involve
a journal of mathematics

On the structure of symmetric spaces of semidihedral groups

Jennifer Schaefer and Kathryn Schlechtweg

msp

2017 vol. 10, no. 4

INVOLVE 10:4 (2017)
dx.doi.org/10.2140/involve.2017.10.665

On the structure of symmetric spaces of semidihedral groups

Jennifer Schaefer and Kathryn Schlechtweg

(Communicated by Scott T. Chapman)

We investigate the symmetric spaces associated to the family of semidihedral groups of order 2^n. We begin this study by analyzing the structure of the automorphism group and by determining which automorphims are involutions. We then determine the symmetric spaces corresponding to each involution and the orbits of the fixed-point groups on these spaces.

1. Introduction

Real symmetric spaces were first introduced by Élie Cartan [1926; 1927] as a special class of homogeneous Riemannian manifolds. They were later generalized by Berger [1957] who gave classifications of the irreducible semisimple symmetric spaces. Since then the theory of symmetric spaces, a theory that plays a key role in many areas of active research, including Lie theory, differential geometry, harmonic analysis, and physics, has developed into an extensive field. The theory of symmetric spaces also has numerous 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 many 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

MSC2010: 20D15, 53C35.

Keywords: semidihedral group, quasidihedral group, symmetric spaces, automorphisms, involutions.

$\tau(g) = g\theta(g)^{-1}$ 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. 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.

In this paper, we investigate the symmetric spaces associated to one particular family of finite groups, namely the semidihedral groups of order 2^n. Semidihedral groups, also known as quasidihedral groups, appear as Sylow-2 subgroups of certain finite simple groups (see [Alperin et al. 1970]). In Section 2, we analyze the family of semidihedral groups of order 2^n, SD_{2^n}, for $n \geqslant 4$. In Section 3, we classify the automorphisms of SD_{2^n} and determine which automorphisms are involutions. In Section 4, we describe the fixed-point group H, the generalized symmetric space Q, and the extended symmetric space R associated with each involution of SD_{2^n}. In Section 5, we study the orbit decomposition of Q by H and SD_{2^n}. Finally in the Appendix, we provide the H, Q, and R associated to each involution of SD_{16}.

The symmetric spaces associated to the more general family of semidihedral groups of order $8k$, SD_{8k}, where $k \geqslant 1$ are considered in [Raza and Imran 2014]. Their result, Lemma 6, regarding the automorphism group of SD_{8k} is incorrect and as a consequence their results about H, Q, and R associated with each involution of SD_{8k} are not completely accurate. The techniques used in our paper and based on the undergraduate honors thesis of the second author under the supervision of the first author could be utilized to consider this more general family of semidihedral groups and the associated symmetric spaces.

2. Preliminaries

Throughout this paper, we consider the semidihedral group SD_{2^n}, which can be described using the following presentation from [Gorenstein 1968]:

$$\mathrm{SD}_{2^n} = \langle r, s \mid r^{2^{n-1}} = s^2 = 1,\ sr = r^{2^{n-2}-1}s \rangle,$$

where $n \geq 4$ is an integer. This particular presentation is convenient for describing the automorphism group of SD_{2^n}.

We begin by providing some basic facts relating to the structure and properties of the elements of SD_{2^n} that will be useful. It is clear from the group presentation given above that SD_{2^n} is a non-Abelian group. The first 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 $sr^k = r^{(2^{n-2}-1)k}s$.*

Using the relation $r^{2^{n-1}} = s^2 = 1$ and the outcome of Lemma 1 repeatedly, we have the following results.

Theorem 2. *Every element of SD_{2^n} has a unique presentation as $r^i s^j$, where i and j are integers with $0 \leq i < 2^{n-1}$ and $j \in \{0, 1\}$.*

We call the presentation given in Theorem 2 the *normal form* of an element of SD_{2^n} and by writing all elements of the group in their normal form, we have the subsequent corollary.

Corollary 3. *The non-Abelian group SD_{2^n} has order 2^n and consists of the elements $1, r, r^2, \ldots, r^{(2^{n-1}-1)}, s, rs, \ldots, r^{(2^{n-1}-1)}s$.*

When determining the automorphism group and the future symmetric spaces, it will be necessary to know the order of each group element and its inverse. The next two results provide this information.

Theorem 4. *For any integer i with $0 \leq i < 2^{n-1}$, we have*

$$|r^i| = \frac{2^{n-1}}{\gcd(i, 2^{n-1})},$$

$|r^i s| = 2$ when i is even, and $|r^i s| = 4$ when i is odd.

