Enseign. Math. (2) 70 (2024), 25–59
DOI 10.4171/LEM/1058

Divisibility of spheres with measurable pieces

Clinton T. Conley, Jan Grebík and Oleg Pikhurko

Abstract. For an r-tuple $(\gamma_1, \dots, \gamma_r)$ of special orthogonal $d \times d$ matrices, we say that the Euclidean $(d-1)$-dimensional sphere $\mathbb{S}^{d-1}$ is $(\gamma_1, \dots, \gamma_r)$*-divisible* if there is a subset $A \subseteq \mathbb{S}^{d-1}$ such that its translations by the rotations $\gamma_1, \dots, \gamma_r$ partition the sphere. Motivated by some old open questions of Mycielski and Wagon, we investigate the version of this notion where the set A has to be measurable with respect to the spherical measure. Our main result shows that measurable divisibility is impossible for a "generic" (in various meanings) r-tuple of rotations. This is in stark contrast to the recent result of Conley, Marks and Unger which implies that, for every "generic" r-tuple, divisibility is possible with parts that have the property of Baire.

Mathematics Subject Classification (2020). Primary 28A05; Secondary 03E15, 33C55, 43A90, 57M60.

Keywords. Euclidean sphere, divisibility under a group action, measurable set, special orthogonal group.

1. Introduction

Let $\mathrm{SO}(d)$ denote the group of *special orthogonal* $d \times d$ matrices, that is, real $d \times d$ matrices M such that the determinant of M is 1 and $M^T M = I_d$, where I_d denotes the identity $d \times d$ matrix. The elements of this group are naturally identified with orientation-preserving isometries of the Euclidean unit sphere

$$\mathbb{S}^{d-1} := \{\boldsymbol{x} \in \mathbb{R}^d \mid \|\boldsymbol{x}\|_2 = 1\},$$

and we will often refer to them as *rotations*.

For an r-tuple $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$, we say that $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$*-divisible* (or *admits a* $\boldsymbol{\gamma}$*-division*) if there is $A \subseteq \mathbb{S}^{d-1}$ such that its translates $\gamma_1.A, \dots, \gamma_r.A$ partition $\mathbb{S}^{d-1}$ (that is, for every $\boldsymbol{x} \in \mathbb{S}^{d-1}$ there are unique $\boldsymbol{y} \in A$ and $i \in [r]$ such that $\boldsymbol{x} = \gamma_i.\boldsymbol{y}$, where we denote $[r] := \{1, \dots, r\}$). Of course, a set A works for $\boldsymbol{\gamma}$ if and only if $\gamma_r.A$ works for $\boldsymbol{\beta} := (\gamma_1\gamma_r^{-1}, \dots, \gamma_{r-1}\gamma_r^{-1}, I_d)$. However, we do not normally assume that any particular rotation is the identity, mostly for the notational convenience so that all indices can be treated uniformly.

We say that $\mathbb{S}^{d-1}$ is *r-divisible* if there is an r-tuple $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$ such that $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible (or, in other words, if we can partition $\mathbb{S}^{d-1}$ into r congruent pieces). The integer pairs $d, r \geqslant 2$ such that $\mathbb{S}^{d-1}$ is r-divisible have been completely classified (see, e.g., the book by Tomkowicz and Wagon [23, Theorem 6.6]). Namely, the only pairs when the answer is in the negative are when $r = 2$ and d is odd. In this case, the impossibility of any (γ_1, γ_2)-division follows from considering a fixed point $\boldsymbol{x} \in \mathbb{S}^{d-1}$ of $\gamma_1^{-1}\gamma_2$ which exists as the dimension $d-1$ of the sphere is even. (Indeed, no set A can work here: the translates $\gamma_1.A$ and $\gamma_2.A$ intersect if $\boldsymbol{x} \in A$ and do not cover $\gamma_1.\boldsymbol{x}$ if $\boldsymbol{x} \notin A$.) On the other hand, the case of $d = 2$ is trivial (e.g., one can take the r rotations of the circle $\mathbb{S}^1$ by multiples of the angle $2\pi/r$) while the first published solution for $\mathbb{S}^2$ seems to be by Robinson [22, p. 254]. Furthermore, the r-divisibility for $\mathbb{S}^{d-1}$ easily implies the r-divisibility of $\mathbb{S}^{d+1}$; see, e.g., the proof of [23, Theorem 6.6] or Lemma 5.1 here.

Mycielski [18] showed that there is a subset $A \subseteq \mathbb{S}^2$ such that for every integer $r \geqslant 3$ there are $\gamma_1, \ldots, \gamma_r$ with $\gamma_1.A, \ldots, \gamma_r.A$ partitioning the sphere. This should be compared with the classical paradox of Hausdorff [13] who produced such a set A that works, apart from a countable subset of $\mathbb{S}^2$ of errors, for every $r \geqslant 2$. (Note that we cannot take $r = 2$ in Mycielski's result because $\mathbb{S}^2$ is not 2-divisible.)

Let μ be the *spherical measure* on $\mathbb{S}^{d-1}$, which can be defined as the $(d-1)$-dimensional Hausdorff measure with respect to the standard *arc-length distance* on the sphere (where the distance between $\boldsymbol{x}, \boldsymbol{y} \in \mathbb{S}^{d-1}$ is the angle between the vectors $\boldsymbol{x}$ and $\boldsymbol{y}$). We call a subset of $\mathbb{S}^{d-1}$ *measurable* if it belongs to the μ-completion of the Borel σ-algebra. Note that the paradoxical set A in the results of Hausdorff [13] and Mycielski [18] cannot be measurable with respect to the (rotation-invariant) measure μ on $\mathbb{S}^2$, for otherwise the existence of a partition $\gamma_1.A, \ldots, \gamma_r.A$ of $\mathbb{S}^{d-1}$ up to a countable (and thus μ-null) set implies that $\mu(A) = \mu(\mathbb{S}^{d-1})/r$, a contradiction to r assuming different values. Mycielski [19,20] asked if one can show that $\mathbb{S}^2$ is r-divisible without using the Axiom of Choice. Wagon [24, Question 4.15] (or [23, Question 5.15]) asked if the 3-divisibility of $\mathbb{S}^2$ can be shown with measurable sets (thus the Axiom of Choice can be applied on a μ-null set). Measurable divisibility for higher-dimensional spheres is easier because of a constructive way of lifting up a division from $\mathbb{S}^{d-1}$ to $\mathbb{S}^{d+1}$. It is known that $\mathbb{S}^{d-1}$ is r-divisible with measurable pieces for $r \geqslant 3$ and odd $d \geqslant 5$ (which follows from the proof of [23, Theorem 6.6 (b)], see Lemma 5.1 here) and with Borel pieces for $r \geqslant 2$ and even $d \geqslant 2$ (see, e.g., [23, Theorem 6.6 (a)]).

The above questions by Mycielski and Wagon are still open, although some related progress was obtained by Conley, Marks and Unger [4] whose general results imply that, unless $r = 2$ and d is odd, the sphere $\mathbb{S}^{d-1}$ is r-divisible so that each piece has the *property of Baire* (that is, under one of equivalent definitions, each piece can be represented as the symmetric difference of a Borel set and a meager set; for more details see, e.g., the textbook on descriptive set theory by Kechris [15, Section 8.F]). The derivation of this result is given in Proposition 1.2 here.

Here we propose to study the more general question of describing the set of those r-tuples $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$ such that $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible with measurable pieces.

