This is the final preprint version of a paper which has appeared in
Communications in Algebra **49** (2021) 2516-2537,
https://doi.org/10.1080/00927872.2021.1874400 .

ON CORE QUANDLES OF GROUPS

GEORGE M. BERGMAN

Abstract. We review the definition of a *quandle,* and in particular of the *core quandle* $\mathrm{Core}(G)$ of a group G, which consists of the underlying set of G, with the binary operation $x \lhd y = xy^{-1}x$. This is an *involutory* quandle, i.e., satisfies the identity $x \lhd (x \lhd y) = y$ in addition to the other identities defining a quandle.

Trajectories $(x_i)_{i\in\mathbb{Z}}$ in groups and in involutory quandles (in the former context, sequences of the form $x_i = xz^i$ $(x, z \in G)$ among other characterizations; in the latter, sequences satisfying $x_{i+1} = x_i \lhd x_{i-1}$) are examined. A family of necessary conditions for an involutory quandle Q to be embeddable in the core quandle of a group is noted. Some implications are established between identities holding in groups and in their core quandles. Upper and lower bounds are obtained on the number of elements needed to generate the quandle $\mathrm{Core}(G)$ for G a finitely generated group. Several questions are posed.

1. Background

The concept of quandle arose in knot theory, as a way of studying knot groups in terms of their conjugation operation. If for G a group one defines

(1.1) $\quad x \lhd y \ = \ x\,y\,x^{-1} \ \ (x, y \in G),$

and denotes by Q the underlying set of G with this operation, one finds that

(1.2) For all $x \in Q$, $x \lhd x \ = \ x$.

(1.3) For all $x \in Q$, the map $y \mapsto x \lhd y$ is a bijection $Q \to Q$.

(1.4) For all $x, y, z \in Q$, $x \lhd (y \lhd z) \ = \ (x \lhd y) \lhd (x \lhd z)$. In other words, for all $x \in Q$, the map $y \mapsto x \lhd y$ is an endomorphism of $(Q, \lhd)$.

More generally, for any integer d, (1.2)-(1.4) hold for the operation on a group G given by

(1.5) $\quad x \lhd y \ = \ x^d\,y\,x^{-d} \ \ (x, y \in G).$

There is one more derived operation on groups G for which (1.2)-(1.4) hold, which has been studied less (though it too has been used in knot theory [9]), but is the main subject of this note; namely

(1.6) $\quad x \lhd y \ = \ x\,y^{-1}\,x \ \ (x, y \in G).$

This last operation also satisfies the identity

(1.7) For all $x, y \in Q$, $x \lhd (x \lhd y) \ = \ y$.

Here is the terminology used for the above sorts of structures (though formalizations and notations vary).

Definition 1.1 (cf. [8], [4], [10])**.** *A* quandle *is a set Q given with a binary operation $\lhd:\ Q^2 \to Q$ satisfying* (1.2), (1.3) *and* (1.4). *A quandle is said to be* involutory *if it also satisfies* (1.7).

If G is a group, then the quandle given by the underlying set of G with the operation (1.1) *is denoted* $\mathrm{Conj}(G)$, *while the (involutory) quandle given by the same set with the operation* (1.6) *is denoted* $\mathrm{Core}(G)$.

2020 *Mathematics Subject Classification.* Primary: 08B99, 20F99, 20N02, 57K12. Secondary: 20F18.

Key words and phrases. Involutory quandle; core quandle of a group; identities in groups and quandles; generating numbers of groups and quandles.

Archived at http://arxiv.org/abs/2006.00641 . After publication, any updates, errata, related references, etc., found will be recorded at http://math.berkeley.edu/~gbergman/papers/.

(Instead of "involutory", the form "involutive" is sometimes used.)

The above terminology was introduced, and many results on quandles developed, in [8]. (See the Introduction to that paper for notes on earlier literature that considered cases of the concept, and cf. also [10].) It is shown in [2, Proposition 3.1] that the operations (1.5) for all $d \in \mathbb{Z}$, and the lone additional operation (1.6), are in fact the only derived group operations that give quandle structures on the underlying sets of all groups G.

My own path to the construction that I subsequently learned is called $\mathrm{Core}(G)$ involved conditions on a group G related to one-sided orderability. Here, sequences of group elements of the form

(1.8) $\quad (x\,z^i)_{i\in\mathbb{Z}} \quad (x, z \in G)$

seemed important. (I will not mention orderability after this paragraph, but for those conversant with the subject, a condition on G weaker than one-sided orderability, called "locally invariant orderability" [5], is equivalent to the existence of a total ordering on the underlying set of G under which each sequence (1.8) is either monotone increasing, monotone decreasing, or decreasing up to a certain point and increasing thereafter. An intermediate condition is, of course, the existence of an ordering under which every sequence (1.8) is monotone increasing or decreasing. Whether one or the other of the implications from one-sided orderability to the latter property to the former is reversible, is not known.) Calling a sequence of the form (1.8) in a group a "trajectory", one sees that trajectories can also be characterized as the sequences $(x_i)_{i\in\mathbb{Z}}$ such that for all i, $x_{i+1} = x_i\,x_{i-1}^{-1}\,x_i$; equivalently, $x_{i-1} = x_i\,x_{i+1}^{-1}\,x_i$. Though I never got anywhere with using them to study orderability, I found the concept of trajectory and the properties of the operation (1.6) that underlies it intriguing. I eventually learned that the kind of structure I was looking at had already been named, as described above.

A disadvantage of condition (1.3) of Definition 1.1 is that it is not expressed by identities. To do that, one can introduce a second binary operation (written $y \rhd x$, or $x \lhd^{-1} y$) which inverts the effect of $x \lhd$. This gives another commonly used formulation of the concept of quandle. However, I have used Definition 1.1 here because in the case of involutory quandles, (1.3) is implied by (1.7), and hence can be dropped, with no additional operation needed.

Let us also note that in the presence of (1.7), the identity of (1.4) is equivalent to the identity gotten by replacing z everywhere in it by $x \lhd z$, applying (1.7) to the resulting occurrence of $x \lhd (x \lhd z)$, and interchanging the two sides:

(1.9) $\quad$ For all $x, y, z \in Q$, $\;(x \lhd y) \lhd z \;=\; x \lhd (y \lhd (x \lhd z))$.

This formula will prove useful in that it allows us to reduce any $\lhd$-expression to one in which parentheses are clustered to the right.

Summarizing, we have

Lemma 1.2. *An involutory quandle can be characterized as a set* Q *given with a binary operation* $\lhd$ *satisfying* (1.2), (1.7) *and* (1.9). □

We note for later reference the easily checked result:

Lemma 1.3. *If* G *is a group, then the following sorts of permutations of the underlying set of* G*, defined in terms of the group structure of* G*, give automorphisms of the involutory quandle* $\mathrm{Core}(G)$.

(i) *For every* $g \in G$*, the map* $x \mapsto x\,g$.

(ii) *For every* $h \in G$*, the map* $x \mapsto h\,x$.

(iii) *The map* $x \mapsto x^{-1}$. □

2. A normal form for free involutory quandles

Let us now prove

Theorem 2.1. *The identities satisfied by the derived operation* (1.6) *on all groups are precisely the consequences of* (1.2), (1.7) *and* (1.9).

Any word in a set of symbols X *and the operation-symbol* $\lhd$ *can be reduced, using these identities, to a unique expression*

(2.1) $\quad x_0 \lhd (x_1 \lhd (\cdots \lhd (x_{n-1} \lhd x_n)\ldots))$ *(with parentheses clustered on the right), where all* $x_i \in X$*, and no two successive arguments* x_i, x_{i+1} *are the same.*

Thus, the expressions (2.1) *give a normal form for elements of the free involutory quandle on* X.

Proof. The verification of (1.2), (1.7) and (1.9) for the operation (1.6) is immediate. Postponing the claim that those three identities imply all identities satisfied by that derived operation, we note that given any word in $\lhd$ and symbols from X, (1.9) can indeed be used recursively to reduce it to one in which parentheses are clustered to the right. (To see formally that recursive application of (1.9) must terminate, let us define the *implicit length* of a $\lhd$-word w in symbols from X by letting the implicit length of each $x \in X$ be 1, and the implicit length of a word $w_1 \lhd w_2$ be the implicit length of w_2, plus twice the implicit length of w_1. We find that any application of (1.9) to a subword of a $\lhd$-word leaves the word's implicit length unchanged, but increases its length (number of occurrences of variable-symbols); so, since the length is bounded above by the implicit length, the process must terminate.) We can, next, use (1.7) recursively to eliminate cases where $x_i = x_{i+1}$ for $i < n-1$, and, finally, use (1.2) recursively to eliminate cases where $x_{n-1} = x_n$, giving a word of the form (2.1).

To show uniqueness, note that given elements $x_0, \ldots, x_n$ in a group G, the expression in (2.1), evaluated in $\mathrm{Core}(G)$, describes the group element

$$(2.2) \qquad x_0\, x_1^{-1}\, x_2 \ldots x_{n-1}^{\mp 1}\, x_n^{\pm 1}\, x_{n-1}^{\mp 1} \ldots x_2\, x_1^{-1}\, x_0.$$

Now if we take for G the free group on the elements of X, then by the condition in (2.1) that no two successive x_i be equal, (2.2) is a reduced word in that free group, whose value in that group determines the sequence $x_0, \ldots, x_n$. So starting with an arbitrary $\lhd$-word in the elements of X, any two expressions of the form (2.1) obtainable from it using (1.2), (1.7) and (1.9) must be the same, which is the desired uniqueness statement.

Returning to the claim whose verification we postponed, suppose $u = v$ is an identity satisfied by $\lhd$ in all groups. Applying (1.2), (1.7) and (1.9) as above, we can reduce u and v to words of the form (2.1). Since we have assumed $u = v$ to hold identically in core quandles of groups, the reduced expressions have, in particular, the same value in the core quandle of the free group on X; so by the above uniqueness result, they must be the same. So the equality $u = v$ is indeed a consequence of (1.2), (1.7) and (1.9). □

This immediately yields the first assertion of

Proposition 2.2. *Let X be a nonempty set. Then the elements of the free group $\langle X \rangle$ of the form* (2.2)*, i.e., the symmetric reduced group words of odd length in the elements of X, in which the exponents alternate between $+1$ and -1, starting with the former, form a subquandle of* $\mathrm{Core}(\langle X \rangle)$ *which is a free involutory quandle on X.*

On the other hand, fixing an element y of X, the set of all *symmetric reduced group words in $X - \{y\}$ (including the empty word 1, and with no condition of odd length or alternating exponents) forms a subquandle of* $\mathrm{Core}(\langle X - \{y\} \rangle)$ *which is a free involutory quandle on the set $X - \{y\} \cup \{1\}$.*

Proof. The assertion of the first paragraph follows from the proof of Theorem 2.1. To deduce the second paragraph, note that by Lemma 1.3(i), the endomap

$$(2.3) \qquad w \;\mapsto\; w y^{-1}$$

of the underlying set of $\langle X \rangle$ is an automorphism of $\mathrm{Core}(\langle X \rangle)$; hence a free involutory subquandle of $\mathrm{Core}(\langle X \rangle)$ is also generated by the elements xy^{-1} $(x \in X)$. Now the elements xy^{-1} $(x \in X - \{y\})$ form a free generating set of a subgroup of $\langle X \rangle$, and that subgroup, of course, also contains $yy^{-1} = 1$, hence it contains our translated free involutory quandle. If we map this free subgroup into $\langle X \rangle$ by sending each free generator xy^{-1} $(x \in X - \{y\})$ to x, we get an isomorphism of that subgroup with $\langle X - \{y\} \rangle$, and we see that the isomorphism of free involutory quandles given by our translation followed by this map fixes each member of $X - \{y\}$, and sends y to 1.