Proof. Because $|\,\mathrm{SD}_{2^n}\,| = 2^n$, we know that the order of every element of SD_{2^n} is a power of 2. By basic properties of cyclic groups, $|r^i| = 2^{n-1}/\gcd(i, 2^{n-1})$. Consider $r^i s$ where $i = 2l$ for some $l \in \mathbb{Z}$. Then by Lemma 1 and the relation $r^{2^{n-1}} = s^2 = 1$,

$$r^i s r^i s = r^{i+i(2^{n-2}-1)} s^2 = r^{2^{n-2}(2l)} = r^{2^{n-1}(l)} = 1.$$

Consider $r^i s$ where $i = 2k + 1$ for some $k \in \mathbb{Z}$. Then

$$(r^i s)^2 = (r^i s)(r^i s) = r^{2^{n-2} i} = r^{2^{n-2}(2k+1)} = r^{2^{n-2}} \neq 1.$$

However, it follows that $(r^i s)^4 = (r^{2^{n-2}})^2 = r^{2^{n-1}} = 1$. □

Theorem 5. *For any integer i with $0 \leq i < 2^{n-1}$, we have $(r^i)^{-1} = r^{2^{n-1}-i}$. When i is even, $(r^i s)^{-1} = r^i s$ and when i is odd, $(r^i s)^{-1} = r^{i+2^{n-2}} s$.*

Proof. Using the relation $r^{2^{n-1}}=1$, it follows that $(r^i)^{-1}=r^{2^{n-1}-i}$ and by Theorem 4, we know that $(r^i s)^{-1}=r^i s$ when i is even. Consider $r^i s$ where $i=2k+1$ for some $k\in\mathbb{Z}$. Then again by Lemma 1 and the relation $r^{2^{n-1}}=s^2=1$, we have

$$\begin{aligned} r^i s r^{i+2^{n-2}} s = r^i r^{(i+2^{n-2})(2^{n-2}-1)} s^2 &= r^{(2^{n-2})i+(2^{n-2})(2^{n-2}-1)} \\ &= r^{(2^{n-2})[(2k+1)+(2^{n-2}-1)]} = r^{2^{n-1}(k+2^{n-3})} = 1. \end{aligned}$$

Thus the result follows. □

3. Automorphisms and involutions of SD_{2^n}

In this section, we investigate the automorphism group of SD_{2^n}, which we denote by $\mathrm{Aut}(\mathrm{SD}_{2^n})$. 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 determining which elements of $\mathrm{Aut}(\mathrm{SD}_{2^n})$ are involutions.

Theorem 6. *A homomorphism $\phi:\mathrm{SD}_{2^n}\to\mathrm{SD}_{2^n}$ is an automorphism if and only if $\phi(r)=r^a$ and $\phi(s)=r^b s$, where a is odd and b is even.*

Proof. Let $\phi\in\mathrm{Aut}(\mathrm{SD}_{2^n})$. Then by properties of automorphisms, r must map to an element of order 2^{n-1} and s must map to an element of order 2 under ϕ. Thus by Theorem 4, $\phi(r)=r^a$, where a is odd, and $\phi(s)=r^b s$ or $r^{2^{n-2}}$, where b is even. However, ϕ would not be onto if s mapped to $r^{2^{n-2}}$. Therefore, if ϕ is an automorphism, $\phi(r)=r^a$ and $\phi(s)=r^b s$, where a is odd and b is even. The converse of this statement can easily be shown. □

Based on the results of Theorem 6, we can represent each automorphism uniquely as ϕ_{ab} where $\phi_{ab}(r)=r^a$ and $\phi_{ab}(s)=r^b s$, where a is odd and b is even. Using this notation, we see that ϕ_{ab} maps an arbitrary element $r^i s^j$ to $r^{ai+bj}s^j$ and ϕ_{10} denotes the identity automorphism.

Corollary 7. *The automorphism group*, $\mathrm{Aut}(\mathrm{SD}_{2^n})$, *has order* 2^{2n-4}.

Proof. Since there are 2^{n-2} elements r^a where a is odd and 2^{n-2} elements $r^b s$ where b is even, $|\mathrm{Aut}(\mathrm{SD}_{2^n})|=2^{n-2}\cdot 2^{n-2}=2^{2n-4}$. □

As one of the most important examples of an automorphism of a group G is provided by conjugation by a fixed element in G, it is interesting to determine which elements of $\mathrm{Aut}(\mathrm{SD}_{2^n})$ are inner automorphisms. Given an arbitrary group G and an element $g\in G$, we will let $\psi_g\in\mathrm{Aut}(G)$ denote conjugation by g and $\mathrm{Inn}(G)$ denote the collection of inner automorphisms of G.

Theorem 8. *The inner automorphisms of* SD_{2^n} *are ϕ_{1b} and $\phi_{(2^{n-2}-1)b}$ where $b\in\mathbb{Z}_{2^{n-1}}$ is even.*

Proof. Consider ψ_g for some $g \in \mathrm{SD}_{2^n}$. Suppose $g = r^i$. Then

$$\psi_{r^i}(r) = r^i r r^{2^{n-1}-i} = r^{2^{n-1}+1} = r,$$
$$\psi_{r^i}(s) = r^i s r^{2^{n-1}-i} = r^i r^{(2^{n-2}-1)(2^{n-1}-i)} s = r^{2i-2^{n-2}i} s = r^{2(i-2^{n-3}i)} s.$$

