J. Group Theory **23** (2020), 847–869
DOI 10.1515/jgth-2019-0174

Classification of the affine structures of a generalized quaternion group of order $\geqslant 32$

Wolfgang Rump

Communicated by Evgenii I. Khukhro

Dedicated to B.V. M.

Abstract. Based on computing evidence, Guarnieri and Vendramin conjectured that, for a generalized quaternion group G of order $2^n \geqslant 32$, there are exactly seven isomorphism classes of braces with adjoint group G. The conjecture is proved in the paper.

Introduction

An affine structure of a group G is given by an action $b \mapsto a \cdot b$ of G on the set G which satisfies the symmetry condition $(a \cdot b)a = (b \cdot a)b$ for all $a, b \in G$. For any affine structure, the operation $a + b := (a \cdot b)a$ makes G into an abelian group A so that the action of G on A provides A with a G-module structure. The identity map $G \to A$ is a 1-cocycle. A G-module A which arises in this way is said to be a *brace* [12]. The standard example of a brace is given by the Jacobson radical J of a ring, with the group operation $a \circ b := ab + a + b$ and the action $a \cdot b := b(1 + a)^{-1}$. The group G of a brace A is therefore called the *adjoint group* of A.

If G is finite, an affine structure of G forces G to be solvable [7]. Not every finite solvable group admits an affine structure, but counterexamples are still hard to find. They can be regarded as discrete versions of non-affine nilvarieties [5] which disprove Milnor's second conjecture [10]. A translation into finite group theory [14] led to a class of p-groups of nilpotency class $\geqslant 9$ and $p \geqslant 23$ which do not admit an affine structure [3].

Recall that the generalized quaternion group Q_{2^m} of order 2^{m+2} ($m \geqslant 1$) is given by the relations

$$a^{2^{m+1}} = 1, \quad b^2 = a^{2^m}, \quad bab^{-1} = a^{-1}.$$

Braces with Q_{2^m} as adjoint group have been called *quaternion braces* [4, 8].

Using computer calculations up to order 512, Guarnieri and Vendramin [8] conjectured that, for each order $2^{m+2} \geqslant 32$, there are exactly 7 isomorphism classes of quaternion braces. If true, this would provide an infinite sequence of groups with increasing order for which the number of affine structures stabilizes at a certain order. Some evidence for this phenomenon is given by papers of Sysak et al. [1,17] which imply that the additive group of a quaternion brace must have a cyclic subgroup of index 4.

In this paper, we classify quaternion braces of order $\geqslant 32$ and confirm the conjecture. As a first step, we show that the socle of such a brace is non-trivial, which implies that the centre of the adjoint group is a brace ideal. Factoring out this ideal turns every quaternion brace into a brace with a dihedral adjoint group. By induction, this implies that all subgroups of $\langle a^4 \rangle$ are brace ideals, while the Frattini subgroup $\langle a^2 \rangle$ of the adjoint group is still an additive subgroup (Proposition 1), reproving the results of Sysak et al. [1,17] in a brace-theoretic manner. It turns out that the subgroup $\langle a^2 \rangle$ need not be a submodule under the adjoint group. Using Proposition 1, it follows that the additive group of a dihedral brace of order 16 is either cyclic or isomorphic to $C_2 \times C_8$ (Propositions 2–4). By an inductive argument, we infer that the additive group of a quaternion brace of order $\geqslant 32$ is either cyclic or isomorphic to $C_2 \times C_{2^{m+1}}$ (Theorem 1).

As a second step, we prove that the brace ideal $\langle a^4 \rangle$ is always contained in the socle (Theorem 2). In the extreme case $\langle a^4 \rangle = \mathrm{Soc}(A)$, the retraction $A/\mathrm{Soc}(A)$ of A is a dihedral brace of order 8. These braces were classified by Bachiller [2] and further investigated in [16]. There are 8 such braces, but we show that only one of them can arise. As a consequence, we infer that the case $\langle a^4 \rangle = \mathrm{Soc}(A)$ leads to a single isomorphism class of quaternion braces (Theorem 3).

So we are left with the case that the subgroup $\langle a^2 \rangle$ is contained in the socle. Then $a \cdot a \notin \langle a \rangle$ again leads to a single isomorphism class of quaternion braces (Theorem 4). The remaining case $a \cdot a \in \langle a \rangle$ includes the cyclic quaternion brace [13]. Apart from this, we find 4 isomorphism classes of quaternion braces, characterized by a classifying pair of invariants (Theorem 5). So we arrive at seven isomorphism classes of quaternion braces, as conjectured.

1 Dihedral and quaternion braces

An *affine structure* [16] of a group G is given by a left action $b \mapsto a \cdot b$ of G on its underlying set such that the equation

$$(a \cdot b)a = (b \cdot a)b \tag{1.1}$$

holds for all $a, b \in G$. It follows that the equations

$$ab \cdot c = a \cdot (b \cdot c), \quad 1 \cdot a = a, \quad a \cdot 1 = 1$$

are satisfied in G. The symmetry condition (1.1) gives rise to an abelian group structure

$$a + b := (a \cdot b)a = (b \cdot a)b \tag{1.2}$$

of G which makes G into a *linear cycle set* [11]:

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c), \tag{1.3}$$

$$(a + b) \cdot c = (a \cdot b) \cdot (a \cdot c), \tag{1.4}$$

providing a solution to the Yang–Baxter equation [11]. If $b \mapsto b^a$ denotes the inverse to $b \mapsto a \cdot b$, the group operation of G can be recovered as $ab := a^b + b$.

Therefore, equations (1.3), (1.4) give an alternative description of an affine structure in terms of addition (1.2) instead of the group structure of G. The prototypical example is given by any (unital associative) ring R with Jacobson radical J. Then the adjoint group $(J; \circ)$ with $a \circ b := ab + a + b$ has an affine structure with $a \cdot b := b(1 + a)^{-1}$.

By analogy, a system $(A; +, \cdot)$ satisfying equations (1.3) and (1.4) is called a *brace* [12] with *adjoint group* $A^\circ := (A; \circ)$ given by

$$a \circ b := a^b + b. \tag{1.5}$$

Thus, in essence, a brace is equivalent to an affine structure of its adjoint group. As in the case of a Jacobson radical J, the unit element of $(A; \circ)$ coincides with the zero element of the additive group $(A; +)$. Therefore, we denote it by 0. Following Jacobson [9], we also write a' for the inverse of a in the adjoint group A°. Note that $a \mapsto a^b$ gives a right action of A° on $(A; +)$ so that equation (1.5) states that the identity map $A^\circ \to A$ is a bijective 1-cocycle for this action. Thus a brace with adjoint group G could also be regarded as a bijective 1-cocycle of G onto a right G-module.

For the basics on braces, we refer to [12]. Motivations, and relationships to various other structures can be looked up in [14]. Here we only recall the main concepts needed for what follows. Like in a ring, there is a concept of ideal for any brace A. To see the analogy, we introduce the *ring multiplication* of a brace, denoted by juxtaposition, and given by the equation $a \circ b = ab + a + b$. Thus $a^b = ab + a$. The reader is warned that ring multiplication is only one-sided distributive: $(a + b)c = ab + ac$. Now a subgroup I of a brace A is said to be a *right ideal* if $a \in I$ and $b \in A$ implies that $ab \in I$. If $ba \in I$ also holds, I is called an *ideal* [12]. As the name suggests, ideals can be factored out to give new braces A/I, like in ring theory. Equivalently, a right ideal is the same as an additive subgroup which is invariant under the adjoint operation $a \mapsto b \cdot a$ for all $b \in A^\circ$. In particular, any right ideal is a subgroup of A°. A right ideal I is an ideal if and only if I° is a normal subgroup of A°.

A brace A and its corresponding affine structure of A° is said to be *trivial* if the action $b \mapsto a \cdot b$ is trivial, or equivalently, $ab = 0$ for all $a, b \in A$. Thus every abelian group can be regarded as a trivial brace.