I now claim that the result of applying this quandle isomorphism to all reduced words of the form (2.2) is the set of all symmetric reduced group words in $X - \{y\}$. Indeed, given a symmetric reduced word u in $X - \{y\}$, we may obtain a w as in (2.2) which maps to it as follows. On the one hand, if u begins (and hence ends) with a symbol having exponent -1, append a y at the beginning and a y the end. Further, wherever u has two successive variable-symbols with the same exponent $+1$ or -1, insert a y with the opposite exponent between them. (In particular, if u has positive *even* length, a y or y^{-1} is inserted in the middle.) Finally, if $u = 1$, let $w = y$.

That the resulting word w has the form (2.2), and is mapped to u under the isomorphism described, is immediate. □

In the proof of Theorem 2.1, we used the identity (1.9) to bring words to a form with parentheses clustered to the right. It is helpful to note a consequence of that identity (of which (1.9) itself is the $n = 2$ case), which describes how such a right-clustered expression acts by $\lhd$.

(2.4) $$x_1 \lhd (x_2 \lhd (\cdots \lhd (x_{n-1} \lhd x_n) \ldots)) \lhd y \ = \\ x_1 \lhd (x_2 \lhd (\cdots \lhd (x_{n-1} \lhd (x_n \lhd (x_{n-1} \lhd (\cdots \lhd (x_2 \lhd (x_1 \lhd y)) \ldots)))) \ldots)).$$

This is straightforward to check in a quandle of the form $\mathrm{Core}(G)$, using the definition (1.6), and the fact that a quandle expression (2.1) corresponds to the group expression (2.2). From this, the same result for a general involutory quandle Q follows by the first statement of Theorem 2.1, since that says that identities holding in every quandle $\mathrm{Core}(G)$ hold in *all* involutory quandles. Alternatively, one can prove (2.4) inductively from (1.9).

3. Trajectories in involutory quandles

As mentioned, I was led to the topic of this note by thinking about *trajectories* in groups G, that is, sequences of the form $(x\,z^i)_{i\in\mathbb{Z}}$ $(x, z \in G)$, equivalently, sequences $(x_i)_{i\in\mathbb{Z}}$ satisfying $x_{i+1} = x_i\, x_{i-1}^{-1}\, x_i$. (It is easy to see that these can also be described as sequences of the form $(w^i\, x)_{i\in\mathbb{Z}}$ $(w, x \in G)$, or more generally, as sequences of the form $(x\, y^i\, x')$ $(x, y, x' \in G)$. In the first two sorts of expression, x and z, respectively w and x, are clearly unique, while in the last, x, y and x' can be replaced by xu, $u^{-1}yu$, $u^{-1}x'$ for any $u \in G$.) Noting the form such a sequence takes in the quandle $Q = \mathrm{Core}(G)$, and abstracting to general involutory quandles, we make

Definition 3.1. *If Q is an involutory quandle, then a sequence $(x_i)_{i\in\mathbb{Z}}$ of elements of Q will be called a* trajectory *in Q if it satisfies*

(3.1) $$x_{i+1} \ = \ x_i \lhd x_{i-1} \quad \text{for all } i \in \mathbb{Z},$$

equivalently (*as one sees by applying $x_i\lhd$ to both sides of* (3.1)), *if*

(3.2) $$x_{i-1} \ = \ x_i \lhd x_{i+1} \quad \text{for all } i \in \mathbb{Z}.$$

In particular, if G is a group, the sequences of elements that are trajectories in the involutory quandle $\mathrm{Core}(G)$ *are precisely those that are trajectories in the group-theoretic sense in G.*

(What we are calling trajectories in an involutory quandle are roughly what are called "geodesics" in [8, §11]; except that there, after involutory quandles have been defined, the concept of a set Q with geodesics is defined independently, and then shown to yield a structure of involutory quandle on Q.)

If $(x_i)_{i\in\mathbb{Z}}$ is a trajectory in a group, then letting $x = x_0$, $y = x_1$, we see that

(3.3) $$x_i \ = \ x\,(x^{-1}y)^i.$$

Given a trajectory $(x_i)_{i\in\mathbb{Z}}$ in an involutory quandle Q, we can likewise, using (3.1) and (3.2), write all x_i in terms of $x = x_0$ and $y = x_1$, though the description is not as simple as (3.3). Let me just list the forms of x_{-3} through x_4, from which the pattern is clear.

(3.4) $$\begin{array}{l} \quad\ \ldots \\ x_{-3} = \ x \lhd (y \lhd (x \lhd y)) \\ x_{-2} = \ x \lhd (y \lhd x) \\ x_{-1} = \ x \lhd y \\ x_0 \ = \ x \\ x_1 \ = \ y \\ x_2 \ = \ y \lhd x \\ x_3 \ = \ y \lhd (x \lhd y) \\ x_4 \ = \ y \lhd (x \lhd (y \lhd x)) \\ \quad\ \ldots \end{array}$$

Again, this family of formulas can be proved either by establishing them in quandles $\mathrm{Core}(G)$, where they are translations of the corresponding cases of (3.3), or by direct computation (in which case (2.4) is helpful). A generalization of (3.1) and (3.2), which can likewise be shown in either of these ways to hold in trajectories $(x_i)_{i\in\mathbb{Z}}$ in involutory quandles, is

(3.5) $$x_i \lhd x_j \ = \ x_{2i-j} \quad \text{for all } i, j \in \mathbb{Z}.$$

Returning to (3.4), note that the expressions on the right are precisely the reduced expressions (2.1) for the elements of the subquandle of Q generated by x and y; so a trajectory is a certain enumeration of a 2-generator subquandle. Let us prove

Proposition 3.2. *Let $(x_i)_{i\in\mathbb{Z}}$ be a trajectory in an involutory quandle Q. Then the following conditions are equivalent:*

(i) *The subquandle $\{x_i \mid i\in\mathbb{Z}\}$ of Q is free on the generators $x_0,\ x_1$.*

(ii) *All x_i are distinct.*

(iii) *$\{x_i \mid i\in\mathbb{Z}\}$ is infinite.*

Proof. The equivalence of (i) and (ii) follows from the last assertion of Theorem 2.1 in view of the enumeration (3.4). The implication (ii) $\Longrightarrow$ (iii) is immediate; to complete the proof, it will suffice to prove $\neg$ (ii) $\Longrightarrow \neg$ (iii). So suppose that for some $i\in\mathbb{Z}$ and $m>0$ we have

(3.6) $\quad x_i \;=\; x_{i+m}.$

For any j, (3.6) implies $x_i \lhd x_{2i-j} = x_{i+m} \lhd x_{2i-j}$, which by (3.5) translates to

(3.7) $\quad x_j \;=\; x_{j+2m}\,;$

so our trajectory is periodic, proving $\neg$ (iii). □

When a trajectory satisfies the equivalent conditions of Proposition 3.2, we see that for each $n\geq 1$, the number of terms whose normal forms, shown in (3.4), have length (number of variable-symbols) $\leq n$ is exactly $2n$. So intuitively, an infinite trajectory "grows linearly". Curiously, this is not true if we allow non-reduced expressions.

Proposition 3.3. *Let $(x_i)_{i\in\mathbb{Z}}$ be a trajectory in an involutory quandle. Then for every positive integer n, the following sets are equal.*

The set A_n of elements expressible by arbitrary $\lhd$-words of length $\leq n$ in x_0 and x_1.

The set B_n of elements expressible by $\lhd$-words of length exactly n in x_0 and x_1, with parentheses clustered on the left.

The set $C_n = \{x_i \mid -2^{n-1} < i \leq 2^{n-1}\}$.

Thus, if the trajectory $(x_i)_{i\in\mathbb{Z}}$ is infinite, then for each n, the common value of these sets has cardinality 2^n.

Proof. Trivially, $A_1 = B_1 = C_1 = \{x_0,\, x_1\}$; so let $n>1$, and let us inductively assume the desired result for all lower n.

Note that by definition, $B_n = (B_{n-1}\lhd x_0)\cup(B_{n-1}\lhd x_1)$. (Here and below, a formula having a set as one or both arguments of $\lhd$ denotes the set of outputs obtained using elements of the indicated input-set(s).) With the help of (3.5) we likewise see that $C_n = (C_{n-1}\lhd x_0)\cup(C_{n-1}\lhd x_1)$. (Indeed, $C_{n-1}\lhd x_0$ consists of all x_i with even i in the indicated range, and $C_{n-1}\lhd x_1$ of all x_i with odd i in that range.) Hence $B_n = C_n$ for all n.

By definition, $A_n\supseteq B_n$, so it will suffice to show that $A_n\subseteq C_n$. For $n>1$, all elements of A_n that do not already lie in A_{n-1} must be members of sets $A_{n-m}\lhd A_m$ with $1\leq m<n$. If $m=1$, then by the inductive assumption that $A_{n-1}=C_{n-1}$, we are in exactly the case of the preceding paragraph, and again get the elements of C_n. If $2\leq m<n$, our inductive hypothesis implies that the elements x_i of our trajectory that lie in A_{n-m} satisfy $-2^{n-3}<i\leq 2^{n-3}$ (since $m\geq 2$), while the x_j that lie in A_m satisfy $-2^{n-2}<j\leq 2^{n-2}$ (since $m\leq n-1$), whence the subscript $2i-j$ of $x_i\lhd x_j \;=\; x_{2i-j}$ will satisfy $-2^{n-1}<2i-j<2^{n-1}$, so in this case too, that element will lie in C_n.

The final assertion is clear, given Proposition 3.2 (iii) $\Longrightarrow$ (i). □

Using the fact that in groups, trajectories have the form $(x\,z^i)_{i\in\mathbb{Z}}$, we can get information about a group G from $\mathrm{Core}(G)$:

Lemma 3.4. *Given elements x and w of a group G, and an integer n, one can determine from the structure of* $\mathrm{Core}(G)$ *whether $x^{-1}w$ is an n-th power in G. Namely, this will hold if and only if there exists a trajectory $(x_i)_{i\in\mathbb{Z}}$ in* $\mathrm{Core}(G)$ *with $x_0=x$ and $x_n=w$; equivalently, if and only if there exists $y\in\mathrm{Core}(G)$ such that w is given by the formula for x_n as in* (3.4). □

It follows in turn that we can tell from $\mathrm{Core}(G)$ whether $x^{-1}w$ is, say, a product of squares in G, since this is equivalent to the existence of a sequence of elements $x=x_{(0)}, x_{(1)}, \ldots, x_{(n)}=w$ with each $x_{(n-1)}^{-1}x_{(n)}$ a square. Likewise, we see that the structure of $\mathrm{Core}(G)$ determines whether a property such as "every product of squares is a square", or "every product of two distinct squares in G has cube the identity" holds in the group G. On the other hand, we shall see in Lemma 7.4 that one cannot always tell from the structure of $\mathrm{Core}(G)$ whether G is abelian.

