involve
a journal of mathematics

The classification of involutions and symmetric spaces of modular groups

Marc Besson and Jennifer Schaefer

msp

2019 vol. 12, no. 4

INVOLVE 12:4 (2019)
dx.doi.org/10.2140/involve.2019.12.565

The classification of involutions and symmetric spaces of modular groups

Marc Besson and Jennifer Schaefer

(Communicated by Kenneth S. Berenhaut)

The involutions and the symmetric spaces associated to the family of modular groups of order 2^m are explored. We begin by analyzing the structure of the automorphism group and by establishing which automorphisms are involutions. We conclude by calculating the fixed-point group and symmetric spaces determined by each involution.

1. Introduction

A first course in group theory usually provides a short introduction to the idea of the automorphism group of a group. Students often begin by calculating the automorphism group for a few familiar groups of small order, such as the symmetric group S_3 or the dihedral group D_4. Computing the automorphism group of one of these groups is an especially fruitful exercise as it requires a student to understand properties of the group itself and results in students making conjectures about the structure of automorphism groups of similar groups. Though this activity is worthwhile on its own, knowing the structure of the automorphism group of a group has also proven essential in a variety of areas, including the theory of symmetric spaces.

First introduced by Élie Cartan [1926; 1927], real symmetric spaces were a special class of homogeneous Riemannian manifolds. Berger [1957] later generalized these spaces and gave classifications of the irreducible semisimple symmetric spaces. Since then the theory of symmetric spaces has expanded into a field that plays a fundamental role in numerous areas of active research, including Lie theory, number theory, differential geometry, harmonic analysis, and physics; see [Harish-Chandra 1984a; 1984b; 1984c; 1984d; Ōshima and Matsuki 1984; Brylinski and Delorme 1992; Carmona and Delorme 1994; van den Ban and Schlichtkrull 1997a; 1997b; Delorme 1998] for mathematics examples and [Olshanetsky and Perelomov 1983; Zirnbauer 1996] for physics examples. The theory of symmetric

MSC2010: 20D15, 53C35.
Keywords: modular 2-group, symmetric spaces, automorphisms, involutions.

spaces also has many generalizations. Symmetric varieties, symmetric k-varieties, Vinberg's theta-groups, spherical varieties, Gelfand pairs, Bruhat–Tits buildings, Kac–Moody symmetric spaces, and generalized symmetric spaces are among these generalizations which have found importance in various areas of mathematics and physics such as number theory, algebraic geometry, and representation theory.

The majority of these generalizations can be studied in the context of generalized symmetry spaces. Generalized symmetric spaces are defined as the homogeneous spaces G/H with G an arbitrary group and $H = G^\theta = \{g \in G \mid \theta(g) = g\}$ the fixed-point group of an order-n automorphism θ. Of special interest are automorphisms of order 2, also called *involutions*. If G is an algebraic group defined over a field k and θ an involution defined over k, then these spaces are also called symmetric k-varieties, first introduced in [Helminck 1994].

For involutions there is a natural embedding of the homogeneous spaces G/H into the group G as follows. Let $\tau : G \to G$ be a morphism of G given by $\tau(g) = g\,\theta(g)^{-1}$ for $g \in G$, where θ is an involution of G. The map τ induces an isomorphism of the coset space G/H onto $\tau(G) = \{g\,\theta(g)^{-1} \mid g \in G\}$. We will take the image $Q = \{g\,\theta(g)^{-1} \mid g \in G\}$ as our definition of the *generalized symmetric space determined by* (G, θ). In addition, we define the *extended symmetric space determined by* (G, θ) as $R = \{g \in G \mid \theta(g) = g^{-1}\}$. Extended symmetric spaces play an important role in generalizing the Cartan decomposition for real reductive groups to reductive algebraic groups defined over an arbitrary field. While for real groups it suffices to use Q for the Cartan decomposition, in the general case one needs the extended symmetric space R. Symmetric spaces and symmetric k-varieties are well known for their role in many areas of mathematics, but they are probably best known for their fundamental role in representation theory. The generalized symmetric spaces as defined above are of importance in a number of areas as well, including group theory, number theory, and representation theory.

Recently, involutions and symmetric spaces have been determined for dihedral groups [Cunningham et al. 2014], dicyclic groups [Bishop et al. 2013], and semidihedral groups [Schaefer and Schlechtweg 2017]. In this paper, we investigate the involutions and symmetric spaces associated to the modular groups of order 2^m. Since all non-Abelian 2-groups of order 2^m which contain a cyclic subgroup of order 2^{m-1} and where $m \geq 4$ are isomorphic to a dihedral group, a generalized quaternion group (contained in the more general class of dicyclic groups), a semidihedral group, or a modular group by [Gorenstein 1968], this work completes the study of involutions and symmetric spaces for groups of this structure. We begin in Section 2 by analyzing the family of modular groups, $\mathrm{M}_m(2)$, of order 2^m for $m \geqslant 4$. In Section 3, we classify the automorphisms of $\mathrm{M}_m(2)$ and establish which automorphisms are involutions. We also consider which involutions arise from inner automorphisms. In Section 4, we describe the fixed-point group H, the generalized

symmetric space Q, and the extended symmetric space R determined by each involution of $\mathrm{M}_m(2)$. Finally in the Appendix, we provide H, Q, and R for each involution of $\mathrm{M}_4(2)$.

2. Preliminaries

Throughout this paper, we consider the modular 2-group $\mathrm{M}_m(2)$, which can be described using the following presentation from [Gorenstein 1968]:

$$\mathrm{M}_m(2) = \langle x, y \mid x^{2^{m-1}} = y^2 = 1,\ yx = x^{2^{m-2}+1} y \rangle,$$

where $m \geq 4$ is an integer. Defined in terms of generators and relations, this presentation is convenient for determining the automorphism group of $\mathrm{M}_m(2)$ and the fixed-point group and symmetric spaces associated with each involution.

We begin by providing some basic structural properties of $\mathrm{M}_m(2)$ that are prerequisites for the rest of the paper. The group presentation given above clearly shows that $\mathrm{M}_m(2)$ is a non-Abelian group. The next result we state provides a commutation relation which we will use to simplify the structure of the group's elements.

Lemma 1. *For any integer $k \geq 1$, we have $yx^k = x^{(2^{m-2}+1)k} y$.*

Using the outcome of Lemma 1 repeatedly, together with the relations $x^{2^{m-1}} = y^2 = 1$ and the uniqueness of a quotient and a remainder in the quotient-remainder theorem, we have the following results.

Proposition 2. *Every element of $\mathrm{M}_m(2)$ has a unique presentation as $x^i y^j$, where i and j are integers with $0 \leq i < 2^{m-1}$ and $j \in \{0, 1\}$.*

We call the presentation given in Proposition 2 the *normal form* of an element of $\mathrm{M}_m(2)$ and by writing all elements of the group in their normal form, we have the subsequent corollary.

Corollary 3. *The non-Abelian group $\mathrm{M}_m(2)$ has order 2^m and consists of the elements $1,\ x,\ x^2, \ldots, x^{2^{m-1}-1},\ y,\ xy,\ x^2y, \ldots, x^{2^{m-1}-1}y$.*

In order to determine the automorphism group and the symmetric spaces, it will be necessary to know the order and inverse of each group element. The next three results establish this information.