Next, consider $g = r^i s$ where $i \in \mathbb{Z}_{2^{n-1}}$ is even. Then

$$\psi_{r^i s}(r) = r^i s r r^i s = r^i r^{(1+i)(2^{n-2}-1)} s^2 = r^{2^{n-2}-1}$$

and $\psi_{r^i s}(s) = r^i s s r^i s = r^{2i} s$. Finally, consider the case when $g = r^i s$ where $i \in \mathbb{Z}_{2^{n-1}}$ is odd. Then

$$\psi_{r^i s}(r) = (r^i s) r (r^{i+2^{n-2}} s) = r^i r^{(2^{n-2}-1)(1+i+2^{n-2})} s^2 = r^{2^{n-2}-1},$$
$$\psi_{r^i s}(s) = r^i s s r^{i+2^{n-2}} s = r^{2i+2^{n-2}} s = r^{2(i+2^{n-3})} s.$$

Conversely, consider $\phi_{1b} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. Note that conjugation by $r^{(b/2)(1-2^{n-3})^{-1}}$ gives

$$r^{(b/2)(1-2^{n-3})^{-1}} r r^{-(b/2)(1-2^{n-3})^{-1}} = r$$

and

$$r^{(b/2)(1-2^{n-3})^{-1}} s r^{-(b/2)(1-2^{n-3})^{-1}} = r^b s.$$

Thus, $\phi_{1b} \in \mathrm{Inn}(\mathrm{SD}_{2^n})$. Similarly, consider $\phi_{(2^{n-2}-1)b} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. If $b/2$ is even, then conjugation by $r^{b/2}s$ gives

$$r^{b/2} s r r^{b/2} s = r^{2^{n-2}-1}$$

and

$$r^{b/2} s s r^{b/2} s = r^b s.$$

If $b/2$ is odd, then conjugation by $r^{b/2-2^{n-3}} s$ gives

$$r^{b/2-2^{n-3}} s r r^{b/2-2^{n-3}+2^{n-2}} s = r^{2^{n-2}-1}$$

and

$$r^{b/2-2^{n-3}} s s r^{b/2-2^{n-3}+2^{n-2}} s = r^b s.$$

Thus, $\phi_{(2^{n-2}-1)b} \in \mathrm{Inn}(\mathrm{SD}_{2^n})$. Therefore, ϕ_{ab} is an inner automorphism of SD_{2^n} if and only if a is 1 or $2^{n-2}-1$ and $b \in \mathbb{Z}_{2^{n-1}}$ is even. $\square$

It follows from this result that 2^{n-1} of the 2^{2n-4} automorphisms in $\mathrm{Aut}(\mathrm{SD}_{2^n})$ are inner automorphisms, which one knew would be the case as $\mathrm{Inn}(\mathrm{SD}_{2^n}) \cong \mathrm{SD}_{2^n}/Z(\mathrm{SD}_{2^n})$ and $|Z(\mathrm{SD}_{2^n})| = 2$ (see [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 characterize the automorphisms of finite order, and in particular the involutions, we provide the following lemma.

Lemma 9. *For any* $\phi_{ab}, \phi_{cd} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$, *we have*

$$\phi_{ab} \circ \phi_{cd} = \phi_{[ac \bmod 2^{n-1}][ad+b \bmod 2^{n-1}]}.$$

Proof. Let $r^i s^j \in \mathrm{SD}_{2^n}$, where $i, j \in \mathbb{Z}$ such that $0 \leq i \leq 2^{n-1} - 1$ and $0 \leq j \leq 1$. Then

$$\begin{aligned} \phi_{ab} \circ \phi_{cd}(r^i s^j) = \phi_{ab}(r^{ci+dj} s^j) = r^{a(ci+dj)+bj} s^j = r^{(ac)i+(ad+b)j} s^j \\ = \phi_{[ac \bmod 2^{n-1}][ad+b \bmod 2^{n-1}]}(r^i s^j). \end{aligned}$$ □

This result concerning composition of automorphisms of SD_{2^n} is quite useful. It allows to us to answer our question regarding automorphisms of finite order via a straightforward modulo 2^{n-1} calculation.

Theorem 10. *Let* $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. *Then* $(\phi_{ab})^d = \phi_{10}$ *if and only if* $a^d \equiv 1 \bmod 2^{n-1}$ *and* $b(1 + a + a^2 + \cdots + a^{d-1}) \equiv 0 \bmod 2^{n-1}$.

Proof. Consider $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. By repeated use of Lemma 9, we find that $(\phi_{ab})^d(r) = r^{a^d}$ and $(\phi_{ab})^d(s) = r^{b(1+a+a^2+\cdots+a^{d-1})}s$. Since $r^{a^d} = r$ when $a^d \equiv 1 \bmod (2^{n-1})$ and $r^{b(1+a+a^2+\cdots+a^{d-1})}s = s$ when $b(1 + a + a^2 + \cdots + a^{d-1}) \equiv 0 \bmod 2^{n-1}$, the result follows. □

We are now able to determine which automorphisms of SD_{2^n} are involutions and the number of involutions in $\mathrm{Aut}(\mathrm{SD}_{2^n})$ for any n.

Corollary 11. *Let* $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. *Then* $(\phi_{ab})^2 = \phi_{10}$ *if and only if* $a^2 \equiv 1 \bmod 2^{n-1}$ *and* $b(1 + a) \equiv 0 \bmod 2^{n-1}$.

