$. This is the same as $\psi(s) = \psi(t)$, and that means that $s(a_1, \dots, a_m) = t(a_1, \dots, a_m)$ in $\mathbf{f}(Q)$. □

Corollary 6.6. *Let $\mathcal{V}$ be a variety of loops and let $\mathbf{f} \in \mathbf{I}$. Then the class of all $\mathbf{f}(Q)$, $Q \in \mathcal{V}$ is also a variety of loops (we shall denote it by $\mathbf{f}(\mathcal{V})$). A law $s(x_1, \dots, x_n) = t(x_1, \dots, x_n)$ holds in $\mathbf{f}(\mathcal{V})$ if and only if the law $\mathbf{f}^*(s) = \mathbf{f}^*(t)$ holds in $\mathcal{V}$.*

Varieties $\mathcal{V}$ and $\mathbf{f}^*(\mathcal{V})$ are said to be *isostrophic*. By Lemma 3.4, $Q \cong \mathbf{s}^3(Q)$ for any loop Q. Hence $\mathbf{f}(\mathcal{V}) = \mathbf{fs}^{3k}(\mathcal{V})$. We see that S_3 acts upon varieties isostrophic to $\mathcal{V}$.

Corollary 6.7. *There are 1 or 2 or 3 or 6 varieties isostrophic to a variety $\mathcal{V}$. Every such variety is equal to $\mathcal{V}$ of $\mathbf{l}(\mathcal{V})$ or $\mathbf{r}(\mathcal{V})$, or it is a variety that is opposite to one of these three varieties.*

To describe isostrophic varieties it thus suffices to be able to express the multiplication and divisions in $\mathbf{o}(Q)$, $\mathbf{l}(Q)$, $\mathbf{r}(Q)$ and $\mathbf{r}(Q)$. We do so in Table 6.

loop	Q	$\mathbf{o}(Q)$	$\mathbf{l}(Q)$	$\mathbf{r}(Q)$
multiplication	xy	yx	$(1/x)\backslash y$	$x/(y\backslash 1)$
left division	$x\backslash y$	y/x	$(1/x)y$	$1/(y\backslash x)$
right division	x/y	$y\backslash x$	$(y/x)\backslash 1$	$x(y\backslash 1)$

Table 6. Operations in isostrophic loops

Proposition 6.8. *Assume $m \in \mathbb{Z}$. Every variety isostrophic to the variety of m-inverse loops is equal to that variety.*

Proof: A loop Q is m-inverse if it fulfils $J^{m+1}(x)J^m(yx) = J^m(y)$. The latter law is equivalent to $I^m(xy)I^{m+1}(x) = I^m(y)$ (cf. Section 3). Now, $\mathbf{o}^*(J^{m+1}(x)J^m(yx)) = I^m(xy)I^{m+1}(x)$ and $\mathbf{o}^*(J^m(y)) = I^m(y)$. Thus Q^{op} is also an m-inverse loop. The statement thus follows from Proposition 5.3. □

The variety of all loops that fulfill a law $s(x_1, \dots, x_m) = t(x_1, \dots, x_m)$ will be denoted by $\mathrm{Eq}[s(x_1, \dots, x_m) = t(x_1, \dots, x_m)]$. In formulas we shall use LIP, RIP etc. to describe the corresponding variety of loops. E.g. $\mathrm{LIP} = \mathrm{Eq}[(1/x)(xy) = y]$.

Lemma 6.9. *Suppose that* $\varepsilon, \eta \in \{-1, 1\}$. *Then:*

(i) $\mathrm{LIP} = \mathrm{Eq}[I^{\varepsilon}(x)(xy) = y] = \mathrm{Eq}[(x/y)(y/x) = 1]$;
(ii) $\mathrm{RIP} = \mathrm{Eq}[(yx)I^{\varepsilon}(x) = y] = \mathrm{Eq}[(x\backslash y)(y\backslash x) = 1]$; *and*
(iii) $\mathrm{AAIP} = \mathrm{Eq}[I^{\varepsilon}(x)I^{\eta}(y) = I(yx)] = \mathrm{Eq}[J^{\varepsilon}(x)J^{\eta}(y) = J(yx)]$.