Lemma 4. *For any integer $k \geq 1$,*

$$(x^i y^j)^k = \begin{cases} x^{ik+ij(k-1)2^{m-3}} y^j & \text{when } k \text{ is odd,} \\ x^{ik+ijk2^{m-3}} & \text{when } k \text{ is even.} \end{cases}$$

Proof. Suppose $k \geq 1$ is an integer and $x^i y^j \in \mathrm{M}_m(2)$ for $0 \leq i < 2^{m-1}$ and $j \in \{0, 1\}$. Then $(x^i y^j)(x^i y^j) = x^{2i+ij2^{m-2}}$ by Lemma 1. When k is odd,

$(x^i y^j)^k$ has $\frac{1}{2}(k-1)$ pairs of the form $(x^i y^j)(x^i y^j)$. Thus

$$(x^i y^j)^k = x^{(2i+ij2^{m-2})\frac{1}{2}(k-1)} x^i y^j$$
$$= x^{(k-1)(i+ij2^{m-3})+i} y^j = x^{ik+ij(k-1)2^{m-3}} y^j.$$

When k is even, $(x^i y^j)^k$ has $\frac{1}{2}k$ pairs of the form $(x^i y^j)(x^i y^j)$. In this case

$$(x^i y^j)^k = x^{(2i+ij2^{m-2})\frac{1}{2}k} = x^{ik+ijk2^{m-3}}$$

as desired. □

Proposition 5. *For any integer i with $0 \le i < 2^{m-1}$,*

$$|x^i| = \frac{2^{m-1}}{\gcd(i, 2^{m-1})} \quad \textit{and} \quad |x^i y| = \frac{2^{m-1}}{\gcd(2^{m-2}, i + i2^{m-3})}.$$

Proof. By basic properties of cyclic groups and the fact that $|x| = 2^{m-1}$,

$$|x^i| = \frac{2^{m-1}}{\gcd(i, 2^{m-1})}.$$

Consider $x^i y$. Then $(x^i y)^2 = x^{2i+i2^{m-2}}$ by Lemma 4, and

$$|x^{2i+i2^{m-2}}| = \frac{2^{m-1}}{\gcd(2^{m-1}, 2i + i2^{m-2})}$$

by above. By Lagrange's theorem, $|(x^i y)^2| \le |x^i y|$. Furthermore, $|x^i y| \le 2|(x^i y)^2|$ by properties of order. Hence we have $|(x^i y)^2| \le |x^i y| \le 2|(x^i y)^2|$.

Since $|\mathrm{M}_m(2)| = 2^m$, we know that $|x^i y|$ is a power of 2 by Lagrange's theorem. So either $|x^i y| = |(x^i y)^2|$ or $|x^i y| = 2|(x^i y)^2|$. We can easily rule out the first case, because $\langle (x^i y)^2 \rangle$ is a proper subgroup of $\langle x^i y \rangle$, seeing as it does not contain $x^i y$ for instance. Thus

$$|x^i y| = 2|(x^i y)^2| = 2\frac{2^{m-1}}{\gcd(2^{m-1}, 2i + i2^{m-2})} = \frac{2^{m-1}}{\gcd(2^{m-2}, i + i2^{m-3})}. \quad \square$$

Proposition 6. *For any integer i with $0 \le i < 2^{m-1}$,*

$$(x^i)^{-1} = x^{2^{m-1}-i} \quad \textit{and} \quad (x^i y)^{-1} = x^{(2^{m-1}-i)(2^{m-2}+1)} y.$$

Proof. The result follows immediately from Lemma 1 and the relations $x^{2^{m-1}} = y^2 = 1$. □

The final result of this section describes which elements compose the center of $\mathrm{M}_m(2)$. Knowing the center allows us to simplify calculations in several instances.

Proposition 7. *The center of $\mathrm{M}_m(2)$ consists of all elements of the form x^i where $0 \le i < 2^{m-1}$ is even. Thus $Z(\mathrm{M}_m(2))$ is a cyclic subgroup of order 2^{m-2}.*

Proof. We break this proof into three cases.

Case 1: Consider $x^{2k} \in M_m(2)$, where $0 \leq k < 2^{m-2}$. Then

$$xx^{2k} = x^{1+2k} = x^{2k+1} = x^{2k}x,$$

and by Lemma 1,

$$yx^{2k} = x^{2k(2^{m-2}+1)}y = x^{k2^{m-1}}x^{2k}y = x^{2k}y.$$

Thus x^{2k} commutes with both generators and $\langle x^2 \rangle \leq Z(M_m(2))$.

Case 2: Consider $x^{2k+1} \in M_m(2)$, where $0 \leq k < 2^{m-2}$. Using the commutation relation of Lemma 1,

$$yx^{2k+1} = x^{(2k+1)(2^{m-2}+1)}y = x^{2k+1}x^{2^{m-2}}y \neq x^{2k+1}y,$$

as $x^{2^{m-2}}$ is not equal to the identity. Thus x^{2k+1} is not central.

Case 3: Consider $x^i y \in M_m(2)$, where $0 \leq i < 2^{m-1}$. Then $xx^i y = x^{i+1}y$. However,

$$x^i yx = x^i x^{2^{m-2}+1}y = x^{2^{m-2}}x^{i+1}y.$$

These two expressions cannot be equal because $x^{2^{m-2}}$ is not equal to the identity. Thus elements of the form $x^i y$ are *not* central.

Therefore, $Z(M_m(2)) = \langle x^2 \rangle$. □

Example. The center of $M_4(2)$ is $Z(M_4(2)) = \{1, x^2, x^4, x^6\}$.

3. Automorphisms and involutions of $\mathrm{M}_m(2)$

In this section, we determine the automorphism group of $\mathrm{M}_m(2)$, denoted by $\mathrm{Aut}(\mathrm{M}_m(2))$. We begin by analyzing the structure of each automorphism and then move to proving some properties of the automorphism group as a whole. We conclude this section by establishing which elements of $\mathrm{Aut}(\mathrm{M}_m(2))$ are involutions and what properties two automorphism must satisfy to be equivalent.

Theorem 8. *A homomorphism $\phi : \mathrm{M}_m(2) \to \mathrm{M}_m(2)$ is an automorphism if and only if $\phi(x) = x^a y^b$ and $\phi(y) = x^{c2^{m-2}}y$ where a is odd and $b, c \in \{0, 1\}$.*

Proof. Let $\phi \in \mathrm{Aut}(\mathrm{M}_m(2))$. Then by properties of automorphisms, ϕ must map x to an element of order 2^{m-1} and y to an element of order 2. Thus by Proposition 5, $\phi(x) = x^a$ or $x^a y$, where a is odd and $\phi(y) = y,\ x^{2^{m-2}}$, or $x^{2^{m-2}}y$. However, ϕ would not be injective if y mapped to $x^{2^{m-2}}$. Therefore, if ϕ is an automorphism, $\phi(x) = x^a y^b$ and $\phi(y) = x^{c2^{m-2}}y$, where a is odd and $b, c \in \{0, 1\}$. The converse of this statement can be proven using cases. □

Corollary 9. *The automorphism group* $\mathrm{Aut}(\mathrm{M}_m(2))$ *has order* 2^m.

Proof. Since there are $2^{m-2} \cdot 2$ elements $x^a y^b$, where a is odd and $b \in \{0, 1\}$, and two elements $x^{c2^{m-2}} y$, where $c \in \{0, 1\}$,

$$|\mathrm{Aut}(\mathrm{M}_m(2))| = 2^{m-2} \cdot 2 \cdot 2 = 2^m. \qquad \square$$

Remark. It is interesting that $|\mathrm{Aut}(\mathrm{M}_m(2))| = |\mathrm{M}_m(2)|$. In the cases of dihedral groups [Cunningham et al. 2014], generalized quaternion groups [Bishop et al. 2013], and semidihedral groups [Schaefer and Schlechtweg 2017], the order of the automorphism group is much larger than the order of the group.

Based on the results of Theorem 8, we can represent each automorphism uniquely as $\phi_{a,b,c}$, where $\phi_{a,b,c}(x) = x^a y^b$ and $\phi_{a,b,c}(y) = x^{c2^{m-2}} y$, where a is odd and $b, c \in \{0, 1\}$. Using this notation, we see that $\phi_{1,0,0}$ denotes the identity automorphism. In the following theorem, we determine where $\phi_{a,b,c}$ maps an arbitrary element $x^i y^j \in M_m(2)$.

Theorem 10. *Let $x^i y^j \in M_m(2)$ for $0 \le i < 2^{m-1}$ and $j \in \{0, 1\}$ and $\phi_{a,b,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $b, c \in \{0, 1\}$. Then*

$$\phi_{a,b,c}(x^i y^j) = \begin{cases} x^{ai+abi2^{m-3}+cj2^{m-2}} y^j & \text{when } i \text{ is even,} \\ x^{ai+ab(i-1)2^{m-3}+cj2^{m-2}} y^{b+j} & \text{when } i \text{ is odd.} \end{cases}$$

Proof. Let $x^i y^j \in M_m(2)$ for $0 \le i < 2^{m-1}$ and $j \in \{0, 1\}$ and $\phi_{a,b,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $b, c \in \{0, 1\}$. By Theorem 8, we have

$$\phi_{a,b,c}(x^i y^j) = (x^a y^b)^i (x^{c2^{m-2}} y)^j.$$

In Proposition 7, we proved $x^{c2^{m-2}} \in Z(\mathrm{M}_m(2))$. Thus $(x^{c2^{m-2}} y)^j = x^{cj2^{m-2}} y^j$. To understand how the term $(x^a y^b)^i$ interacts with $x^{cj2^{m-2}} y^j$, we split into two cases: i even and i odd.

