ON MODULAR MAXIMAL-CYCLIC BRACES

ARPAN DAS AND ARPAN KANRAR

ABSTRACT. Inspired by a conjecture by Guarnieri and Vendramin concerning the number of braces with a generalized quaternion adjoint group, many researchers have studied braces whose adjoint group is a non-abelian 2-group with a cyclic subgroup of index 2. Following this direction, braces with generalized quaternion, dihedral, and semidihedral adjoint groups have been classified. It was found that the number of such braces stabilizes as the group order increases. In this paper, we consider the remaining open case of modular maximal-cyclic groups. We show that these braces possess only one non-cyclic additive group structure, and, in contrast to previous findings, the number of such braces increases with increasing order.

1. Introduction

To study non-degenerate involutive set-theoretic solutions to the Yang-Baxter equation, Rump [21] introduced the algebraic structure called a *brace*. Finite braces can be viewed as groups G with an affine structure, which is a bijective 1-cocycle onto a right G-module. A key invariant of finite involutive solutions is the *Involutive Yang-Baxter group* [14, 9], which is itself a brace. Brace theory has been used to study several key properties of involutive solutions, including decomposability, multi-permutation, and simplicity [14, 19, 8, 24, 6]. Moreover, braces arise in the theory of regular affine groups [5, 10, 7], Hopf-Galois structures [1, 15, 11], and various other related topics.

The non-abelian groups of order 2^n ($n \ge 5$) with a cyclic subgroup of index 2 are of four types [17, 25], namely the dihedral group D_{2^n} , the generalized quaternion group Q_{2^n} , the semidihedral group SD_{2^n} , and the modular maximal-cyclic group M_{2^n} given by the presentations

$$D_{2^{n}} = \langle a, b \mid a^{2^{n-1}} = b^{2} = 1, \ bab^{-1} = a^{-1} \rangle$$

$$Q_{2^{n}} = \langle a, b \mid a^{2^{n-1}} = 1, \ b^{2} = a^{2^{n-2}}, \ bab^{-1} = a^{-1} \rangle$$

$$SD_{2^{n}} = \langle a, b \mid a^{2^{n-1}} = b^{2} = 1, \ bab^{-1} = a^{-1+2^{n-2}} \rangle$$

$$M_{2^{n}} = \langle a, b \mid a^{2^{n-1}} = b^{2} = 1, \ bab^{-1} = a^{1+2^{n-2}} \rangle.$$

Definition 1.1. A set A equipped with two group structures \circ and + is said to be a right brace if

- (1) (A, +) is an abelian group;
- (2) the relation $(b+c) \circ a + a = b \circ a + c \circ a$ holds for all $a, b, c \in A$.

The group (A, \circ) is called *the adjoint group* of the brace A. For convenience, we will often omit the word 'right', referring to 'right braces' simply as 'braces'.

In a foundational work, Guarnieri and Vendramin [16] extended the concept of braces to skew braces by relaxing the commutative property of the additive group. Their paper included computational results for counting braces and skew braces of small order, which led them to propose a conjecture about the number of braces with a generalized quaternion adjoint group of order 4m. This conjecture was subsequently proven by Rump [23] for braces of 2-power size and later in full generality by Byott and Ferri [4]. The latter also classified 2-power dihedral braces.

These findings have inspired a new line of research focused on classifying braces whose adjoint group is a non-abelian 2-group containing a cyclic subgroup of index 2. As part of this effort, semidihedral braces were recently classified in [20]. It's interesting to note that for dihedral (D_{2^n}) , generalized quaternion (Q_{2^n}) , and semidihedral (SD_{2^n}) adjoint groups, the number of corresponding braces stabilizes as the order increases. Furthermore, conjectures regarding the number of braces of orders 8p and 12p for large primes p, based on extensive computations by Bardakov, Neshchadim, and Yadav [2], have been recently confirmed by Crespo, Gil-Muñoz, Rio, and Vela [13, 12].

In this paper, we address the final remaining case: braces where the adjoint group is a modular maximal-cyclic group. Utilizing the methods developed in [13, 12, 20, 23, 4], we demonstrate that these braces have only one possible non-cyclic additive group structure (Theorem 5.4). We then construct all possible brace structures (Theorem 6.6)

 $^{2020\} Mathematics\ Subject\ Classification.\ 16T25,\ 20H25, 20K30, 20D15.$

Key words and phrases. Braces; Holomorphs.

and show that their number increases with increasing order (Corollary 6.7), a surprising contrast to the stabilization observed in the other cases.

2. Basics on braces

In this section, we provide basic definitions and results on braces, and introduce notations used throughout the paper.

For a brace A, set

$$a^b := a \circ b - b$$
 and $\sigma(a)(b) := b^{a^{-1}}$

for a, $b \in A$. It turns out that $\sigma(a) \in \operatorname{Aut}(A,+)$ for all $a \in A$, and the relation $(a+b)^c = a^c + b^c$ holds in A.

Remark 2.1. For a brace $(A, +, \circ)$, the identity element of both the groups is the same and the inverse of an element a w.r.t. \circ is $-\sigma(a)(a)$.

There are two other equivalent ways of thinking about right braces that are relevant to this article.

Remark 2.2. Given a right brace $(A, +, \circ)$ we define the map

$$\rho: (A, \circ) \to \operatorname{Aut}(A, +)$$

by

$$a \mapsto \rho_a := [b \mapsto b^a] = \sigma(a)^{-1}.$$

This makes ρ an anti-homomorphism of groups since

$$\rho_{a \circ b}(c) = c^{a \circ b} = (c^a)^b = \rho_b(\rho_a(c))$$

for all $a, b, c \in A$. One can check that the condition $a^{b \circ c} = (a^b)^c$ is equivalent to $a \circ (b \circ c) = (a \circ b) \circ c$. Consequently, we have a right linear group action $(A, +) \curvearrowleft (A, \circ)$ defined as

$$a * b := \rho_b(a)$$
 for all $a, b \in A$.

Now recall that for a right linear action of a group G on an Abelian group (A, +) a map $f: G \to A$ is called a right 1-cocyle if

$$f(gh) = f(g) * h + f(h)$$
 for all $g, h \in G$.

So given a right brace $(A, +, \circ)$ we can easily check that the identity map $1_A : (A, \circ) \to (A, +)$ is a bijective right 1-cocycle. Conversely, given a group (H, \circ) acting linearly on the right of an abelian group (A, +), and a bijective right 1-cocycle $\pi : H \to A$ (i.e. satisfying $\pi(g \circ h) = \pi(g) * h + \pi(h)$ for all $g, h \in H$) we can define an addition on H by

$$q + h := \pi^{-1}(\pi(q) + \pi(h))$$
 for all $q, h \in H$.

Then we can check that $(H, +, \circ)$ is a right brace. Therefore right braces correspond to bijective right 1-cocycles.

Another way to view right braces are as regular subgroups of holomorph groups. Recall that for a group G we define the holomorph of G to be

$$Hol(G) := G \rtimes Aut(G).$$

Then a regular subgroup of Hol(G) is defined to be a subgroup of the form

$$\{(g, \varphi(g)) \in \operatorname{Hol}(G) \mid g \in G\}$$

for some set function $\varphi: G \to \operatorname{Aut}(G)$. Now given an abelian group (A, +) let

$$\mathcal{B}(A) := \{ (A, +, \circ) \mid (A, +, \circ) \text{ is a right brace} \}$$

and let

$$S(A) := \{G \mid G \text{ is a regular subgroup of } Hol(A, +)\}.$$

Then the map

$$[(A, +, \circ) \mapsto \{(a, \rho_a) \in \operatorname{Hol}(A, +) \mid a \in A\}] : \mathcal{B}(A) \to \mathcal{S}(A)$$

is a bijection. Hence, right braces can be viewed as regular subgroups of holomorphs of abelian groups.

Definition 2.3. For a right brace A, a subgroup I of the additive group (A, +) is called a *right ideal*, if it is stable under the action ρ , that is, $\rho_a(x) \in I$ for all $a \in A$, $x \in I$. It turns out that a right ideal is also a subgroup of the adjoint group. A right ideal is said to be an *ideal* if it is a normal subgroup of (A, \circ) .

Definition 2.4. Two braces $(A_1, +_1, , \circ_1)$ and $(A_2, +_2, , \circ_2)$ are said to be *isomorphic* if there is a bijective map $f: A_1 \to A_2$ satisfying

$$f(x +_1 y) = f(x) +_2 f(y)$$

 $f(x \circ_1 y) = f(x) \circ_2 f(y)$

for all $x, y \in A_1$.