First, we consider the case when the rotations are "generic". More precisely, let us call an r-tuple of matrices $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$ *generic* if, for every polynomial p with rational coefficients in $d^2 r$ variables, $p(\boldsymbol{\gamma}) = 0$ implies that $p(\boldsymbol{\beta}) = 0$ for every $\boldsymbol{\beta} \in \mathrm{SO}(d)^r$, where, e.g., $p(\boldsymbol{\gamma})$ denotes the value of p on the $d^2 r$ individual entries of the matrices corresponding to $\gamma_1, \dots, \gamma_r$ under the standard basis of $\mathbb{R}^d$. In other words, this property states that if a polynomial with rational (equivalently, integer) coefficients vanishes on (the matrix entries of) $\boldsymbol{\gamma}$ then it necessarily vanishes everywhere on $\mathrm{SO}(d)^r$.

Our main result shows that *no* generic $\boldsymbol{\gamma}$ works in the measurable setting, even in a rather relaxed fractional version.

Theorem 1.1. *Let $d \geqslant 2$ and $r \geqslant 2$ be integers. Let $(\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$ be generic. Then every $f \in L^2(\mathbb{S}^{d-1}, \mu)$ with $\sum_{i=1}^r \gamma_i . f = 1$ μ-almost everywhere is the constant function $1/r$ μ-almost everywhere, where $\gamma_i . f$ denotes the function that maps $\boldsymbol{x} \in \mathbb{S}^{d-1}$ to $f(\gamma_i^{-1} . \boldsymbol{x})$.*

In sharp contrast, we can derive with some extra work from the results in [4] that *every* generic $\boldsymbol{\gamma}$ works with pieces that have the property of Baire.

Proposition 1.2. *Let $r \geqslant 2$ and $d \geqslant 2$ be arbitrary integers, except if d is odd then we require that $r \geqslant 3$. Let $(\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$ be generic. Then there is a subset A of $\mathbb{S}^{d-1}$ with the property of Baire such that $\gamma_1 . A, \dots, \gamma_r . A$ partition $\mathbb{S}^{d-1}$.*

Theorem 1.1 and Proposition 1.2 add to a growing body of results in measurable combinatorics (see, e.g., the recent survey by Kechris and Marks [16]), where the requirements that the pieces are measurable and have the property of Baire respectively lead to different answers.

The following lemma shows that, in various meanings, "most" elements of $\mathrm{SO}(d)^r$ are generic.

Lemma 1.3. *Let $r \geqslant 1$, $d \geqslant 2$ and $\mathcal{N}$ be the set of r-tuples in $\mathrm{SO}(d)^r$ that are not generic. Then the following statements hold:*

(i) *The set $\mathcal{N}$ has measure 0 with respect to the Haar measure on the group $\mathrm{SO}(d)^r$.*

(ii) *The set $\mathcal{N}$ is a meager subset of $\mathrm{SO}(d)^r$ with respect to the topology induced by the Euclidean topology on $\mathbb{R}^{d^2 r} \supseteq \mathrm{SO}(d)^r$.*

Also, by using some algebraic geometry, we can give a more concrete characterisation of generic r-tuples of rotations. In particular, the following lemma allows us to write an "explicit" generic point: just let the entries above the diagonals be sufficiently small reals that are algebraically independent over $\mathbb{Q}$ and extend this to an element of $\mathrm{SO}(d)^r$ by Claim 8.3 here.

Lemma 1.4. *Let $r \geqslant 1$, $d \geqslant 2$, and $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$. Then $\boldsymbol{\gamma}$ is generic if and only if the $\binom{d}{2}r$-tuple of the matrix entries of $\boldsymbol{\gamma}$ strictly above the diagonals is algebraically independent over $\mathbb{Q}$.*

In the extreme opposite case, we show that, for odd $d \geqslant 3$, $\boldsymbol{\gamma}$-divisibility cannot be attained when $\boldsymbol{\gamma}$ generates a finite subgroup of $\mathrm{SO}(d)$.

Proposition 1.5. *Let $d \geqslant 3$ be odd. Suppose that $\gamma_1, \ldots, \gamma_r \in \mathrm{SO}(d)$, $r \geqslant 3$, generate a finite subgroup $\Gamma \subseteq \mathrm{SO}(d)$. Then $\mathbb{S}^{d-1}$ is not $(\gamma_1, \ldots, \gamma_r)$-divisible.*

Some standard general results of Borel combinatorics (e.g., [21, Lemma 5.12 and Theorem 5.23]) imply that if $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible and every orbit of the subgroup of $\mathrm{SO}(d)$ generated by $\gamma_1, \ldots, \gamma_r$ is finite, then there is a Borel $\boldsymbol{\gamma}$-division. The following result gives that just one finite orbit is enough to convert a $\boldsymbol{\gamma}$-division into a measurable one.

Proposition 1.6. *Let $d \geqslant 2$ and $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in \mathrm{SO}(d)^r$. Let Γ be the subgroup of $\mathrm{SO}(d)$ generated by $\gamma_1, \ldots, \gamma_r$. Suppose that there is $\boldsymbol{z} \in \mathbb{S}^{d-1}$ such that its Γ-orbit $\Gamma.\boldsymbol{z}$ is finite. Then $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible if and only if $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible with measurable pieces.*

Of course, this leaves a wide range of unresolved cases. As an initial partial step, we completely characterise those r-tuples of rotations for which the circle $\mathbb{S}^1$ is divisible with measurable pieces for $r \leqslant 3$.

This paper is organised as follows. In Section 2 we give a quick overview of basic definitions and facts about spherical harmonics and use these to prove Theorem 1.1, which is the main result of this paper. Proposition 1.5 is proved in Section 3 using Euler's characteristic. Propositions 1.6 and 1.2 are proved in Sections 4 and 7 respectively. In Section 5 we describe the standard construction of how an r-division of $\mathbb{S}^{d-1}$ can be lifted to $\mathbb{S}^{d+1}$ and observe that this gives measurable pieces (Lemma 5.1). In Section 6 we study various versions of measurable divisibility when $d = 2$; in particular, we characterise r-tuples $\boldsymbol{\gamma} \in \mathrm{SO}(2)^r$ for which the circle $\mathbb{S}^1$ is $\boldsymbol{\gamma}$-divisible with measurable pieces for $r \leqslant 3$. The rather technical Section 8 is dedicated to proving Lemmas 1.3 and 1.4. Section 8.1 presents some basics of algebraic geometry. In Section 8.2 we prove some results about $\mathrm{SO}(d)^r$ and use them to prove Lemma 1.3. In particular, we show that the variety $\mathrm{SO}(d)^r \subseteq \mathbb{R}^{d^2 r}$ is irreducible and the entries above the diagonals form a transcendence basis for its function field. While these results are fairly standard, we present their proofs since we could not find any published statements that suffice for our purposes. In Section 8.3 we prove an auxiliary lemma from algebraic geometry and use it to derive Lemma 1.4.

2. Spherical harmonics

Let an integer $d \geqslant 2$ be fixed throughout this section.

For an introduction to spherical harmonics on $\mathbb{S}^{d-1}$ we refer to the book by Groemer [10] whose notation we generally follow. Recall that

$$\sigma_d := \mu(\mathbb{S}^{d-1}) = \frac{2\pi^{d/2}}{\Gamma(d/2)}.$$

As d is fixed, the dependence on d is usually not mentioned except for σ_d (since σ_{d-1} will also appear in some formulas). Also, the shorthand *a.e.* stands for μ-almost everywhere.