Case 1: Let i be even. Then by Lemma 4

$$\begin{aligned} \phi_{a,b,c}(x^i y^j) &= (x^a y^b)^i x^{cj2^{m-2}} y^j \\ &= x^{ai+abi2^{m-3}} x^{cj2^{m-2}} y^j \\ &= x^{ai+abi2^{m-3}+cj2^{m-2}} y^j. \end{aligned}$$

Case 2: Let i be odd. Then by Lemma 4

$$\begin{aligned} \phi_{a,b,c}(x^i y^j) &= (x^a y^b)^i x^{cj2^{m-2}} y^j \\ &= x^{ai+ab(i-1)2^{m-3}} y^b x^{cj2^{m-2}} y^j \\ &= x^{ai+ab(i-1)2^{m-3}+cj2^{m-2}} y^{b+j}. \end{aligned}$$

$\square$

Conjugation by a fixed element of a group G is one of the most important examples of an automorphism of a group. Thus it is interesting to determine which elements of $\mathrm{Aut}(\mathrm{M}_m(2))$ are inner automorphisms. Given an arbitrary group G and

an element $g \in G$, we let $\varphi_g \in \mathrm{Aut}(G)$ denote conjugation by g and $\mathrm{Inn}(G)$ denote the collection of inner automorphisms of G.

Theorem 11. *The inner automorphisms of* $\mathrm{M}_m(2)$ *are* $\phi_{1,0,c}$ *and* $\phi_{(2^{m-2}+1),0,c}$, *where* $c \in \{0, 1\}$.

Proof. Consider φ_g for some $g \in \mathrm{M}_m(2)$. Suppose $g = x^i$. Then

$$\varphi_{x^i}(x) = x^i x x^{2^{m-1}-i} = x^{2^{m-1}+1} = x,$$
$$\varphi_{x^i}(y) = x^i y x^{2^{m-1}-i} = x^i x^{(2^{m-2}+1)(2^{m-1}-i)} y = x^{-i2^{m-2}} y.$$

When $-i$ is even, $x^{-i2^{m-2}} y = y$ and when $-i$ is odd, $x^{-i2^{m-2}} y = x^{2^{m-2}} y$. Next, consider $g = x^i y$. Then

$$\varphi_{x^i y}(x) = (x^i y) x (y x^{2^{m-1}-i}) = x^i (x^{2^{m-2}+1} y)(y x^{2^{m-1}-i}) = x^{2^{m-2}+1},$$
$$\varphi_{x^i y}(y) = (x^i y) y (y x^{2^{m-1}-i}) = x^i (x^{(2^{m-1}-i)(2^{m-2}+1)} y) = x^{-i2^{m-2}} y.$$

Again, when $-i$ is even, $x^{-i2^{m-2}} y = y$ and when $-i$ is odd, $x^{-i2^{m-2}} y = x^{2^{m-2}} y$.

Conversely, consider $\phi_{1,0,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$. Note that conjugation by x^{-c} gives

$$x^{-c} x x^c = x,$$
$$x^{-c} y x^c = x^{c(2^{m-2})} y.$$

Thus, $\phi_{1,0,c} \in \mathrm{Inn}(\mathrm{M}_m(2))$. Similarly, consider $\phi_{2^{m-2}+1,0,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$. Then conjugation by $x^{-c} y$ gives

$$(x^{-c} y) x (y x^c) = x^{2^{m-2}+1},$$
$$(x^{-c} y) y (y x^c) = x^{c(2^{m-2})} y.$$

Thus, $\phi_{2^{m-2}+1,0,c} \in \mathrm{Inn}(\mathrm{M}_m(2))$. Therefore, $\phi_{a,b,c}$ is an inner automorphism of $\mathrm{M}_m(2)$ if and only if a is 1 or $2^{m-2} + 1$, $b = 0$, and $c \in \{0, 1\}$. □

It follows from this result that four of the 2^m automorphisms in $\mathrm{Aut}(\mathrm{M}_m(2))$ are inner automorphisms, which we knew would be the case as $\mathrm{Inn}(\mathrm{M}_m(2)) \cong \mathrm{M}_m(2)/Z(\mathrm{M}_m(2))$ and $|Z(\mathrm{M}_m(2))| = 2^{m-2}$ [Gorenstein 1968]. In Section 4, we will find it useful to understand the structure of the involutions arising from inner automorphisms because it will allow us to simplify the presentation of the fixed-point groups, the generalized symmetric spaces, and the extended symmetric spaces in these cases.

Before we can characterize the involutions, we require the following lemmas.

Lemma 12. *For any* $\phi_{a,b,c}, \phi_{d,e,f} \in \mathrm{Aut}(\mathrm{M}_m(2))$, *where* a *and* d *are odd and* $b, c, e, f \in \{0, 1\}$,

$$\phi_{a,b,c} \circ \phi_{d,e,f} = \phi_{ad+ab(d-1)2^{m-3}+ce2^{m-2},\, b+e,\, c+f}.$$

Proof. Let $\phi_{a,b,c}$ and $\phi_{d,e,f} \in \mathrm{Aut}(M_m(2))$. To determine $\phi_{a,b,c} \circ \phi_{d,e,f}$, we examine $\phi_{a,b,c} \circ \phi_{d,e,f}(x)$ and $\phi_{a,b,c} \circ \phi_{d,e,f}(y)$.

By Theorem 10 and d odd,

$$\phi_{a,b,c} \circ \phi_{d,e,f}(x) = \phi_{a,b,c}(x^d y^e) = x^{ad+ab(d-1)2^{m-3}+ce2^{m-2}} y^{b+e}.$$

Next, by Theorem 10 and $f2^{m-2}$ even,

$$\begin{aligned}\phi_{a,b,c} \circ \phi_{d,e,f}(y) &= \phi_{a,b,c}(x^{f2^{m-2}} y) \\ &= x^{af2^{m-2}+abf2^{m-2}2^{m-3}+c2^{m-2}} y = x^{(af+c)2^{m-2}} y.\end{aligned}$$

Because a is odd, $a = 2k+1$ for $k \in \mathbb{Z}$ and we have

$$x^{(af+c)2^{m-2}} y = x^{((2k+1)f+c)2^{m-2}} y = x^{(f+c)2^{m-2}} y.$$

Thus $\phi_{a,b,c} \circ \phi_{d,e,f}(y) = x^{(c+f)2^{m-2}} y$.

Given the images of x and y under $\phi_{a,b,c} \circ \phi_{d,e,f}$, we can define the general form of automorphism composition:

$$\phi_{a,b,c} \circ \phi_{d,e,f} = \phi_{ad+ab(d-1)2^{m-3}+ce2^{m-2},\, b+e,\, c+f}. \qquad \square$$

This result now allows to us to answer our question regarding automorphisms of order 2. We see in the following theorem that this reduces to evaluating an equation modulo 2^{m-1}.

Lemma 13. *Let $\phi_{a,b,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$, where a is odd and $b, c \in \{0,1\}$. Then $(\phi_{a,b,c})^2 = \phi_{1,0,0}$ if and only if*

$$a^2 + ab(a-1)2^{m-3} + bc2^{m-2} \equiv 1 \bmod 2^{m-1}. \tag{1}$$

Proof. Consider $\phi_{a,b,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$. By Lemma 12, we find that

$$\phi_{a,b,c} \circ \phi_{a,b,c} = \phi_{a^2+ab(a-1)2^{m-3}+bc2^{m-2},\, 2b,\, 2c}.$$

Since $b, c \in \{0,1\}$, we have $2b \equiv 2c \equiv 0 \bmod 2$ always. Thus we only need to solve (1) to determine when $\phi_{a,b,c} \circ \phi_{a,b,c} = \phi_{1,0,0}$. $\square$

Theorem 14. *For $m = 4$, $\mathrm{Aut}(\mathrm{M}_4(2))$ contains 11 involutions and for integers $m \geq 5$, $\mathrm{Aut}(\mathrm{M}_m(2))$ contains 15 involutions.*

Proof. Let $\phi_{a,b,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$, where a is odd and $b, c \in \{0,1\}$, such that $(\phi_{a,b,c})^2 = \phi_{1,0,0}$. Then by Lemma 13, (1) holds.