Given a right brace $(A, +, \circ)$ we define its *socle* to be ker ρ , that is,

$$Soc(A) := \{ a \in A \mid b^a = b \text{ for all } b \in A \} = \{ a \in A \mid \sigma(a) = 1_A \}.$$

In [21], it is proved that Soc(A) is an ideal of the brace A.

3. The additive structures of modular maximal-cyclic braces

A modular maximal-cyclic (MMC) brace is defined as a brace A whose adjoint group is isomorphic to $M_{2^{m+2}}$ for some integer m. In this section, we obtain that the socle of a modular maximal-cyclic brace A of size 2^{m+2} $(m \ge 3)$ is non-trivial, and we determine the possible additive structures of the brace A. We recall the presentation of $M_{2^{m+2}}$ $(m \ge 3)$ given in the Introduction section

(3.1)
$$M_{2^{m+2}} = \langle a, b \mid a^{2^{m+1}} = b^2 = 1, \ bab^{-1} = a^{1+2^m} \rangle.$$

We first classify all normal subgroups of a modular-maximal cyclic group.

Proposition 3.1. Let $M_{2^{m+2}}$ be modular maximal-cyclic group with presentation (3.1) and H be a non-trivial proper subgroup of $M_{2^{m+2}}$. Then, H is one of the following forms $(1 \le s \le m)$

- $H \subseteq \langle a \rangle$;
- $H = \langle b \rangle$;
- $H = \langle ba \rangle$;
- $H = \langle ba^{2^s} \rangle;$
- $H = \langle b, a^{2^s} \rangle$.

Moreover every non-trivial subgroup except $\langle ba^{2^m} \rangle$ and $\langle b \rangle$ is normal and contains $\langle a^{2^m} \rangle$.

Proof. When we say $ba^n \in M_{2m+2}$ we mean $0 \le n \le 2^{m+1} - 1$. For odd i, we have

$$\langle ba^i \rangle = \{1, ba, ba^3, \dots, ba^{2^{m+1}-1}, a^2, a^4, \dots, a^{2^{m+1}-2}\}\$$

and for even i, $(ba^i)^2 = a^{2i}$. Thus every non-trivial subgroup of $M_{2^{m+2}}$ except $\langle ba^{2^m} \rangle$ and $\langle b \rangle$ and contains $\langle a^{2^m} \rangle$. Observe that $a^i(ba^r)a^{-i} = (ba^r)(a^{2^m})^i$ and $ba^i(ba^r)(ba^i)^{-1} = (ba^r)(a^{2^m})^{r-i}$. Thus all the mentioned subgroups except those two are normal.

Now let H be a non-trivial proper subgroup which is neither of the first three forms. We first do some reductions. At first, note that if $ba^i \in H$ then i is even, since otherwise for odd i we have $H = \langle ba^i \rangle = \langle ba \rangle$ or $H = M_{2^{m+2}}$ as $\langle ba \rangle$ has index two. Again, since $H \neq \langle b \rangle$ we know that there is some minimal positive even i_0 for which $ba^{i_0} \in H$. We write this i_0 in the form 2^rq with $r \geq 1$ and q odd. Then $ba^{2^rqq'} \in H$ for all odd q'. We can choose q' such that $qq' \equiv 1 \mod 2^{m+1}$. Therefore, $i_0 = 2^r$ with $r \geq 1$ minimal. In fact, by this argument we have also proved that if $ba^{2^lq} \in H$ (with q odd), then $ba^{2^l} \in H$ and so $l \geq r$. Now the following claim settles the proposition.

Claim. Let $H \neq 1, M_{2^{m+2}}, \langle b \rangle, \langle ba \rangle$ and not a subgroup of $\langle a \rangle$, and let $r \geq 1$ be minimal such that $ba^{2^r} \in H$. We have:

- If $ba^j \in H$ implies $j = 2^r q$ with q odd, then $H = \langle ba^{2^r} \rangle$.
- If $ba^j \in H$ for some $j = 2^l q$ with l > r and q odd, then $b \in H$. Further, if $a^{2^s} \in H$ with $s \ge 0$ minimal, then we have $s \ge 1$ and $H = \langle b, a^{2^s} \rangle$.

Proof of Claim: For the first item, it is enough to show $H \cap \langle a \rangle = \langle a^{2^{r+1}} \rangle$. Otherwise if $a^{2^k} \in H$ for k < r + 1 then $ba^{2^k(2^{r-k}+1)} \in H$. So if k < r, then by the same argument in the previous paragraph, we conclude $ba^{2^k} \in H$, contradicting minimality of r. Hence k = r, but then $ba^{2^{r+1}} \in H$, which again contradicts the hypothesis that $ba^j \in H$ implies $j = 2^r q$ with q odd.

Next, suppose $ba^j \in H$ for some $j = 2^l q$ with l > r and q odd. At first, note that odd powers of a can not be in H. Since otherwise $ba^{2^r}a^{\operatorname{odd}} = ba^{2^r+\operatorname{odd}} \in H$, and so $H = \langle ba \rangle$ or $M_{2^{m+2}}$ which is avoided in our hypothesis. So we assume $a^{2^s} \in H$ with s minimal. Then s > 0. Now since $ba^{2^r} \in H$ we have $a^{2^{r+1}} = (ba^{2^r})^2 \in H$ and so $a^{2^l} \in \langle a^{2^{r+1}} \rangle \subset H$. Also $ba^{2^l} \in H$ (with q odd) implies $ba^{2^l} \in H$ and so $b \in H$. Hence $\langle b, a^{2^s} \rangle \subset H$. Now suppose

 $ba^{2^l} \in H$ with l > r. Then $bba^{2^l} = a^{2^l} \in H$, and my minimality of s we have $l \ge s$. Hence $a^{2^l} \in \langle a^{2^s} \rangle \subset \langle b, a^{2^s} \rangle$ and so $ba^{2^l} \in \langle b, a^{2^s} \rangle$. Therefore, $H = \langle b, a^{2^s} \rangle$.

The proof of the proposition is now complete.

Corollary 3.2. Let A be a MMC brace of size 2^{m+2} for $m \geq 3$, where (A, \circ) is given by the presentation (3.1), then $\{1, a^{2^m}\} \subseteq \operatorname{Soc}(A)$.

Proof. Suppose Soc(A) is trivial. Then the adjoint group A_{\circ} embeds in Aut(A, +). This provides an automorphism of order 2^{m+1} , which is impossible by [3]. Hence Soc(A) is a non-trivial normal subgroup of (A, \circ) . Now we show that every normal subgroup H of (A, \circ) contains $\{1, a^{2^m}\}$. The required result follows from Proposition 3.1.

The proof of the following result goes along the same lines as the proof of [4, Theorem 3.4].

Proposition 3.3. Let A be a MMC brace of size 2^{m+2} for $m \ge 2$. Then the additive group (A, +) must be one of the following groups:

- $\mathbb{Z}/2^{m+2}$;
- $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$;
- $\mathbb{Z}/4 \times \mathbb{Z}/2^m$;
- $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$; $\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^{m-1}$.

Proof. By Remark 2.2, we can assume (A, \circ) be a regular subgroup of Hol(A). So Hol(A) contains an element of order 2^{m+1} . Let rank and exponent of (A, +) be r and 2^d respectively. Then by [4, Lemma 2.6],

$$m+1 < \lceil \log_2(r+1) \rceil + d$$
.

Since A_+ has a cyclic factor H of order 2^d , we have $r-1 \le \text{rank}$ of $A_+/H \le m+2-d$. Thus

$$r-1 \le m+1-d+1 < \lceil \log_2(r+1) \rceil + 1.$$

Hence $r \leq 4$. Therefore, if r=2 then m+2-d=1 or 2; if r=3 then m+2-d=2; if r=4 then m+2-d=3. This gives the listed possible group structures of (A, +).

4. On automorphisms of some abelian 2-groups

In this section we recall how to think of elements of Aut(N), for an abelian p-group N, in terms of matrices having modular entries. We start by taking p to be any prime while recalling the general results and then eventually specialize to the case p=2. We also write a cyclic group of order ℓ additively as \mathbb{Z}/ℓ .

So let p be any prime and let N be an abelian p-group of the form $\mathbb{Z}/p^{e_1} \times \cdots \times \mathbb{Z}/p^{e_n}$ where $e_1 \leq \cdots \leq e_n$ are positive integers. We define

$$R_p := \left\{ (a_{ij})_{1 \leq i,j \leq n} \in \mathbb{Z}^{n \times n} \mid p^{e_i - e_j} \text{ divides } a_{ij} \text{ for all } i \geq j \right\}.$$

Noting that any matrix in R_p can be written as PBP^{-1} for some $B \in \mathbb{Z}^{n \times n}$ and $P = \operatorname{diag}(p^{e_1}, \dots, p^{e_n})$, we easily conclude that, under usual matrix multiplication and addition R_p forms a ring.