There are two ideals of any brace A which deserve particular attention, the *socle*

$$\mathrm{Soc}(A) := \{a \in A \mid \text{for all } b \in A, \text{ we have } a \cdot b = b\},$$

and the "square" A^2 which consists of the finite sums $\sum_{i=1}^n a_i b_i$ with $a_i, b_i \in A$. The latter is the smallest ideal I for which A/I is a trivial brace, hence a counterpart to the socle. The brace homomorphism $A \twoheadrightarrow A/\mathrm{Soc}(A)$ is called the *retraction map*, and $A/\mathrm{Soc}(A)$ is said to be the *retraction* of A. The *fixator*

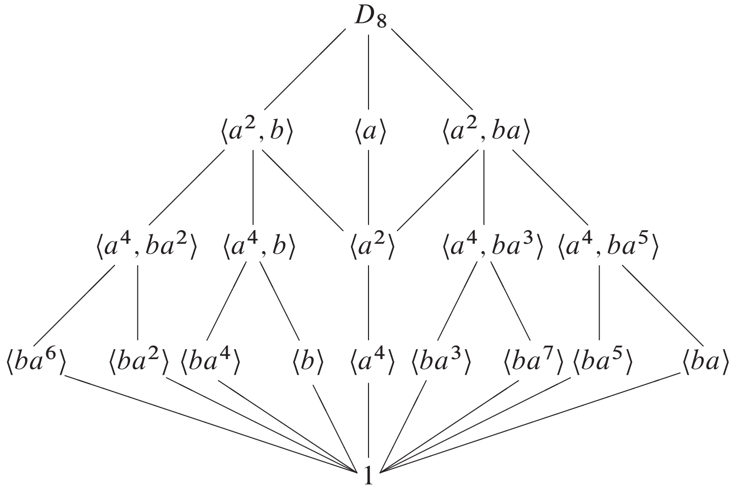
$$\mathrm{Fix}(A) := \{a \in A \mid \text{for all } b \in A, \text{ we have } b \cdot a = a\}$$

is only a right ideal, in general.

Now we turn our attention to the generalized quaternion group Q_{2^m} of order 2^{m+2}, and the dihedral group D_{2^m} of order 2^{m+1}, given by generators and relations

$$\begin{aligned} Q_{2^m} &= \langle a, b \mid a^{2^{m+1}} = 1,\ b^2 = a^{2^m},\ aba = b\rangle \quad (m \geqslant 1), \\ D_{2^m} &= \langle a, b \mid a^{2^m} = b^2 = 1,\ aba = b\rangle \qquad\qquad (m \geqslant 2). \end{aligned} \tag{1.6}$$

We have written the relations in a form which underlines the similarity of both groups and will be useful in what follows. The generators a, b will be kept fixed throughout the paper. The lattices of subgroups of Q_{2^m} and D_{2^m} are almost identical, with the only difference that Q_{2^m} has a smallest subgroup, the centre $Z = \langle a^{2^m}\rangle$, so that $Q_{2^m}/Z \cong D_{2^m}$.



The centre of D_{2^m} is also of order 2, namely, $Z(D_{2^m}) = \langle a^{2^{m-1}} \rangle$. In both cases, the commutator subgroup coincides with the Frattini subgroup $\langle a^2 \rangle$. There are three maximal subgroups: the cyclic group $\langle a \rangle$, and two non-cyclic subgroups $\langle a^2, b \rangle$ and $\langle a^2, ba \rangle$ which are connected by the automorphism $b \mapsto ba$, $a \mapsto a$. Note that any non-cyclic subgroup of D_{2^m} is dihedral, while each non-cyclic subgroup of Q_{2^m} is a generalized quaternion group. We frequently make use of the fact that D_{2^m} and Q_{2^m} admit an automorphism which maps a to an odd power a^i and b to some ba^j. For $i = j = 1$, this automorphism is an involution which fixes the subgroups of $\langle a \rangle$. The normal subgroups of D_{2^m} or Q_{2^m} are exactly the groups which either contain or are contained in the Frattini subgroup $\langle a^2 \rangle$.

For a finite brace A, we call $|A|$ the *order* of A. If the additive group is cyclic, the brace A is said to be *cyclic* [13]. In what follows, we focus upon braces of order 2^n which we also call *2-braces*. We say that a 2-brace is *dihedral* if its adjoint group is a dihedral group. If A° is a generalized quaternion group, we speak of a *quaternion brace*. To classify quaternion braces, we first have to deal with the possible additive groups. In [13], we have shown that, for each 2-power $\geqslant 8$, there is a unique cyclic quaternion brace. Its socle is of index 2. As these braces are completely described, we can restrict ourselves to non-cyclic braces.

Proposition 1. *Let A be a dihedral or quaternion brace of order 2^n. Then all subgroups $\langle a^{4i} \rangle$ of A° are brace ideals. If $|A| \geqslant 16$, then $\langle a^2 \rangle$ is an additive subgroup of A, and $a^{2^{n-2}} \in \operatorname{Soc}(A) \cap \operatorname{Fix}(A)$.*

Proof. By definition (1.6), $|A| \geqslant 8$. For $|A| = 8$, we have $a^4 = 0$. So we can assume that $n \geqslant 4$. Suppose that $\operatorname{Soc}(A) = 0$. Then A° embeds into the automorphism group $\operatorname{Aut}(A^+)$ of the additive group A^+ of A. Thus A^+ admits an automorphism of order 2^{n-1}. By Berkovič's theorem [6], this is impossible. Hence $\operatorname{Soc}(A)$ contains the centre $Z = \langle a^{2^{n-2}} \rangle$ of A°. For $x \in A$ and $z \in Z$, this gives $(x \cdot z)x = (z \cdot x)z = xz = zx$, which yields $x \cdot z = z$. Thus Z is a brace ideal with $Z \subset \operatorname{Soc}(A) \cap \operatorname{Fix}(A)$, and A/Z is a dihedral brace. If $|A/Z| \geqslant 16$, we can proceed in the same fashion to obtain a 2-element brace ideal of A/Z. Its inverse image along $A \twoheadrightarrow A/Z$ is a brace ideal of A. Iterating this procedure, we get a sequence of brace ideals of A,

$$0 = \langle a^{2^{n-1}} \rangle \subset \langle a^{2^{n-2}} \rangle \subset \cdots \subset \langle a^4 \rangle.$$

Thus $B := A/\langle a^4 \rangle$ is a dihedral brace of order 8, and it remains to verify that B satisfies $2a^2 = 0$. Now there are eight braces with adjoint group D_4 (see [2]). In [16, Example 3], they are denoted as $B_1, \dots, B_8$. For $B_1, \dots, B_6$, the socle is non-trivial, which implies that $\langle a^2 \rangle$ is an ideal. The brace B_7 has additive group $C_2 \times C_2 \times C_2$ so that $2a^2 = 0$. For the remaining brace B_8, the additive group is

$C_2 \times C_4$. In terms of vectors $\binom{x}{y}$ with $x \in C_2$ and $y \in C_4$, the additive structure of B_8 is given as follows:

$$a = \begin{pmatrix}0\\1\end{pmatrix}, \quad a^2 = \begin{pmatrix}1\\2\end{pmatrix}, \quad a^3 = \begin{pmatrix}1\\1\end{pmatrix},$$

$$b = \begin{pmatrix}0\\2\end{pmatrix}, \quad ba = \begin{pmatrix}0\\3\end{pmatrix}, \quad ba^2 = \begin{pmatrix}1\\0\end{pmatrix}, \quad ba^3 = \begin{pmatrix}1\\3\end{pmatrix}.$$

Thus $2a^2 = 0$, which completes the proof. □

Dealing with dihedral or quaternion braces, we mostly write xy instead of $x \circ y$. As we make no further use of the ring multiplication in this paper, this cannot lead to confusion. Accordingly, we also write x^{-i} for the inverse of x^i in the adjoint group. In what follows, we frequently use the formula (see [16, equation (2.8)]) which holds in any brace:

$$x \cdot yz = \big((z \cdot x) \cdot y\big)(x \cdot z).$$

2 The additive group of a quaternion brace

In this section, we show that non-cyclic quaternion braces of order $2^{m+2} \geqslant 32$ have an additive group isomorphic to $C_2 \times C_{2^{m+1}}$, where C_n denotes the cyclic group of order n. To this end, we have to prove three non-existence theorems first.