Case 1: Suppose $b = 0$ and $c = 0$. Then (1) reduces to $a^2 \equiv 1 \bmod 2^{m-1}$. There are four elements a in $\mathbb{Z}_{2^{m-1}}$ with $a^2 \equiv 1 \bmod 2^{m-1}$ by [Burton 2010], namely 1, -1, $1 + 2^{m-2}$, and $-1 + 2^{m-2}$. Thus we have four elements of the form $\phi_{a,0,0} \in \mathrm{Aut}(\mathrm{M}_m(2))$ with $(\phi_{a,0,0})^2 = \phi_{1,0,0}$. Because $\phi_{1,0,0}$ has order 1, it follows that there are three involutions of the form $\phi_{a,0,0}$, where $a \in \{-1, 1+2^{m-2}, -1+2^{m-2}\}$.

Case 2: Suppose $b = 0$ and $c = 1$. Then (1) again reduces to $a^2 \equiv 1 \bmod 2^{m-1}$ with solutions 1, -1, $1 + 2^{m-2}$, and $-1 + 2^{m-2}$. Thus in this case we have four involutions of the form $\phi_{a,0,1}$, where $a \in \{1, -1, 1 + 2^{m-2}, -1 + 2^{m-2}\}$.

Case 3: Suppose $b = 1$ and $c = 0$. Then (1) reduces to $a^2 + a(a-1)2^{m-3} \equiv 1 \bmod 2^{m-1}$, which is equivalent to $a^2(1 + 2^{m-3}) - a2^{m-3} - 1 \equiv 0 \bmod 2^{m-1}$. Consider $m = 4$. Then our equation becomes $3a^2 - 2a - 1 \equiv 0 \bmod 8$. It can be shown that 1 and 5 are the only solutions. Thus the only involutions of the form $\phi_{a,1,0}$ when $m = 4$ are $\phi_{1,1,0}$ and $\phi_{5,1,0}$.

Now suppose $m \geq 5$. Because $1 + 2^{m-3}$ is odd, our equation is equivalent to $(1 + 2^{m-3})[a^2(1 + 2^{m-3}) - a2^{m-3} - 1] \equiv 0 \bmod 2^{m-1}$. By using the identity

$$(1 + 2^{m-3})[a^2(1 + 2^{m-3}) - a2^{m-3} - 1] = (a(1 + 2^{m-3}) - 2^{m-4})^2 - (2^{m-4} + 1)^2,$$

our original quadratic equivalence may be expressed as

$$(a(1 + 2^{m-3}) - 2^{m-4})^2 \equiv (2^{m-4} + 1)^2 \bmod 2^{m-1}.$$

Because $(2^{m-4} + 1)^2$ is odd when $m \geq 5$, this congruence has four solutions by [Burton 2010]. It can be shown that 1, $1 + 2^{m-2}$, $-1 - 2^{m-3}$, and $-1 - 2^{m-2} - 2^{m-3}$ are the solutions for a. Thus we have four involutions of the form $\phi_{a,1,0}$, where $a \in \{1, 1 + 2^{m-2}, -1 - 2^{m-3}, -1 - 2^{m-2} - 2^{m-3}\}$.

Case 4: Suppose $b = 1$ and $c = 1$. Then finally (1) reduces to $a^2 + a(a-1)2^{m-3} + 2^{m-2} \equiv 1 \bmod 2^{m-1}$, which is equivalent to

$$a^2(1 + 2^{m-3}) - a2^{m-3} + 2^{m-2} - 1 \equiv 0 \bmod 2^{m-1}.$$

Consider $m = 4$. Then our equation becomes $3a^2 - 2a + 3 \equiv 0 \bmod 8$. It can be shown that 3 and 7 are the only solutions. Thus the only involutions of the form $\phi_{a,1,1}$ when $m = 4$ are $\phi_{3,1,1}$ and $\phi_{7,1,1}$.

Now suppose $m \geq 5$. Because $1 + 2^{m-3}$ is odd, our equation is equivalent to $(1 + 2^{m-3})[a^2(1 + 2^{m-3}) - a2^{m-3} + 2^{m-2} - 1] \equiv 0 \bmod 2^{m-1}$. Using the identity

$$(1 + 2^{m-3})[a^2(1 + 2^{m-3}) - a2^{m-3} + 2^{m-2} - 1] = (a(1 + 2^{m-3}) - 2^{m-4})^2 - (2^{m-4} - 1)^2,$$

our original quadratic equivalence may be expressed as

$$(a(1 + 2^{m-3}) - 2^{m-4})^2 \equiv (2^{m-4} - 1)^2 \bmod 2^{m-1}.$$

Because $(2^{m-4} - 1)^2$ is odd when $m \geq 5$, this congruence has four solutions by [Burton 2010]. It can be shown that -1, $-1 - 2^{m-2}$, $1 + 2^{m-3}$, and $1 + 2^{m-2} + 2^{m-3}$ are the solutions for a. Thus we have four involutions of the form $\phi_{a,1,1}$, where $a \in \{-1, -1 - 2^{m-2}, 1 + 2^{m-3}, 1 + 2^{m-2} + 2^{m-3}\}$.

Considering all cases, it follows that $\mathrm{Aut}(\mathrm{M}_m(2))$ contains 11 involutions when $m = 4$ and 15 involutions $m \geq 5$. □

Remark. Given that the number of involutions increases as m increases in the cases of dihedral groups [Cunningham et al. 2014], generalized quaternion groups [Bishop et al. 2013], and semihedral groups [Schaefer and Schlechtweg 2017], it is a bit surprising that the number of involutions of $\mathrm{M}_m(2)$ is at most 15 for all m.

Example. Consider $\mathrm{M}_4(2)$. Then by Theorem 14 the 11 involutions in $\mathrm{Aut}(\mathrm{M}_4(2))$ are $\phi_{3,0,0}$, $\phi_{5,0,0}$, $\phi_{7,0,0}$, $\phi_{1,0,1}$, $\phi_{3,0,1}$, $\phi_{5,0,1}$, $\phi_{7,0,1}$, $\phi_{1,1,0}$, $\phi_{5,1,0}$, $\phi_{3,1,1}$, and $\phi_{7,1,1}$.

As stated earlier, it is useful to know which of these involutions arise from inner automorphisms. Using the results of Theorems 11 and 14, it is clear that when $a = 1$ or $2^{m-2} + 1$, $b = 0$, and $c = 0$ or 1, equation (1) is satisfied. Thus, we have the following result that characterizes which inner automorphisms are also involutions.

Theorem 15. *All three nonidentity, inner automorphisms of* $\mathrm{M}_m(2)$ *are involutions.*

Example. Consider $\mathrm{M}_4(2)$. It follows by Theorem 15 that the involutions in $\mathrm{Aut}(\mathrm{M}_4(2))$ that arise from inner automorphisms are $\phi_{1,0,1}$, $\phi_{5,0,0}$, and $\phi_{5,0,1}$.

We complete this section by determining which elements of $\mathrm{Aut}(\mathrm{M}_m(2))$ are equivalent, for equivalent involutions produce the same generalized symmetric spaces.

Definition 16. Let G be a group and ϕ, $\sigma \in \mathrm{Aut}(G)$. Then ϕ and σ are said to be isomorphic, written $\phi \sim \sigma$, if and only if there exists $\rho \in \mathrm{Aut}(G)$ such that $\rho\phi\rho^{-1} = \sigma$, i.e., ϕ and σ are conjugate to each other. Two isomorphic automorphisms are said to be in the same equivalence class.

We begin by finding the inverse of an automorphism.

