AUSTRALASIAN JOURNAL OF COMBINATORICS
Volume **45** (2009), Pages 263–276

On an inverse Cayley problem

John McCabe   Kathryn Weld

Department of Mathematics and Computer Science
Manhattan College
Riverdale, NY 10471
U.S.A.

John.McCabe@manhattan.edu   Kathryn.Weld@manhattan.edu

Abstract

Let G be a group. We will call G *a group with Cayley data* if we are given all three of the following: the underlying set G; the collection of all Cayley sets of G; and for each Cayley subset S of G, the corresponding Cayley graph $\mathrm{Cay}(G, S)$. Is it then possible, from the Cayley data, to reconstruct the binary operation of the group? Is it possible to determine the isomorphism class of the group? We show that there are groups for which the reconstruction of the group operation is *not* possible, and we call such a group an *ambiguous group*. We completely characterize ambiguous groups, discuss some properties of the associated Cayley graphs, and we show that the Cayley data for any group does determine the isomorphism class of the group.

1 Introduction

Cayley digraphs were introduced by Cayley in 1878 [2] as a graphical representation of an abstract group, and used by Coxeter and Moser [3] to study groups given by generators and relators. The inverse problem we wish to consider has to do with a group G, for which we are given "Cayley data". That is, we are given either the Cayley digraphs for G, or the Cayley graphs for G. If Γ is a connected Cayley digraph for G, whose edges are labeled, then it is well known that the group operation for G may be recovered from the information provided by Γ. A single connected digraph will suffice. What if, instead of a connected Cayley digraph for G, the "Cayley data" consists one or more of the Cayley graphs for G? We now assume that each graph is given simply as a graph, with no edge labeling. It may be shown that knowledge of a single graph is not enough. For example, the Cayley graph $\mathrm{Cay}(Z_6, \{1, 5\})$ is isomorphic, as a graph, to the Cayley graph $\mathrm{Cay}(S_3, \{(13), (12)\})$, even though the underlying groups are not isomorphic. So instead, let us assume we are given all possible Cayley graphs. We wish to determine how much information may be recovered. This question appears to be new.

In this note, we will show that there are groups whose group operation *cannot* be recovered from this collective information. We call such groups *ambiguous groups*, and we give a complete classification of these groups. We will also show that, for any group G, the complete collection of Cayley graphs contains enough information to determine the isomorphism class of G. The classification will show that *every* Cayley graph of an ambiguous group is a *normal*, or *quasi-abelian* Cayley graph. While our question is new, our classification shows that the ambiguous groups give rise to Cayley graphs which have interesting properties; see, for example, [6], [7].

2 Preliminaries

Let G be a group. A nonempty subset $S \subseteq G$ will be called a *Cayley set of* G provided that $1 \notin S$ and S is inverse closed. The *Cayley graph* $\mathrm{Cay}(G, S)$ is the graph whose vertex set $V_G = G$, with adjacency $a \sim b \Leftrightarrow a^{-1}b \in S$. The neighborhood of an element $a \in V_G$ is the set $N(a) = \{as \mid s \in S\}$.

Definition 2.1. Let G be a group. We will call G *a group with Cayley data*, if we are given all three of the following: the set G; the collection of all Cayley sets of G; and for each Cayley subset S of G, the corresponding Cayley graph $\mathrm{Cay}(G, S)$.

We also point out what we are not given. If S is a Cayley subset of G, we are given $\mathrm{Cay}(G, S)$ as a graph, but the edges are not being associated with corresponding elements of S. Suppose a and b are elements of $V(X) = G$ which are neighbors. Then there is some element c of S such that $b = ac$. The Cayley data does not *directly* provide the identity of c, although we might, or might not, be able to identify c from the information provided.

Proposition 2.2. *Let G be a group with Cayley data. Then the following are determined by the Cayley data:*

(i) the identity element of G,

(ii) for each $a \in G$ the element a^{-1},

(iii) the involutions of G,

(iv) for any element $a \in G$, and any integer n, the element a^n,

(v) the subgroups of G.

Proof. The identity element, 1, is the unique element of G which is not in any Cayley set. Any other element belongs to at least one Cayley set, for example to $G - \{1\}$. Let $a \in G$. If a is an involution, then $\{a\}$ is itself a Cayley subset of G, in which case $a = a^{-1}$ and a^{-1} is determined. If a is not an involution, then $S_a = \{a, a^{-1}\}$ is the only doubleton Cayley set containing a, is uniquely determined by a, and determines a^{-1}. The assertion (iv) is an easy induction argument using $\mathrm{Cay}(G, \{a, a^{-1}\})$. Finally, let $H \subseteq G$. We wish to determine whether H is a subgroup of G. By (ii), above, the

Cayley data determines whether H is inverse closed. If so, then consider the Cayley set $S = H - \{1\}$. Then H is closed with respect to products if and only if for all $a \in S$, the neighborhood of a in $\mathrm{Cay}(G, S)$, $N(a) = \{as \mid s \in S\} \subset H$, and this is determined by the Cayley data. □

Let G be a group with Cayley data. Then G is given as a set of vertices $V_G = \{1_G, g_2, g_3, \dots\}$. Let $a, b \in G$. The problem of *determining the product ab from the Cayley data* is the problem of using the Cayley data to identify which $g \in V_G$ has the property that $g = ab$. Since we are given $b \in V_G$ and all Cayley sets and their associated Cayley graphs, this reduces to the problem of identifying, in the neighborhood $N(a) = \{u, v\}$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$, precisely which element u or v is the element ab. We illustrate this in Fig. 1, by showing a graph fragment.