Corollary 12. *For integers* $n \geqslant 4$, $\mathrm{Aut}(\mathrm{SD}_{2^n})$ *contains* $2^{n-1} + 3$ *involutions.*

Proof. By Corollary 11, for any odd integer a in $\mathbb{Z}_{2^{n-1}}$ such that $a^2 \equiv 1 \bmod 2^{n-1}$, we have $\gcd(a+1, 2^{n-1})$ even elements b in $\mathbb{Z}_{2^{n-1}}$ such that $b(1+a) \equiv 0 \bmod 2^{n-1}$. There are four elements a in $\mathbb{Z}_{2^{n-1}}$ with $a^2 \equiv 1 \bmod 2^{n-1}$ by [Burton 2011], namely $1, -1, 1 + 2^{n-2}$, and $-1 + 2^{n-2}$. Thus we have $2 + 2^{n-2} + 2 + 2^{n-2} = 2^{n-1} + 4$ elements $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$ with $(\phi_{ab})^2 = \phi_{10}$. Because ϕ_{10} has order 1, it follows that there are $2^{n-1} + 3$ involutions in $\mathrm{Aut}(\mathrm{SD}_{2^n})$. □

Example. Consider SD_{16}. Then by Corollary 12 there are 11 involutions in $\mathrm{Aut}(\mathrm{SD}_{16})$, namely $\phi_{14}, \phi_{30}, \phi_{32}, \phi_{34}, \phi_{36}, \phi_{50}, \phi_{54}, \phi_{70}, \phi_{72}, \phi_{74}, \phi_{76}$.

As stated earlier, it is useful to know which of these involutions arise from inner automorphisms. Using Theorem 8 and Corollary 11, it is clear that when $a = 1$, b must have order 2^{n-2} to satisfy the equation $b(1 + a) \equiv 0 \bmod 2^{n-1}$. However, in the case that $a = 2^{n-2} - 1$, it is not as restrictive, for the equation $b(1 + a) =$

$b(2^{n-2}) \equiv 0 \mod 2^{n-1}$ is satisfied by any even in $\mathbb{Z}_{2^{n-1}}$. Thus, we have the following result that characterizes which inner automorphisms are also involutions.

Theorem 13. *The involutions of* SD_{2^n} *which arise from inner automorphisms are* $\phi_{12^{n-2}}$ *and* $\phi_{(2^{n-2}-1)b}$, *where* $b \in \mathbb{Z}_{2^{n-1}}$ *is even.*

Example. Consider SD_{16}. It follows from Theorem 13 that the involutions in $\mathrm{Aut}(\mathrm{SD}_{16})$ that arise from inner automorphisms are ϕ_{14}, ϕ_{30}, ϕ_{32}, ϕ_{34}, and ϕ_{36}.

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

Definition 14. Let G be a group and $\phi, \sigma \in \mathrm{Aut}(G)$. 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.

Theorem 15. *For any* $\phi_{ab}, \phi_{cd} \in \mathrm{SD}_{2^n}$, *we have* $\phi_{ab}^{-1} = \phi_{cd}$ *if and only if* $c = a^{-1}$ *and* $d \equiv a^{-1}(-b) \mod 2^{n-1}$.

Proof. Consider $\phi_{ab}, \phi_{cd} \in \mathrm{SD}_{2^n}$. It follows by Lemma 9 that

$$\phi_{ab} \circ \phi_{cd} = \phi_{[ac \bmod 2^{n-1}][(ad+b) \bmod 2^{n-1}]} = \phi_{10}$$

if and only if $ac \equiv 1 \mod 2^{n-1}$ and $ad + b \equiv 0 \mod 2^{n-1}$. Now c must equal a^{-1} to satisfy $ac \equiv 1 \mod 2^{n-1}$. Next, $ad + b \equiv 0 \mod 2^{n-1}$ becomes $ad \equiv -b \mod 2^{n-1}$. Then, by multiplying both sides by a^{-1}, we get $d \equiv a^{-1}(-b) \mod 2^{n-1}$. □

Theorem 16. *For any* $\phi_{ab}, \phi_{cd} \in \mathrm{SD}_{2^n}$, *we have*

$$\phi_{ab} \circ \phi_{cd} \circ \phi_{ab}^{-1} = \phi_{[c \bmod 2^{n-1}][(-bc+ad+b) \bmod 2^{n-1}]}.$$

Proof. Consider $\phi_{ab}, \phi_{cd} \in \mathrm{SD}_{2^n}$. Then

$$\begin{aligned}\phi_{ab} \circ \phi_{cd} \circ \phi_{ab}^{-1} &= \phi_{ab} \circ \phi_{cd} \circ \phi_{[a^{-1}][a^{-1}(-b) \bmod 2^{n-1}]} \\ &= \phi_{ab} \circ \phi_{[a^{-1}c \bmod 2^{n-1}][(c(a^{-1}(-b))+d) \bmod 2^{n-1}]} \\ &= \phi_{[aa^{-1}c \bmod 2^{n-1}][(a(-ca^{-1}b+d)+b) \bmod 2^{n-1}]} \\ &= \phi_{[c \bmod 2^{n-1}][(-bc+ad+b) \bmod 2^{n-1}]}.\end{aligned}$$

□

Theorem 17. *Two elements* $\phi_{ab}, \phi_{cd} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$ *are equivalent if there exists an* $\phi_{ef} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$ *such that* $a = c$ *and* $d \equiv (f(1-a) + be) \mod 2^{n-1}$.