Lemma 17. *For any* $\phi_{a,b,c}, \phi_{d,e,f} \in \mathrm{M}_m(2)$, *where* a *and* d *are odd and* $b, c, e, f \in \{0, 1\}$, *we have*

$$\phi_{d,e,f} = \phi_{a,b,c}^{-1}$$

if and only if

$$d \equiv (a + ab2^{m-3})^{-1}(1 + ab2^{m-3} - bc2^{m-2}) \bmod 2^{m-1}, \quad e = b \quad \text{and} \quad f = c.$$

Proof. Consider $\phi_{a,b,c}, \phi_{d,e,f} \in \mathrm{M}_m(2)$. It follows by Lemma 12 that

$$\phi_{a,b,c} \circ \phi_{d,e,f} = \phi_{ad+ab(d-1)2^{m-3}+ce2^{m-2},\, b+e,\, c+f} = \phi_{1,0,0}$$

if and only if

$$ad + ab(d-1)2^{m-3} + ce2^{m-2} \equiv 1 \bmod 2^{m-1}, \quad b = e \quad \text{and} \quad c = f.$$

Using the fact that $b = e$, the equation

$$ad + ab(d-1)2^{m-3} + ce2^{m-2} \equiv 1 \bmod 2^{m-1}$$

is equivalent to

$$ad + ab(d-1)2^{m-3} + bc2^{m-2} \equiv 1 \bmod 2^{m-1}.$$

Solving for d, we get

$$d \equiv (a + ab2^{m-3})^{-1}(1 + ab2^{m-3} - bc2^{m-2}) \bmod 2^{m-1}. \qquad \square$$

Lemma 18. *For any $\phi_{a,b,c}, \phi_{d,e,f} \in \mathrm{M}_m(2)$, where a and d are odd and $b, c, e, f \in \{0,1\}$, we have*

$$\phi_{a,b,c} \circ \phi_{d,e,f} \circ \phi_{a,b,c}^{-1} = \phi_{\alpha,e,f},$$

where

$$\alpha \equiv (a+ab2^{m-3})^{-1}[ad+c(e-abd)2^{m-2}+(ab(2d-1)+ade(1-a))2^{m-3}] + b(c+f)2^{m-2}. \quad (2)$$

Proof. Consider $\phi_{a,b,c}, \phi_{d,e,f} \in \mathrm{M}_m(2)$. Then

$$\phi_{a,b,c} \circ \phi_{d,e,f} \circ \phi_{a,b,c}^{-1} = \phi_{ad+ab(d-1)2^{m-3}+ce2^{m-2},\, b+e,\, c+f} \circ \phi_{(a+ab2^{m-3})^{-1}(1+ab2^{m-3}-bc2^{m-2}),\, b,\, c}$$

by Lemmas 12 and 17. Utilizing Lemma 12 again, this composition becomes $\phi_{\beta\gamma+\beta(\gamma-1)(b+e)2^{m-3}+b(c+f)2^{m-2},\, 2b+e,\, 2c+f}$, where

$$\beta = ad + ab(d-1)2^{m-3} + ce2^{m-2},$$
$$\gamma = (a + ab2^{m-3})^{-1}(1 + ab2^{m-3} - bc2^{m-2}),$$

which is equivalent to $\phi_{\alpha,e,f}$, where α satisfies (2), by basic algebra and reduction modulo 2^{m-1} and $2b+e \equiv e \bmod 2$ and $2c+f \equiv f \bmod 2$ by reduction modulo 2. $\square$

Proposition 19. *Two elements $\phi_{d,e,f}, \phi_{p,q,r} \in \mathrm{Aut}(\mathrm{M}_m(2))$ are equivalent if there exists an $\phi_{a,b,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$ such that*

$$p \equiv (a+ab2^{m-3})^{-1}[ad+c(e-abd)2^{m-2}+(ab(2d-1)+ade(1-a))2^{m-3}] + b(c+f)2^{m-2} \bmod 2^{m-1}, \quad (3)$$

$q = e$, *and* $r = f$.

Proof. Let $\phi_{d,e,f}, \phi_{p,q,r} \in \mathrm{Aut}(\mathrm{M}_m(2))$, where d and p are odd and $e, f, p, q \in \{0,1\}$. These elements are conjugate if there exists an $\phi_{a,b,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$, where a is odd and $b, c \in \{0,1\}$, such that

$$\phi_{a,b,c} \circ \phi_{d,e,f} \circ \phi_{a,b,c}^{-1} = \phi_{p,q,r}.$$

Using the results of the previous theorem, this is true if and only if p satisfies (3), $q = e$, and $r = f$. □

Example. Consider $\mathrm{M}_4(2)$ and the 11 involutions in $\mathrm{Aut}(\mathrm{M}_4(2))$, namely $\phi_{3,0,0}$, $\phi_{5,0,0}$, $\phi_{7,0,0}$, $\phi_{1,0,1}$, $\phi_{3,0,1}$, $\phi_{5,0,1}$, $\phi_{7,0,1}$, $\phi_{1,1,0}$, $\phi_{5,1,0}$, $\phi_{3,1,1}$, and $\phi_{7,1,1}$. Take $\phi_{3,0,0}$. Then by Proposition 19 the only involutions $\phi_{3,0,0}$ could be equivalent to are $\phi_{3,0,0}$, $\phi_{5,0,0}$, and $\phi_{7,0,0}$. Using $d = 3$, $e = 0$, and $f = 0$, the equivalence in Proposition 19 reduces to $p \equiv (1 + 2b)^{-1}[3 + 4bc + 2b] + 4bc \bmod 8$. Since $b, c \in \{0, 1\}$, the only possible values for p are 3 and 7. Thus $\phi_{3,0,0}$ is equivalent to itself and $\phi_{7,0,0}$ but not $\phi_{5,0,0}$. We can use similar calculations to show the remaining equivalence classes of involutions in $\mathrm{Aut}(\mathrm{M}_4(2))$ are $\{\phi_{1,0,1}, \phi_{5,0,1}\}$, $\{\phi_{3,0,1}\}$, $\{\phi_{7,0,1}\}$, $\{\phi_{1,1,0}, \phi_{5,1,0}\}$, and $\{\phi_{3,1,1}, \phi_{7,1,1}\}$.

4. Fixed-point groups and symmetric spaces of $\mathrm{M}_m(2)$

Recall from the Introduction that we are interested in determining the fixed-point group H, the generalized symmetric space Q, and the extended symmetric space R for each involution of $\mathrm{M}_m(2)$ found in Theorem 14. Please note that for the remainder of this paper the notation "$\equiv$" will represent equivalence modulo 2^{m-1}.

Let $\phi_{a,b,c} \in \mathrm{Aut}(M_m(2))$ be an involution. Then we know by Theorem 8 that $b = 0$ or $b = 1$. We begin by considering the fixed-point group for an involution of the form $\phi_{a,0,c}$.

Theorem 20. *For an involution $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0, 1\}$, the fixed-point group is*

$$H_{\phi_{a,0,c}} = \{x^i y^j \mid i(a-1) + jc2^{m-2} \equiv 0\},$$

where $0 \le i < 2^{m-1}$ and $j \in \{0, 1\}$.

Proof. Let $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$ be an involution. By definition, an element $x^i y^j \in \mathrm{M}_m(2)$ is in the fixed-point group of $\phi_{a,0,c}$ if $\phi_{a,0,c}(x^i y^j) = x^i y^j$. By Theorem 10, this implies

$$\phi_{a,0,c}(x^i y^j) = x^{ai + cj2^{m-2}} y^j = x^i y^j.$$

For $x^i y^j$ to satisfy this equation, $ai + jc2^{m-2} \equiv i$ or $i(a-1) + jc2^{m-2} \equiv 0$. □

We now consider involutions of the form $\phi_{a,1,c}$.

Theorem 21. *For an involution $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0, 1\}$, the fixed-point group is*

$$H_{\phi_{a,1,c}} = \{x^i y^j \mid i(a - 1 + a2^{m-3}) + jc2^{m-2} \equiv 0 \text{ for } i \text{ even}\},$$

where $0 \le i < 2^{m-1}$ and $j \in \{0, 1\}$.

Proof. Let $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$ be an involution and let $x^i y^j \in M_m(2)$. We break this proof into two cases: i even and i odd.

Case 1: Suppose i is even. Then Theorem 10 implies

$$\phi_{a,1,c}(x^i y^j) = x^{ai+ai2^{m-3}+cj2^{m-2}} y^j = x^i y^j.$$

Thus, $x^i y^j$ is fixed when $ai + ai2^{m-3} + cj2^{m-2} \equiv i$ or $i(a - 1 + a2^{m-3}) + jc2^{m-2} \equiv 0$.