4. Orbits of involutory quandles

A very degenerate class of quandles $\mathrm{Core}(G)$ is noted in

Lemma 4.1. *If G is a group, then the identity*

(4.1) *For all* $x, y \in G,\ \ x \lhd y \ = \ y$

holds in $\mathrm{Core}(G)$ *if and only if G satisfies the identity $x^2 = 1$, i.e., has exponent* 2.

Proof. Condition (4.1) translates to the group-theoretic identity $x\,y^{-1}x = y$, equivalently, $(x\,y^{-1})^2 = 1$, which clearly holds for all $x, y \in G$ if and only if $x^2 = 1$ for all $x \in G$. □

If an involutory quandle T satisfies (4.1), then, of course, every subset of T is a subquandle. Hence given a homomorphism from an involutory quandle Q to such a T, the inverse image of every subset of T is a subquandle of Q.

Every involutory quandle Q has a universal homomorphic image satisfying (4.1), whose elements are the equivalence classes of elements of Q under the quandle congruence $\sim$ generated by relations

(4.2) $x \lhd y \ \sim \ y \quad (x, y \in Q).$

With the help of (1.7) it is easy to show that this congruence has the form

(4.3) $x \sim y \iff (\exists\, z_1, \ldots, z_n \in Q)\ \ y = z_1 \lhd (\cdots \lhd (z_n \lhd x)\ldots).$

These equivalence classes are called the *orbits* of Q. (The term is used, more generally, in [1] for the equivalence classes in not necessarily involutory quandles determined by the equivalence relation generated by (4.2).) We see that the union of any family of orbits is a subquandle of Q.

However, in contrast to the case described in Lemma 4.1, the structure of a general quandle Q is not determined by the separate quandle structures of its orbits: Though each map $x \lhd -\ \ (x \in Q)$ takes every orbit Q_0 of Q into itself, if x is not in Q_0, the involution $x \lhd -$ on Q_0 carries information not determined by the $\lhd$-structure of Q_0.

Instead of constructing subquandles Q' of Q by letting each orbit of Q either wholly belong to Q' or be wholly absent, can we put together a Q' by choosing subquandles of the various orbits of Q more or less independently? Specifically, suppose we start with $\mathrm{Core}(G)$ for G a group, and let N be the normal subgroup of G generated by the squares, so that G/N is the universal exponent-2 image of G. Can we get a subquandle of $\mathrm{Core}(G)$ whose intersections with the various cosets of N include cosets of distinct subgroups of N? For instance, can we do this when G is an infinite cyclic group $\langle x\rangle$? There, $N = \langle x^2\rangle$, so the two orbits are the sets of even and odd integers.

The answer turns out to be no in that case, but yes for some other G.

The negative answer for $Q = \mathrm{Core}(\langle x\rangle)$ follows from the fact, not hard to see, that in that quandle, the elements of every nonempty subquandle Q' form a subtrajectory. (Idea: If Q' has more than one element, choose distinct $x^i, x^j \in Q'$ so as to minimize $|i-j|$, and show that the existence of an element x^k not in the subtrajectory they generate would contradict that minimality.) For such a subtrajectory-determined subquandle Q', the set $\{i \mid x^i \in Q'\}$ either consists entirely of even integers, or consists entirely of odd integers, or the sets of even and of odd elements are cosets of a common subgroup of $\mathbb{Z}$.

But for an example where more interesting things can happen, let G be the infinite dihedral group $\langle x, y \mid y^2 = 1,\ y^{-1}x\,y = x^{-1}\rangle$. It is easy to check that each coset of the subgroup $\langle x\rangle \subseteq G$ has trivial $\lhd$-action on the other:

(4.4) $x^i \lhd (x^j y) \ = \ x^j y \quad \text{and} \quad (x^j y) \lhd x^i \ = \ x^i \qquad (i, j \in \mathbb{Z}).$

Hence the union of any subquandle of one coset with any subquandle of the other gives a subquandle of $\mathrm{Core}(G)$; and those subquandles can, independently, each be a nontrivial subtrajectory, or a singleton, or empty.

(The cosets of $\langle x\rangle$ are not actually the orbits of $\mathrm{Core}(G)$; each is the union of two such orbits. But each coset of $\langle x\rangle$ is a trajectory, so, as discussed above, the intersections of a subquandle of $\mathrm{Core}(G)$ with the two orbits comprising one of these cosets have much less freedom.)

5. Which involutory quandles embed in core quandles of groups?

Not every involutory quandle has the form $\mathrm{Core}(G)$. For instance, letting G be a group of exponent 2, we have noted that every subset of $\mathrm{Core}(G)$ is a subquandle. But if such a subset has finite cardinality not a power of 2, that subquandle clearly cannot be isomorphic to $\mathrm{Core}(H)$ for any group H.

Is every involutory quandle at least *embeddable* in one of the form $\mathrm{Core}(G)$?

No. A hint of what can go wrong was seen in the proof of Proposition 3.2, where for a trajectory satisfying a relation $x_i = x_{i+m}$, we did not deduce $x_j = x_{j+m}$ for all j, as is clearly true in a group-theoretic trajectory, but only $x_j = x_{j+2m}$. The next result analyzes that behavior in detail; in Proposition 5.2 we note the consequences for embeddability of involutory quandles in core quandles.

Proposition 5.1. *Let Q be an involutory quandle, and $(x_i)_{i\in\mathbb{Z}}$ a trajectory in Q in which not all terms are distinct. Then for some positive integer n,*

(5.1) $\quad x_i \ = \ x_{i+n}$ *for all* $i\in\mathbb{Z}$.

Let n be the least *positive integer for which* (5.1) *holds. Then exactly one of the following is true.*

(i) $\quad x_i = x_j$ *if and only if* $i\equiv j \pmod n$.

(ii) $\ n$ *is a multiple of* 4, *and for* $i,j\in\mathbb{Z}$ *we have* $x_i = x_j$ *if and only if either* i *and* j *are both odd, and are congruent modulo* $n/2$, *or they are both even, and are congruent modulo* n.

(ii′) *Like* (ii), *but with "even" and "odd" interchanged.*

Moreover, for each of (i), (ii), (ii′), *and all values of* n *with the indicated properties, there exist trajectories* $(x_i)_{i\in\mathbb{Z}}$ *in involutory quandles* Q *of the sort described.*

Proof. (5.1) holds for some n by the implication (3.6) $\Longrightarrow$ (3.7) in the proof of Proposition 3.2. Let n be the least such value.

For each $x\in\{x_i \mid i\in\mathbb{Z}\}$, let $r(x)$ be the least distance between occurrences of x in our trajectory, i.e., the least $m>0$ such that for some i, $x_i = x = x_{i+m}$. Note that if $r(x)\neq n$, so that x occurs more than once in a cycle of length n, then we must have $r(x)\leq n/2$.

On the other hand, again calling on the implication (3.6) $\Longrightarrow$ (3.7), we see that $x_i = x_{i+2r(x)}$ for all i, so by our choice of n, n is a divisor of $2\,r(x)$, so $n\leq 2\,r(x)$, i.e., $r(x)\geq n/2$. In view of the conclusion of the preceding paragraph, this says that if $r(x)\neq n$, then $r(x)=n/2$. So for each x, either $r(x)=n$, in which case x occurs periodically with period n, or $r(x)=n/2$, so x must occur with period $n/2$. (Of course, the latter is only possible if n is even.)

Assuming $r(x)=n/2$, let $x=x_i$, and let us apply to the relation $x_i = x_{i+n/2}$ the operator $x_{i+1}\lhd$. By (3.5) we get $x_{i+2} = x_{i+2-n/2}$; so we must also have $r(x_{i+2}) = n/2$. Thus, for $j\in\mathbb{Z}$, whether $r(x_j)$ is n or $n/2$ can only depend on the parity of j.

We will have established the main assertion of the proposition once we say why we can't have $r(x_i)=n/2$ for both odd and even i, and why n must be a multiple of 4 (and not just an even integer) in cases (ii) and (ii′). The former point is trivial: if $r(x_i)$ were $n/2$ for both odd and even i, then for all i we would have $x_i = x_{i+n/2}$, so $n/2$, not n, would be the least period of $(x_i)_{i\in\mathbb{Z}}$. To see the other point, note that if $x_i = x_{i+n/2}$, then r has the value $n/2$ at both x_i and $x_{i+n/2}$. If $n/2$ were odd, this would mean that both odd- and even-indexed elements satisfied $r(x)=n/2$, which we have just noted is impossible.

It remains to show that all the cases of (i), (ii) and (ii′) do occur. For every n, the quandle $\mathrm{Core}(\langle x\mid x^n=1\rangle)$ gives a trajectory $(x^i)_{i\in\mathbb{Z}}$ as in (i). If n is a multiple of 4, it is straightforward to verify that the equivalence relation on the above quandle which identifies x^i with $x^{i+n/2}$ when and only when i is odd (respectively, even) is a congruence on that quandle, giving examples of (ii) and (ii′) respectively. (Note that n must be a multiple of 4 for our description of this quandle to make sense, i.e., for i and $i+n/2$ to be of the same parity.) $\square$

Incidentally, note that from a trajectory as in (ii) above, one gets a trajectory as in (ii′) by shifting the indexing by 1, and vice versa; hence the presence of one sort in a given Q is equivalent to the presence of the other. So below, we shall only refer to trajectories of the former sort.

Proposition 5.2. *The following conditions on an involutory quandle Q are equivalent.*

(i) *Q has no finite trajectories of the sort described in Proposition 5.1*(ii).

(ii) *If $(x_i)_{i\in\mathbb{Z}}$ is a trajectory in Q and $i,\ j,\ m$ are integers, then $x_i = x_{i+m} \iff x_j = x_{j+m}$.*

(i′) *Q has no finite trajectories of the sort described in Proposition 5.1*(ii) *with n a power of* 2.

(ii′) *If $(x_i)_{i\in\mathbb{Z}}$ is a trajectory in Q and $m \geq 2$ is a power of* 2, *then $x_0 = x_m \implies x_1 = x_{m+1}$.*

Moreover, every involutory quandle Q that is embeddable in the core quandle of a group satisfies the above equivalent conditions.

Proof. In the light of Proposition 5.1, it is clear that (i) $\iff$ (ii) and (i′) $\iff$ (ii′) (where the m of (ii′) is half the n of (i′)), and clearly the former conditions imply the latter conditions. Conversely, suppose Q fails to satisfy (i), i.e., has a trajectory $(x_i)_{i\in\mathbb{Z}}$ of the sort described in Proposition 5.1(ii). Then writing the period n of that description as $m\,n'$ where m is odd and n' is a power of 2 (which will be ≥ 4), we see that $(x_{m\,i})_{i\in\mathbb{Z}}$ will be a trajectory of period n' of the sort excluded by (i′) above.