Next we take $\pi_i : \mathbb{Z} \to \mathbb{Z}/p^{e_i}$ to be the canonical projection and $\pi : \mathbb{Z}^n \to N$ as $(x_1, \dots, x_n)^{\intercal} \mapsto (\pi_1(x_1), \dots, \pi_n(x_n))^{\intercal}$. Now we define the map

$$\psi: R_p \to \operatorname{End}(N)$$
, $U \mapsto \psi(B) := [\pi(x_1, \dots, x_n)^{\mathsf{T}} \mapsto \pi(B(x_1, \dots, x_n)^{\mathsf{T}})]$.

By [18, Theorem 3.3] the map ψ is a surjective ring homomorphism. Moreover, by Lemma 3.4 (op. cit.) we have

$$\operatorname{Ker}(\psi) = \{(a_{ij}) \in R_p \mid p^{e_i} \text{ divides } a_{ij} \text{ for all } i, j\}.$$

Finally, by Theorem 3.6 (*ibid.*) we have for $B \in R_p$

$$\psi(B) \in \operatorname{Aut}(N) \iff B(\operatorname{mod} p) \in \operatorname{GL}_n(\mathbb{F}_p).$$

Hence, we identify $\operatorname{End}(N)$ with $\bar{R} := R_p/\operatorname{Ker}(\psi)$ and also it is easy to see that \bar{R}^{\times} can be identified with

$$\{(a_{ij}) \mid a_{ij} \in \mathbb{Z}/p^{e_i} \text{ for all } i,j; p^{e_i-e_j} \mid a_{ij} \text{ for all } i \geq j; (a_{ij}) \pmod{p} \in \mathrm{GL}_n(\mathbb{F}_p) \}.$$

Thus we can view elements of Aut(N) as the above type of matrices. Note that one can directly check that under usual matrix multiplication of the coset representatives, the above set forms a ring: more precisely, if (a_{ij}) and (b_{ij}) are two such matrices with modular entries as above, then one can treat a_{ij} and b_{ij} simply as integers and then compute the ij-th entry of the product as $\sum_{k} a_{ik} b_{kj} \pmod{p^{e_i}}$. See also [4, Section 2].

Let N be an abelian p-group as in the previous paragraphs. Now note that we can present any element of $\operatorname{Hol}(N) = N \rtimes \operatorname{Aut}(N)$ by a matrix of the form

$$\begin{pmatrix} B & v \\ 0 & 1 \end{pmatrix}$$

where B is the matrix presentation of an element of Aut(N) and $v \in N$, written as a column vector. Note that this way of presenting the elements of $\operatorname{Hol}(N)$ reflects the multiplication law: $(n_1, \varphi_1) \rtimes (n_2, \varphi_2) = (n_1 \varphi_1(n_2), \varphi_1 \varphi_2)$.

Notation 4.1. We will use capital letters to emphasize the matrix presentation while writing the elements of $M_{2^{m+2}}$ when we treat this as a subgroup of Hol(N) for some abelian p-group.

From this point, we take p=2. We have the following proposition analogous to [4, Section 4].

Proposition 4.2. Let $N = \mathbb{Z}/2^{e_1} \times \cdots \times \mathbb{Z}/2^{e_n}$ with $1 \leq e_1 \leq \cdots \leq e_n$ and $e_1 + \cdots + e_n = m + 2$, let

$$M_{2^{m+2}} = \langle X, Y \mid X^{2^{m+1}} = Y^2 = 1, YXY^{-1} = X^{1+2^m} \rangle$$

be a regular subgroup of Hol(N). We write

$$X = \left(\begin{array}{cc} S & v \\ 0 & 1 \end{array}\right), \quad Y = \left(\begin{array}{cc} T & w \\ 0 & 1 \end{array}\right).$$

Then we have the following relations

(4.1)
$$\begin{cases} S^{2^m} = I, & (1) \\ T^2 = I, & (2) \\ TS = ST. & (3) \end{cases}$$

Proof. Let the brace corresponding the given regular subgroup be A (Remark 2.2), and we assume (A, \circ) has the presentation (3.1). Thus $\rho_a = S$ and $\rho_b = T$, which gives $S^{2^{m+1}} = T^2 = I$ and $TST = S^{1+2^m}$. From Corollary 3.2, we have $S^{2^m} = I$. This induces the required relations.

Now we turn to the special types of Abelian 2-groups obtained in Proposition 3.3. We have the following proposition, the results of which can be proved by other means as well which do not depend on the matrix presentations.

Proposition 4.3. Let $m \geq 2$ and N be one of the abelian 2-groups obtained in Proposition 3.3. We have:

- (a). If $N = \mathbb{Z}/2^{m+2}$, then $|\text{Aut}(N)| = 2^{m+1}$. (b). If $N = \mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$, then $|\text{Aut}(N)| = 2^{m+2}$
- (c). If $N = \mathbb{Z}/4 \times \mathbb{Z}/2^m$, then $|\operatorname{Aut}(N)| = \begin{cases} 2^{m+4} & \text{, for } m > 2\\ 2^5 \times 3 & \text{, for } m = 2 \end{cases}$.
 (d). If $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$, then $|\operatorname{Aut}(N)| = 2^{m+4} \times 3$.

(d). If
$$N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$$
, then $|\operatorname{Aut}(N)| = 2^{m+1} \times 3$.
(e). If $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^{m-1}$, then $|\operatorname{Aut}(N)| = \begin{cases} 2^{m+7} \times 3 \times 7 & \text{for } m > 2\\ 2^6 \times 3^2 \times 5 \times 7 & \text{for } m = 2 \end{cases}$

Moreover, in each of the above cases, the matrices in Aut(N) that reduce mod 2 to upper unipotents form a Sylow 2-subgroup.

Proof. Item (a) is well known, so we prove the Proposition for items (b)-(e). For $N = \mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$ we have

$$\operatorname{Aut}(N) \simeq \left\{ \left(\begin{array}{cc} a & b \\ 2^m c & d \end{array} \right) \; \middle| \; a, b \in \mathbb{Z}/2; \; c, d \in \mathbb{Z}/2^{m+1}; \; ad \equiv 1 \pmod{2} \right\}$$
$$= \left\{ \left(\begin{array}{cc} 1 & b \\ 2^m c & d \end{array} \right) \; \middle| \; b \in \mathbb{Z}/2, \; 2^m c \in \{0, 2^m\}, \; d \in (\mathbb{Z}/2^{m+1})^{\times} \right\}.$$

Hence $|\operatorname{Aut}(N)| = 2^{m+2}$, and clearly every element of $\operatorname{Aut}(N)$ reduces to an upper unipotent mod 2. For $N = \mathbb{Z}/4 \times \mathbb{Z}/2^m$ we first note that

$$\operatorname{Aut}(N) \simeq \left\{ \left(\begin{array}{cc} a & b \\ 2^{m-2}c & d \end{array} \right) \; \middle| \; a,b \in \mathbb{Z}/4; \; c,d \in \mathbb{Z}/2^m; \; ad - 2^{m-2}bc \equiv 1 \pmod{2} \right\}.$$

So we consider at first the case m=2. In this case $\operatorname{Aut}(N) \simeq \operatorname{GL}_2(\mathbb{Z}/4)$. Its order is the number of solutions of the modular equation

$$ad - bc \equiv 1 \pmod{2}$$

for $a, b, c, d \in \mathbb{Z}/4$. This means either ad is odd and bc is even or vice versa. For odd ad there are 4 possibilities for $a, d \in \mathbb{Z}/4$. By same argument there are 16-4=12 possibilities for even bc. Hence there are $2 \times 48=96$ solutions.

Therefore $|\operatorname{Aut}(\mathbb{Z}/4 \times \mathbb{Z}/4)| = 2^5 \times 3$. In this subcase, matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ which reduce to upper unipotents are given by the constraints: a, d = 1 or 3, c = 0 or 2, and $b \in \mathbb{Z}/4$. This has clearly 2^5 many possibilities.

Next consider the case $N = \mathbb{Z}/4 \times \mathbb{Z}/2^m$ for m > 2. We have

$$\operatorname{Aut}(N) \simeq \left\{ \left(\begin{array}{cc} a & b \\ 2^{m-2}c & d \end{array} \right) \; \middle| \; a,b \in \mathbb{Z}/4; \; c,d \in \mathbb{Z}/2^m; \; ad \equiv 1 (\operatorname{mod} 2) \right\}$$

$$= \left\{ \left(\begin{array}{cc} a & b \\ 2^{m-2}c & d \end{array} \right) \; \middle| \; a = 1 \text{ or } 3, \; b \in \mathbb{Z}/4; \; 2^{m-2}c \in \{0,2^{m-2},2^{m-1},3 \times 2^{m-2}\} \text{ mod } 2^m; \; d \in (\mathbb{Z}/2^m)^{\times} \right\}.$$

Hence $|Aut(N)| = 2^{m+4}$, and every matrix reduces to an upper unipotent.

