

AUTOMORPHISM GROUPS OF ROOT SYSTEMS MATROIDS

MATHIEU DUTOUR SIKIRIĆ, ANNA FELIKSON, AND PAVEL TUMARKIN

ABSTRACT. Given a root system R , the vector system \tilde{R} is obtained by taking a representative v in each antipodal pair $\{v, -v\}$. The matroid $M(R)$ is formed by all independent subsets of \tilde{R} . The automorphism group of a matroid is the group of permutations preserving its independent subsets. We prove that the automorphism groups of all irreducible root systems matroids $M(R)$ are uniquely determined by their independent sets of size 3. As a corollary, we compute these groups explicitly, and thus complete the classification of the automorphism groups of root systems matroids.

1. INTRODUCTION

Given a vector $v \in \mathbb{R}^n$, denote by H_v the hyperplane of vectors orthogonal to v and by s_v the orthogonal reflection along H_v . A *root system* R is a finite family of vectors $v \in \mathbb{R}^n$, such that:

- $R \cap \mathbb{R}v = \{v, -v\}$ for all $v \in R$,
- $s_v R = R$ for all $v \in R$.

The norms of the roots are not specified a priori in our definition. If R splits into r orbits under the action of $W(R)$, then r norms, a priori different, are possible. A root system R is *irreducible* if R cannot be decomposed into two orthogonal components.

The groups $W(R)$ generated by the reflections $(s_v)_{v \in R}$ are exactly finite Coxeter groups. We call a finite Coxeter group *indecomposable* if the corresponding root system is irreducible. Finite indecomposable Coxeter groups are classified into the following ones: A_n , B_n , D_n , E_6 , E_7 , E_8 , F_4 , $I_2(m)$, H_3 and H_4 (see e.g. [7, Chapter 2]).

Given a finite set X , a *matroid* M is a family \mathcal{I} of subsets S of X (called *independent sets*) such that:

- $\mathcal{I} \neq \emptyset$
- for any $S \in \mathcal{I}$, any $S' \subset S$ one has $S' \in \mathcal{I}$.

Research supported by the Croatian Ministry of Science, Education and Sport under contract 098-0982705-2707 (M.D.), RFBR grant 07-01-00390-a (A.F. and P.T.), and INTAS grants YSF-06-10000014-5916 (A.F.) and YSF-06-10000014-5766 (P.T.).

- If $A, B \in \mathcal{I}$, $|A| > |B|$ then $\exists x \in A \setminus B$ such that $B \cup \{x\} \in \mathcal{I}$.

One way to get a matroid is to take X to be a family of vectors and \mathcal{I} the linearly independent subsets of X . We denote by \mathcal{B} the set of all *bases*, i.e. maximal independent sets of a matroid. A *circuit* is a non-independent set such that each of its proper subset is independent; we denote by \mathcal{C} , respectively \mathcal{C}_3 , the set of circuits of a matroid, respectively circuits of order 3. A matroid is uniquely defined either by its independent sets, bases or circuits. The matroid automorphism group $\text{Aut}(M)$ is the set of all permutations of X , which preserve \mathcal{I} , or equivalently \mathcal{B} or \mathcal{C} .

Given a root system R , $X = \tilde{R}$ is obtained by selecting a representative in each pair $\{v, -v\}$ of vectors. We define a matroid $M(R)$ on X by taking \mathcal{I} to be the subsets of X that are linearly independent.

We prove the following theorem.

Theorem 1.1. *Let R be an irreducible root system. A permutation ϕ of \tilde{R} is an automorphism of $M(R)$ if and only if it preserves \mathcal{C}_3 .*

The automorphism groups $\text{Aut}(M(R))$ for classic root systems A_n , B_n and D_n were computed in [4]. The root system F_4 , respectively H_3 was investigated in [5], respectively [6]. While proving Theorem 1.1, we compute also the automorphism groups of the root system matroids for the remaining exceptional root systems, so we complete the classification of the groups $\text{Aut}(M(R))$.