Proof. Let $\phi_{ab}, \phi_{cd} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. These elements are conjugate if there exists an $\phi_{ef} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$ such that $\phi_{ef} \circ \phi_{ab} \circ \phi_{ef}^{-1} = \phi_{cd}$. Thus, using the results of the previous theorem, $\phi_{cd} = \phi_{[a \bmod 2^{n-1}][-af+be+f \bmod 2^{n-1}]}$. This is true if and only if $a = c$ and $d \equiv (f(1-a) + be) \mod 2^{n-1}$. □

Example. Consider SD_{16} and the 11 involutions in $\mathrm{Aut}(\mathrm{SD}_{16})$, namely ϕ_{14}, ϕ_{30}, ϕ_{32}, ϕ_{34}, ϕ_{36}, ϕ_{50}, ϕ_{54}, ϕ_{70}, ϕ_{72}, ϕ_{74}, ϕ_{76}. Then by the previous theorem, the equivalence classes of involutions in $\mathrm{Aut}(\mathrm{SD}_{16})$ are $\{\phi_{14}\}$, $\{\phi_{30}, \phi_{32}, \phi_{34}, \phi_{36}\}$, $\{\phi_{50}, \phi_{54}\}$, and $\{\phi_{70}, \phi_{72}, \phi_{74}, \phi_{76}\}$.

4. Fixed-point groups and symmetric spaces of SD_{2^n}

Recall again 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 SD_{2^n} found in Corollary 11. It is important to note that for the remainder of this paper we will let $a \equiv b$ represent $a \equiv b \bmod 2^{n-1}$.

Theorem 18. *For an involution $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$, the fixed-point group is*

$$H_{\phi_{ab}} = \{r^i s^j \in \mathrm{SD}_{2^n} \mid i(a-1) + jb \equiv 0\},$$

where $i \in \mathbb{Z}_{2^{n-1}}$ and $j \in \mathbb{Z}_2$.

Proof. Let $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$. Then $H_{\phi_{ab}} = \{r^i s^j \in \mathrm{SD}_{2^n} \mid \phi_{ab}(r^i s^j) = r^i s^j\}$, where $i \in \mathbb{Z}_{2^{n-1}}$ and $j \in \mathbb{Z}_2$.

Case 1. Let $j = 0$. Then $\phi_{ab}(r^i) = r^{ai} = r^i$ if and only if $ia \equiv i$ or $i(a-1) \equiv 0$.

Case 2. Let $j = 1$. Then $\phi_{ab}(r^i s) = r^{ai+b} s = r^i s$ if and only if $ai + b \equiv i$ or $i(a-1) + b \equiv 0$. $\square$

Example. Consider SD_{16} and four of its involutions: ϕ_{14}, ϕ_{36}, ϕ_{54}, and ϕ_{70}. Using the results of Theorem 18, we have $H_{\phi_{14}} = \{1, r, \dots, r^7\}$, $H_{\phi_{36}} = \{1, r^4, rs, r^5 s\}$, $H_{\phi_{54}} = \{1, r^2, r^4, r^6, rs, r^3 s, r^5 s, r^7 s\}$, and $H_{\phi_{70}} = \{1, r^4, s, r^4 s\}$.

Theorem 19. *For an involution $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$, the generalized symmetric space is*

$$Q_{\phi_{ab}} = \{r^{i(1-a)-jb} \mid i \in \mathbb{Z}_{2^{n-1}} \text{ and } j \in \mathbb{Z}_2\}.$$

Proof. Let ϕ_{ab} be an involution of SD_{2^n}. Then $Q_{\phi_{ab}} = \{(r^i s)\phi_{ab}(r^i s)^{-1} \mid r^i s^j \in \mathrm{SD}_{2^n}\}$, where $i \in \mathbb{Z}_{2^{n-1}}$ and $j \in \mathbb{Z}_2$.

Case 1. Let $j = 0$. Then $(r^i)\phi_{ab}(r^i)^{-1} = r^i (r^{ai})^{-1} = r^i r^{2^{n-1}-ai} = r^{i(1-a)}$.

Case 2. Let $j = 1$. Then $(r^i s)\phi_{ab}(r^i s)^{-1} = (r^i s)(r^{ai+b} s)^{-1}$. Notice that $ai + b$ can be even or odd depending on the value of i since a is odd and b is even.