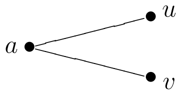

Figure 1: A sample graph fragment

The Cayley data for a group does not provide labels for the edges. So, this graph fragment is meant to illustrate the fact that, while we know $N(a) = \{u, v\} = \{ab, ab^{-1}\}$, we do not know which of u or v is ab, because we do not know which edge corresponds to multiplication by b, and which to b^{-1}. When the product ab cannot be determined from a, b and the Cayley data for G, we say that ab is an *ambiguous product.*

Definition 2.3. Let G be a group with Cayley data. A group G will be called an *ambiguous group* if, given the Cayley data for G, G has an ambiguous product.

Let G be any group. Let G^{Op} denote the opposite group associated with G, that is, the set G with the operation $a \bullet b = ba$. Observe that any Cayley subset S of G is necessarily a Cayley subset of G^{Op}. Let $\mathrm{Cay}^{Op}(G, S) = \mathrm{Cay}(G^{Op}, S)$ be the opposite graph.

Theorem 2.4. *Let G be any group with Cayley data, and let S be any Cayley set of G. The opposite graph,* $\mathrm{Cay}^{Op}(G, S)$*, is determined by the Cayley data for G.*

Proof. The vertices of $\mathrm{Cay}^{Op}(G, S)$, are the elements of the set $G^{Op} = G$, so are given by the Cayley data. Let a and $b \in G$. It is easy to see that $a \sim b$ in $\mathrm{Cay}(G, S) \Leftrightarrow a^{-1} \sim b^{-1}$ in $\mathrm{Cay}^{Op}(G, S)$. Since inverses are given by the Cayley data, we see that the edge set of the opposite graph is given by the Cayley data, so then it follows that $\mathrm{Cay}^{Op}(G, S)$, is determined by the Cayley data for G. □

Let G be any group such that the following two conditions hold:

(i) $G \neq G^{Op}$, and

(ii) for any Cayley subset $S \subseteq G$, $\mathrm{Cay}(G, S) = \mathrm{Cay}(G^{Op}, S)$.

It should be clear that G is ambiguous. The reader will readily verify that the quaternion group Q_8 is such a group, so that ambiguous groups exist. In section 4 we will classify ambiguous groups, and as a consequence of that classification it will become clear that *only* groups satisfying (i) and (ii) are ambiguous. In the next proposition we will show that groups which satisfy condition (ii) above may be characterized by the following condition:

Definition 2.5. A group G is called a *balanced group* if for any elements a and b of G, either a and b commute, or $a^2 = b^2$.

For examples, observe that an abelian group is balanced, and that the quaternion group Q_8 is balanced.

Proposition 2.6. *Let G be a balanced group. Then for any Cayley subset S of G, we have* $\mathrm{Cay}(G, S) = \mathrm{Cay}(G^{Op}, S)$*. In consequence, a balanced group G and its opposite group G^{Op} have identical Cayley data.*

Before beginning the proof we would like to mention that the converse of Proposition 2.6 is true as well, and may be proved by similar methods. The proof is not difficult, but since we don't use the converse directly in anything that follows, and since it will follow from the Classification Theorem 5.5, we omit the proof.

Proof. Let S be a Cayley subset of a balanced group G. Let $a \sim b$ in $\mathrm{Cay}(G, S)$, so that $a^{-1}b = c \in S$. If a and b commute, then b also commutes with a^{-1}. Now, $a^{-1} \bullet b = ba^{-1} = a^{-1}b \in S$, which implies that $a \sim b$ in $\mathrm{Cay}(G^{Op}, S)$.

Suppose instead that $a^2 = b^2$. Then $ab^{-1} = a^{-1}b$, but $a^{-1}b = c \in S$. Now $a \sim b$ in $\mathrm{Cay}(G^{Op}, S)$ if and only if $a^{-1} \bullet b \in S$ and $a^{-1} \bullet b = ba^{-1} = (ab^{-1})^{-1} = c^{-1}$, which is in S, since S is inverse-closed. Thus every edge of $\mathrm{Cay}(G, S)$ is also an edge of $\mathrm{Cay}(G^{Op}, S)$. This shows just as well that every edge of $\mathrm{Cay}(G^{Op}, S)$ is also an edge of $\mathrm{Cay}(G^{Op^{Op}}, S) = \mathrm{Cay}(G, S)$, proving that $\mathrm{Cay}(G, S) = \mathrm{Cay}(G^{Op}, S)$.

□

Corollary 2.7. *Let G be a non-abelian balanced group. Then G is an ambiguous group.*

Proof. Since G is balanced, G and G^{Op} have identical Cayley data. Since G is non-abelian, G and G^{Op} have different binary operations. That is, there are elements a and b of G with $ab \neq ba = a \bullet b$.

But since, for any Cayley set S, the graphs $\mathrm{Cay}(G, S)$ and $\mathrm{Cay}(G^{Op}, S)$ are identical, it follows that the Cayley data is insufficient to distinguish ab and $a \bullet b = ba$. Thus we cannot determine ab from the Cayley data. □

3 The Subgroup Theorem

In this section we obtain some consequences of ambiguity on the structure of G.