Denote by $\text{Isom}(R)$ the group of isometries of \mathbb{R}^n preserving R (see Section 2 for our choice of root lengths). Clearly, any isometry of R is an element of $\text{Aut}(M(R))$, so $\text{Isom}(R)/\pm\text{Id} \subseteq \text{Aut}(M(R))$. Denote also by G_a the subgroup of $W(R)$ of order 2 containing the antipodal involution (if any), and let $W^\sigma(R)$ be the extension of $W(R)$ defined in Section 2.

Theorem 1.2. *Let R be a root system.*

- If R is irreducible then the groups $\text{Aut}(M(R))$ are given in Table 1.*
- If $R = \sum_{i=1}^m p_i R_i$ with R_i irreducible then*

$$\text{Aut}(M(R)) = \prod_{i=1}^m \text{wr}(\text{Sym}(p_i), \text{Aut}(M(R_i)))$$

where wr stands for wreath product.

In Section 2 we introduce coordinates for the root systems and describe additional symmetries. In Section 3 we provide the proof of Theorems 1.1 and 1.2 for all the exceptional root systems. Section 4 is devoted to the proof of Theorem 1.1 for classical root systems.

TABLE 1. Automorphism groups of root system matroids

R	R	W(R)	Isom(R)	Aut(M(R))
A_n	$n(n+1)$	$(n+1)!$	$W(A_n) \times \mathbb{Z}_2$	$W(A_n)$
B_n	$2n^2$	$2^n n!$	$W(B_n)$	$W(B_n)/G_a$
D_4	24	192	$W(F_4)$	$W(F_4)/G_a$
D_n ($n \geq 5$)	$2n(n-1)$	$2^{n-1} n!$	$W(B_n)$	$W(B_n)/G_a$
E_6	72	51840	$W(E_6) \times \mathbb{Z}_2$	$W(E_6)$
E_7	126	2903040	$W(E_7)$	$W(E_7)/G_a$
E_8	240	696729600	$W(E_8)$	$W(E_8)/G_a$
F_4	48	1152	$W(F_4)$	$W^\sigma(F_4)/G_a$
H_3	30	120	$W(H_3)$	$W^\sigma(H_3)/G_a$
H_4	120	14400	$W(H_4)$	$W^\sigma(H_4)/G_a$
$I_2(m)$	$2m$	$2m$	$W(I_2(2m))$	$\text{Sym}(m)$

Remark 1.3. It is worth to mention that the notion of root system can be extended to any finitely generated Coxeter group (see [7, Section 5.4]). It would be interesting to see if Theorem 1.1 holds in such a setting with the corresponding extension of the notion of matroid to infinite sets.

2. ISOMETRIES AND AUTOMORPHISM GROUPS OF ROOT SYSTEMS

We use standard coordinates for root systems of simple Lie algebras (except G_2), see [7, Section 2.10].

The root system A_n is the set of roots $\{e_i - e_j\}$, $1 \leq i, j \leq n+1$, in \mathbb{R}^{n+1} . All the roots are contained in n -dimensional subspace with sum of coordinates equal to zero. The group $W(A_n)$ is the group $\text{Sym}(n+1)$. It is easy to see that $W(A_n)$ does not contain an antipodal involution. The group $\text{Isom}(A_n)$ is a central extension of $W(A_n)$ by the antipodal map.

The root systems E_6 , E_7 and E_8 have special coordinates and are defined in [1, 7]. The groups $\text{Isom}(E_7)$ and $\text{Isom}(E_8)$ coincide with $W(E_7)$ and $W(E_8)$ respectively since the reflection groups already contain an antipodal involution. The group $\text{Isom}(E_6)$ is an extension of $W(E_6)$ by the antipodal map.

The set D_n of roots is $\{\pm e_i \pm e_j\}$, $1 \leq i < j \leq n$, in \mathbb{R}^n . We describe its isometry group below.

All root systems considered so far had only one orbit of roots under $W(R)$ and so only one length of roots. The following root systems of simple Lie algebras have roots of two different lengths.