(i) Suppose i is even. It follows that $ai + b$ is even. Then

$$(r^i s)(r^{ai+b} s)^{-1} = r^i s r^{ai+b} s = r^i r^{(2^{n-2}-1)(ai+b)} s^2 = r^{i-(ai+b)} = r^{i(1-a)-b}.$$

(ii) Suppose i is odd. It follows that $ai + b$ is odd. Then

$$\begin{aligned}(r^i s)(r^{ai+b} s)^{-1} &= (r^i s)(r^{(ai+b)+2^{n-2}} s) \\ &= r^i r^{(2^{n-2}-1)((ai+b)+2^{n-2})} s^2 = r^{i-ai-b+(ai-1)2^{n-2}} = r^{i(1-a)-b}\end{aligned}$$

since $ai - 1$ is even. $\square$

Theorem 20. *For an involution $\phi_{ab} \in \mathrm{Aut}(\mathrm{SD}_{2^n})$, the extended symmetric space is*

$$\begin{aligned} R_{\phi_{ab}} = \{r^i \in \mathrm{SD}_{2^n} \mid i(a+1) \equiv 0\} \\ \cup \{r^i s \in \mathrm{SD}_{2^n} \mid i(a-1)+b \equiv 0 \bmod 2^{n-1} \textit{ and } i \textit{ is even}\} \\ \cup \{r^i s \in \mathrm{SD}_{2^n} \mid i(a-1)+b \equiv 2^{n-2} \bmod 2^{n-1} \textit{ and } i \textit{ is odd}\}. \end{aligned}$$

Proof. Let ϕ_{ab} be an involution of SD_{2^n}. Then

$$R_{\phi_{ab}} = \{r^i s^j \in \mathrm{SD}_{2^n} \mid \phi_{ab}(r^i s^j) = (r^i s^j)^{-1}\}.$$

Case 1. Let $j=0$. Then $\phi_{ab}(r^i) = r^{ai} = r^{-i} = r^{2^{n-1}-i}$ if and only if $ai \equiv 2^{n-1}-i$. In other words, $i(a+1) \equiv 0$.

Case 2. Let $j=1$ and i be even. Then $\phi_{ab}(r^i s) = r^{ai+b}s = (r^i s)^{-1} = r^i s$ if and only if $ai+b \equiv i$. In other words, $i(a-1)+b \equiv 0$.

Case 3. Let $j=1$ and i be odd. Then $\phi_{ab}(r^i s) = r^{ai+b}s = (r^i s)^{-1} = r^{i+2^{n-2}}s$ if and only if $ai+b \equiv i+2^{n-2}$. In other words, $i(a-1)+b \equiv 2^{n-2}$. □

Example. Consider SD_{16} and four of its involutions: ϕ_{14}, ϕ_{36}, ϕ_{54}, and ϕ_{70}. Using the results of Theorem 19, we have that $Q_{\phi_{14}} = \{1, r^4\}$, $Q_{\phi_{36}} = \{1, r^2, r^4, r^6\}$, $Q_{\phi_{54}} = \{1, r^4\}$, and $Q_{\phi_{70}} = \{1, r^2, r^4, r^6\}$. However, by Theorem 20, we have that $R_{\phi_{14}} = \{1, r^4, rs, r^3s, r^5s, r^7s\}$, $R_{\phi_{36}} = \{1, r^2, r^4, r^6, r^3s, r^7s\}$, $R_{\phi_{54}} = \{1, r^4\}$, and $R_{\phi_{70}} = \{1, r, \ldots, r^7, s, r^4s\}$. We see that $Q_{ab} \subseteq R_{ab}$ in all instances, which should be, as $Q \subseteq R$ for all arbitrary groups and all of their respective involutions. However, it is usually the case that $Q \neq R$. Thus the fact that $Q_{\phi_{54}} = R_{\phi_{54}}$ for SD_{16} is noteworthy. We provide the fixed-point group, the generalized symmetric space, and the extended symmetric space for each involution of SD_{16} in the Appendix.

The descriptions of H, Q, and R are more specific when ϕ_{ab} is an inner automorphism. Recall that from Theorem 13, an involution arising from an inner automorphism is of the form $\phi_{12^{n-2}}$ or $\phi_{(2^{n-2}-1)b}$, where $b \in \mathbb{Z}_{2^{n-1}}$ is even.

Theorem 21. *Let ϕ_{ab} be an involution of $\mathrm{SD}_{2^{n-1}}$ which arises from an inner automorphism.*

(1) *If $a=1$ and $b=2^{n-2}$, then $H_{\phi_{ab}} = \{1, r, r^2, \ldots, r^{2^{n-2}}\}$, $Q_{\phi_{ab}} = \{1, r^{2^{n-2}}\}$, and $R_{\phi_{ab}} = \{1, r^{2^{n-2}}, rs, r^3s, \ldots, r^{2^{n-1}-1}s\}$.*

(2) *If $a = 2^{n-2}-1$ and b is even, then $H_{\phi_{ab}} = \{1, r^{2^{n-2}}\} \cup \{r^i s \mid i(2^{n-2}-2)+b \equiv 0\}$, $Q_{\phi_{ab}} = \{1, r^2, r^4, \ldots, r^{2^{n-1}-2}\}$, and*

$$\begin{aligned} R_{\phi_{ab}} = \{r^i \in \mathrm{SD}_{2^n} \mid i \textit{ is even}\} \\ \cup \{r^i s \in \mathrm{SD}_{2^n} \mid i(2^{n-2}-2)+b \equiv 0 \bmod 2^{n-1} \textit{ and } i \textit{ is even}\} \\ \cup \{r^i s \in \mathrm{SD}_{2^n} \mid i(2^{n-2}-2)+b \equiv 2^{n-2} \bmod 2^{n-1} \textit{ and } i \textit{ is odd}\}. \end{aligned}$$

5. Orbits

By Theorem 18, we can view $H_{\phi_{ab}}$ as the disjoint union of $\{r^i \in \mathrm{SD}_{2^n} \mid i(a-1) \equiv 0\}$ and $\{r^i s \in \mathrm{SD}_{2^n} \mid i(a-1)+b \equiv 0\}$. The first set will contain at least the identity and $r^{2^{n-2}}$. However, the second set may be empty if there is no solution, i, to the equation $i(a-1)+b \equiv 0$ for fixed a and b. The question of the existence of such a solution produces two possible outcomes for the $H_{\phi_{ab}}$-orbits on $Q_{\phi_{ab}}$.