By [10, Lemma 1.3.1], the density of the push-forward of μ under the projection to any coordinate axis is

$$\rho(t) := \begin{cases} \sigma_{d-1}\,(1-t^2)^{(d-3)/2}, & -1 < t < 1, \\ 0, & \text{otherwise.} \end{cases} \tag{2.1}$$

A polynomial $p \in \mathbb{R}[\boldsymbol{x}]$, $\boldsymbol{x} = (x_1, \ldots, x_d)$, is called *harmonic* if $\Delta p = 0$, where

$$\Delta := \frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_d^2}$$

is the *Laplace operator*. A *spherical harmonic* is a function from $\mathbb{S}^{d-1}$ to the reals which is the restriction to $\mathbb{S}^{d-1}$ of a harmonic polynomial on $\mathbb{R}^d$. Let $\mathcal{H}$ be the vector space of all spherical harmonics. For an integer $n \geqslant 0$, let $\mathcal{H}_n \subseteq \mathcal{H}$ be the linear subspace consisting of all functions $f\colon \mathbb{S}^{d-1} \to \mathbb{R}$ that are the restrictions to $\mathbb{S}^{d-1}$ of some harmonic polynomial p which is homogeneous of degree n, where we regard the zero polynomial as homogeneous of any degree. By [10, Lemma 3.1.3], the polynomial p is uniquely determined by $f \in \mathcal{H}_n$, so we may switch between these two representations without mention. It can be derived from this ([10, Theorem 3.1.4]) that the dimension of $\mathcal{H}_n$ is

$$N_n := \binom{d+n-1}{n} - \binom{d+n-3}{n-2},$$

where we agree that $\binom{d+n-3}{n-2} = 0$ for $n = 0$ or 1.

Let $\langle\cdot\,,\cdot\rangle$ denote the scalar product on $L^2(\mathbb{S}^{d-1},\mu)$ (while $\boldsymbol{x}\cdot\boldsymbol{y} := \sum_{i=1}^d x_i y_i$ denotes the scalar product of $\boldsymbol{x},\boldsymbol{y}\in\mathbb{R}^d$). It is known ([10, Theorem 3.2.1]) that

$$\langle f,g\rangle = 0 \quad \text{for all } f\in\mathcal{H}_i \text{ and } g\in\mathcal{H}_j \text{ with } i\neq j, \tag{2.2}$$

that is, $\mathcal{H}_0,\mathcal{H}_1,\ldots$ are pairwise orthogonal subspaces of $\mathcal{H}\subseteq L^2(\mathbb{S}^{d-1},\mu)$. Note that the group $\mathrm{SO}(d)$ acts naturally on $L^2(\mathbb{S}^{d-1},\mu)$ via the *shift action*

$$(\gamma.f)(\boldsymbol{v}) := f(\gamma^{-1}.\boldsymbol{v}) \quad \text{for } \gamma\in\mathrm{SO}(d),\ f\in L^2(\mathbb{S}^{d-1},\mu),\ \boldsymbol{v}\in\mathbb{S}^{d-1}. \tag{2.3}$$

Each space $\mathcal{H}_n$ is invariant under this action ([10, Proposition 3.2.4]) since, on $\mathbb{R}^d$, rotations preserve both the Laplace operator as well as the set of homogeneous degree-n polynomials.

An important role is played by the *Gegenbauer polynomials* $(P_0,P_1,\ldots)$ which are obtained from $(1,t,t^2,\ldots)$ by the Gram–Schmidt orthonormalization process on $L^2([-1,1],\rho(t)\,\mathrm{d}t)$, except they are normalised to assume value 1 at $t=1$ (instead of being unit vectors in the L^2-norm). In the special case $d=3$ (when ρ is the constant function), we get the *Legendre polynomials*. Of course, the degree of P_n is exactly n. Let us collect some of their standard properties that we will use.

Lemma 2.1. *For every integer $n\geqslant 0$, the following hold:*

(i) *The polynomial P_n has rational coefficients.*

(ii) *For every $\boldsymbol{v}\in\mathbb{S}^{d-1}$, the function $P_n^{\boldsymbol{v}}\colon\mathbb{S}^{n-1}\to\mathbb{R}$, defined by*

$$P_n^{\boldsymbol{v}}(\boldsymbol{x}) := P_n(\boldsymbol{v}\cdot\boldsymbol{x}) \quad \text{for } \boldsymbol{x}\in\mathbb{S}^{d-1},$$

belongs to $\mathcal{H}_n$.

(iii) *There is a choice of $\boldsymbol{v}_1,\ldots,\boldsymbol{v}_{N_n}\in\mathbb{S}^{d-1}$ such that the functions $P_n^{\boldsymbol{v}_i}$, $i\in[N_n]$, form a basis of the vector space $\mathcal{H}_n$.*

(iv) *For every $\boldsymbol{u},\boldsymbol{v}\in\mathbb{S}^{d-1}$, we have $\langle P_n^{\boldsymbol{u}},P_n^{\boldsymbol{v}}\rangle = \frac{\sigma_d}{N_n}P_n(\boldsymbol{u}\cdot\boldsymbol{v})$.*

Proof. Part (i) follows from the formula of Rodrigues ([10, Proposition 3.3.7]) that provides an explicit expression for P_n, or from the standard recurrence relation that writes P_{n+1} in terms of P_n and P_{n-1} for $n\geqslant 0$ ([10, Proposition 3.3.11]) together with the initial values $P_{-1}(t) := 0$ and $P_0(t)=1$.

Part (ii), namely the claim that each $P_n^{\boldsymbol{v}}$ is in $\mathcal{H}_n$, is one of the statements of [10, Theorem 3.3.3].

Part (iii) is the content of [10, Theorem 3.3.14]. Alternatively, notice that under the action in (2.3), we have for every $\boldsymbol{u},\boldsymbol{v}\in\mathbb{S}^{d-1}$ and $\gamma\in\mathrm{SO}(d)$ that

$$(\gamma.P_n^{\boldsymbol{v}})(\boldsymbol{u}) = P_n(\boldsymbol{v}\cdot(\gamma^{-1}.\boldsymbol{u})) = P_n((\gamma.\boldsymbol{v})\cdot\boldsymbol{u}),$$

that is,

$$\gamma.P_n^{\boldsymbol{v}} = P_n^{\gamma.\boldsymbol{v}}. \tag{2.4}$$

Thus the linear span of $P_n^{\boldsymbol{v}}$, $\boldsymbol{v} \in \mathbb{S}^{d-1}$, is a non-zero SO($d$)-invariant subspace of $\mathcal{H}_n$. By [10, Theorem 3.3.4], the only such subspace is $\mathcal{H}_n$ itself, giving the required result.

Part (iv) follows from

$$\langle P_n^{\boldsymbol{u}}, P_n^{\boldsymbol{v}}\rangle = \left(\int_{-1}^{1} (P_n(t))^2 \rho(t)\,\mathrm{d}t\right) P_n(\boldsymbol{u}\cdot\boldsymbol{v}) = \frac{\sigma_d}{N_n} P_n(\boldsymbol{u}\cdot\boldsymbol{v}),$$

where the first equality is a special case of the Funk–Hecke formula ([10, Theorem 3.4.1]) and the second equality (which by (2.1) amounts to computing the L^2-norm of any $P_n^{\boldsymbol{u}} \in L^2(\mathbb{S}^{d-1}, \mu)$) is proved in [10, Proposition 3.3.6]. ■

We need the following strengthening of Lemma 2.1 (iii), where we additionally require that the vectors $\boldsymbol{v}_i$ are rational.