Case 2: Suppose i is odd. Then again Theorem 10 implies

$$\phi_{a,1,c}(x^i y^j) = x^{ai+a(i-1)2^{m-3}+cj2^{m-2}} y^{j+1} = x^i y^j.$$

Because $j + 1 \neq j$, elements of the form $x^i y^j$ with i odd are *never* in the fixed-point group of $\phi_{a,1,c}$. □

Example. Consider $\mathrm{M}_4(2)$ and four of its involutions: $\phi_{3,0,0}$, $\phi_{5,0,1}$, $\phi_{1,1,0}$, and $\phi_{7,1,1}$. Using the results of Theorems 20 and 21, we have

$$\begin{aligned}
H_{\phi_{3,0,0}} &= \{1, x^4, x^4y, y\},\\
H_{\phi_{5,0,1}} &= \{1, x^2, x^4, x^6, xy, x^3y, x^5y, x^7y\},\\
H_{\phi_{1,1,0}} &= \{1, x^4, x^4y, y\},\\
H_{\phi_{7,1,1}} &= \{1, x^2, x^4, x^6\}.
\end{aligned}$$

Theorem 22. *For an involution $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0, 1\}$, the generalized symmetric space is*

$$Q_{\phi_{a,0,c}} = \{x^{i(1-a)-jc2^{m-2}} \mid 0 \leq i < 2^{m-1} \text{ and } j \in \{0, 1\}\}.$$

Proof. Let $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$ be an involution and let $x^i y^j \in M_m(2)$. Using Theorem 10 and Proposition 6, we have

$$\begin{aligned}
x^i y^j (\phi_{a,0,c}(x^i y^j))^{-1} &= x^i y^j (x^{ai+cj2^{m-2}} y^j)^{-1}\\
&= x^i y^j (y^j x^{-(ai+cj2^{m-2})})\\
&= x^{i(1-a)-jc2^{m-2}}.
\end{aligned}$$

□

Recall by Proposition 7 that elements of the form x^i where i is even are in the center $Z(M_m(2))$. Since for any involution $\phi_{a,b,c}$ the value of a is odd, we have the following corollary:

Corollary 23. *For an involution $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0, 1\}$, the generalized symmetric space satisfies $Q_{\phi_{a,0,c}} \subseteq Z(M_m(2))$.*

Now we will examine the generalized symmetric spaces for involutions of the form $\phi_{a,1,c}$.

Theorem 24. *For an involution $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0,1\}$, the generalized symmetric space is*

$$Q_{\phi_{a,1,c}} = \{x^{a2^{m-3}+i(1-a-a2^{m-3}-a2^{m-2})-jc2^{m-2}} y \mid i \text{ is odd}\} \cup \{x^{i(1-a-a2^{m-3})-jc2^{m-2}} \mid i \text{ is even}\},$$

where $0 \le i < 2^{m-1}$ and $j \in \{0,1\}$.

Proof. Let $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$ and $x^i y^j \in M_m(2)$.

Case 1: Suppose i is even and $j = 0$. By Theorem 10 and Proposition 6,

$$\begin{aligned} x^i(\phi_{a,1,c}(x^i))^{-1} &= x^i(x^{ai+ai2^{m-3}})^{-1} \\ &= x^{i(1-a-a2^{m-3})}. \end{aligned}$$

Case 2: Suppose i is odd and $j = 0$. By Theorem 10, Proposition 6, and Lemma 1,

$$\begin{aligned} x^i(\phi_{a,1,c}(x^i))^{-1} &= x^i(x^{ai+a(i-1)2^{m-3}}y)^{-1} \\ &= x^i x^{(-ai-a(i-1)2^{m-3})(2^{m-2}+1)}y \\ &= x^{i-ai2^{m-2}-ai-a(i-1)2^{m-3}}y \\ &= x^{a2^{m-3}+i(1-a-a2^{m-3}-a2^{m-2})}y. \end{aligned}$$

Case 3: Suppose i is even and $j = 1$. By Theorem 10 and Proposition 6,

$$\begin{aligned} x^i y(\phi_{a,1,c}(x^i y))^{-1} &= x^i y(x^{ai+ai2^{m-3}+c2^{m-2}}y)^{-1} \\ &= x^i(y^2)x^{-ai-ai2^{m-3}-c2^{m-2}} \\ &= x^{i-ai-ai2^{m-3}-c2^{m-2}} \\ &= x^{i(1-a-a2^{m-3})-c2^{m-2}}. \end{aligned}$$

Case 4: Suppose i is odd and $j = 1$. By Theorem 10, Proposition 6, and Lemma 1,

$$\begin{aligned} x^i y(\phi_{a,1,c}(x^i y))^{-1} &= x^i y(x^{ai+a(i-1)2^{m-3}+c2^{m-2}})^{-1} \\ &= x^i(x^{(-ai-a(i-1)2^{m-3}-c2^{m-2})(2^{m-2}+1)})y \\ &= x^{i-ai2^{m-2}-ai-a(i-1)2^{m-3}-c2^{m-2}}y \\ &= x^{a2^{m-3}+i(1-a-a2^{m-3}-a2^{m-2})-c2^{m-2}}y. \end{aligned}$$

□

We now determine the extended symmetric spaces for each involution. We begin with involutions of the form $\phi_{a,0,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$.

Theorem 25. *For an involution $\phi_{a,0,c} \in \mathrm{Aut}(\mathrm{M}_m(2))$, where a is odd and $c \in \{0,1\}$, the extended symmetric space is*

$$R_{\phi_{a,0,c}} = \{x^i y^j \mid i(a + (2^{m-2}+1)^j) + jc2^{m-2} \equiv 0\},$$

where $0 \le i < 2^{m-1}$ and $j \in \{0,1\}$.

Proof. Let $\phi_{a,0,c} \in \mathrm{Aut}(M_m(2))$ and $x^i y^j \in M_m(2)$. To solve the equation $\phi_{a,0,c}(x^i y^j) = (x^i y^j)^{-1}$, we solve the equivalent equation $\phi_{a,0,c}(x^i y^j)x^i y^j = 1$.

By Theorem 10 and Lemma 1, we have

$$\begin{aligned}\phi_{a,0,c}(x^i y^j)x^i y^j &= x^{ai+cj2^{m-2}} y^j x^i y^j \\ &= x^{ai+cj2^{m-2}} x^{i(2^{m-2}+1)^j} y^{2j} \\ &= x^{ai+cj2^{m-2}+i(2^{m-2}+1)^j} = 1\end{aligned}$$

when $i(a + (2^{m-2}+1)^j) + jc2^{m-2} \equiv 0$. □

Next we turn our attention to the extended symmetric spaces of involutions of the form $\phi_{a,1,c}$. As in the fixed-point group case, we find that the extended symmetric spaces of these involutions do not contain elements of the form $x^i y^j$ for i odd.

Theorem 26. *For an involution $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$, where a is odd and $c \in \{0, 1\}$, the extended symmetric space is*

$$R_{\phi_{a,1,c}} = \{x^i y^j \mid i(a + a2^{m-3} + (2^{m-2}+1)^j) + jc2^{m-2} \equiv 0 \text{ and } i \text{ is even}\},$$

where $0 \le i < 2^{m-1}$ and $j \in \{0, 1\}$.

Proof. Let $\phi_{a,1,c} \in \mathrm{Aut}(M_m(2))$ and $x^i y^j \in M_m(2)$. We again split into two cases: i even and i odd.

Case 1: Suppose i is even. Using Theorem 10 and Lemma 1, we have

$$\begin{aligned}\phi_{a,1,c}(x^i y^j)x^i y^j &= x^{ai+ai2^{m-3}+cj2^{m-2}} y^j x^i y^j \\ &= x^{ai+ai2^{m-3}+cj2^{m-2}+i(2^{m-2}+1)^j} y^{2j} \\ &= x^{ai+ai2^{m-3}+cj2^{m-2}+i(2^{m-2}+1)^j} = 1\end{aligned}$$

when $i(a + a2^{m-3} + (2^{m-2}+1)^j) + jc2^{m-2} \equiv 0$.