Proof: In a LIP loop $I(x) = J(x)$ by Lemma 3.3. If $I(x)(xy) = y$ holds, then $y = 1$ yields $I(x)x = 1$, and so $I(x) = J(x)$ again. Now, $(x/y)(y/x) = 1$ is equivalent to $y/(xy) = x\backslash 1$, and that is $y = J(x)(xy)$.

In an AAIP loop $I(x) = J(x)$ by Lemma 3.3. If any of ε and η is equal to -1, then we get $I = J$ by setting $x = 1$ or $y = 1$. The rest is clear. □

From Corollary 6.6 and Table 6 we see that $\mathbf{l}^*(I(x)(xy)) = x\backslash(J(x)\backslash y)$. Since $x\backslash(J(x)\backslash y) = y$ if and only if $J(x)(xy) = y$ we see that $\mathbf{l}^*(\mathrm{LIP}) = \mathrm{LIP}$. Furthermore, $\mathbf{r}^*((x/y)(y/x)) = (xI(y))/I(y(I(x))$, and so $\mathbf{r}^*(\mathrm{LIP}) = \mathrm{Eq}[J(x)I(y) = I(yx)] = \mathrm{AAIP}$. In this way we obtain a direct proof for the following statement. The statement can be also derived from Proposition 3.7. We have chosen a direct proof to illustrate the concept of isostrophic varieties upon a well known and easy example.

Proposition 6.10. $\mathbf{r}^*(\mathrm{AAIP}) = \mathrm{LIP} = \mathbf{o}^*(\mathrm{RIP})$, $\mathbf{l}^*(\mathrm{AAIP}) = \mathrm{RIP} = \mathbf{o}^*(\mathrm{LIP})$, *and* $\mathbf{r}^*(\mathrm{LIP}) = \mathrm{AAIP} = \mathbf{l}^*(\mathrm{RIP})$. *Furthermore,* $\mathbf{l}^*(\mathrm{LIP}) = \mathrm{LIP}$, $\mathbf{r}^*(\mathrm{RIP}) = \mathrm{RIP}$, *and* $\mathbf{o}^*(\mathrm{AAIP}) = \mathrm{AAIP}$.

Every loop variety $\mathcal{V}$ contains a subvariety $\mathrm{Itp}(\mathcal{V})$ of loops Q such that every loop isotope of Q is in $\mathcal{V}$. Loops of this kind are called *isotopically invariant* or *universal* (with respect to $\mathcal{V}$). Note that $\mathrm{Itp}(\mathrm{Itp}(\mathcal{V})) = \mathrm{Itp}(\mathcal{V})$.

Proposition 6.11. *Let* $\mathcal{V}$ *and* $\mathcal{W}$ *be isostrophic varieties, with* $\mathcal{W} = \mathbf{f}(\mathcal{V})$, *where* $\mathbf{f} \in \mathbf{I}$. *Then* $\mathrm{Itp}(\mathcal{W}) = \mathbf{f}(\mathrm{Itp}(\mathcal{V}))$. *In particular, if* $\mathrm{Itp}(\mathcal{V}) = \mathcal{V}$, *then* $\mathrm{Itp}(\mathcal{W}) = \mathcal{W}$.

Proof: This follows from the fact that $\mathbf{f}$ maps classes of isotopes to classes of isotopes, by Proposition 5.2. □

It is well known (and easy to prove) that $\mathrm{Itp}\,\mathrm{Eq}[xy = yx]$ is the variety of abelian groups. If $\mathcal{V}$ is the variety of left cross-commutative loops (cf. Proposition 3.8), then $\mathrm{Itp}(\mathcal{V})$ is the variety of abelian groups again, by Proposition 6.11.