Proposition 2. *There is no dihedral brace with additive group $C_4 \times C_4$.*

Proof. Let A be such a brace. Then the subbrace $2A$ has the Klein four-group as additive group. Suppose first that $2A = \langle a^2 \rangle$. Since $\langle a^2 \rangle$ is cyclic, this implies that $2A$ is a non-trivial brace. Hence $a^2 \cdot a^2 = a^6$. Moreover, $a \cdot a^2$ and $a \cdot a^6$ belong to $\{a^2, a^6\}$. Thus $a^2 \cdot a^2 = a \cdot (a \cdot a^2) = a^2$, a contradiction. So we have $2A \neq \langle a^2 \rangle$, and by symmetry, we can assume that $2A = \langle a^4, b \rangle$. By Proposition 1, $a^4 \in \mathrm{Soc}(A) \cap \mathrm{Fix}(A)$. Hence the above formula yields

$$x \cdot ya^4 = \big((a^4 \cdot x) \cdot y\big)(x \cdot a^4) = (x \cdot y)a^4 \quad \text{for all } x, y \in A.$$

Thus

$$x \cdot ya^4 = (x \cdot y)a^4. \tag{2.1}$$

Suppose that $a + a = a^4$. Then $a \cdot a = a^3$. So

$$a \cdot a^2 = \big((a \cdot a) \cdot a\big)(a \cdot a) = (a^3 \cdot a)a^3 = (a \cdot a^3)a,$$

which gives

$$a^2 \cdot a^2 = a \cdot (a \cdot a^3)a = \big((a \cdot a) \cdot (a \cdot a^3)\big)(a \cdot a)$$
$$= \big(a^3 \cdot (a \cdot a^3)\big)a^3 = (a^4 \cdot a^3)a^3 = a^6.$$

Hence $a^2 + a^2 = (a^2 \cdot a^2)a^2 = 0$. Since $a^2 \notin \langle a^4, b\rangle = 2A$, this is impossible. So we obtain

$$a + a \in \{b, ba^4\}.$$

(Note that $a + a = 0$ would imply that $a \in 2A = \langle a^4, b\rangle$.)

By symmetry, we can assume that $a + a = b$. So $a \cdot a = ba^7$. Furthermore, $b + b = 0$ implies that $b \cdot b = b$. By Proposition 1, $a^2 + a^2 \in 2A \cap \langle a^2\rangle$, which yields $a^2 + a^2 = a^4$. Thus $a^2 \cdot a^2 = a^2$. If $a \cdot b = a^4$, then $b = a^7 \cdot a^4 = a^4$, which is impossible. Since $a \cdot b \in 2A$, this implies that $a \cdot b \in \{b, ba^4\}$. Hence $(a \cdot b)a = (b \cdot a)b$ yields $b \cdot a \in \{a^7, a^3\}$. Thus

$$b \cdot a^2 = \big((a \cdot b) \cdot a\big)(b \cdot a) = (b \cdot a)^2 = a^6.$$

So $(a^2 \cdot b)a^2 = (b \cdot a^2)b = a^6 b = ba^2$ gives $a^2 \cdot b = b$. Therefore, we get

$$b \cdot (a \cdot b) = a^7 \cdot (b \cdot b) = a^7 \cdot b = a \cdot b.$$

Hence

$$a \cdot ba = \big((a \cdot a) \cdot b\big)(a \cdot a) = (ba^7 \cdot b)ba^7 = \big(b \cdot (a \cdot b)\big)ba^7$$
$$= (a \cdot b)ba^7 = (a \cdot b)ab = (b \cdot a)bb,$$

that is, $a \cdot ba = b \cdot a$. Consequently, $ba \cdot ba = b \cdot (b \cdot a) = a$, which yields

$$ba + ba = aba = b.$$

Furthermore, equation (2.1) yields

$$a^5 + a^5 = (a^5 \cdot a^5)a^5 = (a \cdot a^5)a^5 = (a \cdot a)a = b,$$
$$ba^5 + ba^5 = (ba^5 \cdot ba^5)ba^5 = (ba \cdot ba)a^4ba^5 = a^5ba^5 = b.$$

Thus

$$a + a = a^5 + a^5 = ba + ba = ba^5 + ba^5 = b.$$

On the other hand, $ba^7 \cdot ba^7 = ba^7 \cdot (a \cdot a) = b \cdot a$. Hence

$$ba^7 + ba^7 = (b \cdot a)ba^7 = (a \cdot b)aa^7 = a \cdot b \in \{b, ba^4\}.$$

Now the fibers of the map $x \mapsto 2x$ are of cardinality 4. Hence $a \cdot b = ba^4$. Thus $(a \cdot b)a = (b \cdot a)b$ yields $b \cdot a = a^3$, and therefore, $a = b \cdot a^3$. If $a^3 \cdot a^3 = a$, then $a^3 = a^5 \cdot a = a \cdot a$, a contradiction. So $a^3 + a^3 = (a^3 \cdot a^3)a^3 \neq a^4$, which yields $a^3 + a^3 = ba^4$. Thus $a^3 \cdot a^3 = ba$. So we obtain

$$\begin{aligned} ba = a^3 \cdot a^3 = a^3 \cdot (b \cdot a) = ba^5 \cdot a = b \cdot (a \cdot a) \\ = b \cdot ba^7 = \big((a^7 \cdot b) \cdot b\big)(b \cdot a^7) = \big((a \cdot b) \cdot b\big)(b \cdot a^7) \\ = (ba^4 \cdot b)(b \cdot a^3)a^4 = (b \cdot b)aa^4 = ba^5, \end{aligned}$$

a contradiction. So the brace A cannot exist. □

Proposition 3. *There is no dihedral brace with additive group $C_4 \times C_2 \times C_2$.*

Proof. Let A be such a brace. The set I of elements $x \in A$ with $2x = 0$ is a right ideal of index 2, hence a brace ideal of A. In particular, $a^2 \in I$. If $I = \langle a \rangle$, then I is a brace with additive group $C_2 \times C_2 \times C_2$ and cyclic adjoint group. By [15, Proposition 10], this is impossible. Using the symmetry of $A^\circ \cong D_8$, we can assume without loss of generality that $I = \langle a^2, b \rangle$. As the additive group of I is elementary abelian, the dihedral brace I is of type B_7 in the list of braces in [16, Example 3]. By Proposition 1, a^4 belongs to the fixator of A. Hence $a^4 \in \mathrm{Fix}(I)$, contrary to [16, table (5.5)]. Thus A cannot exist. □

Proposition 4. *There is no dihedral brace with additive group $C_2 \times C_2 \times C_2 \times C_2$.*

Proof. Let A be such a brace. Then $2A = 0$. By Proposition 1, $\langle a^4 \rangle \subset \mathrm{Fix}(A)$. Consider the brace ideal A^2 (see [12]), the smallest ideal I for which A/I is a trivial brace. By [12, corollary of Proposition 8], $A^2 \neq A$. Since A/A^2 is trivial, $\langle a^2 \rangle \subset A^2$. If $A^2 = \langle a \rangle$, the adjoint group of A^2 is cyclic, while the additive group is elementary abelian, contrary to [15, Proposition 10]. If $A^2 = \langle a^2, b \rangle$, then A^2 is a dihedral brace of type B_7. As in the preceding proof, this leads to a contradiction. Thus it remains to consider the case $A^2 = \langle a^2 \rangle$. Then $0 = a + a = (a \cdot a)a$ yields $a \cdot a = a^7$. Hence $\langle a \rangle$ is a subbrace of A with cyclic adjoint group. As above, we infer that this is impossible. □

Now we are ready to determine the additive group of a dihedral or quaternion brace.

Theorem 1. *Let A be a non-cyclic brace of order $|A| = 2^n$. If A is dihedral with $n \geqslant 4$ or quaternion with $n \geqslant 5$, then its additive group is isomorphic to $C_2 \times C_{2^{n-1}}$.*

Proof. Assume first that A is dihedral. For $n = 4$, the theorem follows by Propositions 2–4. So we can assume that $n \geqslant 5$. By Proposition 1, $\langle a^4 \rangle$ is a brace ideal, and $\langle a^2 \rangle$ is an additive subgroup of A. Thus $a^2 + a^2 \in \langle a^2 \rangle$, which implies that $a^2 \cdot a^2 \in \langle a^2 \rangle$. Hence $C := \langle a^2 \rangle$ is a subbrace of A with a cyclic adjoint group of order $|C| \geqslant 8$. By [15, Proposition 10], it follows that the additive group C^+ of C is cyclic. Thus, if the theorem were false, the additive group of A would have to be isomorphic either to $C^+ \times C_4$ or $C^+ \times C_2 \times C_2$. Factoring out the ideal $\langle a^8 \rangle$, this would give a dihedral brace with additive group $C_4 \times C_4$ or $C_4 \times C_2 \times C_2$. By Propositions 2 and 3, this is impossible.