The root system \mathbf{B}_n is formed by the roots $(\pm e_i)_{1 \leq i \leq n}$ called *short roots* and the roots $(\pm e_i \pm e_j)_{1 \leq i < j \leq n}$ of \mathbf{D}_n called *long roots*. Note that $W(\mathbf{B}_n)$ preserves \mathbf{D}_n as well. This implies that $\text{Isom}(\mathbf{D}_n) = \text{Isom}(\mathbf{B}_n) = W(\mathbf{B}_n)$.

Denote by \mathbf{D}'_4 the root system formed by the 8 vectors $\pm e_i$ for $1 \leq i \leq 4$ and the 16 vectors $(\pm 1/2, \pm 1/2, \pm 1/2, \pm 1/2)$. It is easy to see that \mathbf{D}'_4 is isomorphic to \mathbf{D}_4 . The root system \mathbf{F}_4 is the union of \mathbf{D}_4 and \mathbf{D}'_4 . The isometry group of \mathbf{F}_4 coincides with $W(\mathbf{F}_4)$. However, there is an isometry σ of \mathbb{R}^4 exchanging \mathbf{D}_4 with $\sqrt{2}\mathbf{D}'_4$. We denote by $W^\sigma(\mathbf{F}_4)$ the group generated by $W(\mathbf{F}_4)$ and σ . The group $W^\sigma(\mathbf{F}_4)$ does not preserve \mathbf{F}_4 , but it preserves the tessellation of \mathbb{R}^4 by fundamental chambers of $W(\mathbf{F}_4)$.

Now let us describe the root systems not corresponding to Lie algebras. Here we use the vectors of unit length only. For $\mathbf{l}_2(m)$ we assume $m \geq 5$ to exclude \mathbf{B}_2 .

The root systems \mathbf{H}_3 and \mathbf{H}_4 , see [2], have coordinates in $\mathbb{Q}(\sqrt{5})$. As a consequence, the Galois involution $\sigma : \sqrt{5} \mapsto -\sqrt{5}$ can transform them into another root system, which is isomorphic to the original one. This involution exchanges the pair of roots of angle $\arccos(\pm \frac{1+\sqrt{5}}{4})$ with the pair of roots of angle $\arccos(\pm \frac{1-\sqrt{5}}{4})$. We denote by $W^\sigma(\mathbf{H}_i)$ the group of permutations of \mathbf{H}_i generated by $W(\mathbf{H}_i)$ and the permutation induced by σ . As in the case of \mathbf{F}_4 , $W^\sigma(\mathbf{H}_i)$ preserves the $W(\mathbf{H}_i)$ -action on \mathbb{R}^i .

The root system $\mathbf{l}_2(m)$ for $m \geq 5$ is formed by the $2m$ vectors $(\cos(\frac{\pi k}{m}), \sin(\frac{\pi k}{m}))_{1 \leq k \leq 2m}$. The roots form a regular $2m$ -gon, so the group $\text{Isom}(\mathbf{l}_2(m))$ is a dihedral group isomorphic to $\mathbf{l}_2(2m)$.

As we have mentioned above, all isometries of \mathbb{R} induce automorphisms of $M(\mathbb{R})$. To compute the groups $\text{Aut}(\mathbb{R})$ we need to list all the automorphisms of $M(\mathbb{R})$ not induced by isometries of root systems.

3. EXCEPTIONAL ROOT SYSTEMS

In this section, we prove Theorems 1.1 and 1.2 for exceptional root systems.

Notice that $M(\mathbb{R})$ is isomorphic to $M(\mathbb{R}')$ if and only if \mathbb{R} and \mathbb{R}' are isomorphic as root systems. Indeed, if c is a circuit of \mathbb{R} , then c is contained in an irreducible root system. Thus, the question is reduced to the irreducible case for which the classification gives the answer by simply noticing that isomorphism preserves the dimension and the number of elements.

Proof of the theorems for $R = E_6, E_7, E_8, F_4, H_3, H_4, I_2(m)$. First, we explain the assertion (ii) of Theorem 1.2. If $R = \sum_{i=1}^m p_i R_i$ and $\phi \in \text{Aut}(M(R))$, then ϕ permutes the components isomorphic to R_i and thus ϕ belongs to the mentioned product of wreath products.