Proposition 3.1. *Let G be a group with Cayley data. If a is an involution of G, and $b \in G$, then the products ab and ba are unambiguous. Moreover, if the neighborhood $N(a)$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$ contains an involution, then neither ab nor ab^{-1} may be ambiguous.*

Proof. We leave part 1 to the reader. For the second part, assume we are given a and b, and we wish to compute ab. Let us represent the neighborhood $N(a)$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$ by $N(a) = \{u, v\}$, and assume without loss of generality, that $u = ab$. If u is an involution, then $a^{-1}u = b$, and this is unambiguously determined, by part 1. But this then affords a method of identifying the element u as the desired product ab, hence ab is unambiguous, and we can also conclude that $ab^{-1} = v$. The same argument may be modified in case v is the involution. Details are left to the reader. □

Lemma 3.2. *Let G be a group with Cayley data. Let a and b be elements of G, and let $H = \langle a, b\rangle$. Then*

(I) $H \cong Q_8$ if and only if the following four conditions hold:

1. *$|a| = |b| = 4$;*
2. *$a^2 = b^2$,*
3. *the neighborhood $N(a)$ in the graph $\mathrm{Cay}(G, \{b, b^{-1}\})$ is a Cayley set of G,*
4. *no proper subset of $N(a)$ in the graph $\mathrm{Cay}(G, \{b, b^{-1}\})$ is a Cayley set of G; and*

(II) the Cayley data suffices to determine whether $H \cong Q_8$.

Proof. Observe first that, by Proposition 2.2, the subgroup H determined by the elements a and b is determined by the Cayley data. Then, since conditions 1-4 are determined by the Cayley data for G, in order to prove (II), it will suffice to establish statement (I).

($\Leftarrow$) Assume conditions 1-4 hold. Consider $N(a) = \{ab, ab^{-1}\}$. If $ab = ab^{-1}$, then $b = b^{-1}$, hence $b^2 = 1$ contradicting statement 1. We conclude $N(a)$ contains two distinct elements.

Since $N(a)$ is a Cayley set, it is inverse closed. Since no proper subset is a Cayley set, $(ab)^{-1} \neq ab$. Therefore $(ab)^{-1} = ab^{-1} \Rightarrow b^{-1}a^{-1} = ab^{-1} \Rightarrow a^{-1} = bab^{-1}$. Thus H satisfies the defining relations for the quaternion group Q_8, and is therefore a homomorphic image of Q_8, hence $|H|$ divides 8. Now $b \in H$, and condition 1 implies that 4 divides $|H|$, but since b does not commute with a we conclude that $b \notin \langle a\rangle$. From this we conclude $|H| = 8$, and therefore that $H \cong Q_8$. We leave the details of the other direction to the reader. □

Theorem 3.3. The Subgroup Theorem

Let G be an ambiguous group, with ambiguous product ab. Let $H = \langle a, b\rangle$. Then $H \cong Q_8$.

Proof. By Lemma 3.2, we need only show that conditions 1-4 of that Lemma hold. We may assume $a \neq 1_G$, $b \neq 1_G$, and by Proposition 3.1 that neither a nor b are involutions, otherwise the product would be unambiguous. By Proposition 3.1, we know that no proper subset of $N(a)$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$ is a Cayley set.

We show first that if ab is ambiguous, then $a^2 = b^2$. Look at the two Cayley graph fragments in Fig. 2. In this figure, the left fragment occurs in $\mathrm{Cay}\big(G, \{b, b^{-1}\}\big)$, while the right fragment uses Cayley set $\{a, a^{-1}\}$. The dotted circle frames a Cayley set. While we have labeled the vertices with the elements ab, ab^{-1}, $b^{-1}a^{-1}$ and $b^{-1}a$, we do not in fact know which element is which.

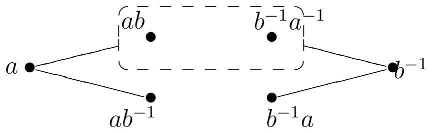

Figure 2: Comparing neighborhoods in $\mathrm{Cay}\big(G, \{b, b^{-1}\}\big)$ and $\mathrm{Cay}\big(G, \{a, a^{-1}\}\big)$. The dotted circle frames a Cayley set.

What we really see are the neighborhoods of a and of b^{-1}. These are depicted in Fig. 3. We will recognize at least one Cayley set, because the union of neighborhoods $N(a)$ and $N(b)$ must, at the least, contain the pair ab, $b^{-1}a^{-1}$.

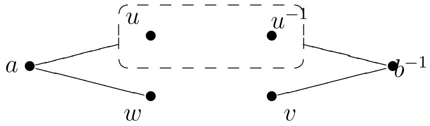

Figure 3: A more representative picture of the Neighborhood Comparison.

If this is the only Cayley pair, we can conclude that $ab = u$, the unique element that is both in $N(a)$ and in the Cayley subset of $N(a) \cup N(b)$. Because ab is ambiguous, we conclude that there must be a second Cayley set $\{v, w\} = \{ab^{-1}, b^{-1}a\}$. Then $ab^{-1} = (b^{-1}a)^{-1} = a^{-1}b \Rightarrow a^2 = b^2$.

Next we show that if ab is ambiguous, then $a^4 = b^4 = 1$. We examine the two graph neighborhoods illustrated in Fig. 4. Again, the dotted circle frames a Cayley set.