Now let A be a quaternion brace with $n \geqslant 5$. By Proposition 1 and [16, Proposition 10], $C = \langle a^2 \rangle$ is a cyclic subgroup of the additive group of A. Suppose that the theorem does not hold. Then the additive group of A must be isomorphic to $C_{2^{n-2}} \times C_4$ or $C_{2^{n-2}} \times C_2 \times C_2$. So the brace $A/\langle a^8 \rangle$ has an additive group isomorphic to $C_4 \times C_4$ of $C_4 \times C_2 \times C_2$, contrary to Proposition 2 or Proposition 3. □

Next we show that the socle of a quaternion brace is relatively large.

Theorem 2. *Let A be a quaternion brace of order $|A| \geqslant 32$. Then $\langle a^4 \rangle \subset \mathrm{Soc}(A)$.*

Proof. If A is cyclic, this follows by [13, Proposition 12]. Thus let A be non-cyclic. By Theorem 1, the additive group of A is of the form $C_2 \times C_{2^{m+1}}$ with $m \geqslant 3$. We identify C_n with the additive group of $\mathbb{Z}/n\mathbb{Z}$ and represent the elements of $C_2 \times C_{2^{m+1}}$ as vectors $\binom{x}{y}$ with $x \in C_2$ and $y \in C_{2^{m+1}}$. Then the automorphisms of $C_2 \times C_{2^{m+1}}$ are matrices

$$A = \begin{pmatrix} 1 & y \\ 2^m x & 1 + 2z \end{pmatrix}$$

with $x, y \in C_2$ and $z \in C_{2^m}$. (The mnemonic reason to write A for the matrix, not to be confused with the brace A, will become obvious below.) Note that the vector $\binom{1}{0} \in C_2 \times 0$ has to be mapped by A to a non-zero vector $\mathbf{v}$ with $2\mathbf{v} = 0$, which forces the lower left entry of A to be of the form $2^m x$. Since A has to be invertible, the diagonal entries must be odd. So we have

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 2^m xy + (1 + 2z)^2 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 1 & 0 \\ 0 & (1 + 2z)^4 \end{pmatrix}.$$

For a second matrix

$$B = \begin{pmatrix} 1 & v \\ 2^m u & 1 + 2w \end{pmatrix}$$

in $\mathrm{Aut}(C_2 \times C_{2^{m+1}})$, we have

$$AB = \begin{pmatrix} 1 & v + y \\ 2^m(x+u) & 2^m xv + (1+2z)(1+2w) \end{pmatrix},$$

and thus

$$ABA = \begin{pmatrix} 1 & v \\ 2^m u & 2^m(x+u)y + 2^m xv + (1+2z)^2(1+2w) \end{pmatrix}.$$

Let $a \mapsto A$ and $b \mapsto B$ be the representation $A^\circ \to \mathrm{Aut}(C_2 \times C_{2^{m+1}})$ given by the map $d \mapsto c \cdot d$ in the brace A. The relation $aba = b$ in A° gives $ABA = B$, that is,

$$1 + 2w = 2^m(x+u)y + 2^m xv + (1+2z)^2(1+2w)$$

in $C_{2^{m+1}}$. Multiplying by the unit $(1+2w)^{-1}$ turns the equation into

$$1 = 2^m(x+u)y + 2^m xv + (1+2z)^2. \tag{2.2}$$

Multiplying with the even number $1 + (1+2z)^2$ yields

$$1 + (1+2z)^2 = (1+2z)^2\bigl(1 + (1+2z)^2\bigr) = (1+2z)^2 + (1+2z)^4.$$

Whence $(1+2z)^4 = 1$. Thus $A^4 = 1$, which shows that $a^4 \in \mathrm{Soc}(A)$. □

3 Quaternion braces with minimal socle

In this section, we classify the non-cyclic quaternion braces A of order $2^{m+2} \geqslant 32$ for which the socle is minimal, that is, $\mathrm{Soc}(A) = \langle a^4 \rangle$. Then $A/\mathrm{Soc}(A)$ is a dihedral brace of order 8. As above, let $a, b \in A$ be represented by the matrices

$$A = \begin{pmatrix} 1 & y \\ 2^m x & 1+2z \end{pmatrix}, \quad B = \begin{pmatrix} 1 & v \\ 2^m u & 1+2w \end{pmatrix}$$

in $\mathrm{Aut}(C_2 \times C_{2^{m+1}})$. The equation $aba = b$ in A° yields equation (2.2), which can be rewritten as

$$4z(z+1) = 2^m(xy + uy + xv), \tag{3.1}$$

while $b^2 = a^{2^m}$ leads to $B^2 = 1$, that is, $2^m uv + (1+2w)^2 = 1$, or equivalently,

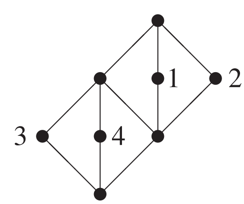
$$4w(w+1) = 2^m uv. \tag{3.2}$$

Since $A^4 = 1$, the equation $a^{2^{m+1}} = 1$ gives no further relation for the matrices A and B. So the representation $A^\circ \to \mathrm{Aut}(C_2 \times C_{2^{m+1}})$ is completely characterized by equations (3.1) and (3.2) in $C_{2^{m+1}}$. Our first aim is to determine the possible types of braces $B = A/\mathrm{Soc}(A)$. In [16, Example 3], the dihedral braces $B_1, \dots, B_8$ of order 8 are described. The cyclic brace B_1 is excluded by the following.

Proposition 5. *Let A be a quaternion brace of order $\geqslant 16$. If $A/\langle a^4 \rangle$ is a cyclic brace, then A is cyclic.*

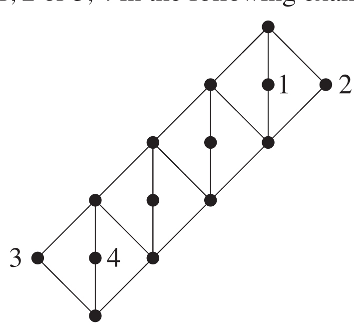
Proof. Assume that $B := A/\langle a^4 \rangle$ is cyclic. Since B° is dihedral, [13, Proposition 12] implies that $\mathrm{Soc}(B) = 2B$. Any $x \in B \smallsetminus 2B$ satisfies $x \circ x = 0$ and $B^\circ \cong \langle x \rangle \times 2B$. Moreover, x generates the additive group of B. Since a is of order 4 modulo $\langle a^4 \rangle$, its residue class in B generates $2B$. Hence $\langle a \rangle / \langle a^4 \rangle = 2B$. So the residue class of b modulo $\langle a^4 \rangle$ generates the additive group of B. As an inverse image of $\mathrm{Soc}(B)$, the subgroup $\langle a \rangle$ of A° is a brace ideal. Its adjoint group is cyclic of order $\geqslant 8$. So the additive group of $\langle a \rangle$ is cyclic, too. Furthermore, $b + b$ generates the additive group of $\langle a \rangle$ since its image modulo $\langle a^4 \rangle$ generates $2B$. Therefore, the brace A itself is cyclic. □

So the additive group of $B = A/\mathrm{Soc}(A)$ must be isomorphic to $C_2 \times C_4$. The lattice of subgroups of $C_2 \times C_4$ looks as follows:

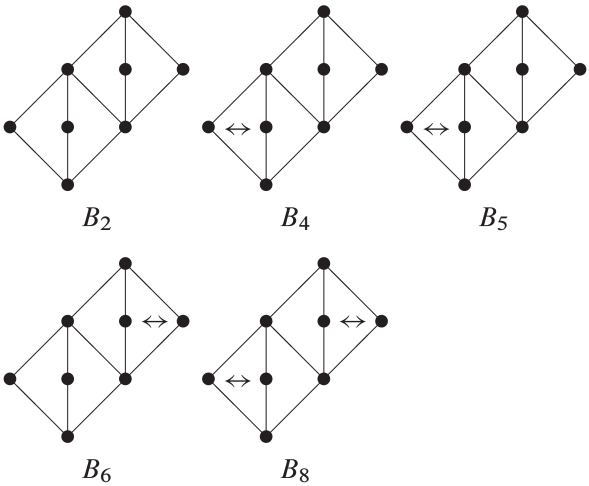


(3.3)

An automorphism of $C_2 \times C_4$ can only permute 1 with 2 or 3 with 4, while the other subgroups have to stay fixed. Similarly, an automorphism of $C_2 \times C_{2^{m+1}}$ induces a lattice automorphism which therefore can only permute the two obvious pairs of subgroups, like $1, 2$ or $3, 4$ in the following example for $m = 3$:



For B_3 and B_7, the additive group is elementary abelian. Thus only the following braces have to be considered:



The orbits of subgroups under automorphisms are indicated in the pictures. Since $B = A/\mathrm{Soc}(A)$, the braces B_4, B_5, and B_8 where the lower pair of subgroups is moved, have to be discarded. Thus only B_2 and B_6 remain to be considered.

For B_2, the residue class of $a \in A^\circ$ acts trivially on the additive group. So the entries of the matrix A satisfy $y = 0$ and $2 \mid z$. As the subgroups 1 and 2 in (3.3) have to stay fixed under the matrix B, it follows that $v = 0$. Thus equation (3.1) becomes $4z = 0$, which implies that $A^2 = 1$. Since $a^2 \notin \mathrm{Soc}(A)$, this contradicts our assumption. So the brace $A/\mathrm{Soc}(A)$ must be of type B_6. We shall obtain this fact independently in the proof of Theorem 3.

We need the construction of braces by socle extension (see [2, Theorem 2.1]).

Proposition 6. *Let B be a brace, and let A be an abelian group with a surjective homomorphism $p\colon A \twoheadrightarrow B$ onto the additive group of B. Furthermore, let $\sigma\colon B^\circ \hookrightarrow \mathrm{Aut}(A)$ be an injective group homomorphism such that*

$$p\big(\sigma(b)(a)\big) = b \cdot p(a) \tag{3.4}$$

holds for $a \in A$ and $b \in B$. Then

$$a \cdot c := \sigma p(a)(c) \tag{3.5}$$

makes A into a brace with retraction map p. Conversely, every brace A is obtained in this way.

Proof. For $a, c, d \in A$, equations (3.4), (3.5) give

$$\begin{aligned}(a+c)\cdot d &= \sigma p(a+c)(d) = \sigma\bigl(p(a)+p(c)\bigr)(d)\\ &= \sigma\bigl((p(a)\cdot p(c))\circ p(a)\bigr)(d) = \sigma\bigl((p(a)\cdot p(c)\bigr)\sigma p(a)(d)\\ &= \sigma p\bigl(\sigma p(a)(c)\bigr)\sigma p(a)(d) = \sigma p(a\cdot c)(a\cdot d) = (a\cdot c)\cdot(a\cdot d).\end{aligned}$$

Thus equations (1.3), (1.4) are satisfied. Hence A is a brace with $\mathrm{Soc}(A) = \mathrm{Ker}\, p$.

Conversely, let A be a brace with retraction map $p\colon A \twoheadrightarrow B$. Then $a \mapsto b\cdot a$ induces a natural embedding $\sigma\colon B \hookrightarrow \mathrm{Aut}(A)$ which satisfies equation (3.5). Furthermore, equation (3.4) follows since p is a brace morphism. □

Remarks. (1) To verify equation (3.4), it is enough to check the equation for the elements b of a generating system of B°. Indeed, let equation (3.4) be satisfied for $b_1, b_2 \in B$. Then

$$\begin{aligned}p\bigl(\sigma(b_1b_2)(a)\bigr) &= p\bigl(\sigma(b_1)\sigma(b_2)(a)\bigr)\\ &= b_1\cdot p\bigl(\sigma(b_2)(a)\bigr) = b_1\cdot(b_2\cdot p(a)) = b_1b_2\cdot p(a).\end{aligned}$$

Similarly, equation (3.4) implies that $p\bigl(\sigma(b^{-1})(a)\bigr) = b^{-1}\cdot p(a)$.

(2) Equation (3.4) states that the diagram

$$\begin{array}{ccc} A & \xrightarrow{\sigma(b)} & A\\ \big\downarrow{\scriptstyle p} & & \big\downarrow{\scriptstyle p}\\ B & \xrightarrow{b\cdot(\ )} & B\end{array}$$

commutes for all $b \in B$. In other words, B° embeds into the group $\mathrm{Aut}^p(A)$ of automorphisms which leave $\mathrm{Ker}\, p$ invariant so that the composed map

$$B^\circ \hookrightarrow \mathrm{Aut}^p(A) \to \mathrm{Aut}(B)$$

coincides with the adjoint action of B.

Theorem 3. *Let $m \geqslant 3$ be an integer. Up to isomorphism, there is a unique quaternion brace A of order 2^{m+2} with $|A/\mathrm{Soc}(A)| \geqslant 8$.*

Proof. For the cyclic quaternion brace, the socle is of index 2. Thus A cannot be cyclic. By Theorem 2, $|A/\mathrm{Soc}(A)| = 8$. We keep the above notation. To make A into a brace, we have to identify the generators a, b of the adjoint group with vectors in the additive group $C_2 \times C_{2^{m+1}}$:

$$a = \begin{pmatrix} p\\ q\end{pmatrix},\quad b = \begin{pmatrix} r\\ s\end{pmatrix}. \tag{3.6}$$

Note that

$$A^{-1} = \begin{pmatrix} 1 & y \\ 2^m x & 2^m xy + (1+2z)^{-1} \end{pmatrix},$$

$$B^{-1} = \begin{pmatrix} 1 & v \\ 2^m u & 2^m uv + (1+2w)^{-1} \end{pmatrix}.$$

Thus, with the identification (3.6),

$$a^2 = a^a + a = A^{-1}\binom{p}{q} + \binom{p}{q} = \begin{pmatrix} yq \\ 2^m x(p+yq) + (1+2z)^{-1}q + q \end{pmatrix},$$

$$a^3 = (a^2)^a + a = \begin{pmatrix} p + yq \\ 2^m xp + (1+2z)^{-2}q + (1+2z)^{-1}q + q \end{pmatrix}.$$

Hence $a^4 = (a^3)^a + a$, which yields

$$a^4 = \begin{pmatrix} 0 \\ (1+2z)^{-3}q + (1+2z)^{-2}q + (1+2z)^{-1}q + q \end{pmatrix}.$$

Now we have $1 + (1+2z) + (1+2z)^2 + (1+2z)^3 = 4(1 + 3z + 4z^2 + 2z^3)$, from which we infer that $a^4 = \binom{0}{4t}$ for some $t \in C_{2^{m+1}}$. Since $a^4 \in \mathrm{Soc}(A)$, it follows that $a^8 = (a^4)^{a^4} + a^4 = \binom{0}{8t}$. Hence $a^{4i} = \binom{0}{4it}$, and thus $a^{2^m} = 0$ if t is even, and $a^{2^m} = \binom{0}{2^m}$ if t is odd. Since

$$\begin{aligned}(1+2z)^{-3}q + (1+2z)^{-2}q + (1+2z)^{-1}q + q \\ = 4q(1+2z)^{-3}(1+3z+4z^2+2z^3),\end{aligned}$$

it follows that q and $1 + 3z$ must be odd, that is, $2 \nmid q$ and $2 \mid z$. Next we have

$$ab = a^b + b = B^{-1}\binom{p}{q} + \binom{r}{s} = \begin{pmatrix} p + v + r \\ 2^m u(p+v) + (1+2w)^{-1}q + s \end{pmatrix}.$$

Thus

$$aba = (ab)^a + a = \begin{pmatrix} v + r + y + ys \\ 2^m x(p+v+r) + 2^m xy(1+s) + 2^m u(p+v) \\ +(1+2z)^{-1}(1+2w)^{-1}q + (1+2z)^{-1}s + q \end{pmatrix}.$$