For $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$ we have

$$\operatorname{Aut}(N) \simeq \left\{ \left(\begin{array}{ccc} a & b & c \\ r & s & t \\ 2^{m-1}x & 2^{m-1}y & z \end{array} \right) \;\middle|\; a,b,c,r,s,t \in \mathbb{Z}/2;\; x,y,z \in \mathbb{Z}/2^m; \; \text{and} \; z(as-br) \equiv 1 (\operatorname{mod} 2) \right\}$$

$$= \left\{ \left(\begin{array}{ccc} a & b & c \\ r & s & t \\ 2^{m-1}x & 2^{m-1}y & z \end{array} \right) \;\middle|\; c,t \in \mathbb{Z}/2;\; x,y \in \{0,1\};\; z \in (\mathbb{Z}/2^m)^\times; \; \text{and} \; \left(\begin{array}{ccc} a & b \\ r & s \end{array} \right) \in \operatorname{GL}_2(\mathbb{Z}/2) \right\}.$$

Therefore, $|\operatorname{Aut}(N)| = 2^{m+4} \times 3$. And matrices that reduce to upper unipotents are given by the following constraints : a = s = 1, $z \in (\mathbb{Z}/2^m)^{\times}$, r = 0, $b, c, t \in \mathbb{Z}/2$, and $x, y \in \{0, 1\}$. These constraints account for 2^{m+4} many possibilities.

Finally consider the case when $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^{m-1}$. Here we have

$$\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ p & q & r & s \\ 2^{m-2}t & 2^{m-2}u & 2^{m-2}v & w \end{pmatrix} \in \operatorname{Aut}(N)$$

if and only if

$$\begin{cases} a, b, c, d, e, f, g, h, p, q, r, s \in \mathbb{Z}/2, \\ t, u, v \in \{0, 1\}, w \in \mathbb{Z}/2^{m-1}, \\ & a & b & c & d \\ & e & f & g & h \\ & p & q & r & s \\ & 2^{m-2}t & 2^{m-2}u & 2^{m-2}v & w \end{cases} \equiv 1 \pmod{2}.$$

Here again we consider first the case when m=2. Then clearly $\operatorname{Aut}(N) \simeq \operatorname{GL}_4(\mathbb{Z}/2)$ so that $|\operatorname{Aut}(N)| = 2^6 \times 3^2 \times 5 \times 7$. The matrices that reduce to upper unipotents are given by the constraints : a=f=r=w=1, e=p=q=t=u=v=0, and $b,c,d,g,h,s\in\mathbb{Z}/2$. These have 2^6 many solutions.

Next we consider the situation when m > 2. Then the condition

$$w \times \left\| \begin{array}{ccc} a & b & c \\ e & f & g \\ p & q & r \end{array} \right\| \equiv 1 \pmod{2}$$

is equivalent to $w \in (\mathbb{Z}/2^{m-1})^{\times}$ and $\begin{pmatrix} a & b & c \\ e & f & g \\ p & q & r \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}/2)$, which account for $2^{m+1} \times 3 \times 7$ many choices. For

each of these choices the constraints $d, h, s \in \mathbb{Z}/2$ and $t, u, v \in \{0, 1\}$ have 2^6 many solutions. Putting these together we have

$$|\operatorname{Aut}(N)| = 2^{m+7} \times 3 \times 7.$$

Finally, the matrices that reduce mod 2 to upper unipotents are given by the following constraints

$$\begin{cases} a = f = r = 1, \\ w \in (\mathbb{Z}/2^{m-1})^{\times}, \\ e = p = q = 0, \\ t, u, v \in \{0, 1\}, \\ b, c, d, g, h, s \in \mathbb{Z}/2, \end{cases}$$

having $2^{m-2} \times 2^3 \times 2^6 = 2^{m+7}$ many solutions as expected.

The proof of the proposition is now complete.

5. When the additive group is not $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$

In this section, we filter the additive structures of a modular maximal-cyclic brace. We show that the only possible additive structure of non-cyclic MMC brace is $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$.

The possibility of cyclic structure follows from the following result proved in [22, Section 7, Theorem 3].

Proposition 5.1. There is a unique cyclic brace of size 2^{m+2} (m > 3) with MMC adjoint group.

Byott and Ferri [4, Section 7] proved that the holomorph group $\operatorname{Hol}(\mathbb{Z}/4 \times \mathbb{Z}/2^m)$ contains no quaternion or dihedral regular subgroups for $m \geq 3$. Their technique, however, yields a slightly more general result.

Proposition 5.2. Let G be a group of size 2^{m+2} $(m \ge 3)$ contains an element of order 2^{m+1} . Then G can not be a regular subgroup of $\operatorname{Hol}(\mathbb{Z}/4 \times \mathbb{Z}/2^m)$.

Proof. Suppose G is a regular subgroup of $\operatorname{Hol}(\mathbb{Z}/4 \times \mathbb{Z}/2^m)$ of size 2^{m+2} . By the arguments of [4, Section 7], there is a homomorphism $f: G \to \operatorname{Hol}(\mathbb{Z}/4 \times \mathbb{Z}/8)$ such that $\left|\frac{G}{\ker f}\right| \geq 2^5$. To the contrary, suppose there is an element $x \in G$ such that $o(x) = 2^{m+1}$. Let $o(x \ker f) = 2^r$, and consider the subgroup $H = \langle x^{2^r} \rangle$ of $\ker f$. Since $|G/H| = 2^{r+1} \ge 2^5$, we obtain $r \ge 4$. Thus $G/\ker f$ contains an element of order 16, which is not possible by [4, Lemma 7.1].

Corollary 5.3. There is no regular subgroup of type $M_{2^{m+2}}$ in $\operatorname{Hol}(\mathbb{Z}/4 \times \mathbb{Z}/2^m)$ for $m \geq 3$.

The following example confirms the existence of regular subgroups of type $M_{2^{m+2}}$ in $\text{Hol}(\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1})$.

Example. Consider the groups $A = M_{2m+2}$ and $N = \mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$ for $m \geq 3$. From remark 2.2, it is enough to provide a bijective map $\gamma: A \to N$ and a right action $\rho: A \to \operatorname{Aut}(N)$ such that with respect to ρ, γ becomes a bijective right 1-cocycle. Consider (with respect to the presentation (3.1) of A)

$$\rho(a) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \rho(b) = \begin{pmatrix} 1 & 0 \\ 0 & 1 + 2^m \end{pmatrix};$$
$$\gamma(a^i) = \begin{pmatrix} 0 \\ i \end{pmatrix}, \qquad \gamma(ba^i) = \begin{pmatrix} 1 \\ i \end{pmatrix} \qquad \text{for } 0 \le i \le 2^{m+1} - 1.$$

One can easily verify (see also Proposition 6.1) that γ becomes a bijective right 1-cocycle with respect to the ρ .

We now prove the main result of this section following [4, Section 8 and 9] only making necessary changes suited to our case.

Theorem 5.4. The additive structure of a non-cyclic MMC brace of size 2^{m+2} for $m \geq 3$ is $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$.