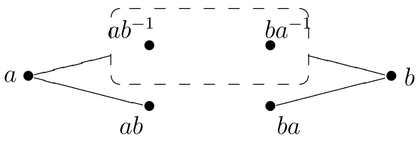

Figure 4: Comparing the neighborhoods $\mathrm{Cay}\big(G, \{b, b^{-1}\}\big)$ and $\mathrm{Cay}\big(G, \{a, a^{-1}\}\big)$. The dotted circle frames a Cayley set.

In Fig. 4, the left fragment uses the Cayley set $\{b, b^{-1}\}$, while the right fragment uses $\{a, a^{-1}\}$. As before, the inverse pair $\{ab^{-1}, ba^{-1}\}$ will determine ab, *unless* $\{ab, ba\}$ is also a Cayley set. But then, $ab = (ba)^{-1} = a^{-1}b^{-1} \Rightarrow a^2 = b^{-2} = b^2 \Rightarrow b^4 = 1 = a^4$.

Finally, we we establish that if ab is ambiguous, then $N(a)$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$ is a Cayley set. Again, let the neighborhood $N(a) = \{u, v\}$ in $\mathrm{Cay}(G, \{b, b^{-1}\})$. Now we compare the neighborhood $N(a)$ in $\mathrm{Cay}(G, \{u, u^{-1}\})$, with $N(a)$ in $\mathrm{Cay}(G, \{v, v^{-1}\})$. Assume, without loss of generality, that $ab = u$, and $ab^{-1} = v$.

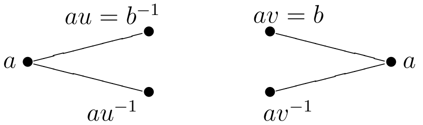

Figure 5: Comparing the neighborhoods $\mathrm{Cay}\big(G, \{u, u^{-1}\}\big)$ and $\mathrm{Cay}\big(G, \{v, v^{-1}\}\big)$.

We refer to the graph fragments in Fig. 5, where the left fragment is from $\mathrm{Cay}\big(G, \{u, u^{-1}\}\big)$ and the right fragment is from $\mathrm{Cay}\big(G, \{v, v^{-1}\}\big)$. Since $b^{-1} = b^3$ and $b^2 = a^2$, we can deduce that $au = a(ab) = b^{-1}$ and $av = a(ab^{-1}) = b^2b^{-1} = b$. This will determine the product ab — it is the element u, such that $N(a)$ in $\mathrm{Cay}\big(G, \{u, u^{-1}\}\big)$ contains b^{-1}, as opposed to b itself. But ab is ambiguous, so determination by this method must be flawed. In particular, it must be true that both neighborhoods $\{au, au^{-1}\}$ and $\{av, av^{-1}\}$ are exactly the Cayley set $\{b, b^{-1}\}$. We conclude that $au = av^{-1}$, which implies that $u = v^{-1}$, hence $N(a) = \{u, v\}$ is a Cayley set. By Lemma 3.2, this completes the proof. □

Corollary 3.4. *If, in a group with Cayley data, the elements a and b commute, then their product is unambiguous.*

Before going further, perhaps we should set out some facts about any group H that is isomorphic to the quaternion group Q_8. We let i, and j denote the usual generators of the quaternion group, Q_8, whose squares are the element -1. Following this convention, we let k denote ij. The assertions below follow from well known facts about the quaternion group. We leave the details to the reader.

Proposition 3.5. *Let H be a group that is isomorphic to Q_8. Let a and b be elements which generate H. Then H possesses a unique involution which we will denote by -1, and $Z(H)$, the center of H, is the subgroup $\langle -1 \rangle$. Both a and b are of order 4, and $a^2 = b^2 = -1$. The elements, a and b, satisfy the equations $ba = -ab = a^{-1}b = ab^{-1}$, whence $bab = a$, and $b^{-1}ab = a^{-1}$. Moreover, if c is any element of H of order 4, then $c^{-1} = (-1)c$. And, finally, there is a unique isomorphism $\phi : Q_8 \longrightarrow H$ such that $\phi(i) = a$ and $\phi(j) = b$.*

Lemma 3.6. *Let G be a group with Cayley data and let a and b be elements of G, and let $H = \langle a, b \rangle$, and assume that $H \cong Q_8$. Let $\phi : Q_8 \longrightarrow H$ be an isomorphism such that $\phi(i) = a$ and $\phi(j) = b$. Then the Cayley data for G determines $\phi(q)$ for all $q \in Q_8$ except possibly for the elements k and k^{-1}. The set $\{\phi(k), \phi(k^{-1}\}$ is determined by the Cayley data for G.*

Proof. By Proposition 3.5, there is a unique isomorphism $\phi : Q_8 \to H$ such that $\phi(i) = a$, $\phi(j) = b$. Now consider the element i^{-1} of Q_8. The isomorphism ϕ maps i^{-1} to a^{-1}, and, by Proposition 2.2, a^{-1} is determined by the Cayley data for G. Thus $\phi(i^{-1})$ is determined, and similarly, the Cayley data for G determines ϕ on all elements of Q_8 except perhaps k and k^{-1}. Since ϕ is an isomorphism, ϕ must map k to ab, but the Cayley data for G won't determine ab if ab is an ambiguous product. We do know that ab is one of the elements of the neighborhood $N(a) = \{ab, ab^{-1}\}$ in $\text{Cay}(G, \{b, b^{-1}\}$. Since $H \cong Q_8$, by Proposition 3.5, $(ab)^{-1} = ab^{-1}$. Thus $\phi(k) = ab$ is one of the elements of $N(a) = \{ab, ab^{-1}\}$, and $\phi(k^{-1})$ is the other element of $N(a)$. □