Since $aba = b$, this yields

$$v = y(1+s), \tag{3.7}$$

and therefore,

$$\begin{aligned}&2^m x(p+r) + 2^m u(p+v)\\&\qquad + (1+2z)^{-1}(1+2w)^{-1}q + q + (1+2z)^{-1}s = s.\end{aligned}$$

Multiplication with $(1+2z)(1+2w)$ gives

$$2^m x(p+r) + 2^m u(p+v) + q + q(1+2z)(1+2w) = 2zs(1+2w).$$

Modulo 4, this yields, since z is even, $4 \mid q + q(1+2w) = 2q(1+w)$. Hence w is odd. Thus, by equations (3.1) and (3.7),

$$4z = 2^m(xy + uy + xv) = 2^m y(x + u + x(1+s)),$$

which yields

$$4z = 2^m y(u + xs). \tag{3.8}$$

Similarly, equation (3.2) gives

$$4(w+1) = 2^m uy(1+s). \tag{3.9}$$

Using equations (3.7), (3.8), we obtain

$$\begin{aligned}&2^m x(p+r) + 2^m u(p+v) + 2q(1+z+w) - 2zs\\&\quad = -4qzw + 4zsw = 2^m y(u+xs)(-qw+sw)\\&\quad = 2^m y(u+xs)(1+s) = 2^m y(u + xs + us + xs)\\&\quad = 2^m yu(1+s) = 2^m uv.\end{aligned}$$

Hence

$$2^m x(p+r) + 2^m up + 2q(z+w+1) = 2zs. \tag{3.10}$$

Furthermore,

$$b^2 = b^b + b = B^{-1}\binom{r}{s} + \binom{r}{s} = \begin{pmatrix} vs \\ 2^m ur + 2^m uvs + (1+2w)^{-1}s + s\end{pmatrix}.$$

Since $b^2 = \binom{0}{2^m}$, this yields $2^m u(r+vs) + (1+2w)^{-1}s + s = 2^m$. Note that $2 \mid vs$ already follows by equation (3.7). Thus, multiplying with $1+2w$, we obtain $2^m ur + s + s(1+2w) = 2^m$. Whence

$$2^m(ur+1) = 2s(1+w). \tag{3.11}$$

Up to here, we have not assumed that $\operatorname{Soc}(A) = \langle a^4\rangle$. Now we add this condition. Then $2^m xy + (1+2z)^2 \neq 1$ in $C_{2^{m+1}}$, that is, $4z(z+1) \neq 2^m xy$. By (3.8), this is equivalent to $2^m y(u+xs) \neq 2^m xy$, that is, $2^m y(u+x(s+1)) \neq 0$. So we obtain

$$y = 1, \quad u = x(s+1)+1. \tag{3.12}$$

Suppose that $x = 1$. Then $u = s$, and equation (3.10) gives

$$2^m(p+r) + 2^m sp + 2q(z+w+1) = 2zs.$$

Equations (3.8) and (3.9) turn into

$$4z = 2^m(s+s) = 0 \quad \text{and} \quad 4(w+1) = 2^m s(s+1) = 0.$$

If s is even, then equation (3.11) gives $2^m(sr+1) = 0$, hence $2 \mid sr+1$, a contradiction. So s is odd. Hence $2^m r + 2q(z+w+1) = 2zs$, and thus

$$2^m r = 2z(q+s) + 2q(1+w) = 2q(1+w) = 2(1+w).$$

On the other hand, equation (3.11) yields

$$2(1+w) = 2s(1+w) = 2^m(ur+1) = 2^m(r+1),$$

a contradiction. So we get

$$x = 0. \tag{3.13}$$

Since

$$ba = b^a + a = \begin{pmatrix} 1 & 1 \\ 0 & (1+2z)^{-1} \end{pmatrix}\begin{pmatrix} r \\ s \end{pmatrix} + \begin{pmatrix} p \\ q \end{pmatrix} = \begin{pmatrix} r+s+p \\ (1+2z)^{-1}s+q \end{pmatrix},$$

the transformation $b \mapsto ba$ changes the parity of s. So we can assume that s is even. Then equations (3.7), (3.12) and (3.13) give $u = v = y = 1$, and equations (3.8), (3.9) turn into

$$4z = 4(w+1) = 2^m.$$

So $1+2z = 1 \pm 2^{m-1}$ and $(1+2z)^2 = (1+2z)^{-2} = 1+2^m$. Hence

$$ba^2 = b^{a^2} + a^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1+2^m \end{pmatrix}\begin{pmatrix} r \\ s \end{pmatrix} + \begin{pmatrix} 1 \\ (1 \mp 2^{m-1})q + q \end{pmatrix}$$
$$= \begin{pmatrix} r+1 \\ (1+2^m)s + (2 \mp 2^{m-1})q \end{pmatrix}.$$

Since $m \geqslant 3$, using a possible transformation $b \to ba^2$ if necessary, we can assume without loss of generality that $4 \mid s$. So equations (3.10), (3.11) become

$$2^m p = 2(z+w+1)$$

and $2^m(r+1)=0$, which yields $r=1$. Thus

$$A=\begin{pmatrix}1 & 1\\ 0 & 1\pm 2^{m-1}\end{pmatrix},\quad B=\begin{pmatrix}1 & 1\\ 2^m & 2^m p-1\mp 2^{m-1}\end{pmatrix}.$$

Since

$$A^3=\begin{pmatrix}1 & 1\\ 0 & 1\mp 2^{m-1}\end{pmatrix},$$

we can assume, possibly after a transformation $a\mapsto a^3$, that the sign in the matrix A is positive. Applying the involution

$$\alpha=\begin{pmatrix}1 & p\\ 0 & 1\end{pmatrix}$$

to the additive group $C_2\times C_{2^{m+1}}$, the vector $\binom{p}{q}$ is mapped to $\binom{0}{q}$, while $\binom{1}{s}$ remains fixed. Furthermore,

$$\alpha A\alpha^{-1}=A,\quad \alpha B\alpha^{-1}=\begin{pmatrix}1 & 1\\ 2^m & -1-2^{m-1}\end{pmatrix}.$$

So we can assume that $p=0$, which yields

$$A=\begin{pmatrix}1 & 1\\ 0 & 1+2^{m-1}\end{pmatrix},\quad B=\begin{pmatrix}1 & 1\\ 2^m & -1-2^{m-1}\end{pmatrix}. \tag{3.14}$$

In particular,

$$\begin{aligned}&(1+2z)^{-3}q+(1+2z)^{-2}q+(1+2z)^{-1}q+q\\ &\quad=(1+2^{m-1})q+(1+2^m)q+(1-2^{m-1})q+q=4q+2^m,\end{aligned}$$

which gives $a^4=\binom{0}{4q+2^m}$. Therefore, $ba^4=\binom{1}{s+4q+2^m}$. Since $m\geqslant 3$, we can replace b by some ba^{4i} so that $s=0$. Finally, by changing the generator of the second factor in the additive group $C_2\times C_{2^{m+1}}$, the matrices (3.14) are not altered, and q is multiplied by an odd number. So we can assume that $q=1$. Thus

$$a=\begin{pmatrix}0\\1\end{pmatrix},\quad b=\begin{pmatrix}1\\0\end{pmatrix},$$

which shows that A is unique, up to isomorphism.