Proof. It now remains to be shown, by the above Corollary and Proposition 3.3, that there is no regular subgroup

of type $M_{2^{m+2}}$ in $\operatorname{Hol}(N)$ if $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$ or $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^{m-1}$ for $m \geq 3$. At first, we let $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^m$. To the contrary suppose $M_{2^{m+2}} = \left\langle X, Y | X^{2^{m+1}} = 1 = Y^2, \ YXY = X^{2^m+1} \right\rangle$ be a regular subgroup of Hol(N). Write X as

$$\begin{pmatrix} S & v \\ 0 & 1 \end{pmatrix}$$

for some S in Aut(N) and $v \in N$ (written as a column). By Proposition 4.2 we know that S lies in a Sylow 2-subgroup of $\operatorname{Aut}(N)$. By conjugating A with some C in $\operatorname{Aut}(N)$ (and then conjugating $M_{2^{m+2}}$ by $\begin{pmatrix} C & 0 \\ 0 & 1 \end{pmatrix} \in \operatorname{Hol}(N)$) we can assume that S(mod 2) is upper unipotent (see Proposition 4.3). So we can write

$$X = \begin{pmatrix} 1 & a & b & v_1 \\ 0 & 1 & c & v_2 \\ 2^{m-1}d & 2^{m-1}e & \alpha & v_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

where $a, b, c \in \mathbb{Z}/2$, $d, e \in \mathbb{Z}/2^m$, $\alpha \in (\mathbb{Z}/2^m)^{\times}$, $v_1, v_2 \in \mathbb{Z}/2$, and $v_3 \in \mathbb{Z}/2^m$. Now we compute the powers of X by first multiplying the matrices treating the entries as integers and then we reduce the first two rows mod 2 and the third mod 2^m . We obtain

$$X^2 = \begin{pmatrix} 1 & 0 & ac & av_2 + bv_3 \\ 0 & 1 & 0 & cv_3 \\ 0 & 2^{m-1}ad & 2^{m-1}(bd + ce) + \alpha^2 & 2^{m-1}dv_1 + 2^{m-1}ev_2 + (1+\alpha)v_3 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Again repeating the same strategy, we get

$$X^{4} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \alpha^{4} & 2^{m-1}acdv_{3} + (1+\alpha)(1+\alpha^{2})v_{3} \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Now since $\alpha \in (\mathbb{Z}/2^m)^{\times}$ so α is represented by an odd integer, and hence $\alpha^4 \equiv 1 \pmod{4}$. Also m > 2 and $(1+\alpha)(1+\alpha^2)$ is divisible by 4. Hence treating X^4 as a matrix with integer entries we have

$$X^4 \equiv I \pmod{4}$$
.

We claim that X satisfies

$$X^{2^{\ell}} \equiv I(\text{mod } 2^{\ell}), \quad \text{for all } \ell \ge 2.$$

This can be shown easily by an induction argument, which we omit. Therefore we have shown that $X^{2^m} = I$ in Hol(N) since m > 2, which contradicts the fact that order of X is 2^{m+1} .

Next, we let $N = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2^{m-1}$. As in the previous case, we proceed by contradiction. We suppose $M_{2^{m+2}}$ is a regular subgroup of Hol(N). Then we can write

$$X = \begin{pmatrix} 1 & a & b & c & v_1 \\ 0 & 1 & d & e & v_2 \\ 0 & 0 & 1 & f & v_3 \\ 2^{m-2}g & 2^{m-2}h & 2^{m-2}i & \alpha & v_4 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then we compute X^2 by treating integer entries and next reduce the first three rows mod 2 and the fourth row mod 2^{m-1} :

$$X^{2} = \begin{pmatrix} 1 & 0 & ad & ae + bf & av_{1} + bv_{2} + cv_{3} \\ 0 & 1 & 0 & df & dv_{3} + ev_{4} \\ 0 & 0 & 1 & 0 & fv_{4} \\ 0 & 2^{m-2}ga & 2^{m-2}(gb+hd) & \alpha^{2} + 2^{m-2}(gc+he+if) & (1+\alpha)v_{4} + 2^{m-2}(gv_{1} + hv_{2} + iv_{3}) \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Squaring and reducing again we get

$$X^{4} = \begin{pmatrix} 1 & 0 & 0 & 0 & adfv_{4} \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{4} + 2^{m-2}gadf & (1+\alpha)(1+\alpha^{2})v_{4} + 2^{m-2}\ell \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

for some integer ℓ . Now when m=3 we compute

$$X^{8} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2adfv_{4} \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^{8} + 4\alpha gadf & (\alpha^{4} + 2gadf + 1)((1+\alpha)(1+\alpha^{2})v_{4} + 2\ell) \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$
 (reducing the first row mod 2, fourth row mod 4)

where we observe that in the last equality we have used the fact that α is odd and so $\alpha^4 \equiv 1 \pmod{4}$ and $(1+\alpha)(1+\alpha^2) \equiv 0 \pmod{4}$. Hence when m=3 we have $X^8=I$ in $\operatorname{Hol}(N)$ which contradicts that $X \in M_{32}$ has order 16. But when $m \geq 4$ we have $X^8 \equiv I \pmod{4}$ and as in the first case an induction argument gives $X^{2^k} \equiv 1 \pmod{2^{k-1}}$ for every integer $k \geq 3$. This implies $X^{2^m} = I$ in $\operatorname{Hol}(N)$ which contradicts that X has order 2^{m+1} . This completes the proof.

6. When the additive group is $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$

In the previous section, we showed that the possible non-cyclic additive structure of an MMC brace is $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$. We first give a criteria to test for the existence of MMC braces.

Proposition 6.1. Let (A, \circ) be a group with a presentation 3.1 and $T, S \in \operatorname{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1})$ such that $S^{2^m} = T^2 = I$ and TST = S. Further assume $\gamma: (A, \circ) \to \mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$ be a bijective map such that $\gamma(1) = 0$ and satisfies the following for all i, j, k

(6.1)
$$\gamma(a^{i+j}) = S^j \gamma(a^i) + \gamma(a^j)$$

(6.2)
$$\gamma(ba^i) = S^i \gamma(b) + \gamma(a^i)$$

(6.3)
$$\gamma(a^ib) = T\gamma(a^i) + \gamma(b)$$

$$(6.4) T\gamma(b) = -\gamma(b)$$

$$\gamma(a^{2^m}) = \begin{pmatrix} 0\\2^m \end{pmatrix}.$$

Then

$$\rho: (A, \circ) \to \operatorname{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}), \qquad \rho(a) := S, \ \rho(b) := T$$

defines a right action of (A, \circ) on $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$, and with respect to this action γ becomes bijective 1-cocyle, that is for all $x, y \in A$, $\gamma(xy) = \rho(y)(\gamma(x)) + \gamma(y)$.

Proof. We have $(S^{-1})^{2^{m+1}} = (T^{-1})^2 = I$ and $T^{-1}S^{-1}T^{-1} = (S^{-1})^{2^m+1}$, thus ρ^{-1} (where $\rho^{-1}(x) := \rho(x)^{-1}$) defines an left action. This yields that ρ is a right action. Clearly for any automorphism $U \in \operatorname{Aut}(\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1})$, we have

$$(6.6) U\gamma(a^{2^m i}) = \gamma(a^{2^m i}).$$

Using Eqs. (6.1)-(6.4), (6.6) and presentation (3.1), we get

$$\gamma((ba^{i})(ba^{j})) = \gamma(a^{2^{m}i+i+j}) = S^{2^{m}i}\gamma(a^{i+j}) + \gamma(a^{2^{m}i})$$

$$= \gamma(a^{i+j}) + \gamma(a^{2^{m}i}),$$

$$S^{j}T\gamma(ba^{i}) + \gamma(ba^{j}) = S^{j}T\gamma(a^{2^{m}i+i}b) + \gamma(ba^{j})$$

$$= S^{j}T(T(S^{2^{m}i}\gamma(a^{i}) + \gamma(a^{2^{m}i})) + \gamma(b)) + \gamma(ba^{j})$$

$$= S^{j}\gamma(a^{i}) + S^{j}\gamma(a^{2^{m}i}) - S^{j}\gamma(b) + S^{j}\gamma(b) + \gamma(a^{j})$$

$$= S^{j}\gamma(a^{i}) + \gamma(a^{j}) + \gamma(a^{2^{m}i}) = \gamma(a^{i+j}) + \gamma(a^{2^{m}i}).$$

Using the similar arguments, one can show

$$\gamma((ba^i)(a^j)) = S^j \gamma(ba^i) + \gamma(a^j)$$
$$\gamma((a^i)(ba^j)) = S^j T \gamma(a^i) + \gamma(ba^j).$$

Hence we have obtained $\gamma(xy) = \rho(y)\gamma(x) + \gamma(y)$ for all $x, y \in A$.

We now shift our focus to counting the number of MMC braces of a fixed size. While the adjoint group of a brace can be viewed as a regular subgroup in the holomorph of its additive group, the representation of an element $x \in (A, \circ)$ as a matrix containing $\rho(x)$ and $\gamma(x)$ introduces computational complexities (see Remark 2.2, Section 3). To remove these difficulties, we consider the components of these matrices separately; in other words, we adopt the approach of viewing braces as bijective 1-cocycles, a method previously utilized in [20, 23].

We consider (A, \circ) to be the group with presentation 3.1. We denote the bijective 1-cocycle by $\gamma: (A, \circ) \to$ $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$ and by the proof of the Proposition 4.3, the right action ρ of the generators a and b can be written by the invertible matrices

(6.7)
$$\rho(a) = \sigma(a)^{-1} = S := \begin{pmatrix} 1 & y \\ 2^m x & 1 + 2z \end{pmatrix}, \qquad \rho(b) = \sigma(b)^{-1} = T := \begin{pmatrix} 1 & v \\ 2^m u & 1 + 2w \end{pmatrix}$$

with $x, y, u, v \in \mathbb{Z}/2$ and $z, w \in \mathbb{Z}/2^m$.