Lemma 2.2. *For every integer $n \geqslant 0$, there is a choice of $\boldsymbol{v}_1, \dots, \boldsymbol{v}_{N_n} \in \mathbb{S}^{d-1} \cap \mathbb{Q}^d$ such that the functions $P_n^{\boldsymbol{v}_i}$, $i \in [N_n]$, form a basis of the vector space $\mathcal{H}_n$.*

Proof. We pick $\boldsymbol{v}_i$ in $\mathbb{S}^{d-1} \cap \mathbb{Q}^d$ one by one as long as possible so that the corresponding functions $P_n^{\boldsymbol{v}_i}$ are linearly independent as elements of $\mathcal{H}_n$. Let this procedure produce $\boldsymbol{v}_1, \dots, \boldsymbol{v}_\ell$. Suppose that $\ell < N_n$ as otherwise we are done. Let $\boldsymbol{v}_{\ell+1} = \boldsymbol{x}$, with $\boldsymbol{x} = (x_1, \dots, x_d) \in \mathbb{S}^{d-1}$ being viewed as a vector of unknown variables. Consider the $(\ell+1) \times (\ell+1)$ matrix $M = M(\boldsymbol{x})$ with entries

$$M_{ij} := \frac{1}{\sigma_d}\langle P_n^{\boldsymbol{v}_i}, P_n^{\boldsymbol{v}_j}\rangle \quad \text{for } i, j \in [\ell+1]. \tag{2.5}$$

In other words, $\sigma_d M$ is the Gram matrix of the vectors $P_n^{\boldsymbol{v}_1}, \dots, P_n^{\boldsymbol{v}_{\ell+1}} \in L^2(\mathbb{S}^{d-1}, \mu)$. In particular, the determinant $\det(M)$ of M is 0 if and only if $P_n^{\boldsymbol{v}_{\ell+1}}$ is in the span of the (linearly independent) vectors $P_n^{\boldsymbol{v}_1}, \dots, P_n^{\boldsymbol{v}_\ell}$ (by, e.g., [14, Theorem 7.2.10]).

By Lemma 2.1 (iv), we have that $M_{ij} = \frac{1}{N_n} P_n(\boldsymbol{v}_i \cdot \boldsymbol{v}_j)$. Thus the determinant of M is a polynomial function of $\boldsymbol{x}$.

By Lemma 2.1 (iii) and $\ell < N_d$ (and the linear independence of $P_n^{\boldsymbol{v}_1}, \dots, P_n^{\boldsymbol{v}_\ell}$), there is some choice of $\boldsymbol{v}_{\ell+1} \in \mathbb{S}^{d-1}$ with $\det(M) \neq 0$. That is, the polynomial $\det(M)$ is not identically zero on $\mathbb{S}^{d-1}$.

We need the following easy claim that can be proved, for example, by induction on $d \geqslant 2$ with the base case $d = 2$ following from $\mathbb{S}^1$ containing all points of the form

$$\frac{1}{m^2+n^2}(m^2-n^2, 2mn)$$

for $(m, n) \in \mathbb{Z}^2 \setminus \{(0,0)\}$.

Claim 2.3. *For every $d \geqslant 1$, the set $\mathbb{S}^{d-1} \cap \mathbb{Q}^d$ of the points on the sphere with all coordinates rational is dense in $\mathbb{S}^{d-1}$ with respect to the standard topology on the sphere (i.e., the one inherited from the Euclidean space $\mathbb{R}^d \supseteq \mathbb{S}^{d-1}$).* ■

Since $\det(M)$, as a polynomial function of $\boldsymbol{x} \in \mathbb{S}^{d-1}$, is continuous and not identically zero, it has to be non-zero on some point $\boldsymbol{x}$ of the dense subset $\mathbb{S}^{d-1} \cap \mathbb{Q}^d$. Thus, if we let $\boldsymbol{v}_{\ell+1}$ to be such a vector $\boldsymbol{x}$, then the functions

$$P_n^{\boldsymbol{v}_1}, \ldots, P_n^{\boldsymbol{v}_{\ell+1}} \in L^2(\mathbb{S}^{d-1}, \mu)$$

are linearly independent. This contradiction to the maximality of $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_\ell$ proves the lemma. ■

For an integer $n \geqslant 0$, an r-tuple $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in \mathrm{SO}(d)^r$ and a unit vector $\boldsymbol{v} \in \mathbb{S}^{d-1}$ define

$$G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}} := \sum_{i=1}^{r} P_n^{\gamma_i^{-1}.\boldsymbol{v}}. \tag{2.6}$$

By Lemma 2.1 (ii), each function $G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}} \colon \mathbb{S}^{d-1} \to \mathbb{R}$, as a linear combination of some spherical harmonics $P_n^{\gamma_i^{-1}.\boldsymbol{v}} \in \mathcal{H}_n$, is itself in $\mathcal{H}_n$.

Lemma 2.4. *If $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$ is generic then, for every integer $n \geqslant 0$, the linear span of $\{G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}} \mid \boldsymbol{v} \in \mathbb{S}^{d-1}\}$ is the whole space $\mathcal{H}_n$.*

Proof. By Lemma 2.2, we can fix some vectors $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{N_n} \in \mathbb{S}^{d-1} \cap \mathbb{Q}^d$ such that $P_n^{\boldsymbol{v}_1}, \ldots, P_n^{\boldsymbol{v}_{N_n}}$ form a basis for $\mathcal{H}_n$. Let $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_r)$ be an arbitrary element of $\mathrm{SO}(d)^r$ (not necessarily generic). Consider the $N_n \times N_n$ matrix $L = L(\boldsymbol{\beta})$ with entries

$$L_{ij} := \frac{1}{\sigma_d} \langle G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_i}, P_n^{\boldsymbol{v}_j} \rangle \quad \text{for } i, j \in [N_n].$$

Recall that the vectors $P_n^{\boldsymbol{v}_i}$, $i \in [N_n]$, form a (not necessarily orthonormal) basis of the linear space $\mathcal{H}_n$. Write the vectors $G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_i}$ in this basis:

$$(G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_1}, \ldots, G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_{N_n}})^T = A(P_n^{\boldsymbol{v}_1}, \ldots, P_n^{\boldsymbol{v}_{N_n}})^T,$$

for some $N_n \times N_n$ matrix A. Then L is the matrix product AM, where M is the Gram matrix of the vectors $P_n^{\boldsymbol{v}_i}$ multiplied by the constant σ_d^{-1} (that is, the entries of M are defined by the formula in (2.5)). The matrix M is non-singular by the linear independence of $P_n^{\boldsymbol{v}_i}$, $i \in [N_n]$. Thus, $\det(L) \neq 0$ if and only if $G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_1}, \ldots, G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}_{N_n}}$ are linearly independent as vectors in $\mathcal{H}_n$.