To show that A is a brace, we apply Proposition 6. Thus, if

$$p\colon C_2\times C_{2^{m+1}}\twoheadrightarrow C_2\times C_4$$

denotes the retraction map between the additive groups, we have to verify that $C_2 \times C_4$ is the additive group of a brace such that $p\big(\sigma p(a)(\mathbf{v})\big) = p(a) \cdot p(\mathbf{v})$ and $p\big(\sigma p(b)(\mathbf{v})\big) = p(b) \cdot p(\mathbf{v})$ holds for all $\mathbf{v} \in C_2 \times C_{2^{m+1}}$. By Remark (2) after Proposition 6, this means that the reduced matrices

$$\overline{A} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \overline{B} = \begin{pmatrix} 1 & 1 \\ 0 & 3 \end{pmatrix} \tag{3.15}$$

make $C_2 \times C_4$ into a dihedral brace B of order 8:

$$a = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad a^2 = \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \quad a^3 = \begin{pmatrix} 1 \\ 3 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad ba = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad ba^2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}, \quad ba^3 = \begin{pmatrix} 0 \\ 3 \end{pmatrix}.$$

Indeed, let $p\colon C_2 \times C_4 \twoheadrightarrow C_4$ be the homomorphism with kernel $\left\{\binom{1}{2}\right\}$. Then the matrices (3.15) induce automorphisms of C_4 which make C_4 into a cyclic brace with Klein four-group as adjoint group. By Proposition 6, B is a brace. □

4 The case $\langle a^2 \rangle \subset \mathrm{Soc}(A)$ with $a \cdot a \notin \langle a \rangle$

By Theorem 3, it remains to consider the quaternion braces A of order 2^{m+2} with $m \geqslant 3$ and $a^2 \in \mathrm{Soc}(A)$. Here we focus upon the adjoint group. To classify the possible affine structures, we have to check equation (1.1) for the elements of A°. Note first that the adjoint action on the socle is by conjugation: for $x \in A$ and $s \in \mathrm{Soc}(A)$, we have $xs = (s \cdot x)s = (x \cdot s)x$, which gives

$$x \cdot s = xsx^{-1}. \tag{4.1}$$

Thus, if $x, y \in A$ and $s \in \mathrm{Soc}(A)$, then $x \cdot ys = \big((s \cdot x) \cdot y\big)(x \cdot s)$, hence

$$x \cdot ys = (x \cdot y)xsx^{-1}. \tag{4.2}$$

In this section, we consider the case $a \cdot a \notin \langle a \rangle$.

Applying an automorphism of A° which maps b to some ba^k, we can assume that

$$a \cdot a = b. \tag{4.3}$$

Then $a = a^{-1} \cdot b = a \cdot b$, which gives

$$a \cdot b = a. \tag{4.4}$$

By equation (1.1), this implies that

$$b \cdot a = ba^{2^m - 2}. \tag{4.5}$$

Suppose that $b \cdot b \notin \langle a \rangle$, say, $b \cdot b = ba^k$. Then

$$a \cdot ba = \big((a \cdot a) \cdot b\big)(a \cdot a) = (b \cdot b)b = ba^k b = ba^k b^{-1} a^{2^m} = a^{2^m - k}.$$

Hence $ba = a \cdot a^{2^m - k}$. If k is even, then (4.1) would imply that $ba \in \langle a^2 \rangle$. Thus k is odd, and $ba = (a \cdot a)a^{2^m - k - 1} = ba^{2^m - k - 1}$, which yields $1 = 2^m - k - 1$ in $C_{2^{m+1}}$, a contradiction. So we obtain $b \cdot b = a^r$ for some $r \in \{0, \dots, 2^{m+1} - 1\}$. Since $b \cdot a^r = b$, the integer r must be odd. Hence equations (4.2) and (4.5) give $b = (b \cdot a)a^{1-r} = ba^{2^m - 2}a^{1-r} = ba^{2^m - 1 - r}$. Thus

$$b \cdot b = a^{2^m - 1}. \tag{4.6}$$

By equations (4.1)–(4.6), the affine structure of A is uniquely determined:

$$a^i \cdot a^j := \begin{cases} a^j & \text{for } i \text{ or } j \text{ even}, \\ ba^{j-1} & \text{for } i, j \text{ odd}, \end{cases}$$

$$a^i \cdot ba^j := \begin{cases} ba^j & \text{for } i \text{ even}, \\ a^{j+1} & \text{for } i \text{ odd}, \ j \text{ even}, \\ ba^{2^m + j} & \text{for } i, j \text{ odd}, \end{cases}$$

$$ba^i \cdot a^j := \begin{cases} a^{-j} & \text{for } j \text{ even}, \\ ba^{2^m - j - 1} & \text{for } i \text{ even}, \ j \text{ odd}, \\ a^{2^m - j} & \text{for } i, j \text{ odd}, \end{cases}$$

$$ba^i \cdot ba^j := \begin{cases} a^{2^m - 1 - j} & \text{for } i, j \text{ even}, \\ ba^{2^m - j - 2} & \text{for } i + j \text{ odd}, \\ ba^{-j-2} & \text{for } i, j \text{ odd}. \end{cases}$$

Now it is easily checked that these equation define a brace. To show that they define an action, it is enough to confirm that the equations are obtained by iterating the adjoint actions of a and b. To check the identity $(x \cdot y)x = (y \cdot x)y$, the cases $(x, y) = (a^i, a^j)$ and (ba^i, ba^j) are particularly simple because we only have to verify that $(x \cdot y)x$ is symmetric in i and j. Moreover, the three cases of $(x, y) = (a^i, ba^j)$ are complementary to the three cases of $(x, y) = (ba^j, a^i)$: for example, if i is odd and j even, then $(a^i \cdot ba^j)a^i = a^{j+1}a^i$, while

$$(ba^j \cdot a^i)ba^j = ba^{2^m - i - 1}ba^j = b^2 a^{2^m + i + 1}a^j = a^{i+j+1}.$$

So we have proved the following theorem.

Theorem 4. *Let m be a positive integer. Up to isomorphism, there is a unique quaternion brace A of order $\geqslant 32$ with $a^2 \in \mathrm{Soc}(A)$ and $a \cdot a \notin \langle a \rangle$.*

5 The case $\langle a^2 \rangle \subset \mathrm{Soc}(A)$ with $a \cdot a \in \langle a \rangle$

Now let A be a quaternion brace of order 2^{m+2} with $m \geqslant 3$ such that $a^2 \in \mathrm{Soc}(A)$ and $a \cdot a = a^{k+1}$ for some integer k. Then $a = a \cdot a^{k+1}$, which shows that k is even. Hence $a = a \cdot a^{k+1} = (a \cdot a)a^k = a^{2k+1}$, which yields

$$a \cdot a = a^{k+1}, \quad k \in \{0, 2^m\}. \tag{5.1}$$

If $a \cdot b = a^i$, then $b = a \cdot a^i \in \langle a \rangle$, which is impossible. Hence $a \cdot b = ba^\ell$ for some integer ℓ. If ℓ is odd, then

$$\begin{aligned} b \cdot ba^\ell &= \big((a^\ell \cdot b) \cdot b\big)(b \cdot a^\ell) = \big((a \cdot b) \cdot b\big)(b \cdot a)ba^{\ell-1}b^{-1} \\ &= \big((a \cdot b) \cdot b\big)(a \cdot b)aa^{\ell-1}b^{-1} = \big(b \cdot (a \cdot b)\big)ba^\ell b^{-1} = (b \cdot ba^\ell)a^{-\ell}. \end{aligned}$$

Hence ℓ is even, contrary to our assumption. Thus ℓ cannot be odd, which yields $b = a \cdot ba^\ell = (a \cdot b)a^\ell = ba^{2\ell}$. So we obtain

$$a \cdot b = ba^\ell, \quad \ell \in \{0, 2^m\}. \tag{5.2}$$

Since $(b \cdot a)b = (a \cdot b)a = ba^{\ell+1}$, this implies that

$$b \cdot a = a^{-\ell-1}. \tag{5.3}$$

Hence $\langle a \rangle$ is a right ideal of A. Since $\langle a \rangle$ is of index 2, it is even a brace ideal. In particular, this implies that $b \cdot b \notin \langle a \rangle$. Assume that $b \cdot b = ba^r$. The parity of r is an invariant.