At first we write down some technical lemmas.

Lemma 6.2. Let $k \ge 1$ and $\beta := 1 + 2z$, then we have :

(6.8)
$$S^{n} = \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & \beta^{4k} \end{pmatrix} & if \ n = 4k \\ \begin{pmatrix} 1 & y \\ 2^{m}x & \beta^{4k+1} \end{pmatrix} & if \ n = 4k+1 \\ \begin{pmatrix} 1 & 0 \\ 0 & 2^{m}xy + \beta^{4k+2} \end{pmatrix} & if \ n = 4k+2 \\ \begin{pmatrix} 1 & y \\ 2^{m}x & 2^{m}xy + \beta^{4k+3} \end{pmatrix} & if \ n = 4k+3. \end{cases}$$

Proof. This is direct computation.

Lemma 6.3. Let k be an integer, then there are integers k_1, k_2 such that for $m \geq 2$,

$$(4k+1)^{2^{m-1}} + (4k+1)^{2^{m-2}} + \dots + (4k+1) + 1 = 2^{m+1}k_1 + 2^m$$
$$(4k+3)^{2^{m-1}} + (4k+3)^{2^{m-2}} + \dots + (4k+3) + 1 = 2^{m+1}k_2.$$

In particular, let
$$\beta \in (\mathbb{Z}/2^{m+1})^{\times}$$
 with $m \geq 2$, and $x = \beta^{2^m - 1} + \dots + \beta + 1$. Then we have :
$$x \equiv \begin{cases} 2^m \mod 2^{m+1} & \text{if } \beta \equiv 1 \mod 4, \\ 0 \mod 2^{m+1} & \text{if } \beta \equiv 3 \mod 4. \end{cases}$$

Proof. This result follows from an easy induction on m, and the fact that for all $m \ge 1$

$$\beta^{2^{m}-1} + \dots + \beta + 1 = (1 + \beta^{2^{m-1}})(\beta^{2^{m-1}-1} + \dots + \beta + 1).$$

Lemma 6.4. Let $\beta = 4k + 1$ for some k > 0, then

$$(\beta^n + \dots + \beta + 1) \not\equiv 0 \pmod{2^{m-1}}$$

whenever $1 \le n \le 2^{m+1} - 2$ and $n \ne 2^m - 1$, $2^{m-1} - 1$, $2^m + 2^{m-1} - 1$. And if $1 \le n \le 2^{m+1} - 2$ and $n \ne 2^m - 1$,

$$(\beta^n + \dots + \beta + 1) \not\equiv 0 \pmod{2^m}$$
.

Proof. Let $o(\beta) = 2^r$ in $(\mathbb{Z}/2^{m+1})^{\times}$. If $(\beta^n + \cdots + \beta + 1) \not\equiv 0 \pmod{2^{m-1}}$, then the relation $(\beta^{n+1} - 1) = (\beta - 1)(\beta^n + \dots + \beta + 1).$

gives
$$\beta^{n+1} = 1$$
, that is $n = 2^r s - 1$ for some s. Now

$$\begin{split} \beta^n + \cdots + \beta + 1 &= \beta^{2^r s - 1} + \beta^{2^r s - 2} + \cdots + \beta + 1 \\ &= \beta^{2^r (s - 1)} (\beta^{2^r - 1} + \beta^{2^r - 2} + \cdots + 1) + \beta^{2^r (s - 1) - 1} + \beta^{2^r (s - 1) - 2} + \cdots + 1 \\ &= (\beta^{2^r - 1} + \beta^{2^r - 2} + \cdots + 1) + \beta^{2^r (s - 2)} (\beta^{2^r - 1} + \cdots + 1) + \beta^{2^r (s - 2) - 1} + \beta^{2^r (s - 2) - 2} + \cdots + 1 \\ &= s (\beta^{2^r - 1} + \beta^{2^r - 2} + \cdots + \beta + 1) \\ &= s (2^{r + 1} k' + 2^r) \qquad \text{by Lemma 6.3.} \end{split}$$

Let $s = 2^{l}q$, where q is odd. Thus we obtain

(6.9)
$$2^{r+l+1}k'q + 2^{r+l}q = 2^{m-1}k'',$$

since $2 \le 2^{r+l}q \le 2^{m+1} - 1$, modulo 2^{r+l+1} of (6.9) implies $n = 2^{m-1}u - 1$ for some u, which is not possible. When $(\beta^n + \cdots + \beta + 1) \not\equiv 0 \pmod{2^m}$, the Eq. (6.9) can be replaced by

$$2^{r++l+1}k'q + 2^{r+l}q = 2^m k'',$$

and modulo 2^{r+l+1} implies r+l=m, then $n=2^m-1$ which is not possible.

We first strengthen Corollary 3.2 in the proposition below.

Proposition 6.5. Let A be a non-cyclic MMC brace of size 2^{m+2} , where $m \geq 3$. Then $a^{2^{m-1}} \in Soc(A)$.

Proof. This follows from the relation $(1+2z)^{2^{m-1}} = 1$ in $(\mathbb{Z}/2^{m+1})^{\times}$, and using Eq 6.8, one can see that $S^{2^{m-1}} = 1$ when m > 3.

Now we carry out some reductions. From the relations $T^2 = I$, TST = S, we get

$$(6.10) 4w(w+1) = 2^m uv$$

(6.11)
$$4w(1+w)(1+2z) = 2^m(uv + uy + xv),$$

in $\mathbb{Z}/2^{m+1}$. The above two equation gives

$$(6.12) xv = yu \text{ in } \mathbb{Z}/2.$$

We assume $\gamma(a) = \binom{p}{q}$ and $\gamma(b) = \binom{r}{s}$. Thus the relation $\gamma(b^2) = 0$ gives

$$(6.13) vs = 0 in \mathbb{Z}/2$$

(6.14)
$$2s(1+w) = 2^m ur \text{ in } \mathbb{Z}/2^{m+1}.$$

Note that

For
$$k \ge 2$$
, $\gamma(a^2) = \begin{pmatrix} yq \\ 2^m xp + \beta q + q \end{pmatrix}$ and $\gamma(a^{2^k}) = \begin{pmatrix} 0 \\ (\beta^{2^k-1} + \dots + \beta + 1)q \end{pmatrix}$, since $\gamma(a^{2^m}) \ne 0$ and $\gamma(a^{2^{m+1}}) = 1$, thus

(6.15)
$$(\beta^{2^m - 1} + \dots + \beta + 1)q = 2^m, \qquad \gamma(a^{2^m}) = \begin{pmatrix} 0 \\ 2^m \end{pmatrix}.$$

From the relation $bab = a^{2^m+1}$, we obtain

$$\gamma(bab) = \gamma(a^{2^m+1})$$

$$T\gamma(ba) + \gamma(b) = S^{2^m}\gamma(a) + \gamma(a^{2^m})$$

$$TS\gamma(b) + T\gamma(a) + \gamma(b) = \gamma(a) + \gamma(a^{2^m}),$$

this yields

(6.16)
$$vq + s(y+v) = 0 \text{ in } \mathbb{Z}/2$$

(6.17)
$$2^{m}(xr + ur + xvs + up + 1) + q = \alpha\beta s + \alpha q + s.$$

Using (6.14), Eq. (6.17) reduces to

(6.18)
$$2^{m}(xr + xvs + up + 1) = 2(wq - sz).$$

From Lemma 6.3 and Eq. (6.15), we obtain z is even and q is odd. Therefore, we can assume $\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. The Eqs.(6.15), (6.16) and (6.18) reduce to

(6.19)
$$(\beta^{2^m - 1} + \dots + \beta + 1) = 2^m \text{ in } \mathbb{Z}/2^{m+1}$$

(6.20)
$$v + s(y + v) = 0 \text{ in } \mathbb{Z}/2$$

(6.21)
$$2^{m}(xr + xvs + 1) = 2w - 2zs \text{ in } \mathbb{Z}/2^{m+1}.$$

Modulo 4 of Eq. (6.21) gives w is even. Hence Eqs (6.10) and (6.14) reduce to

$$(6.22) 4w = 2^m uv$$

$$(6.23) 2s = 2^m ur.$$

Now 4s = 0 implies $s \in \{0, 2^{m-1}, 2^m, 2^m + 2^{m-1}\}$, and observe that $\gamma(ba^{2^m}) = \binom{r}{s+2^m}$, thus using the transformation $(a, b) \mapsto (a, ba^{2^m})$, we can further assume

$$(6.24) s \in \{0, 2^{m-1}\}.$$

Since z is even, (6.20) and (6.21) turn into

$$(6.25) v = 0 in \mathbb{Z}/2$$

(6.26)
$$2^{m}(xr+1) = 2w \text{ in } \mathbb{Z}/2^{m+1}.$$

Theorem 6.6. Let A be a non-cyclic MMC brace of size 2^{m+2} , where $m \geq 3$. Then the brace structure is either of the form

$$S = \begin{pmatrix} 1 & y \\ 2^m x & 1 + 2z \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & 1 + 2^m (1+x) \end{pmatrix};$$
$$\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \qquad \gamma(b) = \begin{pmatrix} 1 \\ 0 \end{pmatrix};$$

or

$$S = \begin{pmatrix} 1 & 0 \\ 2^m x & 1 + 2z \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 2^m & 1 + 2^m (1+x) \end{pmatrix};$$

$$\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \qquad \gamma(b) = \begin{pmatrix} 1 \\ 2^{m-1} \end{pmatrix};$$

where $z \in \mathbb{Z}/2^m$ is even and $x, y \in \mathbb{Z}/2$. Conversely these two forms define brace structures on the group (A, \circ) of presentation (3.1). Moreover, these two types of braces are non-isomorphic.