Corollary 3.7. *Let G be a group with Cayley data. Let a and b be elements of G, let $H = \langle a, b\rangle$ and assume that $H \cong Q_8$. Then if the product of a and b is unambiguous in G, then all products of elements of H are unambiguous in G.*

Proof. Let $\phi : Q_8 \to H$ be an isomorphism with $\phi(i) = a$ and $\phi(j) = b$. Since $\phi(k) = \phi(ij) = \phi(i)\phi(j) = ab$ is determined by the Cayley data for G, ϕ itself is determined by the Cayley data for G. It follows that the groups operation in H is determined from the group operation in Q_8 via ϕ. □

Corollary 3.8. *Let G be a group isomorphic to Q_8. Then there are exactly two group operations on G which are consistent with the Cayley data for G, namely that of G itself and that of G^{Op}.*

Proof. It follows from Lemma 3.6 that, on G, there are at most two operations consistent with the Cayley data for G. Since $G \cong Q_8$, G is a balanced group. By Corollary 2.7, there are at least two operations consistent with the Cayley data for G, namely the operation of G itself, and that of G^{Op}. □

4 The Structure of Ambiguous Groups

Lemma 4.1. *Let G be a group with Cayley data, let a and b be elements of G whose product is ambiguous. Let $ab = c$. Then the product bc is ambiguous.*

Proof. Let $H = \langle a, b\rangle$. By Theorem 3.3, $H \cong Q_8$. Since $a = cb^{-1}$ we also have $H = \langle b, c\rangle$. Now, suppose that bc is unambiguous. Then by Corollary 3.7, we know that all products in H are unambiguous. In particular, the product ab is unambiguous, contradiction. □

Theorem 4.2. *Let G be a group with ambiguous product ab, and let $H = \langle a, b\rangle$. Let λ be an element of G such that the products $a\lambda$ and $b\lambda$ are unambiguous. Then:*

1. *The product $(a\lambda)(b\lambda)$ is ambiguous; and*

2. *$\lambda \in C_G(H)$.*

3. *The order of every element of G is finite and a divisor of 4.*

4. If λ is an involution of G, then $\lambda \in C_G(H)$.

5. $C_G(H) = \{\lambda \in G \mid \lambda^2 = 1\}$.

Proof. Suppose the product $(a\lambda)(b\lambda)$ is unambiguous. Then in $\mathrm{Cay}(G, \{b\lambda, (b\lambda)^{-1}\})$ consider the graph fragment in Fig. 6.

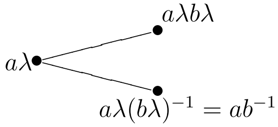

Figure 6: $N(a\lambda)$ in $\mathrm{Cay}(G, \{b\lambda, (b\lambda)^{-1}\})$

Since $(a\lambda)(b\lambda)$ is unambiguously determined, so also is ab^{-1}, and using Proposition 3.5, we have $ab^{-1} = (ab)^{-1}$. Since by Lemma 3.6, the Cayley data determines the set $\{ab, (ab)^{-1}\}$, and since $(ab)^{-1}$ has been determined, it follows that ab is unambiguously determined, a contradiction. We conclude that the product $(a\lambda)(b\lambda)$ is ambiguous. This establishes (1).

Let $K = \langle a\lambda, b\lambda\rangle$. By Theorem 3.3, $K \cong Q_8$. It follows that $(a\lambda)^2 = (b\lambda)^2$. This implies that $b^{-1}a\lambda ab^{-1} = \lambda$. Put $c = ab$. Within $H \cong Q_8$ one finds, using Proposition 3.5, that $b^{-1}a = c$ and $ab^{-1} = c^{-1}$. Thus $c\lambda c^{-1} = \lambda$, which implies that λ and c commute.

By Corollary 3.4, the product $c\lambda$ is unambiguous. By Lemma 4.1 the product bc is ambiguous. Since $b\lambda$ and $c\lambda$ are unambiguous while bc is ambiguous, we may apply what was just proven to conclude that λ commutes with $bc = a$. It is readily seen that $H = \langle c, a\rangle$ and that therefore $\lambda \in C_G(H)$. This establishes (2). In particular, applying Proposition 3.1, this implies that every involution of G is a member of $C_G(H)$, establishing (4).

To prove (3) we need to show that every element of G has an order that is finite and a divisor of 4. Let $\lambda \in G$. If $a\lambda$ is ambiguous, then by Theorem 3.3, $|\lambda| = 4$. Similarly if $b\lambda$ is ambiguous, then $|\lambda| = 4$.

In either case the assertion is true. So we may assume that the products $a\lambda$ and $b\lambda$ are unambiguous. By Theorem 4.2, parts (1) and (2), the product $(a\lambda)(b\lambda)$ is ambiguous and $\lambda \in C_G(H)$. If we set $K = \langle a\lambda, b\lambda\rangle$ then, again by the Subgroup Theorem, $K \cong Q_8$. This implies, in particular, that $(a\lambda)^4 = 1$. However since $\lambda \in C_G(H)$, we have $(a\lambda)^4 = a^4\lambda^4 = (1)\lambda^4 = \lambda^4$. Thus $\lambda^4 = 1$.