Proposition 7. *A is a cyclic brace if and only if r is odd.*

Proof. By [15, Proposition 10], $\langle a \rangle$ is a cyclic brace. Assume that r is odd. Then equation (5.3) gives

$$\begin{aligned} b = b \cdot ba^r &= \big((a^r \cdot b) \cdot b\big)(b \cdot a^r) = (ba^\ell \cdot b)(b \cdot a)a^{1-r} \\ &= ba^r a^{-\ell-1}a^{1-r} = ba^{-\ell}. \end{aligned}$$

Hence $a \cdot b = b$, and thus

$$\begin{aligned} ba^r = b \cdot b = ba \cdot b = a^{-1}b \cdot b = a \cdot ba^r &= \big((a^r \cdot a) \cdot b\big)(a \cdot a^r) \\ &= (a^{k+1} \cdot b)(a \cdot a)a^{r-1} = ba^{k+1}a^{r-1} = ba^{k+r}. \end{aligned}$$

So we obtain $a \cdot a = a^{k+1} = a$, which shows that the brace $\langle a \rangle$ is trivial. Since $b + b = (b \cdot b)b = ba^r b = a^{2^m - r}$ generates $\langle a \rangle$, it follows that b generates the additive group of A. The converse follows by [13, Proposition 12]. □

So we can assume that r is even. If $r \equiv 2 \pmod 4$, then

$$\begin{aligned} ba \cdot ba &= b \cdot (a \cdot ba) = b \cdot \big((a \cdot a) \cdot b\big)(a \cdot a) = b \cdot (a^{k+1} \cdot b)a^{k+1} \\ &= b \cdot ba^{\ell} a^{k+1} = \big((a^{\ell+k+1} \cdot b) \cdot b\big)(b \cdot a^{\ell+k+1}) \\ &= (ba^{\ell} \cdot b)(b \cdot a)a^{-\ell-k} = ba^r a^{-\ell-1} a^{-\ell-k} = ba^{r-k-1} = (ba)a^{r-k-2}. \end{aligned}$$

Hence, if we replace b by ba, the new r will be divisible by 4. Thus $j := \frac{r}{2}$ is even, and $ba^j \cdot ba^j = b \cdot ba^j = (b \cdot b)a^{-j} = ba^{r-j} = ba^j$. Therefore, if we replace b by ba^j, we obtain

$$b \cdot b = b. \tag{5.4}$$

Proposition 8. *Let A be a quaternion brace of order 2^{m+2} with $m \geqslant 3$ such that $b \cdot b = b$. Then $k, l \in \{0, 2^m\}$ are invariants for the isomorphism class of A.*

Proof. Consider the group automorphism given by $a \mapsto a^i$ and $b \mapsto ba^j$ with i odd. Then $a^i \cdot a^i = a \cdot a^i = (a \cdot a)a^{i-1} = a^{k+i}$. Thus k is transformed into k' with $a^{k+i} = a^{i(k'+1)}$. Because of (5.1), this shows that $k' = i^{-1}k = k$. So k is invariant. Assume first that j is even. Then

$$a^i \cdot ba^j = a \cdot ba^j = (a \cdot b)a^j = ba^{\ell+j} = ba^j a^{i\ell},$$

which shows that ℓ is invariant.

Now let j be odd. Then

$$\begin{aligned} ba^j \cdot ba^j &= b \cdot (a \cdot ba^j) = b \cdot \big((a^j \cdot a) \cdot b\big)(a \cdot a^j) \\ &= b \cdot (a^{k+1} \cdot b)(a \cdot a)a^{j-1} = b \cdot ba^{\ell} a^{k+1} a^{j-1} = b \cdot ba^{\ell+k+j} \\ &= \big((a^{\ell+k+j} \cdot b) \cdot b\big)(b \cdot a^{\ell+k+j}) = (ba^{\ell} \cdot b)(b \cdot a)a^{1-\ell-k-j} \\ &= (b \cdot b)a^{-\ell-1} a^{1-\ell-k-j} = ba^{-k-j}. \end{aligned}$$

To maintain equation (5.4), we have to assume that $ba^j = ba^{-k-j}$. Since $2^m \mid k$, this is impossible. □

Thus it remains to verify that the four remaining cases of Proposition 8 can be realized. Using equations (5.1)–(5.4), a straightforward calculation gives

$$a^i \cdot a^j := \begin{cases} a^j & \text{for } i \text{ or } j \text{ even}, \\ a^{k+j} & \text{for } i, j \text{ odd}, \end{cases}$$

$$a^i \cdot ba^j := \begin{cases} ba^j & \text{for } i \text{ even}, \\ ba^{\ell+j} & \text{for } i \text{ odd}, \ j \text{ even}, \\ ba^{\ell+k+j} & \text{for } i, j \text{ odd}, \end{cases}$$

$$ba^i \cdot a^j := \begin{cases} a^{-j} & \text{for } j \text{ even,} \\ a^{\ell-j} & \text{for } i \text{ even, } j \text{ odd,} \\ a^{\ell+k-j} & \text{for } i, j \text{ odd,} \end{cases}$$

$$ba^i \cdot ba^j := \begin{cases} ba^{-j} & \text{for } i, j \text{ even,} \\ ba^{\ell-j} & \text{for } i + j \text{ odd,} \\ ba^{k-j} & \text{for } i, j \text{ odd.} \end{cases}$$

At some places, we made use of the fact that $-k \equiv k$ and $-\ell \equiv \ell \pmod{2^{m+1}}$ according to (5.1), (5.2). It is easily checked that the equations define an affine structure on Q_{2^m}, hence a quaternion brace. Thus we obtain our main result.

Theorem 5. *Let $m \geqslant 3$ be an integer. Up to isomorphism, there are 7 quaternion braces of order 2^{m+2}, namely,*

(a) *the cyclic brace A_1,*

(b) *the brace A_2 with $|A_2/\mathrm{Soc}(A_2)| = 8$,*

(c) *the brace A_3 with $a^2 \in \mathrm{Soc}(A_3)$ and $a \cdot a \notin \langle a \rangle$,*

(d) *the 4 braces $A_{i,j}$ with $i, j \in \{0, 1\}$, where $a^2 \in \mathrm{Soc}(A_{i,j})$, $a \cdot a \in \langle a \rangle$ and $b \cdot b = b$, given by the invariants $k = 2^m i$ and $\ell = 2^m j$ in* (5.1), (5.2).

Bibliography

[1] B. Amberg, P. Hubert and Y. Sysak, Local nearrings with dihedral multiplicative group, *J. Algebra* **273** (2004), no. 2, 700–717.

[2] D. Bachiller, Classification of braces of order p^3, *J. Pure Appl. Algebra* **219** (2015), no. 8, 3568–3603.

[3] D. Bachiller, Counterexample to a conjecture about braces, *J. Algebra* **453** (2016), 160–176.

[4] D. Bachiller, F. Cedó and E. Jespers, Solutions of the Yang–Baxter equation associated with a left brace, *J. Algebra* **463** (2016), 80–102.

[5] Y. Benoist, Une nilvariété non affine, *J. Differential Geom.* **41** (1995), no. 1, 21–52.

[6] V. G. Berkovič, Groups of order p^n that admit an automorphism of order p^{n-1}, *Algebra i Logika* **9** (1970), 3–8.

[7] P. Etingof, T. Schedler and A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, *Duke Math. J.* **100** (1999), no. 2, 169–209.

[8] L. Guarnieri and L. Vendramin, Skew braces and the Yang–Baxter equation, *Math. Comp.* **86** (2017), no. 307, 2519–2534.

[9] N. Jacobson, *Structure of Rings*, Amer. Math. Soc. Colloq. Publ. 37, American Mathematical Society, Providence, 1956.

[10] J. Milnor, On fundamental groups of complete affinely flat manifolds, *Adv. Math.* **25** (1977), no. 2, 178–187.

[11] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, *Adv. Math.* **193** (2005), no. 1, 40–55.

[12] W. Rump, Braces, radical rings, and the quantum Yang-Baxter equation, *J. Algebra* **307** (2007), no. 1, 153–170.

[13] W. Rump, Classification of cyclic braces, *J. Pure Appl. Algebra* **209** (2007), no. 3, 671–685.

[14] W. Rump, The brace of a classical group, *Note Mat.* **34** (2014), no. 1, 115–144.

[15] W. Rump, Classification of cyclic braces, II, *Trans. Amer. Math. Soc.* **372** (2019), no. 1, 305–328.

[16] W. Rump, Construction of finite braces, *Ann. Comb.* **23** (2019), no. 2, 391–416.

[17] Y. P. Sysak and S. Di Termini, Local nearrings with generalized quaternion multiplicative group, *Ric. Mat.* **56** (2007), no. 1, 61–72.

Received November 23, 2019; revised April 1, 2020.

Author information

Wolfgang Rump, Institute for Algebra and Number Theory, University of Stuttgart,
Pfaffenwaldring 57, 70550 Stuttgart, Germany.
E-mail: `rump@mathematik.uni-stuttgart.de`