Proof. From the various relations (above Proposition 6.1), we obtain that z is even and $\gamma(a)$ can be assumed $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Furthermore, from Eq. (6.24), we have $s \in \{0, 2^{m-1}\}$. The relations (6.26), (6.25), and (6.23), yield the first form when s = 0, and the second form when $s = 2^{m-1}$. The first part is complete.

Notice that $\beta=1+2z\in (\mathbb{Z}/2^{m+1})^{\times}$ and $|(\mathbb{Z}/2^{m+1})^{\times}|=2^m$, therefore $\beta^{2^m}=1$. Since $m\geq 2$, from Eq.(6.8), we obtain $S^{2^m}=I$. Thus Eq. (6.26) implies $T^2=1$ and $T^{-1}S^{-1}T^{-1}=S^{-1}$, therefore from Proposition 6.1,

$$a \mapsto S$$
, $b \mapsto T$,

define a right action of (A, \circ) on $\mathbb{Z}/2 \times \mathbb{Z}/2^{m+1}$.

We consider the first form. Using Eq. (6.8), the relations (6.1) and (6.2), we obtain, for $k \geq 0$:

$$\gamma(a^{4k+4}) = \begin{pmatrix} 0 \\ \beta^{4k+3} + \dots + 1 \end{pmatrix}, \qquad \gamma(a^{4k+1}) = \begin{pmatrix} 0 \\ \beta^{4k} + \dots + 1 \end{pmatrix},
\gamma(a^{4k+2}) = \begin{pmatrix} y \\ \beta^{4k+1} + \dots + 1 \end{pmatrix}, \qquad \gamma(a^{4k+3}) = \begin{pmatrix} y \\ 2^m xy + \beta^{4k+2} + \dots + 1 \end{pmatrix},
\gamma(ba^{4k+4}) = \begin{pmatrix} 1 \\ \beta^{4k+3} + \dots + 1 \end{pmatrix}, \qquad \gamma(ba^{4k+1}) = \begin{pmatrix} 1 \\ 2^m x + \beta^{4k} + \dots + 1 \end{pmatrix},
\gamma(ba^{4k+2}) = \begin{pmatrix} y+1 \\ \beta^{4k+1} + \dots + 1 \end{pmatrix}, \qquad \gamma(ba^{4k+3}) = \begin{pmatrix} y+1 \\ 2^m x(1+y) + \beta^{4k+2} + \dots + 1 \end{pmatrix}$$

Clearly in this case, we have relation (6.4), and since z is even, by Lemma 6.3, the γ satisfies (6.5), this implies $\gamma(1) = 0$. Now we will verify (6.3), it is clearly true for i = 0. For i = 4k + 1, $k \ge 0$, using the relations (6.27),

Lemma 6.3 and the fact $\beta^{2^m} = 1$, we have

$$T\gamma(a^{i}) + \gamma(b) = \begin{pmatrix} 1 \\ 2^{m}x + \beta^{4k} + \dots + 1 + 2^{m} \end{pmatrix}$$

$$\gamma(a^{i}b) = \gamma(ba^{2^{m}+4k+1}) = \begin{pmatrix} 1 \\ 2^{m}x + \beta^{2^{m}+4k} + \dots + 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 2^{m}x + \beta^{2^{m}}(\beta^{4k} + \dots + 1) + \beta^{2^{m}-1} + \dots + 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 \\ 2^{m}x + \beta^{4k} + \dots + 1 + 2^{m} \end{pmatrix};$$

Similarly, we can obtain $\gamma(a^ib) = T\gamma(a^i) + \gamma(b)$, by considering i = 4k + 2 and i = 4k + 3. Thus by Proposition 6.1, we are only left with showing γ is a bijection. Suppose for some $1 \le j \le i \le 2^{m+1} - 2$ and u, we have

$$\beta^{i} + \beta^{i-1} + \dots + 1 = 2^{m}u + \beta^{j} + \dots + 1,$$

then $\beta^{i-j+1}+\beta^{i-j}+\cdots+1=2^m u$. By Lemma 6.3 and Lemma 6.4, $i-j+1=2^m-1$ and u=1. Therefore

if
$$j \equiv 1 \pmod{4}$$
, then $i \equiv 3 \pmod{4}$

if
$$j \equiv 2 \pmod{4}$$
, then $i \equiv 0 \pmod{4}$

if
$$j \equiv 3 \pmod{4}$$
, then $i \equiv 1 \pmod{4}$

if
$$j \equiv 0 \pmod{4}$$
, then $i \equiv 2 \pmod{4}$.

Now since u = 1,

$$\gamma(a^{4k_1+4}) \neq \gamma(a^{4k_2+2}), \ \gamma(ba^{4k_1+4}) \neq \gamma(ba^{4k_2+2}), \ \gamma(a^{4k_1+4}) \neq \gamma(ba^{4k_2+2}), \ \gamma(ba^{4k_1+4}) \neq \gamma(a^{4k_2+2}).$$

Now if $\gamma(a^{4k_1+1}) = \gamma(a^{4k_2+3})$ then y = 0, but then u = 1 implies the second coordinate of these elements are not equal, which is a contradiction, in this way we can show

$$\gamma(a^{4k_1+1}) \neq \gamma(ba^{4k_2+3}), \ \gamma(b^{4k_1+3}) \neq \gamma(ba^{4k_2+1}), \gamma(ba^{4k_1+1}) \neq \gamma(ba^{4k_2+3}).$$

Hence, we get γ is a bijection.

Similarly, we can show that the second form also defines brace structures.

Now we show that these two type of braces are not isomorphic. Suppose the braces for s=0 and $s=2^{m-1}$ be A_1 (the cocycle be γ_1) and A_2 (cocycle be γ_2) respectively, and $f:A_1\to A_2$ be a brace isomorphism. With respect to the presentation (3.1), the generators for (A_1,\circ) be a_1,b_1 , and for (A_2,\circ) be a_2,b_2 . The elements the in the group (3.1) of order 2^{m+1} are a^i or ba^i where i is odd; the elements of order 2 are a^{2^m},b , and ba^{2^m} ; and $a^2 \in \langle ba \rangle = \langle ba^i \rangle$ for all odd i. Thus $f(b_1)$ is either b_2 or $b_2a_2^{2^m}$. But order of $\gamma_1(b_1)$ is 2, and the order of both $\gamma_2(b_2)$ and $\gamma_2(b_2a_2^{2^m})$ is 4. Which is not possible.

From Proposition 3.1, we have information of all normal subgroups of a modular maximal-cyclic group. Now using Theorem 6.6, we exhibit all MMC braces of size 2^{m+2} ($m \ge 3$) by considering all possible socles.

6.1. If $\langle ba \rangle = \mathbf{Soc}(A)$. Here TS = 1, that is S = T. If $s = 2^{m-1}$, then x = 1 and 2z = 0. Thus in this case

$$T = S = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad \gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ \gamma(b) = \begin{pmatrix} 1 \\ 2^{m-1} \end{pmatrix}.$$

And if s = 0, then

$$T = S = \begin{pmatrix} 1 & 0 \\ 0 & 1 + 2^m \end{pmatrix}, \qquad \gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \ \gamma(b) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Thus for this case we have two non-isomorphic braces.