By Lemma 2.1 (iv), we have for every $i, j \in [N_d]$ that

$$L_{ij} := \frac{1}{\sigma_d} \sum_{s=1}^{r} \langle P_n^{\beta_s^{-1}.\boldsymbol{v}_i}, P_n^{\boldsymbol{v}_j} \rangle = \frac{1}{N_n} \sum_{s=1}^{r} P_n((\beta_s^{-1}.\boldsymbol{v}_i) \cdot \boldsymbol{v}_j)$$
$$= \frac{1}{N_n} \sum_{s=1}^{r} P_n(\boldsymbol{v}_i \cdot (\beta_s.\boldsymbol{v}_j)).$$

Since $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_{N_n}$ are fixed, this writes each L_{ij} as a polynomial in the $d^2 r$ entries of the matrices $\beta_1, \ldots, \beta_r$. Moreover, all coefficients of this polynomial are rational since each $\boldsymbol{v}_i$ belongs to $\mathbb{Q}^d$ and all coefficients of P_n are rational by Lemma 2.1 (i). Thus the determinant of L is equal to $p(\boldsymbol{\beta})$ for some polynomial p with coefficients in $\mathbb{Q}$.

Note that if we let each β_i be the identity matrix I_d, then $G_{n,\boldsymbol{\beta}}^{\boldsymbol{v}}$ becomes $rP_n^{\boldsymbol{v}}$ for every $\boldsymbol{v} \in \mathbb{S}^{d-1}$, and we have $L_{ij} = \frac{r}{\sigma_d} \langle P_n^{\boldsymbol{v}_i}, P_n^{\boldsymbol{v}_j} \rangle$ for $i, j \in [N_n]$ and $\det(L) \neq 0$ (since $P_n^{\boldsymbol{v}_1}, \ldots, P_n^{\boldsymbol{v}_{N_n}}$ are linearly independent). Thus, $p(I_d, \ldots, I_d) \neq 0$. Since $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$ is generic, we have that $p(\boldsymbol{\gamma}) \neq 0$, that is, the matrix L for $\boldsymbol{\beta} := \boldsymbol{\gamma}$ is non-singular. This means that the functions $G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}_i}$, $i \in [N_n]$, are linearly independent. Since they all lie in $\mathcal{H}_n$ and their number equals the dimension of this linear space, they span $\mathcal{H}_n$. The lemma is proved. ∎

Given the above auxiliary results, we can derive Theorem 1.1 rather easily.

Proof of Theorem 1.1. Recall that $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in \mathrm{SO}(d)^r$, $r \geqslant 2$, is generic and we have to show that $\mathbb{S}^{d-1}$ is not "fractionally" $\boldsymbol{\gamma}$-divisible.

So take any $f \in L^2(\mathbb{S}^{d-1}, \mu)$ such that

$$\sum_{i=1}^{r} \gamma_i.f = 1 \quad \text{a.e.}$$

Since spherical harmonics are dense in $L^2(\mathbb{S}^{d-1}, \mu)$ ([10, Corollary 3.2.7]), and we have the direct sum $\mathcal{H} = \oplus_{n=0}^{\infty} \mathcal{H}_n$, whose components are orthogonal to each other by (2.2), we can uniquely write

$$f = \sum_{n=0}^{\infty} F_n$$

in $L^2(\mathbb{S}^{d-1}, \mu)$ with $F_n \in \mathcal{H}_n$ for every $n \geqslant 0$. Since the action of $\mathrm{SO}(d)$ preserves each space $\mathcal{H}_n$ as well as the scalar product on $L^2(\mathbb{S}^{d-1}, \mu)$, we have that

$$\gamma.f = \sum_{n=0}^{\infty} \gamma.F_n$$

is the harmonic expansion of $\gamma.f \in L^2(\mathbb{S}^{d-1}, \mu)$.

Take any integer $n \geqslant 1$. Recall that the sum $\sum_{i=1}^{r} \gamma_i.f$ is a constant function 1 a.e. By (2.2), the invariance of the scalar product under $SO(d)$ and by (2.4), we have that, for every $\boldsymbol{v} \in \mathbb{S}^{d-1}$,

$$
\begin{aligned}
0 &= \langle P_n^{\boldsymbol{v}}, 1\rangle = \langle P_n^{\boldsymbol{v}}, \gamma_1.f + \cdots + \gamma_r.f\rangle = \langle P_n^{\boldsymbol{v}}, \gamma_1.F_n + \cdots + \gamma_r.F_n\rangle \\
&= \langle \gamma_1^{-1}.P_n^{\boldsymbol{v}} + \cdots + \gamma_r^{-1}.P_n^{\boldsymbol{v}}, F_n\rangle = \langle G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}}, F_n\rangle,
\end{aligned}
$$

where $G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}}$ was defined by (2.6). Since the functions $G_{n,\boldsymbol{\gamma}}^{\boldsymbol{v}}$, $\boldsymbol{v} \in \mathbb{S}^{d-1}$, span the whole space $\mathcal{H}_n$ by Lemma 2.4, we must have that $F_n = 0$.

As $n \geqslant 1$ was arbitrary, we have that f is a constant function a.e. (whose value must be $1/r$). This finishes the proof of Theorem 1.1. ∎

Remark 2.5. The statement of Theorem 1.1 remains true also when $\gamma_r = I_d$ and $(\gamma_1, \ldots, \gamma_{r-1})$ is a generic point of $SO(d)^{r-1}$. One way to see this is to run the same proof except the r-th component of each encountered r-tuple of matrices is always set to be the identity matrix I_d.

3. Rotations generating a finite subgroup

Proof of Proposition 1.5. We have to show that an even-dimensional sphere $\mathbb{S}^{d-1}$ is not $(\gamma_1, \ldots, \gamma_r)$-divisible if the subgroup Γ of $SO(d)$ generated by the rotations $\gamma_1, \ldots, \gamma_r$ is finite.

Since d is odd, the 2-divisibility of $\mathbb{S}^{d-1}$ is impossible because of a fixed point of $\gamma_1^{-1}\gamma_2$. So assume that $r \geqslant 3$. Let

$$V := \Gamma.\{\pm \boldsymbol{e}_1, \ldots, \pm \boldsymbol{e}_d\},$$

that is, we take all possible images of the standard basis vectors and their negations when moved by Γ. Clearly, the set V is a finite. Let P be the convex hull of V. Then P is a full-dimensional polytope containing $\mathbf{0}$ in its interior (as already the convex hull of $\{\pm \boldsymbol{e}_1, \ldots, \pm \boldsymbol{e}_d\} \subseteq V$ has these properties). Its boundary ∂P is homeomorphic to $\mathbb{S}^{d-1}$ by the map that sends $\boldsymbol{x} \in \partial P$ to $\boldsymbol{x}/\|\boldsymbol{x}\|_2 \in \mathbb{S}^{d-1}$.

Let a *hyperplane* mean a $(d-1)$-dimensional affine subspace of $\mathbb{R}^d$. Identify each oriented hyperplane $H \subseteq \mathbb{R}^d$ with the pair $(\boldsymbol{n}, a) \in \mathbb{S}^{d-1} \times \mathbb{R}$ so that

$$H = \{\boldsymbol{x} \in \mathbb{R}^d \mid \boldsymbol{n} \cdot \boldsymbol{x} = a\}.$$

Its *open half-spaces* are $H^+ := \{\boldsymbol{x} \in \mathbb{R}^d \mid \boldsymbol{n} \cdot \boldsymbol{x} > a\}$ and $H^- := \{\boldsymbol{x} \in \mathbb{R}^d \mid \boldsymbol{n} \cdot \boldsymbol{x} < a\}$. Call H *supporting* if $H \cap P \neq \emptyset$ and $H^- \cap P = \emptyset$. Call H a *facet hyperplane* if it is supporting and $\dim_{\mathrm{aff}}(H \cap P) = d - 1$, where $\dim_{\mathrm{aff}}(X)$ denotes the dimension of the affine subspace of $\mathbb{R}^d$ spanned by X.