Finally, since in a quandle of the form $\mathrm{Core}(G)$, every trajectory $(x_i)_{i\in\mathbb{Z}}$ has the form $(x\,z^i)_{i\in\mathbb{Z}}$, the conditions $x_0 = x_m$ and $x_1 = x_{m+1}$ both come down to $z^m = 1$, from which all of (i)-(ii′) are clear. □

Question 5.3. *Are the equivalent conditions of Proposition 5.2 sufficient, as well as necessary, for an involutory quandle Q to be embeddable in the core quandle of a group?*

Digressing from the main subject of this paper, we end this section with some observations on not-necessarily-involutory quandles, and a question on these, parallel to Question 5.3.

Added in proof: Question 5.3 above, and Question 5.5 below, have negative answers. See link at `https://math.berkeley.edu/~gbergman/papers/abstracts.html#inv_qndl` .

Lemma 5.4. *For the remainder of this section, we shall call a sequence $(x_i)_{i\in\mathbb{Z}}$ of elements of a* not necessarily involutory *quandle Q a trajectory if it satisfies* (3.1)*; equivalently, if it satisfies the analog of* (3.2) *with $\lhd^{-1}$ in place of $\lhd$.*

If $(x_i)_{i\in\mathbb{Z}}$ is a trajectory in a quandle Q, then

(a) *Every index-translate $(x_{i+r})_{i\in\mathbb{Z}}$ of $(x_i)_{i\in\mathbb{Z}}$ is again a trajectory.*

(b) *Writing $x_0 = x,\ x_1 = y$, the formulas of* (3.4) *for x_i with $i \geq 0$ hold, while those with $i < 0$ become true if $\lhd$ is everywhere replaced by $\lhd^{-1}$.*

(c) *For all i, $x_{i+2} = y \lhd (x \lhd x_i)$.*

(d) *For all integers $i,\ j$ and n, we have $x_i = x_j \iff x_{i+2n} = x_{j+2n}$.*

(e) *If Q is embeddable in* $\mathrm{Conj}(G)$ *for G a group, then for all integers $i,\ j$ and n, we have $x_i = x_j \iff x_{i+n} = x_{j+n}$.*

Proof. (a) is immediate from the above definition of a trajectory, and (b) is easily proved by induction, with the help of the fact that a common string $y \lhd (x \lhd (y \lhd \ldots))$ or $x \lhd^{-1} (y \lhd^{-1} (x \lhd^{-1} \ldots))$ with which two successive terms of (3.4) begin acts on Q by an automorphism, by (1.3) and (1.4). (c) is quickly verified by looking separately at the four cases $i < -1,\ i = -1,\ i = 0$ and $i > 0$. Since $y \lhd (x \lhd -)$ is an automorphism of Q, (d) follows from (c).

In proving (e), it suffices to establish the case $n = 1$. Moreover, we can assume without loss of generality that $i < j$, and then, using (a), assume $i = 0$. Thus, what we must prove is the equivalence, for $j > 0$, of $x_0 = x_j$ with $x_1 = x_{j+1}$.

If j is odd, say $j = 2m+1$, these equations, expressed using the operations of G, become $x = (yx)^m y\,(yx)^{-m}$ and $y = (yx)^m yxy^{-1}(yx)^{-m}$. If, on the other hand, $j = 2m$, they become $x = (yx)^{m-1} yxy^{-1}(yx)^{-(m-1)}$ and $y = (yx)^m y\,(yx)^{-m}$. In each case, the equivalence of the two group-theoretic relations is straightforward: Each of the first pair of equations reduces (on bringing all negative-exponent terms to the opposite side, and cancelling equal end-terms if these occur) to $x(yx)^m = (yx)^m y$; each of the second pair to $(xy)^m = (yx)^m$. □

It is not clear to me how natural the concept of trajectory is in non-involutory quandles. When $Q = \mathrm{Conj}(G)$, a trajectory in Q will not, in general, be a trajectory in the group G as defined in (1.8). The terms of a trajectory in a quandle Q do not, in general, comprise a subquandle (e.g., they do not, in general, include $y \lhd (y \lhd x)$). In particular, trajectories do not, in general, satisfy (3.5). The failure of that condition means that if $(x_i)_{i\in\mathbb{Z}}$ is a trajectory, then for $n \neq 1$, $(x_{ni})_{i\in\mathbb{Z}}$ will not in general be one. (Indeed, it will not be one for $n = -1$ if $x \lhd y \neq x \lhd^{-1} y$.)

Nevertheless, point (e) of the above lemma suggests the following analog of Question 5.3.

Question 5.5. *Suppose Q is a (not necessarily involutory) quandle such that for all trajectories $(x_i)_{i\in\mathbb{Z}}$ in Q and all positive integers j, we have*

$$x_0 = x_j \iff x_1 = x_{j+1}. \tag{5.2}$$

Must Q be embeddable in $\mathrm{Conj}(G)$ *for some group G?*

We remark that for trajectories in quandles obtained from groups G by the formula (1.5) with $|d| > 1$, (5.2) need *not* hold. For example, one finds that in such a quandle, the left-hand equation of the $j = 2$ case of (5.2) says that in G, y^d commutes with x, and the right-hand equation says that x^d commutes with y; but if we take for G a group having elements x and y which do not commute, and such that x has order prime to d, while y has order dividing d, then for these x and y, the first of the above conditions clearly holds, while the second fails.

I do not know whether there are interesting conditions on quandles that *are* implied by embeddability in quandles so obtained for values of $d > 1$. (The conditions satisfied for d and for $-d$ can be obtained from each other by interchanging $\lhd$ and $\lhd^{-1}$, so the cases with negative d don't have to be examined separately.)

6. More on mapping involutory quandles into core quandles of groups

Proposition 5.2 gives us restrictions on involutory quandles embeddable in quandles of the form $\mathrm{Core}(G)$. Nevertheless, there is a natural homomorphism of any involutory quandle into a core quandle, which often does a good job of separating elements.

Proposition 6.1. *Let Q be any involutory quandle, and* $\mathrm{Perm}(Q)$ *the group of all permutations of the set Q. For $x \in Q$, define $\overline{x} \in \mathrm{Perm}(Q)$ by*

$$\overline{x}(a) \;=\; x \lhd a \qquad (a \in Q). \tag{6.1}$$

Then $x \mapsto \overline{x}$, is a quandle homomorphism $Q \to \mathrm{Core}(\mathrm{Perm}(Q))$.

If Q above has the form $\mathrm{Core}(G)$ for a group G, then elements $x, x' \in Q$ fall together under this homomorphism if and only if, as members of G, they belong to the same coset of the group of elements of exponent 2 in the center *of G.*

Proof. That the maps $\overline{x} : Q \to Q$ are invertible, i.e., belong to $\mathrm{Perm}(Q)$, is property (1.3). (Though we did not make (1.3) part of our characterization of involutory quandle in Lemma 1.2, we noted that it follows from (1.7), which says that every map $\overline{x}$ has exponent 2.)

To check that $x \mapsto \overline{x}$ is a homomorphism of quandles, let $x, y \in Q$. Then we see (using (1.9) at the second step below, and the fact that $\overline{y}$ has exponent 2 at the fourth) that for all $z \in Q$,

$$\begin{aligned}(\overline{x \lhd y})(z) \;&=\; (x \lhd y) \lhd z \;=\; x \lhd (y \lhd (x \lhd z)) \;=\\ (\overline{x}\,\overline{y}\,\overline{x})(z) \;&=\; (\overline{x}\,\overline{y}^{-1}\overline{x})(z) \;=\; (\overline{x} \lhd \overline{y})(z),\end{aligned} \tag{6.2}$$

so $\overline{x \lhd y} = \overline{x} \lhd \overline{y}$, as required.

To get the last assertion of the proposition, note that for $x, x' \in G$, we have $\overline{x} = \overline{x'}$ if and only if all $y \in G$ satisfy $x\,y^{-1}x = x'y^{-1}x'$. Multiplying on the left by x'^{-1} and on the right by x^{-1}, this becomes

$$x'^{-1}x\,y^{-1} \;=\; y^{-1}x'\,x^{-1}. \tag{6.3}$$

Taking $y = 1$ in (6.3) gives

$$x'^{-1}x \;=\; x'x^{-1}. \tag{6.4}$$

Hence (6.3) says that the common value of the two sides of (6.4) is central in G. Hence, in particular, the right-hand side of (6.4) is unaffected by conjugation by x; but the result of that conjugation is the inverse of the left-hand side, so the common value of the two sides also has exponent 2, giving the "only if" direction of the desired statement. The "if" direction is straightforward. □

(The map $\overline{x}$ of (6.1), for Q a not necessarily involutory quandle, is called in [8, Definition 1.1] the *symmetry* $S(x)$ of Q at x; it is an automorphism of Q.)

If elements of an involutory quandle Q fall together under the map $Q \to \mathrm{Core}(\mathrm{Perm}(Q))$ of Proposition 6.1, this may be because Q cannot be embedded in the core quandle of a group, as is the case for the trajectories of Proposition 5.1(ii); or that may not be so, as we see from the last paragraph of Proposition 6.1.

To avoid "unnecessary falling-together", one can try to embed Q in a larger involutory quandle Q', such that even if two elements $x \neq x'$ satisfy $x \lhd y = x' \lhd y$ for all $y \in Q$, this equality fails for some $y \in Q'$, so that Proposition 6.1 yields a representation of Q' that distinguishes them. When Q has the form $\mathrm{Core}(G)$ for some group G, this will always work: construct a group H by adjoining to G one new generator z and no relations. Then nonidentity elements of G will not centralize z, so in $\mathrm{Perm}(\mathrm{Core}(H))$ the cases of elements of G falling together as described in Proposition 6.1 become trivial.

Given an arbitrary involutory quandle Q, there will similarly exist a universal involutory quandle Q' generated by an image of Q and one additional generator z. If we could find a normal form for elements of this Q' in terms of Q, we could use it to tell which pairs of elements x, x' fall together under all maps into core quandles of groups. (Namely, if and only if $x \lhd z = x' \lhd z$.) But I do not see how to get such a normal form. Obviously, we can reduce any element of Q' to an expression (2.1) in elements of $Q \cup \{z\}$. But the identities of involutory quandles will imply further equalities among such expressions. For instance, suppose we have an expression $\dots \lhd (x_i \lhd (x_{i+1} \lhd (\dots))) \dots$ with x_i and x_{i+1} both coming from Q. Let us use (1.7) in reverse, to insert two terms x_i after x_{i+1}, getting an expression $\dots \lhd (x_i \lhd (x_{i+1} \lhd (x_i \lhd (x_i \lhd (\dots))))) \dots$, then apply (1.9) to the first three of the terms shown. Then our element becomes $\dots \lhd (x'_{i+1} \lhd (x_i \lhd (\dots))) \dots$, where $x'_{i+1} = x_i \lhd x_{i+1} \in Q$. For another example: if five successive terms $x_i, \dots, x_{i+4}$ all come from Q and satisfy $x_i = x_{i+2} = x_{i+4}$, then we can apply (1.9) either to x_i, x_{i+1}, x_{i+2}, or to x_{i+2}, x_{i+3}, x_{i+4}, getting different reductions of our expression.

Contrast this with the case of the *group* gotten by adjoining a new generator z to an arbitrary group G. This has a normal form consisting of all alternating strings of nonidentity elements of G and nonzero powers of z, from which one quickly sees that no nonidentity element of G is central in the new group.