Put $\mathrm{lBol} = \mathrm{Itp}(\mathrm{LIP})$, $\mathrm{mBol} = \mathrm{Itp}(\mathrm{AAIP})$ and $\mathrm{rBol} = \mathrm{Itp}(\mathrm{RIP})$. Propositions 6.10 and 6.11 immediately yield:

Corollary 6.12. $\mathbf{r}^*(\mathrm{mBol}) = \mathrm{lBol} = \mathbf{o}^*(\mathrm{rBol})$, $\mathbf{l}^*(\mathrm{mBol}) = \mathrm{rBol} = \mathbf{o}^*(\mathrm{lBol})$, *and* $\mathbf{r}^*(\mathrm{lBol}) = \mathrm{mBol} = \mathbf{l}^*(\mathrm{rBol})$. *Furthermore,* $\mathbf{l}^*(\mathrm{lBol}) = \mathrm{lBol}$, $\mathbf{r}^*(\mathrm{rBol}) = \mathrm{rBol}$, *and* $\mathbf{o}^*(\mathrm{mBol}) = \mathrm{mBol}$.

Lemma 6.13. *Let* $\mathcal{V}$ *be a variety of loops such that* $Q \cong Q^{\mathrm{op}} \in \mathcal{V}$ *for every* $Q \in \mathcal{V}$. *Then* $\mathrm{Itp}(\mathcal{V})$ *consists of all loops* Q *such that the left isotope* $(x/e)y$ *belongs to* $\mathcal{V}$ *for every* $e \in Q$.

Proof: Suppose that a loop Q fulfils the condition of the statement. We need to show that a right isotope $x \cdot (e\backslash y)$ belongs to $\mathcal{V}$ as well, for every $e \in Q$. Fix e and consider an isomorphism $\varphi : Q \to Q^{\mathrm{op}}$. We get $\varphi(x(e\backslash y)) = (\varphi(y)/\varphi(e))\varphi(x)$. The right isotope is hence isomorphic to the opposite loop of a left isotope. Since the left isotope belongs to $\mathcal{V}$, the opposite loop has to belong to $\mathcal{V}$ as well. □

Lemma 6.14. *Let Q be a loop and $e \in Q$. Denote by S the left isotope $(x/e)y$. Then $J_S(x) = (e/x)e$ and $I_S(x) = (x/e)\backslash e$.*

Proof: This can be verified in a direct way. □

The first part of the next statement was formulated by Robinson as Theorem 3.1 of [23]. The second part seems to have appeared for the first time in Chapter XI of Belousov's book [6].

Proposition 6.15. *The variety* lBol *is equal to* $\mathrm{Eq}[x(y \cdot xz) = (x \cdot yx)z]$, rBol *is equal to* $\mathrm{Eq}[z(xy \cdot x) = (zx \cdot y)x]$. *Furthermore,* mBol *is equal to* $\mathrm{Eq}[(x/y)(z\backslash x) = (x/(zy))x] = \mathrm{Eq}[(x/y)(z\backslash x) = x((zy)\backslash x)]$.

Proof: By Corollary 6.12 it suffices to prove only the first equality in the each part of the statement since $\mathbf{o}(\mathrm{lBol}) = \mathrm{rBol}$ and $\mathbf{o}(\mathrm{mBol}) = \mathrm{mBol}$.

Denote by L_x the left translation $y \mapsto xy$. A loop Q has the LIP if and only if $L_y^{-1} \in \{L_x;\ x \in Q\}$ for each $y \in Q$ (i.e. the left translations are closed under inverses).

Let Q be a LIP loop. The left translations of a left principle isotope $(x/e)y$ are closed under inverses for any $e \in Q$. The left translations of a right principle isotope $x(f\backslash y)$ are closed under inverses if and only if for all $x, f \in Q$ there exists $z \in Q$ such that $(L_x L_f^{-1})^{-1} = L_z L_f^{-1}$. In such a case $L_z = L_f L_x^{-1} L_f$. Thus if $Q \in \mathrm{lBol}$, then for all $x, y \in Q$ there exists $z \in Q$ such that $L_x L_y L_x = L_z$, and so $x(y \cdot xw) = (x \cdot yx)w$ for all x, y, x, w. By plugging $y = 1/x$ we get the LI property, and hence the argument can be reversed.