6.2. If $\langle b, a^{2^k} \rangle = \operatorname{Soc}(A)$ for $k \geq 1$. Since T = 1, s = 0 and x = 1. Thus

$$S = \begin{pmatrix} 1 & y \\ 2^m & 1+2z \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$
$$\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \qquad \gamma(b) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

By Proposition 6.5, $1 \le k \le m-1$. Since $o(1+2^{m+1-k})=2^k$ in $(\mathbb{Z}/2^{m+1})^{\times}$, for each such k, there is a brace. Therefore in this case we have at least m-1 distinct braces.

6.3. If $\langle a^{2^k} \rangle = \operatorname{Soc}(A)$ for $0 \le k \le m$. In this case $T \ne 1$, thus when s = 0, x = 0. Hence

$$S = \begin{pmatrix} 1 & y \\ 0 & 1+2z \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 0 & 1+2^m \end{pmatrix}$$
$$\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \qquad \gamma(b) = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

And when $s = 2^{m-1}$

$$S = \begin{pmatrix} 1 & 0 \\ 2^m x & 1 + 2z \end{pmatrix}, \qquad T = \begin{pmatrix} 1 & 0 \\ 2^m & 1 + 2^m (1+x) \end{pmatrix}$$

$$\gamma(a) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \qquad \qquad \gamma(b) = \begin{pmatrix} 1 \\ 2^{m-1} \end{pmatrix}.$$

Again we have $1 \le k \le m-1$. Same reason like above, for each case we have brace for all such values of k, and by Theorem 6.6, these braces are non-isomorphic, hence in this case we have at least 2(m-1) distinct braces.

6.4. If $\langle a^{2^k}b\rangle = \operatorname{Soc}(A)$ for $1 \leq k \leq m$. By Propositions 3.1 and 6.5, $k \leq m-2$. For $s=2^{m-1}$,

$$TS^{2^k} = \begin{pmatrix} 1 & 0 \\ 2^m & \beta^{2^k} + 2^m(1+x) \end{pmatrix} \neq 1.$$

Hence s = 0, since $T \neq 1$, x = 0, and

$$TS^{2^k} = \begin{pmatrix} 1 & 0 \\ 0 & \beta^{2^k} + 2^m \end{pmatrix}.$$

There always exist a $\beta \equiv 1 \pmod{4}$ in $(\mathbb{Z}/2^{m+1})^{\times}$ such that $\beta^{2^k} + 2^m = 1$ and $\beta^{2^{k-1}} + 2^m \neq 1$, for example $\beta = 1 + 2^{m-k}$. Therefore, we have at least m-2 distinct such braces.

Suppose $f: A_1 \to A_2$ be a brace isomorphism, where A_1, A_2 are MMC braces, if $f(a_1) = a_2^i$ where i is odd, then the fact $f(\operatorname{Soc}(A_1)) = \operatorname{Soc}(A_2)$ implies all the mentioned braces are distinct. We can assume $f(a_1) = b_2 a_2$, then $f(a_1^{2k}) \in \{a_2^{2k}, a_2^{2^m+2k}\}$ for all $k \ge 1$. Therefore, the braces obtained in Subsections 6.2–6.4 are distinct. Hence we obtain

Corollary 6.7. Number of non-cyclic MMC braces of size 2^{m+2} with $m \ge 3$ is at least 4m-5.

Remark 6.8. A remarkable fact is that the number of braces associated with dihedral, semidihedral and generalized quaternion groups stabilizes with increasing order. We have proved that this pattern does not follow for the modular maximal-cyclic group case.

ACKNOWLEDGMENT

The second author is grateful to Professor Wolfgang Rump for introducing this problem.

References

- Iván Angiono, César Galindo, and Leandro Vendramin, Hopf braces and Yang-Baxter operators, Proc. Amer. Math. Soc. 145
 (2017), no. 5, 1981–1995. MR 3611314
- Valeriy G. Bardakov, Mikhail V. Neshchadim, and Manoj K. Yadav, Computing skew left braces of small orders, Internat. J. Algebra Comput. 30 (2020), no. 4, 839–851. MR 4113853 1
- 3. V. G. Berkovič, Groups of order pⁿ that admit an automorphism of order pⁿ⁻¹, Algebra i Logika 9 (1970), 3-8. MR 283084 3
- Nigel P. Byott and Fabio Ferri, On the number of quaternion and dihedral braces and Hopf-Galois structures, J. Algebra 665 (2025), 72–102. MR 4830431 1, 3, 3, 4, 4, 5, 5, 5
- A. Caranti, F. Dalla Volta, and M. Sala, Abelian regular subgroups of the affine group and radical rings, Publ. Math. Debrecen 69
 (2006), no. 3, 297–308. MR 2273982 1
- Marco Castelli, Marzia Mazzotta, and Paola Stefanelli, Simplicity of indecomposable set-theoretic solutions of the Yang-Baxter equation, Forum Math. 34 (2022), no. 2, 531–546. MR 4388351 1
- Francesco Catino, Ilaria Colazzo, and Paola Stefanelli, Regular subgroups of the affine group and asymmetric product of radical braces, J. Algebra 455 (2016), 164–182. MR 3478858 1
- 8. F. Cedó and J. Okniński, Constructing finite simple solutions of the Yang-Baxter equation, Adv. Math. 391 (2021), Paper No. 107968, 40. MR 4300920 1
- 9. Ferran Cedó, Eric Jespers, and Ángel del Río, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. **362** (2010), no. 5, 2541–2558. MR 2584610 1
- 10. Ferran Cedó, Eric Jespers, and Jan Okniński, Braces and the Yang-Baxter equation, Comm. Math. Phys. 327 (2014), no. 1, 101–116. MR 3177933 1
- Lindsay N. Childs, Fixed-point free endomorphisms and Hopf Galois structures, Proc. Amer. Math. Soc. 141 (2013), no. 4, 1255–1265.
 MR 3008873 1

- 12. Teresa Crespo, Daniel Gil-Muñoz, Anna Rio, and Montserrat Vela, *Inducing braces and Hopf Galois structures*, J. Pure Appl. Algebra **227** (2023), no. 9, Paper No. 107371, 16. MR 4559373 1
- 13. _____, Left braces of size 8p, J. Algebra 617 (2023), 317–339. MR 4513787 1
- Pavel Etingof, Travis Schedler, and Alexandre Soloviev, Set-theoretical solutions to the quantum Yang-Baxter equation, Duke Math. J. 100 (1999), no. 2, 169–209. MR 1722951 1
- 15. S. C. Featherstonhaugh, A. Caranti, and L. N. Childs, Abelian Hopf Galois structures on prime-power Galois field extensions, Trans. Amer. Math. Soc. **364** (2012), no. 7, 3675–3684. MR 2901229 1
- L. Guarnieri and L. Vendramin, Skew braces and the Yang-Baxter equation, Math. Comp. 86 (2017), no. 307, 2519–2534.
 MR 3647970 1
- 17. Marshall Hall, Jr., The theory of groups, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition. MR 414669 1
- 18. Christopher J. Hillar and Darren L. Rhea, Automorphisms of finite abelian groups, Amer. Math. Monthly 114 (2007), no. 10, 917–923. MR 2363058 4
- Arpan Kanrar and Wolfgang Rump, A decomposition problem for involutive solutions to the Yang-Baxter equation, Bull. Belg. Math. Soc. Simon Stevin 31 (2024), no. 5, 688–702. MR 4842840 1
- 20. _____, Braces with adjoint group of maximal nilpotency class, J. Algebra 664 (2025), 328-343. MR 4829401 1, 6
- 21. Wolfgang Rump, Braces, radical rings, and the quantum Yang-Baxter equation, J. Algebra 307 (2007), no. 1, 153–170. MR 2278047 1, 2
- 22. _____, Classification of cyclic braces, J. Pure Appl. Algebra 209 (2007), no. 3, 671–685. MR 2298848 5
- 23. _____, Classification of the affine structures of a generalized quaternion group of order \geqslant 32, J. Group Theory 23 (2020), no. 5, 847–869. MR 4141382 1, 6
- 24. _____, Classification of non-degenerate involutive set-theoretic solutions to the Yang-Baxter equation with multipermutation level two, Algebr. Represent. Theory 25 (2022), no. 5, 1293–1307. MR 4483006 1
- 25. H. J. Zassenhaus, The theory of groups, 2nd ed., Chelsea, New York, 1958. 1

HARISH-CHANDRA RESEARCH INSTITUTE, A CI OF HOMI BHABHA NATIONAL INSTITUTE, CHHATNAG ROAD, JHUNSI, PRAYAGRAJ-211 019. INDIA

Email address: arpandas@hri.res.in

HARISH-CHANDRA RESEARCH INSTITUTE, A CI OF HOMI BHABHA NATIONAL INSTITUTE, CHHATNAG ROAD, JHUNSI, PRAYAGRAJ-211 019, INDIA

Email address: arpankanrar@hri.res.in