The reader might find it interesting to examine the case where Q is the involutory quandle of Proposition 5.1(ii) with $n = 4$, consisting of the three elements x_0, $x_1 = x_3$, and x_2, and see how the axioms for an involutory quandle force $x_0 \lhd z = x_2 \lhd z$. (Outline: In $x_2 \lhd z$, substitute $x_1 \lhd x_0$ for x_2, and expand the result using (1.9). Write the last x_1 in the resulting expression as $x_0 \lhd x_1$ and again expand by (1.9). Then apply (1.7) twice. This 3-element quandle is called $\mathrm{Cs}(4)$ in [8, next-to-last paragraph of §6].)

By general nonsense (see [3, Exercise 9.9:8, or better, Theorem 10.4:3]) one can associate to any involutory quandle Q a group $\mathrm{Group}(Q)$ with a universal involutory quandle homomorphism $Q \to \mathrm{Core}(\mathrm{Group}(Q))$. The pairs x, x' of elements of Q that fall together under this homomorphism will be those that fall together under all homomorphisms to core quandles of groups. But, as in the approach of adjoining a universal z to Q as an involutory quandle, it is not clear how to get a good enough picture of $\mathrm{Group}(Q)$ to detect such pairs.

Incidentally, the abovementioned universal homomorphism $Q \to \mathrm{Core}(\mathrm{Group})(Q)$ can never be surjective. To see this, take any nontrivial group G and any $g \in G - \{1\}$. Then a homomorphism $c_g : Q \to \mathrm{Core}(G)$ is given by the constant map $c_g(x) = g$ $(x \in Q)$. By the universal property of $\mathrm{Group}(Q)$, c_g must factor $Q \to \mathrm{Core}(\mathrm{Group}(Q)) \to \mathrm{Core}(G)$, where the second map is induced by some group homomorphism $\mathrm{Group}(Q) \to G$. Since c_g takes no element of Q to $1 \in G$, our map $Q \to \mathrm{Core}(\mathrm{Group}(Q))$ cannot take any element of Q to $1 \in \mathrm{Core}(\mathrm{Group}(Q))$, and so cannot be surjective.

Returning to our observation that every involutory quandle Q that can be embedded in the core quandle of a group G can in fact be embedded in $\mathrm{Core}(\mathrm{Perm}(H))$ for an appropriate overgroup H of G, by sending each $x \in G$ to the permutation (6.1) of the underlying set of H, note that each of these permutations (6.1) has exponent 2. We record this, along with some straightforward observations, in the next result (where Inv stands for "set of involutions").

Proposition 6.2. *For any group G, the elements of exponent 2 in G form a subquandle $\mathrm{Inv}(G)$ both of $\mathrm{Core}(G)$ and of $\mathrm{Conj}(G)$, on which the restrictions of the operations of those two quandles agree.*

An involutory quandle Q can be embedded in the core quandle of a group G if and only if it can be embedded in the involutory quandle $\mathrm{Inv}(H)$ for some group H. □

(Cf. [8, Corollary 10.3], which shows that the free involutory quandle on an A-tuple of elements embeds naturally in $\mathrm{Conj}(G)$, for G the group presented by an A-tuple of elements of exponent 2. From this the second assertion of our Theorem 2.1 can be deduced. More generally, [8] defines an *n-quandle* to be a quandle in which the n-th power of each derived operation $x \lhd$ is the identity, with the special case $n = 2$ being named an involutory quandle. The cited corollary gives the above result for n-quandles, and G presented by an A-tuple of generators of exponent n.)

Proposition 6.2 shows that if an involutory quandle can be embedded in a quandle $\mathrm{Core}(G)$, it can also be embedded in a quandle $\mathrm{Conj}(H)$. I don't know whether the converse is true:

Question 6.3. *Can every* involutory *quandle Q that is embeddable in* Conj(G) *for some group G be embedded in* Inv(H) *for some group H? Equivalently* (*by the final statement of Proposition 6.2*) *can any such Q be embedded in the core quandle of a group?*

An involutory subquandle of $\mathrm{Conj}(G)$ that is, in general, larger than $\mathrm{Inv}(G)$ is the set of elements whose squares are *central*. This set also forms a subquandle of $\mathrm{Core}(G)$, but the two quandle structures are, in general, distinct (easily seen in the case $G = Z$).

We remark that for G a group, we can get an embedding of $\mathrm{Core}(G)$ in a quandle of the form $\mathrm{Inv}(H)$ as in the second statement of Proposition 6.2 using a group H that is not as enormous as the permutation group of the underlying set of the group gotten by freely adjoining a new element z to G, discussed in the third paragraph following Proposition 6.1. To motivate the description of such an H, let G^* be the result of adjoining such a z to G. Note that the $\lhd$-actions on G^* of elements of G carry into itself the subset $G\{z,\, z^{-1}\}\,G$, and that their actions on that subset belong to the subgroup of $\mathrm{Perm}(G\{z,\, z^{-1}\}\,G)$ generated by left multiplication by members of G, right multiplication by members of G, and the operation $(\ )^{-1}$. That subgroup is isomorphic to the semidirect product $Z_2 \ltimes (G \times G)$, where the nonidentity element of Z_2, which we shall denote u, acts on $G \times G$ by interchanging the factors. Namely, we let elements of the form $(1, x, y) \in Z_2 \ltimes (G \times G)$ act on $G\{z,\, z^{-1}\}\,G$ by $h \mapsto x\,h\,y^{-1}$, and let u act by $h \mapsto h^{-1}$. Thus, for $x \in G$, $x \lhd -$ is represented by $(u, x, x^{-1}) \in Z_2 \ltimes (G \times G)$. It is straightforward to verify (without calling on the above motivation) that, in the notation of Proposition 6.2,

$$(6.5) \qquad x \ \mapsto\ (u, x, x^{-1}) \qquad \text{is an embedding of involutory quandles} \qquad \mathrm{Core}(G) \to \mathrm{Inv}(Z_2 \ltimes (G \times G)).$$

In another direction, let us note a property of quandles of the form $\mathrm{Core}(G)$ which follows immediately from Lemma 1.3(i).

Lemma 6.4. *If G is a group, then the automorphism group of* Core(G) *is transitive on the underlying set of that quandle.* □

An easy example of an involutory quandle whose automorphism group is not transitive is the 3-element quandle of Proposition 5.1(ii) with $n = 4$ (mentioned in the fourth paragraph before Proposition 6.2 above). The element $x_1 = x_3$ is fixed under all the operations $x \lhd -$, while the elements x_0 and x_2 are not; so no automorphism of Q can carry $x_1 = x_3$ to x_0 or x_2.

The above example is a homomorphic image of a quandle of the form $\mathrm{Core}(G)$. A quandle Q which is, rather, embeddable in one of the form $\mathrm{Core}(G)$, but again does not have transitive automorphism group, is the case of the example in the paragraph containing (4.4) where, as subsets of the cosets $\langle x \rangle$ and $\langle x \rangle y$, we take all of one coset, and a singleton subset of the other. Then Q consists of an infinite trajectory together with a lone element which belongs only to trajectories of ≤ 2 elements; so no automorphism can carry that element to any other.

7. Identities in groups and their core quandles

If a group G satisfies nontrivial identities (identities not implied by the identities defining groups), this can lead to nontrivial identities on the involutory quandle $\mathrm{Core}(G)$. We saw this in an extreme way in Lemma 4.1; let us examine some other examples.

Theorem 7.1. *The identities satisfied by* Core(G) *for all* abelian *groups G are the consequences* (*given the defining identities* (1.2), (1.7) *and* (1.9)) *of the identity*

$$(7.1) \qquad w \lhd (x \lhd (y \lhd z)) \ =\ y \lhd (x \lhd (w \lhd z)).$$

Proof. That (7.1) holds in $\mathrm{Core}(G)$ when G is abelian is immediate. (Cf. the group-theoretic expansion (2.2) of the general involutory quandle expression (2.1).)

To see that the only identities holding in all such quandles are the consequences of (7.1), first note that given an expression $x_0 \lhd (x_1 \lhd (\cdots \lhd (x_{n-1} \lhd x_n) \dots))$, where the x_i are symbols in a set X, we can, using (7.1), rearrange in any way the x_i having *even* subscripts $i < n$, and likewise rearrange in any way the x_i having *odd* subscripts $i < n$. In particular, if some $x \in X$ occurs in both even and odd positions, we can rearrange the terms so that these occurrences of x appear in adjacent positions, and then use (1.2) or (1.7) to shorten the word. (We use (1.2) if one of these occurrences of x is x_n, so that it was the other occurrence that had to be moved to become adjacent to it; (1.7) if neither occurrence is x_n, so that one, the other, or both could be moved to make them adjacent.)

Now suppose that $u = v$ is an identity in symbols from X satisfied by $\mathrm{Core}(G)$ for all abelian groups G. Using (1.9) we can assume without loss of generality that in both u and v, parentheses are clustered to the right, while using (7.1), (1.2), and (1.7) as above, we can assume that in each of these words, no member of X occurs in both even-subscripted and odd-subscripted positions. Let us now evaluate u and v in the free abelian group G on X (which we will write multiplicatively). For $x \in X$, an occurrence of x as the i-indexed term of the expression u or v will contribute $(-1)^i\, 2$ to the exponent of x in the resulting element of G, unless the term in question is the final term (i.e., x_n if our expression is $x_0 \lhd (\cdots \lhd x_n) \dots)$ in which case it will contribute just $(-1)^i$. Since no term occurs in both even and odd positions in u or in v, we can conclude from the structure of free abelian groups that u and v must have the same length, the same number of occurrences of each element of X in nonfinal even position, the same number of occurrences of each element of X in nonfinal odd position, and the same final term. Hence u can be transformed into v by applications of (7.1); hence the identity $u = v$ is indeed a consequence of (1.2), (1.7), (1.9), and (7.1). ☐

What about the other direction? I.e., for which groups G will $\mathrm{Core}(G)$ satisfy (7.1)?

Theorem 7.2. *If G is a group, then $\mathrm{Core}(G)$ satisfies (7.1) if and only if G is nilpotent of nilpotency class ≤ 2, i.e., if and only if*

(7.2) *every commutator* $[x,y] \;=\; x^{-1}y^{-1}x\,y \quad (x,y \in G)$ *is central in* G.

Proof. The quandle identity (7.1) on $\mathrm{Core}(G)$ translates to the group-theoretic identity on G,

(7.3) $$w\,x^{-1}\,y\,z^{-1}\,y\,x^{-1}\,w \;=\; y\,x^{-1}\,w\,z^{-1}\,w\,x^{-1}\,y.$$

Let us start with the case where $x = 1$, write $z^{-1} = u$, and multiply the resulting equation both on the left and on the right by $y^{-1}\,w^{-1}$. Then we get

(7.4) $$u\,y\,w\,y^{-1}w^{-1} \;=\; y^{-1}w^{-1}y\,w\,u.$$

Taking $u = 1$, this tells us that $y\,w\,y^{-1}\,w^{-1}$ equals $y^{-1}\,w^{-1}\,y\,w$, i.e., $[y,\,w]$. So the general case of (7.4) tells us that $u\,[y,\,w] = [y,\,w]\,u$; so indeed, every commutator $[y,\,w]$ in G is central.