From Proposition 6.10 and Lemma 6.13 it follows that $Q \in \mathrm{mBol}$ if and only if the loop $(x/e)y$ has the AAIP for every $e \in Q$. Fix e and denote the loop by S. From Lemma 6.14 we get $J_S(y) = (e/y)e$ and $I_S(ze) = z\backslash e$. From Lemma 6.9 it follows that S is an AAIP loop if and only if $(e/y)(z\backslash e) = (e/(zy))e$. □

It is usual to call elements of lBol, rBol and mBol *left, right* and *middle Bol* loops, respectively.

Let Q be a left Bol loop. Then $x\backslash y = x^{-1}y$ since it is a LIP loop. The operation of the middle Bol loop $\mathbf{r}(Q)$ can be thus expressed as x/y^{-1}. Gvaramija [11] notes that there is another expression: $y(y^{-1}x \cdot y)$. This follows from the fact that the left Bol identity gives $x/y = y^{-1}(yx \cdot y^{-1})$.

Syrbu [25], [26] gives further middle Bol loop identities. These identities differ only by rearranging the right hand side, when we put $u = zy$ and express $x(u\backslash x)$ (or $(x/u)x$) in an equivalent way. We shall finish this section by showing that this phenomenon can be explained by the properties of

$$\mathrm{Itp}\,\mathrm{Eq}[1/x = x\backslash 1] \supseteq \mathrm{lBol} \cup \mathrm{rBol}. \cup \mathrm{mBol}.$$

Lemma 6.16. *Every loop from the variety* $\operatorname{Itp}\operatorname{Eq}[1/x = x\backslash 1]$ *satisfies the laws* $(y/x)\backslash x = (x/y)x$ *and* $x/(x\backslash y) = x(y\backslash x)$.

Proof: Using Lemma 6.14 we obtain the identity $(x/e)\backslash e = (e/x)e$. The mirror law describes the coincidence of the left and right inverses in the right isotopes. □

Corollary 6.17. *The variety of middle Bol loops is equal to* $\operatorname{Eq}[(x/y)(z\backslash x) = ((zy)/x)\backslash x]$ *and to* $\operatorname{Eq}[(x/y)(z\backslash x) = x/(x\backslash(zy))]$.

Proof: With respect to Lemma 6.16 and Proposition 6.15 it suffices to show that the new identities imply the AAIP. However, that is immediate from Lemma 6.9 (set $x = 1$). □

7. Conclusions and open problems

Let $\mathcal{V}$ be a variety of loops. Say that Q_1 and Q_2 are *equivalent modulo* $\mathcal{V}$ if they are term equivalent and if t_1, t_2 and t_3 can be chosen in both directions (i.e. when passing from Q_1 to Q_2 and when passing from Q_2 to Q_1) in such a way that the equalities $x \cdot y = t_1(x, y)$, $x\backslash y = t_2(x, y)$ and $x/y = t_3(x, y)$ are true in $\mathcal{V}$.

In the variety of abelian groups any term can be evaluated as $ix + jy$, where $i, j \in \mathbb{Z}$. It is thus obvious that any two term equivalent abelian groups have to coincide (indeed, if $x \oplus y = ix + jy$ then $x = 0$ yields $j = 1$ and $y = 0$ yields $i = 1$). This means that any two term equivalent loops are equivalent modulo the abelian groups. This observation can be strengthened by noting that a term $t(x, y) \in F(x, y)$ can be simplified to $x^i \cdot s(y)$, $s \in F(y)$ if x is assumed to be central. If $Q(\circ)$ is such that $x \circ y = t(x, y)$ and if x central in $Q(\cdot)$, then $x \circ y = x^i \cdot s(y)$. In such a case we obtain $i = 1$ by setting $y = 1$, and $s(y) = y$ by setting $x = 1$. By working along these lines we see that the centers of two term equivalent loops always coincide. In view of Proposition 2.10 we hence come to this conclusion:

Proposition 7.1. *Term equivalent loops share both the upper and lower central series.*

Parallels between the commutative and the associative law do exist, but they are limited. This is well illustrated by the fact that the *nucleus* $N(Q) = N_\lambda(Q) \cap N_\mu(Q) \cap N_\rho(Q)$ need not be a normal subloop of Q, and so there is no direct analogue of central series that would be based not upon the notion of center, but upon the notion of the nucleus.