The intersections of supporting hyperplanes with ∂P represent the boundary of the polytope P as a CW-complex. Namely, for $i \in \{0, \ldots, d-1\}$, its i-dimensional cells are precisely the *i-dimensional faces* of P, that is, the convex hulls of the sets in

$$\mathcal{C}_i := \{X \subseteq V \mid \dim_{\mathrm{aff}}(X) = i \text{ and } \exists \text{ supporting hyperplane } H \text{ with } H \cap V = X\}.$$

For a finite non-empty set $X \subseteq \mathbb{R}^d$, let

$$\boldsymbol{m}_X := \frac{1}{|X|} \sum_{\boldsymbol{x} \in X} \boldsymbol{x}$$

be the *centre of mass* of X.

Let $i \in \{0, \ldots, d-1\}$ and $X \in \mathcal{C}_i$. Observe that $\boldsymbol{m}_X \neq 0$ since P is full-dimensional. So we can define $\boldsymbol{n}_X := \boldsymbol{m}_X / \|\boldsymbol{m}_X\|_2$ to be the normalised version of $\boldsymbol{m}_X$. Let us show that for every $Y \in \mathcal{C}_i$ different from X, we have $\boldsymbol{n}_X \neq \boldsymbol{n}_Y$. As it is well known (see, e.g., [11, Theorem 3.1.7]), we can pick facet hyperplanes $H_1, \ldots, H_k$ such that $V \cap (\cap_{j=1}^k H_j) = X$. Since $X \neq Y$, the affine subspaces that these two sets span differ. Since these subspaces have the same dimension, there is $\boldsymbol{y} \in Y$ not in the affine span of X. Since $\boldsymbol{y} \in V$ and each H_j is supporting, there is $j \in [k]$ such that $\boldsymbol{y}$ belongs to the open half-space H_j^+. By $Y \subseteq H_j \cup H_j^+$, we have that $\boldsymbol{m}_Y$ belongs to H_j^+. It follows from $\boldsymbol{m}_Y, \boldsymbol{0} \in H_j^+$ and $\boldsymbol{m}_X \in H_j$ that if $\boldsymbol{n}_X = \boldsymbol{n}_Y$, then $\boldsymbol{m}_Y = c\, \boldsymbol{m}_X$ for some scalar c with $0 < c < 1$. By swapping X and Y in the above argument, we see that $\boldsymbol{n}_X = \boldsymbol{n}_Y$ is impossible, as claimed.

Thus $|M_i| = |\mathcal{C}_i|$, where $M_i := \{\boldsymbol{m}_X / \|\boldsymbol{m}_X\|_2 \mid X \in \mathcal{C}_i\} \subseteq \mathbb{S}^{d-1}$ denotes the set of the normalised centres of mass of the vertex sets of i-dimensional faces. Clearly, the set family $\mathcal{C}_i$ is invariant under the natural action of Γ on finite subsets of $\mathbb{S}^{d-1}$. Thus the set $M_i \subseteq \mathbb{S}^{d-1}$ is also Γ-invariant.

Since d is odd, the Euler characteristic $\chi(\mathbb{S}^{d-1})$ of the $(d-1)$-dimensional sphere is 2; see, e.g., [25, Remark 4.2.21]. Since the faces of ∂P give a representation of the sphere as a CW-complex, we have (by, e.g., [25, Theorem 4.2.20]) that

$$2 = \chi(\mathbb{S}^{d-1}) = \sum_{i=0}^{d-1} (-1)^i |\mathcal{C}_i|.$$

Thus, for at least one $i \in \{0, \ldots, d-1\}$, it holds that $r \geqslant 3$ does not divide $|\mathcal{C}_i| = |M_i|$. By the Γ-invariance of M_i, there is no choice of $A \cap M_i$ such that its translates by $\gamma_1, \ldots, \gamma_r$ partition M_i. Thus $\mathbb{S}^{d-1}$ is not $(\gamma_1, \ldots, \gamma_r)$-divisible. ■

Remark 3.1. Under the assumptions of Proposition 1.5, its proof gives that if there are d linearly independent vectors on $\mathbb{S}^{d-1}$ such that each has a finite orbit under Γ (where some of these orbits may coincide) then $\mathbb{S}^{d-1}$ is not $\boldsymbol{\gamma}$-divisible. However, this seemingly weaker assumption is equivalent to the assumption that Γ is finite (e.g., via a version of Claim 4.2 below).

4. Actions with a finite orbit

Here we prove Proposition 1.6 that, in the presence of at least one finite orbit, $\boldsymbol{\gamma}$-divisibility is equivalent to measurable $\boldsymbol{\gamma}$-divisibility.

Proof of Proposition 1.6. Recall that Γ is the subgroup of $\mathrm{SO}(d)$ generated by $\gamma_1,\ldots,\gamma_r$. For $\boldsymbol{x}\in\mathbb{S}^{d-1}$, let $L_{\boldsymbol{x}}$ be the linear subspace of $\mathbb{R}^d$ spanned by $\Gamma.\boldsymbol{x}\subseteq\mathbb{R}^d$.

Claim 4.1. *For every* $\boldsymbol{x}\in\mathbb{S}^d$*, both* $L_{\boldsymbol{x}}\subseteq\mathbb{R}^d$ *and its orthogonal complement* $L_{\boldsymbol{x}}^{\perp}\subseteq\mathbb{R}^d$ *are invariant under the action of* Γ *on* $\mathbb{R}^d$.

Proof of the claim. Any $\gamma\in\Gamma$ permutes the set $\Gamma.\boldsymbol{x}$. Since γ is a linear map, it preserves the linear subspace $L_{\boldsymbol{x}}$ spanned by $\Gamma.\boldsymbol{x}$. Thus, $L_{\boldsymbol{x}}$ is Γ-invariant.

Since Γ consists of orthogonal matrices, its action preserves the scalar product on $\mathbb{R}^d$. Thus if $\boldsymbol{y}\in\mathbb{R}^d$ is orthogonal to $L_{\boldsymbol{x}}$ then, for every $\gamma\in\Gamma$, we have that $\gamma.\boldsymbol{y}$ is orthogonal to $\gamma.L_{\boldsymbol{x}}=L_{\boldsymbol{x}}$. It follows that $L_{\boldsymbol{x}}^{\perp}$ is Γ-invariant. ■

Recall that $\boldsymbol{z}\in\mathbb{S}^{d-1}$ is a vector such that its orbit $\Gamma.\boldsymbol{z}$ is finite. Let $z_1,\ldots,z_n$ be the elements of $\Gamma.\boldsymbol{z}$.

Claim 4.2. *If* $\boldsymbol{x}\in L_{\boldsymbol{z}}\cap\mathbb{S}^{d-1}$ *then* $|\Gamma.\boldsymbol{x}|\leqslant n!$.