Conversely, suppose that in G every commutator is central. Note that in any group, an element $w\,x^{-1}\,y$ (such as we have at the beginning of the left side of (7.3) and the end of the right side) differs from $y\,x^{-1}\,w$ (as at the end of the left side of (7.3) and the beginning of the right side) by a product of commutators. Since commutators are central, if we multiply each side of (7.3) by that product of commutators, we can let that product act on the beginning of the left side and the end of the right side, reducing (7.3) to the trivial identity $(y\,x^{-1}\,w)\,z^{-1}\,(y\,x^{-1}\,w) = (y\,x^{-1}\,w)\,z^{-1}\,(y\,x^{-1}\,w)$. So (7.3) indeed holds in every group where commutators are central. ☐

If a quandle of the form $\mathrm{Core}(G)$ satisfies (7.1), can it also be written $\mathrm{Core}(H)$ for an abelian group H? In general, no, as seen in the final statement of

Lemma 7.3. *For any group G, the following conditions are equivalent:*

(i) *In G, every product of squares is a square.*

(ii) *In $\mathrm{Core}(G)$, for all elements $x,\,y,\,z$ there exists an element w such that*

(7.5) $$x \lhd (y \lhd z) \;=\; w \lhd z.$$

Thus, every abelian group, since it satisfies (i), *satisfies* (ii). *On the other hand, the group G free on two generators in the variety determined by* (7.2)*, equivalently, the group of upper triangular 3×3 matrices over $\mathbb{Z}$ with 1's on the diagonal, does not satisfy* (ii). *Hence the core quandle of the latter group, though it satisfies* (7.1)*, is not isomorphic to the core quandle of an abelian group.*

Proof. In the paragraph following Lemma 3.4, we noted that condition (i) above could be expressed in terms of the structure of $\mathrm{Core}(G)$; condition (ii) is the explicit form that that condition takes. (Idea: multiplying a group element on one side by an n-th power corresponds to moving it n steps along some trajectory; and by (3.4), moving an element x_0 two steps along a trajectory is equivalent to applying some operation $y\lhd$ to it. So (7.5) says that the result of multiplying $z \in G$ on a given side by a square, and then by another square, can always be achieved by multiplying it by a single square.)

That every abelian group satisfies (i) is clear. To see that the free group H of nilpotency class 2 on generators $x,\,y$ does not satisfy (ii), let us write the general element thereof as $x^i\,y^j\,[y,x]^k \quad (i,\,j,\,k \in \mathbb{Z})$, and note that the group operation is given by

(7.6) $$(x^i\,y^j\,[y,x]^k)\;(x^{i'}\,y^{j'}\,[y,x]^{k'}) \;=\; x^{i+i'}\,y^{j+j'}\,[y,x]^{k+k'+ji'}.$$

(Rough idea: $yx = xy\,[y,x]$, so in bringing the product on the left-hand side to normal form, each time we push one of the j occurrences of y in the first factor past one of the i' occurrences of x in the second, a $[y,x]$ is created.)

Note that if for this H, we evaluate the left-hand side of (7.5) with the element y^{-1} in the role of y, and 1 in the role of z, we get, in group-theoretic terms, $x\,y\,1\,y\,x$, i.e., $x\,y^2\,x$, which by (7.6) equals

$$x^2\,y^2\,[y,x]^2. \tag{7.7}$$

Now suppose that some choice of $w = x^i\,y^j\,[y,x]^k$ makes the right-hand side of (7.5) equal (7.7). Since we have taken $z = 1$, that right-hand side is w^2, and we see from (7.6) that for this to equal (7.7), we must have $i = j = 1$. But this gives the exponent of $[y,x]$ the value $2k+1$, so the expression cannot agree with (7.7). □

On the other hand, if we adjoin to the nilpotent group of the above lemma a central square root of $[y,x]$, the above problem goes away:

Lemma 7.4. *Let G be the free abelian group on three generators x, y, z, and H the group obtained by adjoining to the free group of nilpotency class 2 on generators x, y a central square root of the element $[y,x]$, which we shall write $[y,x]^{1/2}$. Thus, the general element of H can be written in the normal form $x^i\,y^j\,[y,x]^{k/2}$ with $i, j, k \in \mathbb{Z}$, and the group operation of H is given by (7.6) with k and k' everywhere replaced by $k/2$ and $k'/2$.*

Then $\mathrm{Core}(H) \cong \mathrm{Core}(G)$, *by the map*

$$x^i\,y^j\,[y,x]^{k/2} \ \mapsto\ x^i\,y^j\,z^{k-ij}. \tag{7.8}$$

Proof. The map (7.8) is clearly a bijection. Computation shows that it respects $\lhd$. □

(The computation of the exponent of z in the image of the $\lhd$-product of two elements of H is messy; I wish I could offer a nicer verification.)

Returning to the consequence of Lemma 7.3, that the core quandles of the free abelian group of rank three and the free group of nilpotency class 2 on two generators are not isomorphic, we remark that each can nonetheless be embedded in the other. In one direction, restricting (7.8) to the case where $[y,x]$ has integer exponent, we get a $\lhd$-embedding of the free nilpotent group in the free abelian group,

$$x^i\,y^j\,[y,x]^{k} \ \mapsto\ x^i\,y^j\,z^{2k-ij}. \tag{7.9}$$

For the other direction, note that the inverse of (7.8) carries the subgroup of G generated by x, y^2 and z^2, which is free abelian on these generators, into the subgroup of H consisting of elements in which $[y,x]$ has integer exponent, i.e., our free group of nilpotency class 2.

Turning back to the identity (7.1), here is another way to look at that condition.

Lemma 7.5. *Let Q be a nonempty involutory quandle, and let us fix an arbitrary element $u \in Q$. Then Q satisfies (7.1) if and only if (in the notation of Proposition 6.1) the elements of the set $\{\,\overline{x}\,\overline{u} \mid x \in Q\} \subseteq$* $\mathrm{Perm}(Q)$ *all commute with one another; in other words, if and only if the map*

$$x \ \mapsto\ \overline{x}\,\overline{u}, \tag{7.10}$$

which is a $\lhd$-homomorphism $Q \to$ $\mathrm{Core}(\mathrm{Perm}(Q))$ *(since it is a group-theoretic right translate of the $\lhd$-homomorphism $x \mapsto \overline{x}$ of Proposition 6.1), has image in an abelian subgroup of* $\mathrm{Perm}(Q)$.

Hence if that condition holds, and if, moreover, the map $x \mapsto \overline{x}$ is one-to-one, then Q is embeddable in $\mathrm{Core}(G)$ *for an abelian group G.*

In particular, for every group H of nilpotency class ≤ 2 whose center has no elements of order 2, $\mathrm{Core}(H)$ *is embeddable in* $\mathrm{Core}(G)$ *for an abelian group G.*

Proof. Suppose first that for some $u \in Q$, the elements $\overline{x}\,\overline{u}$ $(x \in Q)$ all lie in an abelian subgroup of $\mathrm{Perm}(Q)$. Since $\overline{u}^2 = 1$, these elements can be written $\overline{x}\,\overline{u}^{-1}$, hence for any $x, y \in Q$, that abelian subgroup contains $(\overline{x}\,\overline{u}^{-1})\,(\overline{y}\,\overline{u}^{-1})^{-1} = \overline{x}\,\overline{y}^{-1}$; so our hypothesis is equivalent to the statement (independent of the choice of an element u) that all elements of $\mathrm{Perm}(Q)$ of the form $\overline{x}\,\overline{y}^{-1}$ $(x, y \in Q)$ commute. Again using the fact that the exponent ${}^{-1}$ on an element of the form $\overline{x}$ makes no difference, we see in particular that for all $w, x, y \in Q$, we have $(\overline{w}\,\overline{x})\,(\overline{y}\,\overline{x}) = (\overline{y}\,\overline{x})\,(\overline{w}\,\overline{x})$, which, cancelling the $\overline{x}$'s on the right, gives $\overline{w}\,\overline{x}\,\overline{y} = \overline{y}\,\overline{x}\,\overline{w}$. Applying this element of $\mathrm{Perm}(Q)$ to elements $z \in Q$, we get (7.1).

The reverse implication works essentially the same way.

The assertion of the second paragraph follows immediately. The final assertion then follows in view of the last assertion of Proposition 6.1. □

(We remark that [8, Definition 1.3] defines an "abelian quandle" to be a not necessarily involutory quandle satisfying an identity equivalent to (7.1), and that in [8, Theorem 10.5], a description is given of the free abelian involutory quandle on finitely many generators.)

Let us take a brief look at the other very simple sort of identity a group can satisfy, saying that its elements all have exponent n, for some fixed n. The technique of Lemma 3.4 shows us that for each n, the groups satisfying this identity can be characterized by a $\lhd$-identity on their core quandles. Namely, comparing (3.3) and (3.4), we see

Lemma 7.6. *Let n be a positive integer. Then a group G satisfies the identity $x^n = 1$ if and only if $\mathrm{Core}(G)$ satisfies the identity equating the formulas for x_0 and x_n in (3.4); i.e., for n even, the identity $x = y\lhd(x\lhd(\cdots\lhd x))$ with $n/2$ y's and $n/2$ x's in the right-hand expression; for n odd, $x = y\lhd(x\lhd(\cdots\lhd y))$ with $(n+1)/2$ y's and $(n-1)/2$ x's.* □

The above "if and only if" shows that in this case, we don't have the complication that we had for commutativity, where the effect of our $\lhd$-identity was weaker than the group identity we started with. But we have the opposite sort of complication. For each positive integer n we can ask

Question 7.7. *Does the $\lhd$-identity described in Lemma 7.6 imply, for general involutory quandles,* all *identities satisfied by the core-quandles of groups of exponent n?*

Equivalently, is the free involutory quandle Q on any set of generators, subject to that identity, embeddable in the involutory quandle of a group of exponent n?

Observe that in the quandle Q of the final sentence of the above question, all trajectories have period dividing n. Hence if n is not divisible by 4, so that Q satisfies condition (i) of Proposition 5.2, an affirmative answer to Question 5.3 would imply that Q is embeddable in the core quandle of some group. So assuming the answer to Question 5.3 is affirmative, suppose $Q \subseteq \mathrm{Core}(G)$. Then the $\lhd$-identity in question implies that for all $x, y \in Q$, the element $xy^{-1} \in G$ has exponent n. By a translation, we may assume that Q contains $1 \in G$. The fact that elements xy^{-1} $(x, y \in Q)$ have exponent n in G then implies that elements of Q themselves have exponent n in G, as do pairwise products $xy \in G$ of elements of Q (since $y^{-1} \in Q$, as it belongs to the trajectory in G determined by $x_0 = 1$, $x_1 = y$).