Theorem 22. *Let ϕ_{ab} be an involution of* SD_{2^n}.

(1) *If there is no solution, i, to the equation $i(a-1)+b \equiv 0$ for fixed a and b, then the $H_{\phi_{ab}}$-orbits on $Q_{\phi_{ab}}$ are*

$$H_{\phi_{ab}} \backslash Q_{\phi_{ab}} = \bigl\{\{r^k\} \bigm| k = i(1-a) - jb \text{ where } i \in \mathbb{Z}_{2^{n-1}} \text{ and } j \in \mathbb{Z}_2\bigr\}.$$

(2) *If there is a solution, i, to the equation $i(a-1)+b \equiv 0$ for fixed a and b, then the $H_{\phi_{ab}}$-orbits on $Q_{\phi_{ab}}$ are*

$$H_{\phi_{ab}} \backslash Q_{\phi_{ab}} = \bigl\{\{r^k, r^{-k}\} \bigm| k = i(1-a) - jb \text{ where } i \in \mathbb{Z}_{2^{n-1}} \text{ and } j \in \mathbb{Z}_2\bigr\}.$$

Proof. In general, a group G acts on its extended symmetric space R, and thus its generalized symmetric space Q, via θ-twisted conjugation defined as $g.r = gr\theta(g)^{-1}$ for $g \in G$ and $r \in R$, where θ is an involution of G. Given that $H_{\phi_{ab}}$ is the fixed-point group of ϕ_{ab}, the action of $H_{\phi_{ab}}$ on $Q_{\phi_{ab}}$ reduces to conjugation. In addition, we found in Theorem 19 that $Q_{\phi_{ab}} \subset \langle r^2 \rangle \subset \mathrm{SD}_{2^n}$. Thus to determine the orbits of $H_{\phi_{ab}}$ on $Q_{\phi_{ab}}$, it is sufficient to evaluate the action of $H_{\phi_{ab}}$ on a general element r^k, keeping in mind that k is even. Let $r^i \in H_{\phi_{ab}}$ such that $i(a-1) \equiv 0$. Then $r^i r^k (r^i)^{-1} = r^k$ and it follows that elements of the form $r^i \in H_{\phi_{ab}}$ fix $Q_{\phi_{ab}}$ pointwise. Now suppose $r^i s \in H_{\phi_{ab}}$ such that $i(a-1)+b \equiv 0$. Consider the case when i is even. Then

$$\begin{aligned}(r^i s)(r^k)(r^i s)^{-1} &= (r^i s)(r^k)(r^i s)\\ &= (r^i s)(r^{k+i} s) = r^i r^{(2^{n-2}-1)(k+i)} s^2 = r^{(2^{n-2}-1)k} = r^{-k}\end{aligned}$$

since k is even. Finally, suppose i is odd. Then

$$\begin{aligned}(r^i s)(r^k)(r^i s)^{-1} &= (r^i s)(r^k)(r^{i+2^{n-2}} s)\\ &= (r^i s)(r^{k+i+2^{n-2}} s) = r^i r^{(2^{n-2}-1)(k+i+2^{n-2})} s^2 = r^{2^{n-2}(i-1)-k} = r^{-k}\end{aligned}$$

since k and $i-1$ are both even. □

Theorem 23. *Let ϕ_{ab} be an involution of* SD_{2^n}. *There is one* SD_{2^n}*-orbit on $Q_{\phi_{ab}}$, i.e.,* $\mathrm{SD}_{2^n} \backslash Q_{\phi_{ab}} = \{Q_{\phi_{ab}}\}$.

Proof. We proceed by proving that every element of SD_{2^n} is in the SD_{2^n}-orbit of the identity, 1, in $Q_{\phi_{ab}}$. By Theorem 19, every element of $Q_{\phi_{ab}}$ can be written in the form $r^{i(1-a)}$ or $r^{i(1-a)-b}$ for some $i \in \mathbb{Z}_{2^{n-1}}$. We know $r^i \in \mathrm{SD}_{2^n}$ for $i \in \mathbb{Z}_{2^{n-1}}$

and $r^i.1 = r^i\phi_{ab}(r^i)^{-1} = r^i(r^{ai})^{-1} = r^i r^{-ai} = r^{i(1-a)}$. We also know $r^i s \in \mathrm{SD}_{2^n}$ for $i \in \mathbb{Z}_{2^{n-1}}$. In the case that i is even,