Now consider irreducible root systems. We prove the theorems using case by case analysis. For $I_2(m)$ it is clear that any two non-antipodal roots form a basis and thus $\text{Aut}(M(I_2(m))) = \text{Sym}(m)$. All the circuits are of order 3, so Theorem 1.1 holds as well.

If \mathcal{F} is a family of subsets of X , denote by $G(X, \mathcal{F})$ the graph on $|X| + |\mathcal{F}|$ vertices with vertex $x \in X$ being adjacent to $S \in \mathcal{F}$ if and only if $x \in S$. The group $\text{Aut}(G(X, \mathcal{F}))$ of automorphisms of the graph $G(X, \mathcal{F})$ is identified with a subgroup of the symmetric group $\text{Sym}(X)$. The program `nauty` [8] can compute the automorphism group of a graph G . Moreover, if one attributes colors to vertices then this program can compute the group of automorphism preserving those colors.

If \mathcal{F} is a family of subsets of X invariant under the automorphism group $\text{Aut}(M)$ of a matroid M on X , then $\text{Aut}(M) \subset \text{Aut}(G(X, \mathcal{F}))$. If one takes $\mathcal{F} = \mathcal{I}, \mathcal{B}$ or \mathcal{C} , then we have equality. Take R an irreducible root system. If we can check that all elements of $\text{Aut}(G(X, \mathcal{C}_3))$ are actually symmetries of $M(R)$ then we have $\text{Aut}(M(R)) = \text{Aut}(G(X, \mathcal{C}_3))$ and proved Theorem 1.1 for R . At the same time, the set \mathcal{C}_3 is not large for the exceptional root systems, and it can be easily computed, as well as the group $\text{Aut}(G(X, \mathcal{C}_3))$. This method works directly for the root systems E_6, E_7, E_8, F_4, H_3 and H_4 ¹.

In particular, we compute the automorphism groups of the root systems matroids themselves. The results are listed in Table 1, which completes the proof of Theorem 1.2.

□

4. PROOF OF THE A_n, D_n, B_n CASES

In [3] the correspondence between circuits in root systems of simple Lie algebras and Euclidean simplices generating discrete reflection groups is described.

Any circuit in a root system defines (up to similarity) a Euclidean simplex generating a discrete reflection group. Given $(n + 1)$ -tuple of roots, we take $n + 1$ hyperplanes orthogonal to these roots and passing through the origin. Now choose any of the hyperplanes and translate

¹All sources of the programs of this paper are available at <http://www.liga.ens.fr/~dutour/RootMatroid/>

it in such a way that the image does not contain the origin. The new hyperplane together with the remaining n ones define a simplex.

Conversely, any Euclidean simplex generating a discrete reflection group defines a circuit in some root system in the following way: faces of codimension one are orthogonal to roots of some affine root system. These roots define a circuit of the underlying finite root system.

As a consequence, using the classification of simplices generating discrete reflection groups obtained in [3], we get the circuits of the root systems A_n , B_n , and D_n .

Denote by $V(\mathbf{R})$ the set of pairs of opposite roots of \mathbf{R} . If J is a subset of $V(\mathbf{R})$, we say that a root $v \in \mathbf{R}$ belongs to J if J contains a vertex $(v, -v) \in V(\mathbf{R})$. In fact, there is no difference in defining J in terms of roots or pairs of opposite roots. We will use pairs sometimes to emphasize that we are able to choose any representative from a pair.

To prove Theorem 1.1 it is sufficient to show that if the set of circuits of $M(\mathbf{R})$ of order 3 is invariant under some permutation of elements of $V(\mathbf{R})$, then the set of all circuits of $M(\mathbf{R})$ is invariant, too. The latter is an immediate corollary of the following lemma.

Lemma 4.1. *Let $k \geq 3$ be an integer not exceeding n , and let f be a permutation of elements of $V(\mathbf{R})$. If the set of circuits of $M(\mathbf{R})$ of order not exceeding k is invariant under f , then so is the set of circuits of order $k + 1$.*

Proof. We prove the lemma for root systems A_n , D_n , and B_n separately:

Case $\mathbf{R} = A_n$.