Case 2: Suppose i is odd. Using Theorem 10 and Lemma 1, we have

$$\begin{aligned}\phi_{a,1,c}(x^i y^j)x^i y^j &= x^{ai+a(i-1)2^{m-3}+cj2^{m-2}} y^{j+1} x^i y^j \\ &= x^{ai+a(i-1)2^{m-3}+cj2^{m-2}+i(2^{m-2}-1)^{j+1}} y.\end{aligned}$$

An element of this form can never be equivalent to the identity. Thus, when i is odd, $x^i y^j \notin R_{\phi_{a,1,c}}$. □

Example. Consider $\mathrm{M}_4(2)$ and four of its involutions: $\phi_{3,0,0}$, $\phi_{5,0,1}$, $\phi_{1,1,0}$, and $\phi_{7,1,1}$. Using the results of Theorems 22 and 24, we have

$$\begin{aligned}Q_{\phi_{3,0,0}} &= \{1, x^2, x^4, x^6\}, \\ Q_{\phi_{5,0,1}} &= \{1, x^4\},\end{aligned}$$

$$Q_{\phi_{1,1,0}} = \{1, x^4, x^4y, y\},$$
$$Q_{\phi_{7,1,1}} = \{1, x^4, x^2y, x^6y\}.$$

In addition, we have

$$R_{\phi_{3,0,0}} = \{1, x^2, x^4, x^6, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y\},$$
$$R_{\phi_{5,0,1}} = \{1, x^4, x^2y, x^6y\},$$
$$R_{\phi_{1,1,0}} = \{1, x^2, x^4, x^6, y, x^2y, x^4y, x^6y, \},$$
$$R_{\phi_{7,1,1}} = \{1, x^4, x^2y, x^6y\}$$

by Theorems 25 and 26.

Remark. In general, $Q \subseteq R$ for all arbitrary groups and all of their respective involutions. Thus it is not a surprise that $Q_{\phi_{a,b,c}} \subseteq R_{\phi_{a,b,c}}$ in these instances. However, it is usually the case that $Q \neq R$. Thus the fact that $Q_{\phi_{7,1,1}} = R_{\phi_{7,1,1}}$ for $\mathrm{M}_4(2)$ is notable. The fixed-point group, the generalized symmetric space, and the extended symmetric space for all involutions of $\mathrm{M}_4(2)$ are provided in the Appendix.

The descriptions of H, Q, and R can be simplified when $\phi_{a,b,c}$ is an inner automorphism. Recall from Theorem 15 that an involution arising from an inner automorphism is of the form $\phi_{1,0,1}$ or $\phi_{2^{m-2}+1,0,c}$, where $c \in \{0, 1\}$.

Theorem 27. *Let $\phi_{a,0,c}$ be an involution of $\mathrm{M}_{m-1}(2)$ which arises from an inner automorphism.*

(1) *If $a = 1$ and $c = 1$, then*

$$H_{\phi_{1,0,1}} = \{1, x, x^2, \ldots, x^{2^{m-1}-1}\},$$
$$Q_{\phi_{1,0,1}} = \{1, x^{2^{m-2}}\},$$
$$R_{\phi_{1,0,1}} = \{1, x^{2^{m-2}}, x^{2^{m-3}}y, x^{3\cdot 2^{m-3}}y\}.$$

(2) *If $a = 2^{m-2} + 1$ and $c = 0$, then*

$$H_{\phi_{2^{m-2}+1,0,0}} = \{x^i y^j \mid i \text{ is even and } j \in \{0, 1\}\},$$
$$Q_{\phi_{2^{m-2}+1,0,0}} = \{1, x^{2^{m-2}}\},$$
$$R_{\phi_{2^{m-2}+1,0,0}} = \{1, x^{2^{m-2}}, y, x^{2^{m-2}}y\}.$$

(3) *If $a = 2^{m-2} + 1$ and $c = 1$, then*

$$H_{\phi_{2^{m-2}+1,0,1}} = \{x^i y^j \mid i + j \text{ is even and } j \in \{0, 1\}\},$$
$$Q_{\phi_{2^{m-2}+1,0,1}} = \{1, x^{2^{m-2}}\},$$
$$R_{\phi_{2^{m-2}+1,0,1}} = \{1, x^{2^{m-2}}, x^{2^{m-3}}y, x^{3\cdot 2^{m-3}}y\}.$$

Appendix: Fixed-point groups and symmetric spaces for involutions of $M_4(2)$

	H	Q	R
$\phi_{3,0,0}$	$\{1, x^4, y, x^4y\}$	$\{1, x^2, x^4, x^6\}$	$\{1, x^2, x^4, x^6, xy, x^2y, x^3y, x^4y, x^5y, x^6y, x^7y\}$
$\phi_{5,0,0}$	$\{1, x^2, x^4, x^6, y, x^2y, x^4y, x^6y\}$	$\{1, x^4\}$	$\{1, x^4, y, x^4y\}$
$\phi_{7,0,0}$	$\{1, x^4, y, x^4y\}$	$\{1, x^2, x^4, x^6\}$	$\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, y, x^2y, x^4y, x^6y\}$
$\phi_{1,0,1}$	$\{1, x, x^2, x^3, x^4, x^5, x^6, x^7\}$	$\{1, x^4\}$	$\{1, x^4, x^2y, x^6y\}$
$\phi_{3,0,1}$	$\{1, x^4, x^2y, x^6y\}$	$\{1, x^2, x^4, x^6\}$	$\{1, x^2, x^4, x^6\}$
$\phi_{5,0,1}$	$\{1, x^2, x^4, x^6, xy, x^3y, x^5y, x^7y\}$	$\{1, x^4\}$	$\{1, x^4, x^2y, x^6y\}$
$\phi_{7,0,1}$	$\{1, x^4, x^2y, x^6y\}$	$\{1, x^2, x^4, x^6\}$	$\{1, x, x^2, x^3, x^4, x^5, x^6, x^7, xy, x^3y, x^5y, x^7y\}$
$\phi_{1,1,0}$	$\{1, x^4, y, x^4y\}$	$\{1, x^4, y, x^4y\}$	$\{1, x^2, x^4, x^6, y, x^2y, x^4y, x^6y\}$
$\phi_{5,1,0}$	$\{1, x^4, x^4y, y\}$	$\{1, x^4, y, x^4y\}$	$\{1, x^2, x^4, x^6, y, x^2y, x^4y, x^6y\}$
$\phi_{3,1,1}$	$\{1, x^2, x^4, x^6\}$	$\{1, x^4, x^2y, x^6y\}$	$\{1, x^4, x^2y, x^6y\}$
$\phi_{7,1,1}$	$\{1, x^2, x^4, x^6\}$	$\{1, x^4, x^2y, x^6y\}$	$\{1, x^4, x^2y, x^6y\}$

Acknowledgements

This paper is based on the undergraduate honors thesis of Besson under the supervision of Schaefer. Besson would like to thank Professor Schaefer for her consistent advice, support, mentoring and mathematical guidance. He'd also like to thank Professors Hermann and Tesman for inspiring his love of algebra. Schaefer would like to thank the Research Experiences for Undergraduate Faculty (REUF) program, a joint program of the American Institute of Mathematics and the Institute for Computational and Experimental Research in Mathematics, and Aloysius G. Helminck, in particular, for introducing her to the deep and rich theory of generalized symmetric spaces.

References

[van den Ban and Schlichtkrull 1997a] E. P. van den Ban and H. Schlichtkrull, "The most continuous part of the Plancherel decomposition for a reductive symmetric space", *Ann. of Math.* (2) **145**:2 (1997), 267–364. MR Zbl

[van den Ban and Schlichtkrull 1997b] E. van den Ban and H. Schlichtkrull, "Fourier transforms on a semisimple symmetric space", *Invent. Math.* **130**:3 (1997), 517–574. MR Zbl

[Berger 1957] M. Berger, "Les espaces symétriques noncompacts", *Ann. Sci. École Norm. Sup.* (3) **74** (1957), 85–177. MR Zbl

[Bishop et al. 2013] A. Bishop, C. Cyr, J. Hutchens, C. May, N. Schwartz, and B. Turner, "On involutions and generalized symmetric spaces of dicyclic groups", preprint, 2013. arXiv

[Brylinski and Delorme 1992] J.-L. Brylinski and P. Delorme, "Vecteurs distributions H-invariants pour les séries principales généralisées d'espaces symétriques réductifs et prolongement méromorphe d'intégrales d'Eisenstein", *Invent. Math.* **109**:3 (1992), 619–664. MR Zbl

[Burton 2010] D. M. Burton, *Elementary number theory*, 7th ed., McGraw-Hill, Boston, 2010.