To complete the proof that $C_G(H) = \{\lambda \in G \mid \lambda^2 = 1\}$, it suffices to show that if $\lambda \in C_G(H)$, then $\lambda^2 = 1$. Let $\lambda \in C_G(H)$. It follows that λ commutes with both a and b. By Corollary 3.4 the products $a\lambda$ and $b\lambda$ are unambiguous. By Theorems 3.3 and 4.2, $\langle a\lambda, b\lambda\rangle \cong Q_8$. Note that $H = \langle a, b\rangle \cong Q_8$, whence $aba = b$, similarly $a\lambda b\lambda a\lambda = b\lambda$. Since at the same time $a\lambda b\lambda a\lambda = aba\lambda^3 = b\lambda^3$, it follows that $\lambda^2 = 1$. □

Corollary 4.3. *Let G be a group with ambiguous product ab, and let $H\langle a, b\rangle$. The subgroup $C_G(H)$ is abelian, and $C_G(H) \lhd G$.*

Proof. Since $\lambda^2 = 1$ for all elements $\lambda \in C_G(H)$, $C_G(H)$ is abelian. Since $C_G(H) = \{\lambda \in G \mid \lambda^2 = 1\}$, it is clear that $C_G(H)$ is closed under conjugation by elements of G. □

Proposition 4.4. *Let G be a group with ambiguous product ab, let $H = \langle a, b\rangle$ and let -1 be the unique involution of $H \cong Q_8$. If λ is any element of G of order 4, then $\lambda^2 = -1$.*

Proof. Let λ be an element of G of order 4. If $\lambda \in H$, then $\lambda^2 = -1$. Therefore we may assume that $\lambda \notin H$.

If both $a\lambda$ and $b\lambda$ are unambiguous, then by Theorem 4.2, $\lambda \in C_G(H)$, and $\lambda^2 = 1$, contradicting the assumption that $|\lambda| = 4$. We conclude that at least one of $a\lambda$ and $b\lambda$ must be ambiguous.

Without loss of generality, we may assume that it is $a\lambda$ that is ambiguous. By Theorem 4.2, the subgroup $K = \langle a, \lambda\rangle \cong Q_8$. It follows that $a^2 = \lambda^2$, but $a^2 = -1$, so $\lambda^2 = -1$. □

Theorem 4.5. *Let G be a group with ambiguous product ab. Let $H = \langle a, b\rangle$, and let $c = ab$. Then each of the subgroups $\langle a\rangle, \langle b\rangle$ and $\langle c\rangle$ is normal in G, and $H \lhd G$.*

Proof. Let g be any element of G. Consider the elements ag, bg, cg. If any two of these are unambiguous, then by Theorem 4.2, g is in the centralizer of H in G, which is contained in each of the normalizers of H, $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ in G. Now suppose that no two of the above products are unambiguous. It follows that two (or maybe three) of these products are ambiguous. Without loss of generality, we may assume that the products ag, and bg are ambiguous. By Theorem 3.3, $\langle a, g\rangle \cong Q_8$ which implies that $g^{-1}ag = a^{-1}$ so that $g^{-1}\langle a\rangle g$ is contained in $\langle a\rangle$ and so in H. Similarly $g^{-1}bg = b^{-1}$ and $g^{-1}\langle b\rangle g \subseteq H$. Now consider the element $c = ab$. We have $g^{-1}abg = (g^{-1}ag)(g^{-1}bg) = a^{-1}b^{-1} = ab = c$. Thus g commutes with c, and therefore of course g is in the normalizer of $\langle c\rangle$ in G. Since H is the union of $\langle a\rangle$, $\langle b\rangle$ and $\langle c\rangle$, it follows that g is in the normalizer of H in G. As g was arbitrary in G , this shows that H is normal in G. The proof establishes at the same time that $\langle a\rangle$, $\langle b\rangle$, and $\langle c\rangle$ are normal in G. □

5 The Classification Theorem

Definition 5.1. Let G be a group, and let ϕ be an automorphism of G. Let A be a subgroup of G. We say that A *is stable under* ϕ if $\phi\mid_A$ is an automorphism of A.

Let $H = \langle a, b\rangle$ be a group which is isomorphic to Q_8. Now $\langle a\rangle$ is a normal subgroup of H, which implies that $\langle a\rangle$ is stable under an inner automorphism of H. Similarly, $\langle b\rangle$ is stable under an inner automorphism of H. We next show that the only automorphisms ϕ of H which stabilize the subgroups $\langle a\rangle$ and $\langle b\rangle$ are inner automorphisms.

Lemma 5.2. *Let $H = \langle a, b\rangle$ be a group which is isomorphic to Q_8. Let ϕ be a automorphism of H, and suppose that $\langle a\rangle$ and $\langle b\rangle$ are stable under ϕ. Then ϕ is an inner automorphism of H.*

Proof. First observe that ϕ must map a to a generator of $\langle a\rangle$, and b to a generator of $\langle b\rangle$, so that $\phi(a) = \pm a$ and $\phi(b) = \pm b$. Hence there may be at most four automorphisms of H which stabilize the subgroups $\langle a\rangle$ and $\langle b\rangle$.