For any set J of elements of $V(\mathbf{R})$ we draw the following graph $\Gamma(J)$:

- the vertices of $\Gamma(J)$ are e_i for those i which take part in the expression of at least one element of J ;
- two vertices e_i and e_j are joined by an edge if the root $\pm(e_i - e_j) \in J$.

As it is shown in [3], graphs $\Gamma(J)$ corresponding to circuits J of $M(A_n)$ are cycles, and conversely. The order of J is equal to the number of edges in $\Gamma(J)$. Take any circuit J of order $k + 1$. It is sufficient to prove that $f(J)$ is linearly dependent.

Since $\Gamma(J)$ is a cycle, we may assume that $J = \{e_1 - e_2, e_2 - e_3, \dots, e_k - e_{k+1}, e_1 - e_{k+1}\}$. Now consider $J' = J \cup \{e_1 - e_3\}$. The graph $\Gamma(J')$ consists of cycles $\{e_1 - e_2, e_2 - e_3, e_1 - e_3\}$ and $\{e_1 - e_3, e_3 - e_4, \dots, e_k - e_{k+1}, e_1 - e_{k+1}\}$. By the assumption of the lemma, the images of these circuits under f are circuits. Therefore, from one cycle we may express $f(e_1 - e_3)$ as a linear combination of $f(e_1 - e_2)$ and $f(e_2 - e_3)$, and from another cycle we may express $f(e_1 - e_3)$ as a linear

combination of $f(e_3 - e_4), \dots, f(e_k - e_{k+1}), f(e_1 - e_{k+1})$. Subtracting one expression from another, we obtain a dependence on vectors of $f(J)$.

Case $R = D_n$.

For any set J of elements of $V(R)$ we draw the following edge colored graph $\Gamma(J)$:

- the vertices are e_i for those i which take part in the expression of at least one element of J ;
- two vertices e_i and e_j are joined by a *red* edge if the root $\pm(e_i + e_j) \in J$;
- two vertices e_i and e_j are joined by a *black* edge if the root $\pm(e_i - e_j) \in J$.

According to [3], circuits correspond either to

- cycles with even number of red edges,
- or to two cycles C_1, C_2 , possibly of length 2, joined by a path, such that the number of red edges in each cycle is odd (edges of the path are colored in any way).

We take any circuit J of order $k + 1$ and show that $f(J)$ is linearly dependent. If one of the cycles of $\Gamma(J)$ contains at least 4 vertices, we do almost the same procedure as in the A_n case. Suppose the cycle contains vertices e_1, e_2, e_3 , and e_4 . Consider J' obtained from J by adding either $e_1 - e_3$ or $e_1 + e_3$ so that the number of red edges in the new cycle of order 3 is even. Then we obtain two new circuits of order at most k , and they intersect by a unique root. A reasoning similar to the one for A_n completes the proof of this case.

So, we may assume that all cycles have length at most 3. Since $k + 1 \geq 4$, $\Gamma(J)$ contains two cycles. Now, take two vertices of valency two belonging to distinct cycles of $\Gamma(J)$, and join them by an edge. Choose the color of the edge in such a way that one of the shortest cycles containing this edge contains an even number of red edges. Clearly, this cycle corresponds to a circuit of order not exceeding k . If we hide the edges of this cycle belonging to two initial cycles of $\Gamma(J)$, we obtain another circuit of $M(R)$ of order not exceeding k . By the assumption, the images of corresponding sets of roots under f are circuits again. By minimality, the corresponding linear dependencies contains all the roots with non-zero coefficients. Eliminating the new root from two linear dependencies, we obtain that $f(J)$ is linearly dependent.

Case $R = B_n$.

For any set J of elements of $V(R)$ we draw the following graph $\Gamma(J)$ with colored edges and some vertices marked:

- the vertices are e_i for those i which take part in the expression of at least one element of J ;
- two vertices e_i and e_j are joined by a *red* edge if the root $\pm(e_i + e_j) \in J$;
- two vertices e_i and e_j are joined by a *black* edge if the root $\pm(e_i - e_j) \in J$;
- a vertex e_i is *marked* if the root $\pm e_i \in J$.