Can we conclude that under the above assumption regarding Question 5.3, and for Q translated as above to contain 1, *all* elements of the subgroup of G generated by Q have exponent n, which would give an affirmative answer to Question 7.7 for such n? Not so far as I can see. The products xy mentioned above need not lie in Q itself, so there is no evident reason why larger products, e.g., xyz for $x, y, z \in Q$, should have exponent n. (If we start with two elements $x, y \in Q$, then an element of the form $x^i y^j x^k$ *will* have exponent n, since it is conjugate in G to $x^{i+k} y^j$, and x^{i+k} and y^j lie in Q, being members of the trajectories beginning $1, x$ and $1, y$. But I see no reason why longer expressions in x and y, e.g., $[x, y] = x^{-1}y^{-1}x\,y$, should have exponent n.) The subgroup of G generated by Q will, of course, have a universal exponent-n homomorphic image; but some elements of Q might fall together in that image.

(Groups subject to identities $x^n = 1$ have also been used in knot theory, [6], [7].)

I have not examined the consequences for $\mathrm{Core}(G)$ of any other identities on a group G.

8. Counting generators of core quandles

Given a finitely generated group G, what can be said about the number of elements needed to generate the quandle $\mathrm{Core}(G)$? Here is a lower bound, which when G is abelian gives the precise value.

Theorem 8.1. *For G a group, let $\mathrm{gen}(G)$ denote the minimum number of elements needed to generate G as a group, and for Q an involutory quandle, let $\mathrm{gen}(Q)$ denote the minimum number of elements needed to generate Q as a quandle.*

Then if $\mathrm{gen}(G)$ is finite, and we write N for the subgroup of G generated by the squares (clearly normal; so G/N is the universal exponent-2 homomorphic image of G), then we have

(8.1) $\mathrm{gen}(\mathrm{Core}(G)) \ \geq\ \max(\mathrm{gen}(G){+}1,\ [G:N]).$

If G is abelian, we have equality in (8.1).

Proof. In view of Lemma 4.1, the homomorphic image $\mathrm{Core}(G/N)$ of $\mathrm{Core}(G)$ cannot be generated by any proper subset of G/N, hence requires $[G:N]$ generators; hence $\mathrm{Core}(G)$ itself requires at least that many; so to get (8.1) it remains to show that $\mathrm{Core}(G)$ also requires at least $\mathrm{gen}(G)+1$ generators.

Suppose $\mathrm{Core}(G)$ is generated by a set S. Since $\mathrm{Core}(G)$ is nonempty, S must be nonempty; choose $x \in S$. Since translations under the group structure are automorphisms of $\mathrm{Core}(G)$, $\mathrm{Core}(G)$ is also generated by $x^{-1}S$; hence (since the $\lhd$-operation of $\mathrm{Core}(G)$ is a derived operation of G), the group G is generated by $x^{-1}S$. But $1 \in x^{-1}S$; so $x^{-1}S - \{1\}$ also generates G, so $\mathrm{card}(S) \geq \mathrm{gen}(G)+1$, as required.

To get the reverse inequality for abelian groups, let us first note that if G is an abelian group and X any subset of G containing 1, then an element $z \in G$ will belong to the subquandle of $\mathrm{Core}(G)$ generated by X if and only if

(8.2) z can be written as a product of powers of elements of $X - \{1\}$, in which the exponents of all but at most one of those elements are even.

Indeed, if we take an expression (2.2) with all x_i in X, drop factors with $x_i = 1$, and combine the occurrences of each element of X, we get a product as described in (8.2), where the only member of $X - \{1\}$ that can appear with odd exponent is the x_n of (2.2) if this is not 1. (If all the x_i in (2.2) are 1, we regard the resulting expression as an empty product (8.2), which we understand to have value 1.)

Given a finitely generated abelian group G, we now wish to construct a generating set for $\mathrm{Core}(G)$ of the cardinality shown on the right-hand side of (8.1). To do this we will start with a set X of possibly larger cardinality, which it is easy to verify generates $\mathrm{Core}(G)$, then show how to "combine" certain pairs of elements of X to get a set $X' \subseteq \mathrm{Core}(G)$ of the asserted cardinality, whose closure under $\lhd$ contains X, whence X' also generates $\mathrm{Core}(G)$.

To construct X, let $\mathrm{gen}(G) = n$ (no connection with the n of (2.2)). Being a finitely generated abelian group, G is a direct product of n cyclic subgroups $\langle g_i \mid g_i^{d_i} = 1 \rangle$ $(i = 1, \ldots, n)$ where each $g_i \in G$, and each d_i is either 0 or > 1. Without loss of generality, assume $d_1, \ldots, d_m$ even and $d_{m+1}, \ldots, d_n$ odd, where $0 \leq m \leq n$. Thus, the universal exponent-2 homomorphic image G/N has order 2^m. Let

$$X \;=\; X_0 \;\cup\; X_1 \;\cup\; X_2 \;\cup\; X_3, \tag{8.3}$$

where

$$X_0 = \{1\}, \quad X_1 = \{g_1, \ldots, g_m\}, \quad X_2 = \{\text{products of } \geq 2 \text{ of } g_1, \ldots, g_m\}, \quad X_3 = \{g_{m+1}, \ldots, g_n\}. \tag{8.4}$$

Note that $X_0 \cup X_1 \cup X_2$ is the set of all products of subsets of $\{g_1, \ldots, g_m\}$, and so has cardinality 2^m, while $X_0 \cup X_1 \cup X_3$ has cardinality $n+1$.

To express an arbitrary $z \in G$ as in (8.2) using this X, start with the product of those g_i with $1 \leq i \leq m$ that occur with odd exponent in z, a member of $X_0 \cup X_1 \cup X_2$; multiply this element by appropriate *even* powers of $g_1, \ldots, g_m \in X_1$ so as to achieve precisely the desired powers of each of those elements, and, finally, note that each $g_i \in X_3$ has odd order, hence the subgroup it generates is also generated by its square, so that every power of g_i can be regarded as an even power of g_i; so those g_i can also be brought into our product (8.2) with even exponents so as to achieve the desired value z. Hence X indeed generates $\mathrm{Core}(G)$.

The trick for getting a generating set of smaller cardinality is to combine elements of the sets X_2 and X_3. Given $g_{i_1} \ldots g_{i_k} \in X_2$ and $g_j \in X_3$, I claim that using the operation $\lhd$, we can obtain these two elements of X from their product

$$y \;=\; g_{i_1} \cdots g_{i_k}\, g_j \tag{8.5}$$

and the members of $X_0 \cup X_1$. Indeed, first note that $y^2 g_{i_1}^{-2} \ldots g_{i_k}^{-2} = g_j^2$ will lie in the subquandle generated by these elements (cf. (8.2), noting that $1, g_{i_1}, \ldots, g_{i_k} \in X_0 \cup X_1$). Since g_j has odd order, some power of g_j^2 gives us g_j, as desired. Multiplying y by an even power of this element g_j which equals g_j^{-1}, we get $g_{i_1} \ldots g_{i_k}$, the other element we wanted to recover.

By combining in this way pairs of elements, one from X_2 and one from X_3, until all elements of one of these sets have been used, we can replace $X_2 \cup X_3$ in our generating set for $\mathrm{Core}(G)$ by a set $X_{2,3}$, whose cardinality is the greater of the cardinalities of X_2 and X_3. (Namely, $X_{2,3}$ will consist of the products $g_{i_1} \ldots g_{i_k}\, g_j$ that we have introduced, together with the unused elements, if any, of one of X_2 and X_3.) The cardinality of the resulting generating set, $X_0 \cup X_1 \cup X_{2,3}$, will be the greater of the cardinalities of $X_0 \cup X_1 \cup X_2$ and $X_0 \cup X_1 \cup X_3$, which are $2^m = [G:N]$ and $n+1 = \mathrm{gen}(G)+1$ respectively, giving equality in (8.1), as desired. □

What about an upper bound for $\mathrm{gen}(\mathrm{Core}(G))$ for a not necessarily abelian group G? Can we even expect the core quandle of, say, a free group on more than one generator to be finitely generated? At first sight it seems implausible that the *symmetric* expressions (2.2) in the elements of some finite set X should be able to represent *arbitrary* elements of G, which need not have any sort of symmetry – unless, perhaps, we can somehow arrange that most of the terms on, say, the right sides of our expressions (2.2) cancel one another, while the left sides carry the structure of our elements.

Surprisingly, we can do this. The key idea is that the distinction between free abelian groups and free groups concerns commutators, and that if for every pair of generators $g_i,\ g_j\ (i<j)$ of our free group, we include in the set with which we plan to generate $\mathrm{Core}(G)$ the elements $g_i,\ g_j$ and $g_i\,g_j$, then $g_i^{-1},\ g_j^{-1}$ and $g_i\,g_j$, multiplied in one order, give the commutator $[g_i,g_j]$, while multiplied in the reverse order, they give 1 :

$$(8.6)\qquad g_i^{-1}\,g_j^{-1}\,(g_i\,g_j)\ =\ [g_i,g_j],\qquad (g_i\,g_j)\,g_j^{-1}\,g_i^{-1}\ =\ 1.$$

I will describe below how to use this fact to get a generating set of cardinality 2^n for the core of a free group on n generators, then show in Theorem 8.2 how to improve that bound somewhat for more general finitely generated groups.

Let G be the free group on generators $g_1,\dots,g_n$, and let X be the set of all 2^n products $g_{i_1}\dots g_{i_r}$ with $0\le r\le n$ and $i_1<\dots<i_r$. (In particular, X contains the empty product, 1.)

Given $z\in G$, we wish to find an expression (2.2) with all x_i in X, which has in G the value z.

Since $1\in X$, we can, by using 1 for various x_i, represent in the form (2.2) any symmetric string of elements of X with exponents ±1 (with no restriction that these exponents alternate between $+1$ and -1).

Let G' be the commutator subgroup of G, so that G/G' is free abelian on the images of $g_1,\dots,g_n$. As in the proof of Theorem 8.1, we can find a word w_0 of the form (2.2) in the elements of X which, evaluated in G/G', agrees with z. Thus if, instead, we evaluate w_0 in G, it gives an element z_0 which is congruent to z modulo G'. Say $z=u\,z_0$ with $u\in G'$.

The group G' is generated by conjugates in G of elements $[g_i,\,g_j]$ with $1\le i<j\le n$. Each such conjugate will be the value of an expression $v\,g_i^{-1}g_j^{-1}(g_i\,g_j)\,v^{-1}$, where v is an expression in the elements of X, and by v^{-1} we mean the expression gotten by reversing the order of factors and interchanging exponents $+1$ and -1. Let w_1 denote a word gotten by multiplying together a family of such expressions for conjugates of commutators, and inverses of such expressions, which, when evaluated in G, gives u.

Now let $\overline{w_1}$ denote the word gotten by reversing the order of the terms from X appearing in w_1 (without changing the exponents $+1$ and -1), and take $w=w_1\,w_0\,\overline{w_1}$. Since w_0 was symmetric, w will be symmetric, hence when evaluated in G, it gives a member of the subquandle of $\mathrm{Core}(G)$ generated by X. Moreover, as noted earlier, our expressions in w_1 for commutators, when reversed in $\overline{w_1}$, give expressions which, evaluated in G, give 1, hence the same is true for the formal conjugates $v\,g_i^{-1}g_j^{-1}(g_i\,g_j)\,v^{-1}$ we used, hence $\overline{w_1}$ itself, evaluated in G, gives 1. Hence $w=w_1\,w_0\,\overline{w_1}$, evaluated in G, gives $u\,z_0\,1=z$, as desired. So X indeed generates $\mathrm{Core}(G)$.