Since for any group G, $\mathrm{Inn}(G) \cong G/Z(G)$, we have $\mathrm{Inn}(H) \cong H/\langle -1\rangle$, which has order 4. Since every inner automorphism stabilizes $\langle a\rangle$ and $\langle b\rangle$, it follows that the automorphisms of H that stabilize $\langle a\rangle$ and $\langle b\rangle$ are exactly the inner automorphisms. □

Theorem 5.3. *Let G be a group with ambiguous product ab, and let $H = \langle a, b\rangle$. Then $G = H \cdot C_G(H)$.*

Proof. By Theorem 4.5, $H \lhd G$. If $\lambda \in G$, then λ determines an automorphism ϕ_λ of H by conjugation: $\phi_\lambda : x \mapsto \lambda^{-1}x\lambda$. Also by Theorem 4.5, $\langle a\rangle, \langle b\rangle$ are both normal in G. Therefore the mapping ϕ_λ carries each of $\langle a\rangle, \langle b\rangle$ into itself. By Lemma 5.2, ϕ_λ is an inner automorphism of H. Therefore, there is an element $h \in H$ such that $\lambda^{-1}x\lambda = h^{-1}xh, \forall x \in H$. It follows that $h\lambda^{-1}x\lambda h^{-1} = x \Rightarrow (\lambda h^{-1})^{-1}x(\lambda h^{-1}) = x \Rightarrow \lambda h^{-1} \in C_G(H)$, say $\lambda h^{-1} = c$, where $c \in C_G(H)$. Then $\lambda = ch = hc \in H \cdot C_G(H)$. This proves that $G = H \cdot C_G(H)$. □

Corollary 5.4. *Let G be a group with ambiguous product ab, and let $H = \langle a, b\rangle$. Then $Z(G) = C_G(H)$. Consequently, $Z(G) = \{\lambda \in G \mid \lambda^2 = 1\}$, and $Z(G)$ is an elementary abelian 2-group. The Cayley data for a group G determines the center $Z(G)$ of G.*

Proof. Of course, $Z(G) \subseteq C_G(H)$. On the other hand, suppose $\lambda \in C_G(H)$. By Corollary 4.3, $C_G(H)$ is abelian, so λ commutes with all of the elements of $C_G(H)$. And, λ commutes with the members of H, so λ commutes with the members of $H \cdot C_G(H) = G$, proving that $\lambda \in Z(G)$. The remaining assertions follow from Theorem 4.2 and Proposition 2.2. □

Theorem 5.5. The Classification Theorem
Let G be an ambiguous group. Then G is isomorphic to a direct product of the quaternion group Q_8 and an elementary abelian two-group.

Proof. Let a and b be elements of G whose product ab is ambiguous. Let $H = \langle a, b\rangle$. We know that $H \cong Q_8$. Let $C = C_G(H) = Z(G)$. Theorem 4.2 tells us that C is an elementary abelian two-group. From Theorem 5.3, $G = H \cdot C$. Let $A \subseteq C$ be any maximal subgroup of C which does not contain -1. Such a subgroup must exist by Zorn's Lemma. Let $\phi : H \times A \to G$ be defined as follows: $\phi(h, a) = ha$. The reader will easily verify that ϕ is an isomorphism. □

Corollary 5.6. *An ambiguous group is balanced. Consequently the ambiguous groups are precisely the non-abelian groups for which, for all Cayley sets S, we have $\mathrm{Cay}(G, S) = \mathrm{Cay}^{Op}(G, S)$.*

Proof. Let G be ambiguous and let a and $b \in G$. If a and b do not commute, then a and $b \in G - Z(G)$, so both must have order 4, by Corollaries 5.4 and 4.2. But then, by Theorem 4.4, $a^2 = -1 = b^2$, so G is balanced. The remaining statements follow from Corollary 2.7. □

Recall that if every subgroup of G is a normal subgroup, then G is called *Hamiltonian.* These groups were so named by Richard Dedekind, who proved, [4], that every finite non-abelian Hamiltonian group must contain a copy of the quaternion group. The classification of the non-abelian Hamiltonian groups, whether finite or infinite, was completed by Reinhold Baer in 1933, [1], [5]. Baer proved that a group G is a non-abelian Hamiltonian group if and only if $G \cong Q_8 \times A \times B$ with A an elementary abelian two group and B an abelian group with every element of odd order. The following corollary follows immediately from Baer's Theorem and Theorem 5.5.

Corollary 5.7. *Let G be an ambiguous group. Then G is Hamiltonian.*

Let G be a group and S be any Cayley subset of G. Let S^g denote the set of conjugates $\{g^{-1}sg \mid s \in S\}$. A Cayley graph $\mathrm{Cay}(G,S)$ is called *normal* if $S^g = S$, for all $g \in G$, (see, for example, [6]). (These graphs have also been called *quasiabelian*; see, for example, [7]). We will show that if G is an ambiguous group, then for every Cayley set $S \subseteq G$, the graph $\mathrm{Cay}(G,S)$ is normal, or quasi-abelian. The following corollary will be useful:

Corollary 5.8. *Let G be an ambiguous group. The following three statements are equivalent:*

1. *The product ab is ambiguous.*
2. *$H = \langle a, b\rangle \cong Q_8$.*
3. *The elements a and b do not commute.*

Proof. (1) ⇒ (2). This is Theorem 3.3.

(2) ⇒ (3). The result follows from Proposition 3.5.