Proof of the claim. Write $\boldsymbol{x}\in L_{\boldsymbol{z}}$ as $\sum_{i=1}^n c_i\boldsymbol{z}_i$ for some reals $c_1,\ldots,c_n$. For every $\alpha\in\Gamma$, we have by linearity that $\alpha.\boldsymbol{x}=\sum_{i=1}^n c_i(\alpha.\boldsymbol{z}_i)$. Since $\boldsymbol{z}_1,\ldots,\boldsymbol{z}_n$ enumerate a whole orbit of Γ, the element $\alpha\in\Gamma$ permutes these vectors. Thus every element of $\Gamma.\boldsymbol{x}$ is of the form $\sum_{i=1}^n c_i\boldsymbol{z}_{\sigma(i)}$ for some permutation σ of $[n]$. Thus $\Gamma.\boldsymbol{x}$ indeed has at most $n!$ elements. ■

Now we are ready to prove the (non-trivial) forward direction of Proposition 1.6. By rotating the sphere (and moving $\boldsymbol{z}$ and conjugating γ_i's accordingly), we can assume that $L_{\boldsymbol{z}}=\mathbb{R}^m\times\mathbf{0}$ and $L_{\boldsymbol{z}}^{\perp}=\mathbf{0}\times\mathbb{R}^{d-m}$ for some $m\in[d]$. By Claim 4.1, every matrix γ_i, $i\in[r]$, consists now of two diagonal blocks that correspond to some $\alpha_i\in\mathrm{O}(m)$ and $\beta_i\in\mathrm{O}(d-m)$. (Note that these matrices may have determinant -1.) When we write a vector in $\mathbb{R}^d$ as $(\boldsymbol{x},\boldsymbol{y})$, we mean that $\boldsymbol{x}\in\mathbb{R}^m$ and $\boldsymbol{y}\in\mathbb{R}^{d-m}$; thus,

$$\gamma_i.(\boldsymbol{x},\boldsymbol{y})=(\alpha_i.\boldsymbol{x},\beta_i.\boldsymbol{y}).$$

Fix $C\subseteq\mathbb{S}^{d-1}$ such that $\gamma_1.C,\ldots,\gamma_r.C$ partition $\mathbb{S}^{d-1}$. By the invariance of $L_{\boldsymbol{z}}$ and $L_{\boldsymbol{z}}^{\perp}$, the translates of the set $C\cap(\mathbb{R}^m\times\mathbf{0})$ (resp. $C\cap(\mathbf{0}\times\mathbb{R}^{m-d})$) by $\gamma_1,\ldots,\gamma_r$ partition $\mathbb{S}^{m-1}\times\mathbf{0}$ (resp. $\mathbf{0}\times\mathbb{S}^{d-m-1}$). By Claim 4.2, every orbit of the action of Γ on the invariant subset $X:=\mathbb{S}^{m-1}\times\mathbf{0}$ has at most $n!$ elements. Obviously, the same holds for the action on $\mathbb{S}^{m-1}$ of the subgroup $\Gamma'\subseteq\mathrm{O}(m)$ generated by $\alpha_1,\ldots,\alpha_r$. Fix a Borel total order on $\mathbb{S}^{m-1}$ (e.g., the restriction of the lexicographic order on $\mathbb{R}^m$) and let $A' \subseteq X$ be obtained by picking from every orbit $\Gamma'.\boldsymbol{x} \subseteq \mathbb{S}^{m-1}$ the lexicographically smallest subset such that its translates by $\alpha_1, \dots, \alpha_r$ partition $\Gamma'.\boldsymbol{x}$. Such a set always exists since $\{\boldsymbol{y} \in \Gamma'.\boldsymbol{x} \mid (\boldsymbol{y}, \mathbf{0}) \in C\}$ is one possible choice. In the terminology of [21], the set A' can be computed by a local rule of radius $n!$ on the *coloured Schreier digraph* of $\Gamma' \curvearrowright \mathbb{S}^{m-1}$ (where the vertex set is $\mathbb{S}^{d-1}$ and we put a directed colour-i arc from $\boldsymbol{y}$ to $\alpha_i.\boldsymbol{y}$ for all $\boldsymbol{y} \in \mathbb{S}^{m-1}$ and $i \in [r]$). As the action is Borel, this is known to imply (see, e.g., [21, Lemma 5.17]) that the constructed set $A' \subseteq \mathbb{S}^{m-1}$ is Borel. Define

$$
\begin{aligned}
A &:= \bigcup_{\rho \in [0,1)} \left(\sqrt{1-\rho^2}\, A' \times \rho \mathbb{S}^{d-m-1}\right) \\
&= \bigcup_{\rho \in [0,1)} \left\{\left(\sqrt{1-\rho^2}\, \boldsymbol{x}, \rho \boldsymbol{y}\right) \mid \boldsymbol{x} \in A', \boldsymbol{y} \in \mathbb{S}^{d-m-1}\right\}
\end{aligned}
$$

and

$$
B := C \cap (\mathbf{0} \times \mathbb{R}^{m-d}).
$$

Then $\gamma_1.A, \dots, \gamma_r.A$ partition $\mathbb{S}^{d-1} \setminus (\mathbf{0} \times \mathbb{S}^{d-m-1})$ and, as we observed earlier, $\gamma_1.B, \dots, \gamma_r.B$ partition $\mathbf{0} \times \mathbb{S}^{d-m-1}$. Thus $A \cup B$ witnesses the $\boldsymbol{\gamma}$-divisibility of $\mathbb{S}^{d-1}$. Note that the set B, which lies inside the intersection of $\mathbb{S}^{d-1}$ with the linear subspace $L_{\boldsymbol{z}}^{\perp}$ of dimension less than d, has measure zero. On the other hand, the set A can be equivalently defined as the pre-image of the Borel set $A' \times \mathbb{R}^{d-m}$ under the natural homeomorphism between $\mathbb{S}^{d-1} \setminus (\mathbf{0} \times \mathbb{S}^{d-m-1})$ and $\mathbb{S}^{m-1} \times \mathbb{R}^{d-m}$ that maps $(\boldsymbol{x}, \boldsymbol{y})$ to $(\boldsymbol{x}/\|\boldsymbol{x}\|_2, \boldsymbol{y}/\|\boldsymbol{x}\|_2)$. Thus, A is Borel and $A \cup B$ is measurable, proving the proposition. ∎

Remark 4.3. One can show via Claims 4.1 and 4.2 that if $d = 3$ and a subgroup $\Gamma \subseteq \mathrm{SO}(d)$ has a finite orbit of size at least 3, then Γ is finite (and thus Proposition 1.5 applies). However, this implication is not true in general for $d \geqslant 4$. For example, we can take the subgroup of $\mathrm{SO}(d)$ generated by a diagonal block matrix M whose first (resp. second) block is a 2×2 special orthogonal matrix of order 3 (resp. of infinite order), while all remaining blocks are the 1×1 identity matrices. Then M has an infinite order (coming from the second block) but its action on $\mathbb{S}^{d-1}$ has an orbit with exactly 3 elements (e.g., the orbit of the first standard basis vector $(1, 0, \dots, 0)$).

5. Measurable divisibility of higher-dimensional spheres

As we mentioned in the Introduction, $\mathbb{S}^{d-1}$ is r-divisible with Borel pieces for every $r \geqslant 2$ and even $d \geqslant 2$ ([23, Theorem 6.6 (a)]). The proof of [23, Theorem 6.6 (b)] for any $r \geqslant 3$ and odd $d \geqslant 5$ gives measurable pieces. Since this conclusion does not seem to be explicitly stated anywhere in [23], we provide the simple proof from [23].