The next result records the consequence of the above bound, then notes how it can be strengthened.

Theorem 8.2. *If G is a finitely generated group with $\mathrm{gen}(G)=n$, then*

$$(8.7)\qquad \mathrm{gen}(\mathrm{Core}(G))\ \le\ 2^n.$$

More sharply, if N is the subgroup of G generated by all squares (a normal subgroup), and $\mathrm{gen}(G/N)=m\le n$, we have

$$(8.8)\qquad \mathrm{gen}(\mathrm{Core}(G))\ \le\ (1+n+n(n{-}1)/2)+2^m-(1+m+m(m{-}1)/2).$$

Namely, if we take a generating set $\{g_1,\dots,g_n\}$ for the group G such that the images in G/N of $g_1,\dots,g_m$ generate G/N, while $g_{m+1},\dots,g_n\in N$, then a generating set X for $\mathrm{Core}(G)$ with the above cardinality is given by the set of those products $g_{i_1}\dots g_{i_k}$ (including the empty product, with $k=0$) such that $i_1<\dots<i_k$, and either $i_k\le m$, or $k\le 2$.

Proof. Above, we established (8.7) under the simplifying assumption that G was the free group on n generators. Since any n-generator group is a homomorphic image of such a free group, the same bound holds for all n-generator groups.

To get the sharper bound (8.8), note first that starting with any n-element generating set for G, we can index it so that the images of $g_1,\dots,g_m$ generate G/N, then modify each of $g_{m+1},\dots,g_n$ by a product of terms $g_1,\dots,g_m$ so that the new $g_{m+1},\dots,g_n$ all have trivial image in G/N, as in the last sentence of the theorem.

Now let X be the set of products of elements of $\{g_1,\dots,g_n\}$ described in that same sentence. To count the elements of X, note that the numbers of such products of $0,\ 1$ and 2 factors from $\{g_1,\dots,g_n\}$ are respectively $1,\ n$, and $n(n-1)/2$, while the set of products arising from arbitrary subsets of $\{g_1,\dots,g_m\}$ has 2^m elements. These two sets intersect in the set of products of $0,\ 1$ and 2 factors from $\{g_1,\dots,g_m\}$, which has cardinality $1+m+m(m-1)/2$, which we therefore subtract off; so the cardinality of X is indeed the right-hand side of (8.8).

Given any $z \in G$, let us now describe how to represent it as a symmetric expression in the elements of X. We choose the middle term of the expression to be a member of X having the same image in G/N as z has. As in the proof of Theorem 8.1 (but without the complication of splitting apart products $g_{i_1} \dots g_{i_k} g_j$), we surround that term symmetrically with terms $g_1^{\pm 1}, \dots, g_n^{\pm 1}$, so that the result has the same image in the abelian group G/G' as z. Finally, as in the discussion of the case of free G, we surround the resulting expression with expressions which, on the left-hand side, give a product of conjugates of commutators $[g_i, g_j]$ $(1 \leq i < j \leq n)$ which brings our expression to exactly the value z, while on the right-hand side, they reduce to 1. We have thus written z as a $\lhd$-expression in elements of X. $\square$

Note that if $m = n$ above, then the lower bound of Theorem 8.1 and the upper bound of the above theorem agree, and we get the exact result $\mathrm{gen}(\mathrm{Core}(G)) = 2^n$.

In the opposite direction, if $m \leq 2$, no subsets of $\{g_1, \dots, g_m\}$ have > 2 elements, so the upper bound of (8.8) simplifies to $1 + n + n(n-1)/2$; but this is in general larger than the lower bound of (8.1).

We have seen that the lower bound of (8.1) is witnessed by abelian groups, but we ask

Question 8.3. *Can the upper bound of* (8.8) *be improved?*

Of course, that bound can be strengthened for groups satisfying additional conditions. For instance, if in some group G with generators $g_1, \dots, g_n$ as shown, we know that a certain commutator $[g_i, g_j]$ is 1, or more generally, is expressible as a product of conjugates of other commutators, and $j > m$, then the generator $g_i g_j$, no longer needed to get an expression for $[g_i, g_j]$ as in (8.6), can be dropped from our set X.

I have not examined

Question 8.4. *If a group* G *is* finitely presented*, is the same true of the involutory quandle* $\mathrm{Core}(G)$ *? If so, what bound can be put on the number of relators needed by a presentation of* $\mathrm{Core}(G)$*, in terms of the numbers of generators and relators in a presentation of* G *?*

We end this note with a few tangential observations.

9. Comparison with heaps

A derived operation on groups related to the core quandle operation $\lhd$ is the ternary operation

(9.1) $\quad \tau(x, y, z) \ = \ x\, y^{-1} z,$

which satisfies the identities

(9.2) $\quad \tau(\tau(v, w, x), y, z) \ = \ \tau(v, \tau(y, x, w), z) \ = \ \tau(v, w, \tau(x, y, z)),$

(9.3) $\quad \tau(x, x, y) \ = \ y \ = \tau(y, x, x).$

A set with an operation τ satisfying (9.2) and (9.3) is called a *heap.* (See [3, Exercises 9.6:10-11] for some background and references.) For G a group, let us write $\mathrm{Heap}(G)$ for the heap with the same underlying set as G, and the operation (9.1).

As with involutory quandle structures, the heap structure on $\mathrm{Heap}(G)$ does not determine the group structure: again, every right or left translation operation of the group structure is an automorphism of the heap structure. But in contrast to the case of involutory quandles, every heap structure on a nonempty set H does arise as above from a group structure on H, which is unique *up to isomorphism,* and which becomes unique as soon as one chooses an element $e \in H$ to be the identity element. The group structure is then given by

(9.4) $\quad x\, y \ = \ \tau(x, e, y), \quad x^{-1} \ = \ \tau(e, x, e).$

Because of this near-equivalence with groups, heaps are not much studied for their own sake, though one sometimes calls on the concept in situations where a natural heap structure exists but a natural group structure does not. Namely, given two objects C and D of a category, the set of isomorphisms $C \to D$ has only a natural structure of heap, given by the same formula (9.1).

The core quandle structure on the underlying set of a group is, clearly, expressible in terms of the heap structure:

(9.5) $\quad x \lhd y \ = \ \tau(x, y, x).$

But this loses much more information about the group than the heap structure did. As we have seen, not every involutory quandle arises from a group, or is even embeddable in one arising in that way, and when it does arise from a group, it need not determine that group up to isomorphism (Lemma 7.4).

10. A class of structures weaker than involutory quandle structures

In this note, special behavior has repeatedly involved the exponent 2 in groups (e.g., Lemma 4.1, Proposition 5.1(ii), the second paragraphs of Proposition 6.1 and Theorem 8.1, and Theorem 8.2). A generalization of the subject, in which more exponents can be expected to show such behavior, would be to study, for general $n > 1$, the binary operator $\lhd_n$ on underlying sets of groups defined to carry the terms x_1 and x_0 of a trajectory to x_n; in other words,

$$(10.1) \qquad x \lhd_n y \ = \ x\,(y^{-1}x)^{n-1}.$$

The operation we have called $\lhd$ is in this notation $\lhd_2$. For $n > 2$, $\lhd_n$ is not, in general, a quandle operation.

If $(x_i)_{i\in\mathbb{Z}}$ is a trajectory in a group, and S any subset of $\mathbb{Z}$, then it is not hard to show that the set of terms generated under $\lhd_n$ by $\{x_i \mid i \in S\}$ will have the property that each of its members is x_j for some j which is both congruent modulo n to some member of S and congruent modulo $n-1$ to some (possibly different) member of S. Note also that the right-hand side of (10.1) has value x if and only if $(y^{-1}x)^{n-1} = 1$, and value y if and only if $(y^{-1}x)^n = 1$. So it seems that the $\lhd_n$-analogs of core quandles of groups will show interesting behavior involving exponents that divide n or $n-1$.

11. On language and notation

When I first looked at the operation $x\,y^{-1}x$ on groups, and the identities it satisfies, not knowing that these had already been studied, I wrote a draft of this note in which a set with an operation satisfying those identities was called a “flip-set”, since that operation can be looked at as flipping y past x in the trajectory they generate. After learning that such structures had already been studied, I brought this note into conformity with standard language. However, I find “involutory quandle” cumbersome compared with “flip-set”. I leave it to workers more involved in the subject to decide whether it might be worth switching to a name such as “flip-quandle”.

The notation I originally used for $x\,y^{-1}x$ was $x \natural y$ (which I read “ x flip y ” – I don’t know how $x \lhd y$ is pronounced). It might in some contexts be convenient to distinguish the operations of $\mathrm{Conj}(G)$ and $\mathrm{Core}(G)$ as $\lhd$ and $\natural$. (The quandle operations $x^n\,y\,x^{-n}$, and the non-quandle operations (10.1) discussed above could then be distinguished as $\lhd_n$ and $\natural_n$.)

12. Acknowledgements

I am indebted to Yves de Cornulier and Ualbai Umirbaev for pointing out that the objects I was calling flip-sets are known as involutory quandles, to Valeriy Bardakov, J. Scott Carter, and Józef H. Przytycki for pointing me to related material on the subject, and to the referee for several helpful suggestions.

References

[1] V. Bardakov, T. Nasybullov and M. Singh, *Automorphism groups of quandles and related groups,* Monatsh. Math. **189** (2019) 1–21. MR3948284

[2] Valeriy Bardakov, Timur Nasybullov and Mahender Singh, *General constructions of biquandles and their symmetries*, `https://arxiv.org/pdf/1908.08301.pdf` .

[3] George M. Bergman, *An Invitation to General Algebra and Universal Constructions,* 2015, Springer Universitext, x+572 pp.. `http://dx.doi.org/10.1007/978-3-319-11478-1` . MR3309721

[4] J. Scott Carter, *A Survey of Quandle Ideas,* pp. 22-53 in *Introductory lectures on knot theory,* Series on Knots and Everything, v. 46, World Sci. Publ., 2012. MR2885229. `https://arxiv.org/pdf/1002.4429.pdf` .

[5] I. M. Chiswell, *Locally invariant orders on groups,* Internat. J. Algebra Comput. **16** (2006) 1161–1179. MR2286427

[6] Mieczysław K. Dąbkowski and Józef H. Przytycki, *Burnside obstructions to the Montesinos-Nakanishi 3-move conjecture*, Geometry and Topology **6** (2002) 355–360. MR1914572. `https://arxiv.org/abs/math.GT/0205040`

[7] Mieczysław K. Dąbkowski and Józef H. Przytycki, *Unexpected connections between Burnside groups and knot theory,* Proc. Natl. Acad. Sci. USA **101** (2004) 17357–17360. MR2110443. `https://arxiv.org/abs/math.GT/0309140`

[8] David Joyce, *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Algebra **23** (1982) 37–65. MR0638121

[9] Józef H. Przytycki and Witold Rosicki, *The topological interpretation of the core group of a surface in* S^4, Canad. Math. Bull. **45** (2002) 131–137. MR3363816. `https://arxiv.org/abs/math.GT/0403475`

[10] Wikipedia, *Racks and quandles*, `https://en.wikipedia.org/wiki/Quandle` .

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
Email address: `gbergman@math.berkeley.edu`