[Carmona and Delorme 1994] J. Carmona and P. Delorme, "Base méromorphe de vecteurs distributions H-invariants pour les séries principales généralisées d'espaces symétriques réductifs: equation fonctionnelle", *J. Funct. Anal.* **122**:1 (1994), 152–221. MR Zbl

[Cartan 1926] E. Cartan, "Sur une classe remarquable d'espaces de Riemann", *Bull. Soc. Math. France* **54** (1926), 214–264. MR Zbl

[Cartan 1927] E. Cartan, "Sur une classe remarquable d'espaces de Riemann, II", *Bull. Soc. Math. France* **55** (1927), 114–134. MR Zbl

[Cunningham et al. 2014] K. K. A. Cunningham, T. Edgar, A. G. Helminck, B. F. Jones, H. Oh, R. Schwell, and J. F. Vasquez, "On the structure of involutions and symmetric spaces of dihedral groups", *Note Mat.* **34**:2 (2014), 23–40. MR Zbl

[Delorme 1998] P. Delorme, "Formule de Plancherel pour les espaces symétriques réductifs", *Ann. of Math.* (2) **147**:2 (1998), 417–452. MR Zbl

[Gorenstein 1968] D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968. MR Zbl

[Harish-Chandra 1984a] Harish-Chandra, *Collected papers, I: 1944–1954*, edited by V. S. Varadarajan, Springer, 1984. MR Zbl

[Harish-Chandra 1984b] Harish-Chandra, *Collected papers, II: 1955–1958*, edited by V. S. Varadarajan, Springer, 1984. MR Zbl

[Harish-Chandra 1984c] Harish-Chandra, *Collected papers, III: 1959–1968*, edited by V. S. Varadarajan, Springer, 1984. MR Zbl

[Harish-Chandra 1984d] Harish-Chandra, *Collected papers, IV: 1970–1983*, edited by V. S. Varadarajan, Springer, 1984. MR Zbl

[Helminck 1994] A. G. Helminck, "Symmetric k-varieties", pp. 233–279 in *Algebraic groups and their generalizations: classical methods* (University Park, PA, 1991), edited by W. J. Haboush and B. J. Parshall, Proc. Sympos. Pure Math. **56**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Olshanetsky and Perelomov 1983] M. A. Olshanetsky and A. M. Perelomov, "Quantum integrable systems related to Lie algebras", *Phys. Rep.* **94**:6 (1983), 313–404. MR

[Ōshima and Matsuki 1984] T. Ōshima and T. Matsuki, "A description of discrete series for semisimple symmetric spaces", pp. 331–390 in *Group representations and systems of differential equations* (Tokyo, 1982), edited by K. Okamoto, Adv. Stud. Pure Math. **4**, North-Holland, Amsterdam, 1984. MR Zbl

[Schaefer and Schlechtweg 2017] J. Schaefer and K. Schlechtweg, "On the structure of symmetric spaces of semidihedral groups", *Involve* **10**:4 (2017), 665–676. MR Zbl

[Zirnbauer 1996] M. R. Zirnbauer, "Riemannian symmetric superspaces and their origin in random-matrix theory", *J. Math. Phys.* **37**:10 (1996), 4986–5018. MR Zbl

Received: 2017-07-06 Revised: 2018-08-21 Accepted: 2018-10-30

marmarc@live.unc.edu *Mathematics Department, University of North Carolina at Chapel Hill, Chapel Hill, NC, United States*

schaefje@dickinson.edu *Department of Mathematics and Computer Science, Dickinson College, Carlisle, PA, United States*

involve

msp.org/involve

INVOLVE YOUR STUDENTS IN RESEARCH

Involve showcases and encourages high-quality mathematical research involving students from all academic levels. The editorial board consists of mathematical scientists committed to nurturing student participation in research. Bridging the gap between the extremes of purely undergraduate research journals and mainstream research journals, *Involve* provides a venue to mathematicians wishing to encourage the creative involvement of students.

MANAGING EDITOR

Kenneth S. Berenhaut Wake Forest University, USA

BOARD OF EDITORS

Colin Adams	Williams College, USA	Chi-Kwong Li	College of William and Mary, USA
Arthur T. Benjamin	Harvey Mudd College, USA	Robert B. Lund	Clemson University, USA
Martin Bohner	Missouri U of Science and Technology, USA	Gaven J. Martin	Massey University, New Zealand
Nigel Boston	University of Wisconsin, USA	Mary Meyer	Colorado State University, USA
Amarjit S. Budhiraja	U of N Carolina, Chapel Hill, USA	Frank Morgan	Williams College, USA
Pietro Cerone	La Trobe University, Australia	Mohammad Sal Moslehian	Ferdowsi University of Mashhad, Iran
Scott Chapman	Sam Houston State University, USA	Zuhair Nashed	University of Central Florida, USA
Joshua N. Cooper	University of South Carolina, USA	Ken Ono	Emory University, USA
Jem N. Corcoran	University of Colorado, USA	Yuval Peres	Microsoft Research, USA
Toka Diagana	Howard University, USA	Y.-F. S. Pétermann	Université de Genève, Switzerland
Michael Dorff	Brigham Young University, USA	Jonathon Peterson	Purdue University, USA
Sever S. Dragomir	Victoria University, Australia	Robert J. Plemmons	Wake Forest University, USA
Joel Foisy	SUNY Potsdam, USA	Carl B. Pomerance	Dartmouth College, USA
Errin W. Fulp	Wake Forest University, USA	Vadim Ponomarenko	San Diego State University, USA
Joseph Gallian	University of Minnesota Duluth, USA	Bjorn Poonen	UC Berkeley, USA
Stephan R. Garcia	Pomona College, USA	Józeph H. Przytycki	George Washington University, USA
Anant Godbole	East Tennessee State University, USA	Richard Rebarber	University of Nebraska, USA
Ron Gould	Emory University, USA	Robert W. Robinson	University of Georgia, USA
Sat Gupta	U of North Carolina, Greensboro, USA	Javier Rojo	Oregon State University, USA
Jim Haglund	University of Pennsylvania, USA	Filip Saidak	U of North Carolina, Greensboro, USA
Johnny Henderson	Baylor University, USA	Hari Mohan Srivastava	University of Victoria, Canada
Glenn H. Hurlbert	Arizona State University,USA	Andrew J. Sterge	Honorary Editor
Charles R. Johnson	College of William and Mary, USA	Ann Trenk	Wellesley College, USA
K. B. Kulasekera	Clemson University, USA	Ravi Vakil	Stanford University, USA
Gerry Ladas	University of Rhode Island, USA	Antonia Vecchio	Consiglio Nazionale delle Ricerche, Italy
David Larson	Texas A&M University, USA	John C. Wierman	Johns Hopkins University, USA
Suzanne Lenhart	University of Tennessee, USA	Michael E. Zieve	University of Michigan, USA

PRODUCTION

Silvio Levy, Scientific Editor

Cover: Alex Scorpan

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2019 is US $195/year for the electronic version, and $260/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFlow® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

© 2019 Mathematical Sciences Publishers

involve

2019 vol. 12 no. 4

Euler's formula for the zeta function at the positive even integers 541
SAMYUKTA KRISHNAMURTHY AND MICAH B. MILINOVICH

Descents and des-Wilf equivalence of permutations avoiding certain nonclassical patterns 549
CADEN BIELAWA, ROBERT DAVIS, DANIEL GREESON AND QINHAN ZHOU

The classification of involutions and symmetric spaces of modular groups 565
MARC BESSON AND JENNIFER SCHAEFER

When is $a^n + 1$ the sum of two squares? 585
GREG DRESDEN, KYLIE HESS, SAIMON ISLAM, JEREMY ROUSE, AARON SCHMITT, EMILY STAMM, TERRIN WARREN AND PAN YUE

Irreducible character restrictions to maximal subgroups of low-rank classical groups of types B and C 607
KEMPTON ALBEE, MIKE BARNES, AARON PARKER, ERIC ROON AND A. A. SCHAEFFER FRY

Prime labelings of infinite graphs 633
MATTHEW KENIGSBERG AND OSCAR LEVIN

Positional strategies in games of best choice 647
AARON FOWLKES AND BRANT JONES

Graphs with at most two trees in a forest-building process 659
STEVE BUTLER, MISA HAMANAKA AND MARIE HARDT

Log-concavity of Hölder means and an application to geometric inequalities 671
AUREL I. STAN AND SERGIO D. ZAPETA-TZUL

Applying prospect theory to multiattribute problems with independence assumptions 687
JACK STANLEY AND FRANK P. A. COOLEN

On weight-one solvable configurations of the Lights Out puzzle 713
YUKI HAYATA AND MASAKAZU YAMAGISHI

1944-4176(2019)12:4;1-1