By Proposition 2.10 loops that are not only term equivalent, but also equivalent modulo the variety of groups (we shall also say that they are equivalent modulo associativity) share structures that can be defined via subloops and associativity. As an example take (the associator subloop) $A(Q)$, i.e. the smallest subloop $S \trianglelefteq Q$ such that Q/S is a group.

Loops Q and Q^{op} are not necessarily equivalent modulo associativity ($xy = yx$ does not hold in all groups). However, groups G and G^{op} are isomorphic via $x \mapsto x^{-1}$. Hence structures that are defined via subloops and the associativity are retained when passing from Q to Q^{op}. As an example let us mention again the associator subloop $A(Q)$. In fact, such structures are retained by any isostrophism as every loop is equivalent to its left (or right) inverse modulo the variety of IP loops. Hence any two elements of $\langle \mathbf{l}, \mathbf{r}\rangle(Q)$ are equivalent modulo the IP law (cf. Section 5).

LIP and RIP and AAIP loops satisfy $I = J$. The intersection of any two of the three named varieties is the variety of IP loops. There are many results on intersections of loop varieties. However, there seem to be practically no results on their joins. Hence we ask:

Problem 7.2. Let $\mathcal{V}$ be the least variety that contains all LIP loops, all RIP loops and all AAIP loops. Is the variety $\mathcal{V}$ equal to the variety of all loops in which $1/x = x\backslash 1$?

Let us note that an affirmative answer would imply, amongst others, that all commutative loops are in $\mathcal{V}$. A similar question can be stated for the associated varieties that are isotopically invariant:

Problem 7.3. Let $\mathcal{W}$ be the least variety that contains all left Bol loops, all right Bol loops and all middle Bol loops. Is the variety $\mathcal{W}$ equal to $\operatorname{Itp}\operatorname{Eq}[1/x = x\backslash 1]$?

Left Bol loops can be also obtained as isotopically invariant left alternative loops [23], i.e. lBol $= \operatorname{Itp}\operatorname{Eq}[x \cdot xy = xx \cdot y]$. In [25] Syrbu raised the question whether middle Bol loops correspond to isotopically invariant flexible loops (the law $x \cdot yx = xy \cdot x$). M. Kinyon found a middle Bol loop of order 16 that is not flexible (personal communication). According to him the following problem may be still open:

Problem 7.4. Let Q be a loop such that every isotope of Q is flexible and has the AAIP. Must Q be middle Bol?

Isotopically invariant CI loops are abelian groups [1] and isotopically invariant WIP loops have the property that Q/N is Moufang ($N = N(Q)$ is the nucleus and has to be a normal subloop) [21]. Classical papers of Artzy [2] and Osborn [21] contain a number of results on isotopes that are CI or WIP loops. It might be worth to reexamine their results and consider the possibility of generalizations to m-inverse loops.

In [14] Karklinš and Karkliň investigated a situation when a CI loop Q is not necessarily an isotopically invariant CI loop, but every of its isotopes is an m-inverse loop for some $m \in \mathbb{Z}$. They proved that then Q has to be an abelian group if m is even, and commutative Moufang loop if m is odd.

Onoĭ [20] gave an example of a $(2k+1)$-inverse loop that is isotopic to an IP loop and is not a WIP loop.

Buchsteiner loops are isotopically invariant [8] and hence they give an example of isotopically invariant 1-inverse loops (i.e. doubly WIP loops). No other class of algebraically interesting isotopically invariant m-inverse loops seems to be known.

The first noncommutative regular case of $\mathbf{I}(Q)$ is that of AIP loops that are neither commutative nor LIP nor RIP. In such a case $\mathbf{I}(Q)$ is equivalent (as a permutation group) to the regular representation of S_3. This could be regarded as an impetus to study the variety $\operatorname{Itp}\operatorname{Eq}[J(xy) = J(x)J(y)]$. Belousov's school paid certain attention to this variety in the past, e.g. [15], [5].

Acknowledgment. We thank M. Kinyon for several discussions on the topic of this paper and for sharing with us the construction of a nonflexible middle Bol loop. We also thank the anonymous referee for several useful suggestions and for pointing out the relevance of WCIP loops.