(3) ⇒ (1). If a and b do not commute then a and $b \in G - Z(G)$, so both must have order 4, by Corollaries 5.4 and 4.2. By Theorem 5.3 and Corollary 5.4, $G = H \cdot Z(G)$, where H is a subgroup of G containing an ambiguous product and $H \cong Q_8$. Then $a = h_1 z_1$ and $b = h_2 z_2$, for suitable $h_1,\ h_2 \in H$, and $z_1,\ z_2 \in Z(G)$. It follows that $ab = (h_1 z_1)(h_2 z_2) = (h_1 h_2)(z_1 z_2)$. Since a and b, do not commute, neither do h_1 and h_2, so h_1 and h_2 must generate H. Now, if ab is unambiguous, then the product $h_1 h_2$ must also be unambiguous. By Corollary 3.7, this implies the Cayley data for G determines all products in H, contradiction. □

Proposition 5.9. *Let G be an ambiguous group. Then for every Cayley set $S \subseteq G$, the graph* $\mathrm{Cay}(G,S)$ *is normal.*

Proof. Let G be an ambiguous group and S be any Cayley subset of G. Let $g \in G$, and $s \in S$. By Corollary 5.6, G is balanced. Consider $g^{-1}sg$. If g and s commute, then $g^{-1}sg = s \in S$. If g and s do not commute, then by Corollary 5.8, the product gs is ambiguous, and the elements g and s generate a subgroup $H \cong Q_8$. Direct computation using Corollary 3.5 now shows that $g^{-1}sg = s^{-1} \in S$, so that $S^g = S$. Since g was arbitrary it therefore follows that $S^g = S$, and so $\mathrm{Cay}(G,S)$ is normal. But S was also arbitrary, and the result follows. □

We now address the question of whether or not the Cayley data determines the isomorphism type of the group.

Lemma 5.10. *Given any group G, the Cayley data for G determines whether or not G is ambiguous.*

Proof. By Corollary 5.6, G is ambiguous if and only if the following two conditions hold:

1. $\mathrm{Cay}(G, S) = \mathrm{Cay}(G^{Op}, S)$ holds for any Cayley set S of G, and

2. G is not abelian.

By Theorem 2.4 the Cayley data for G determine whether or not $\mathrm{Cay}(G, S) = \mathrm{Cay}(G^{Op}, S)$ holds for any Cayley set S of G. So if this condition is not met, G is not ambiguous, and we are done.

Suppose condition 1 holds for G. By Lemma 3.2, for any pair of elements in G, the Cayley data suffices to determine whether or not a and b generate a subgroup isomorphic to Q_8. If some a and b do generate such a group, then G is not abelian, and must be ambiguous. If not, then G cannot be ambiguous by Theorem 3.3. This completes the proof. □

Theorem 5.11. *Let G be any group. Then the isomorphism class for G is determined by the Cayley data for G. Moreover if G is ambiguous, there are precisely two group operation tables for the set G which are consistent with the Cayley data.*

Proof. By Lemma 5.10, the Cayley data for G determines whether G is ambiguous or not. If a group G is not ambiguous, the Cayley data determines the group operation, so it necessarily determines the isomorphism type.

Now we consider the case where G is ambiguous. As in Theorem 5.5, let A be some maximal subgroup of $Z(G)$ with $-1 \notin A$. By Corollary 5.4, the Cayley data for G determines $Z(G)$, but, in general, A need not be uniquely determined. However, since $A \cong Z(G)/\langle -1 \rangle$, the isomorphism class for A *is* determined by the Cayley data and since Theorem 5.5 tells us that $G \cong Q_8 \times A$, it follows that the isomorphism class for G is determined by the Cayley data.

Let H be a subgroup of G which is isomorphic to Q_8, such that $G = H \times A$. We claim that there are precisely two possible multiplications in $H \times A$. Consider two elements of $H \times A$, say (h_1, a_1) and (h_2, a_2). In A, multiplication is unambiguous. However, by Corollary 3.8, there are precisely two multiplications possible for H, corresponding to the inherent multiplications in Q_8 and in ${Q_8}^{Op}$, and thus there are two possible binary operations for $H \times A$ which are consistent with the Cayley data. □

Acknowledgement

The authors thank the members of the Manhattan College Algebraic Graph Theory Seminar, Anetta Bajer, Katalin Bencsath, Richard Goldstone, Carol Hurwitz, Gregory Taylor, Helene Tyler, and Bjorn Schellenberg.

References

[1] Reinhold Baer, *Situation der Untergruppen und Struktur der Gruppe*, S.-B. Heidelberg, Akad. Math.-Nat. Klasse, 2, (1933), 12–17.

[2] Arthur Cayley, The Theory of Groups: Graphical Representations, *Amer. J. Math.* 11 (1878), 139–157.

[3] H.S.M. Coxeter and W.O.J. Moser, *Generators and Relations for Discrete Groups. 4th ed.*, Springer Verlag, New York, 1980

[4] Richard Dedekind, Ueber Gruppen, deren sämmtliche Theiler Normaltheiler sind, *Mathematische Annalen* 48 (1887), 548–561.

[5] Marshall Hall, *The Theory of Groups*, Macmillan NY, 1959.

[6] Benoit LaRose, Francois Laviolette and Claude Tardif, On Normal Cayley Graphs and Hom-Idempotent Graphs, *Europ. J. Combin.* (1998) 19, 867–881.

[7] J. Wang and M.-Y. Xu, A Class of Hamiltonian Cayley Graphs and Parson's Graphs, *Europ. J. Combin.* 18 (1997), 597–600.

(Received 29 Sep 2008; revised 9 Nov 2008)