By [3], circuits correspond either to

- the graphs of D_n case,
- or a path with two end vertices being marked,
- or to a cycle with an odd number of red edges and a path linking the cycle to a unique marked vertex.

The order of J is the number of edges of $\Gamma(J)$ plus the number of marked vertices. Again, we consider any circuit J of order $k + 1$ and show that $f(J)$ is linearly dependent.

If $\Gamma(J)$ does not contain any marked vertices, then J contains long roots only, so it belongs to D_n and the proof repeats the above one. Thus, we may assume that we have at least one marked vertex.

Suppose that $\Gamma(J)$ contains a path to a marked vertex e_1 . Let the neighboring vertex be e_2 . Consider $J' = J \cup \{e_2\}$. Then J' consists of two circuits of $M(\mathbb{R})$, namely of circuit of order 3 containing e_1 , e_2 and the edge joining these two vertices, and the remaining elements of J together with e_2 . Both circuits have order at most k . By the same method we see that $f(J)$ is linearly dependent.

We are left with the case when $\Gamma(J)$ is a cycle with one vertex marked. If there are at least 4 vertices in $\Gamma(J)$, we take two non-neighboring non-marked vertices, join them by an edge of an appropriate color and use the same method as in the D_n case. So, the only interesting case is when J is of order 4. We may assume that $J = \{e_1, e_1 \pm e_2, e_2 \pm e_3, e_1 \pm e_3\}$ and that the number of plus signs occurring in its expression is odd. The set $J' = J \cup \{e_2\}$ contains the following two circuits of $M(\mathbb{R})$: $\{e_1, e_1 \pm e_2, e_2\}$, and $\{e_2, e_2 \pm e_3, e_1 \pm e_3, e_1\}$. Since they both have paths to marked vertices, their images under f are still circuits; so we have two linear dependencies on the images. Eliminating e_2 from them, we obtain a dependence on $f(J)$. The result is not trivial since one of the dependencies contains $f(e_1 \pm e_2)$ with non-zero coefficient, and the other one contains images of two long roots with non-zero coefficients.

□

REFERENCES

- [1] N. Bourbaki, *Groupes et algèbres de Lie, Chapitres IV–VI*, Hermann, Paris, 1968.
- [2] H.S.M. Coxeter, *Regular polytopes*, Dover Publications, New York, 1973.
- [3] A. Felikson, P. Tumarkin, *Euclidean simplices generating discrete reflection groups*, European J. Combin. **28** (2007) 1056–1067.
- [4] L. Fern, G. Gordon, J. Leasure and S. Pronchik, *Matroid Automorphisms and Symmetry Groups*, Combinatorics, Probability and Computing **9** (2000) 105–123.
- [5] S. Fried, A. Gerek, G. Gordon and A. Peruničić, *Matroid automorphisms of the F_4 root system*, Electronic journal of combinatorics **14** (2007) R78.
- [6] K. Ehly, G. Gordon, *Matroid automorphisms of the root system H_3* , Geom. Dedicata **130** (2007) 149–161.
- [7] J.E. Humphreys, *Reflection groups and Coxeter groups*, Cambridge University Press, 1990.
- [8] B.D. McKay, *The nauty program*, <http://cs.anu.edu.au/people/bdm/nauty/>

MATHIEU DUTOUR SIKIRIĆ, RUDJER BOSKOVIĆ INSTITUTE, BIJENICKA 54,
10000 ZAGREB, CROATIA
E-mail address: mdsikir@irb.hr

ANNA FELIKSON, INDEPENDENT UNIVERSITY OF MOSCOW, B. VLASSIEVSKII
11, 119002 MOSCOW, RUSSIA
E-mail address: felikson@mccme.ru

PAVEL TUMARKIN, INDEPENDENT UNIVERSITY OF MOSCOW, B. VLASSIEVSKII
11, 119002 MOSCOW, RUSSIA
E-mail address: pasha@mccme.ru