References

[1] Artzy R., *On loops with a special property*, Proc. Amer. Math. Soc. **6** (1955), 448–453.

[2] Artzy R., *Crossed-inverse and related loops*, Trans. Amer. Math. Soc. **91** (1959), 480–492.

[3] Artzy R., *Relations between loop identities*, Proc. Amer. Math. Soc. **11** (1960), 847–851.

[4] Artzy R., *Net motions and loops*, Arch. Math. (Basel) **14** (1963), 95–101.

[5] Basarab A.S., Belioglo A.I., *Universalno-avtomorfno-inversnye $\mathcal{G}$-lupy*, Mat. Issled. **51** (1979), 3–7.

[6] Belousov V.D., *Osnovy teorii kvazigrupp i lup*, Nauka, Moskva, 1967.

[7] Belousov V.D., *Vzaimmobratnye kvazigruppy i lupy*, Izvestiia Akademii nauk Moldavskoi SSR 1963, issue 11, 3–10.

[8] Csörgő P., Drápal A., Kinyon M.K., *Buchsteiner loops*, Internat. J. Algebra Comput. **19** (2009), 1049–1088.

[9] Evans T., *On multiplicative systems defined by generators and relations, I. Normal form theorems*, Proc. Cambridge Philos. Soc. **47** (1951), 637–649.

[10] Evans T., *On multiplicative systems defined by generators and relations, II. Monogenic loops*, Proc. Cambridge Philos. Soc. **49** (1953), 579–589.

[11] Gvaramija A.A., *Ob odnom klasse lup*, Moskov. Gos. Ped. Inst. Učen. Zap. No. 375 (1971), 25–34.

[12] Greer M., Kinyon M., *Pseudoautomorphisms of Bruck loops and their generalizations*, Comment. Math. Univ. Carolin. **53** (2012), no. 3, 383–389.

[13] Johnson K.W., Sharma B.L., *A variety of loops*, Ann. Soc. Sci. Bruxelles Sér. I **92** (1975), 25–41.

[14] Karkliňš B.B., Karkliň V.B., *Inversnyje lupy*, Mat. Issled. **39** (1976), 87–101.

[15] Karkliňš B.B., Karkliň V.B., *Universalno-avtomorfno-inversnyje lupy*, Mat. Issled. **39** (1976), 82–86.

[16] Keedwell A.D., *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin. **20** (1999), 241–250.

[17] Keedwell A.D., Shcherbacov V.A., *On m-inverse loops and quasigroups with a long inverse cycle*, Australas. J. Combin. **26** (2002), 99–119.

[18] Keedwell A.D., Shcherbacov V.A., *Construction and properties of (r,s,t)-inverse quasigroups. I*, Discrete Math. **266** (2003), 275–291.

[19] Keedwell A.D., Shcherbacov V.A., *Construction and properties of (r,s,t)-inverse quasigroups. II*, Discrete Math. **288** (2004), 61–71.

[20] Onoĭ V.I., *Solution of a problem on inverse loops* (Russian), General algebra and discrete geometry **161** (1980), 53–58.

[21] Osborn J.M., *Loops with weak inverse properties*, Pacific J. Math. **10** (1960), 295–304.

[22] Pflugfelder H.O., *Quasigroups and Loops: Introduction*, Helderman, Berlin, 1990.

[23] Robinson D.A., *Bol loops*, Trans. Amer. Math. Soc. **123** (1966), 341–354.

[24] Sade A., *Paratopie et autoparatopie des quasigroupes*, Ann. Soc. Sci. Bruxelles Sér. I **76** (1962), 88–96.
[25] Syrbu P., *Loops with universal elasticity*, Quasigroups Related Systems **1** (1994), 57–65.
[26] Syrbu P., *On middle Bol loops*, ROMAI J. **6** (2010), 229–236.

Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 186 75 Prague 8, Czech Republic

E-mail: drapal@karlin.mff.cuni.cz

Institute of Mathematics and CS, Academy of Sciences of Moldova, Academiei 5, MD 2028, Chişinâu, Moldova

E-mail: scerb@math.md

(*Received* March 15, 2012, *revised* May 14, 2012)