$$\begin{aligned} r^i s\,.\,1 &= r^i s\phi_{ab}(r^i s)^{-1} \\ &= r^i s(r^{ai+b}s)^{-1} = r^i s(r^{ai+b}s) = r^i r^{(2^{n-2}-1)(ai+b)}s^2 = r^{i(1-a)-b} \end{aligned}$$

by $ai+b$ even. Likewise when i is odd,

$$\begin{aligned} r^i s\,.\,1 &= r^i s\phi_{ab}(r^i s)^{-1} \\ &= r^i s(r^{ai+b}s)^{-1} = r^i s(r^{ai+b+2^{n-2}}s) = r^i r^{(2^{n-2}-1)(ai+b+2^{n-2})}s^2 = r^{i(1-a)-b} \end{aligned}$$

since $ai-1$ is even. □

Example. Again, consider the involutions ϕ_{14}, ϕ_{36}, ϕ_{54}, and ϕ_{70} of SD_{16} and their respective fixed-point groups and generalized symmetric spaces from Section 4. By applying Theorem 22, we find that because $i(0)+4 \equiv 0$ has no solution for i and $Q = \{1, r^4\}$,

$$H_{\phi_{14}}\backslash Q_{\phi_{14}} = \big\{\{1\}, \{r^4\}\big\} \quad \text{for } \phi_{14};$$

because $i(2)+6 \equiv 0$ has $i = 1$ as a solution and $Q = \{1, r^2, r^4, r^6\}$,

$$H_{\phi_{36}}\backslash Q_{\phi_{36}} = \big\{\{1\}, \{r^4\}, \{r^2, r^6\}\big\} \quad \text{for } \phi_{36};$$

because $i(4)+4 \equiv 0$ has $i = 1$ as a solution and $Q = \{1, r^4\}$,

$$H_{\phi_{54}}\backslash Q_{\phi_{54}} = \big\{\{1\}, \{r^4\}\big\} \quad \text{for } \phi_{54};$$

because $i(6)+0 \equiv 0$ has $i = 4$ as a solution and $Q = \{1, r^2, r^4, r^6\}$,

$$H_{\phi_{70}}\backslash Q_{\phi_{70}} = \big\{\{1\}, \{r^4\}, \{r^2, r^6\}\big\} \quad \text{for } \phi_{70}.$$

Appendix: Symmetric spaces and fixed-point groups for SD_{16}

involution	H	Q	R
ϕ_{14}	$\{1, r, \ldots, r^7\}$	$\{1, r^4\}$	$\{1, r^4, rs, r^3s, r^5s, r^7s\}$
ϕ_{30}	$\{1, r^4, s, r^4s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r^2, r^4, r^6, s, r^4s\}$
ϕ_{32}	$\{1, r^4, r^3s, r^7s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r^2, r^4, r^6, rs, r^5s\}$
ϕ_{34}	$\{1, r^4, r^2s, r^6s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r^2, r^4, r^6, r^2s, r^6s\}$
ϕ_{36}	$\{1, r^4, rs, r^5s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r^2, r^4, r^6, r^3s, r^7s\}$
ϕ_{50}	$\{1, r^2, r^4, r^6, s, r^2s, r^4s, r^6s\}$	$\{1, r^4\}$	$\{1, r^4, s, rs, \ldots, r^7s\}$
ϕ_{54}	$\{1, r^2, r^4, r^6, rs, r^3s, r^5s, r^7s\}$	$\{1, r^4\}$	$\{1, r^4\}$
ϕ_{70}	$\{1, r^4, s, r^4s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r, \ldots, r^7, s, r^4s\}$
ϕ_{72}	$\{1, r^4, rs, r^5s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r, \ldots, r^7, r^3s, r^7s\}$
ϕ_{74}	$\{1, r^4, r^2s, r^6s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r, \ldots, r^7, r^2s, r^6s\}$
ϕ_{76}	$\{1, r^4, r^3s, r^7s\}$	$\{1, r^2, r^4, r^6\}$	$\{1, r, \ldots, r^7, rs, r^5s\}$

Acknowledgements

This paper is based on the undergraduate honors thesis of Schlechtweg, which Schaefer supervised. 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

[Alperin et al. 1970] J. L. Alperin, R. Brauer, and D. Gorenstein, "Finite groups with quasi-dihedral and wreathed Sylow 2-subgroups", *Trans. Amer. Math. Soc.* **151** (1970), 1–261. MR Zbl

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

[Burton 2011] D. M. Burton, *Elementary number theory*, 7th ed., McGraw-Hill, Boston, 2011.

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

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

[Gorenstein 1968] D. Gorenstein, *Finite groups*, Harper & Row, New York, 1968. 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**, Part 1, American Mathematical Society, Providence, RI, 1994. MR Zbl

[Raza and Imran 2014] Z. Raza and Imran, "On the structure of involutions and symmetric spaces of quasi dihedral group", preprint, 2014. arXiv

Received: 2016-02-03 Revised: 2016-04-20 Accepted: 2016-05-12

schaefje@dickinson.edu Department of Mathematics and Computer Science, Dickinson College, Carlisle, PA 17013, United States

kms2278@cumc.columbia.edu Columbia University, New York, NY 10027, 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.

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2017 is US $175/year for the electronic version, and $235/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers 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/

involve

2017 vol. 10 no. 4