Lemma 5.1. *For any $d \geqslant 5$ and $r \geqslant 3$, $\mathbb{S}^{d-1}$ is r-divisible with measurable pieces.*

Proof. Informally speaking, we will use the Borel r-divisibility of $\mathbb{S}^1$ in the last two coordinates of $\mathbb{S}^{d-1} \subseteq \mathbb{R}^d$, resorting to the r-divisibility of $\mathbb{S}^{d-3}$ only on the null set of points where the last two coordinates are zero.

Namely, choose rotations $\alpha_1, \ldots, \alpha_r \in \mathrm{SO}(d-2)$ and a (not necessarily measurable) subset $A \subseteq \mathbb{S}^{d-3}$ such that $\alpha_1.A, \ldots, \alpha_r.A$ partition $\mathbb{S}^{d-3}$, which is possible by, e.g., [23, Theorem 6.6]. Let $\beta \in \mathrm{SO}(2)$ be the rotation of the circle $\mathbb{S}^1$ by the angle $2\pi/r$. (Thus the order of β, as an element of the group SO(2), is r.) For $i \in [r]$, let γ_i send $(\boldsymbol{x}, \boldsymbol{y}) \in \mathbb{R}^{d-2} \times \mathbb{R}^2$ to $(\alpha_i.\boldsymbol{x}, \beta^i.\boldsymbol{y})$, where we view $\mathrm{SO}(m)$ as also acting on $\mathbb{R}^m$. Clearly, γ_i preserves both the scalar product on $\mathbb{R}^d$ and the orientation; thus it is an element of $\mathrm{SO}(d)$.

Let $B := \{(\cos\theta, \sin\theta) \mid 0 \leqslant \theta < 2\pi/r\} \subseteq \mathbb{S}^1$. Then the half-open arcs $\beta.B, \ldots, \beta^r.B$ partition $\mathbb{S}^1$. Let $C := A' \cup B'$, where $A' := A \times \{(0,0)\}$ and

$$B' := \bigcup_{\rho \in [0,1)} \left(\rho\, \mathbb{S}^{d-3} \times \sqrt{1-\rho^2}\, B\right).$$

Clearly, A' is a μ-null subset of $\mathbb{S}^{d-1}$ and B' is a Borel subset of $\mathbb{S}^{d-1}$. Thus, C is measurable. Also, $\gamma_1.C, \ldots, \gamma_r.C$ partition $\mathbb{S}^{d-1}$. Indeed,

$$\gamma_i.A' = \alpha_i.A \times \{(0,0)\}, \quad i \in [r],$$

partition $\mathbb{S}^{d-3} \times \{(0,0)\}$, while

$$\gamma_i.B' = \cup_{\rho \in [0,1)} \left(\rho \mathbb{S}^{d-3} \times \sqrt{1-\rho^2}\, (\beta^i.B)\right), \quad i \in [r],$$

partition the rest of $\mathbb{S}^{d-1}$. ∎

6. Measurable divisibility for $d = 2$ and $r \leqslant 4$

We parametrise $\mathbb{S}^1 = \{(\cos t, \sin t) \mid t \in [0, 2\pi)\}$ and use the parameter t instead of the Cartesian coordinates. Thus we have the interval $[0, 2\pi)$ with μ being the Lebesgue measure on it. The space $\mathcal{H}_n$ for $n \geqslant 1$ becomes the span of $\cos nt$ and $\sin nt$ (while, of course, $\mathcal{H}_0$ consists of all constant functions). Here, the harmonic expansion is nothing else as the Fourier series. We identify SO(2) with the additive group $\mathbb{T} := \mathbb{R}/2\pi\mathbb{Z}$ of reals taken modulo 2π. Thus the action of $\gamma \in \mathbb{T}$ on $[0, 2\pi)$ is to send $t \in [0, 2\pi)$ to $t + \gamma \pmod{2\pi}$. We also identity $[0, 2\pi)$ with $\mathbb{T}$; thus we have the natural action $\mathbb{T} \curvearrowright \mathbb{T}$.

Let us investigate various possible versions of "measurable" divisibility, stated in terms of the action $\mathbb{T} \curvearrowright \mathbb{T}$. Let $\mathcal{B}_r$ (resp. $\mathcal{M}_r$) consist of those r-tuples $(t_1, \ldots, t_r) \in \mathbb{T}^r$

for which there is a Borel (resp. measurable) subset $A \subseteq \mathbb{T}$ such that $t_1 + A, \dots, t_r + A$ partition $\mathbb{T}$, where we denote $t + A := \{t + a \mid a \in A\}$. Also, let $\mathcal{M}_r'$ consist of those $(t_1, \dots, t_r) \in \mathbb{T}^r$ for which there is a measurable (equivalently, Borel) $A \subseteq \mathbb{T}$ such that the translates $t_1 + A, \dots, t_r + A$ are pairwise disjoint and the set of elements of $\mathbb{T}$ not covered by them has measure zero. Finally, let $\mathcal{F}_r$ consist of those $(t_1, \dots, t_r) \in \mathbb{T}^r$ for which there is $f \in L^2([0, 2\pi), \mu)$ such that $t_1.f + \dots + t_r.f = 1$ a.e., while $f \neq 1/r$ on a set of positive measure. As it is easy to see, the definition of $\mathcal{F}_r$ does not change if we require $t_1.f + \dots + t_r.f = 1$ to hold everywhere. Trivially, it holds that

$$\mathcal{B}_r \subseteq \mathcal{M}_r \subseteq \mathcal{M}_r' \subseteq \mathcal{F}_r.$$

First, we investigate $\mathcal{F}_r$. Suppose that we have some $f \in L^2([0, 2\pi), \mu)$ such that $t_1.f + \dots + t_r.f = 1$ a.e. Take the Fourier series,

$$f(t) = c_0 + \sum_{n=1}^{\infty} (c_n \cos nt + s_n \sin nt) \quad \text{for a.e. } t \in [0, 2\pi).$$

Clearly, $c_0 = 1/r$. For $i \in [r]$, by translating everything by t_i, we get that

$$(t_i.f)(t) = \frac{1}{r} + \sum_{n=1}^{\infty} \big(c_n \cos n(t - t_i) + s_n \sin n(t - t_i)\big) \quad \text{for a.e. } t \in [0, 2\pi).$$

Summing this up for all $i \in [r]$ and using the formula for the sine and the cosine of a difference of two angles, we get that for a.e. $t \in [0, 2\pi)$,

$$\begin{aligned} 1 = 1 + \sum_{i=1}^{r} \Bigg(\sum_{n=1}^{\infty} & c_n (\cos nt \cos nt_i + \sin nt \sin nt_i) \\ & + s_n (\sin nt \cos nt_i - \cos nt \sin nt_i) \Bigg) \\ = 1 + \sum_{n=1}^{\infty} \Bigg(& \sum_{i=1}^{r} (c_n \cos nt_i - s_n \sin nt_i) \cos nt \\ & + \sum_{i=1}^{r} (c_n \sin nt_i + s_n \cos nt_i) \sin nt \Bigg). \end{aligned}$$

(Recall that $\sum_{i=1}^{r} t_i.f = 1$ a.e.)

Let $n \geqslant 1$. By the uniqueness of the Fourier coefficients, we have that

$$\sum_{i=1}^{r} (c_n \cos nt_i - s_n \sin nt_i) = 0 \quad \text{and} \quad \sum_{i=1}^{r} (c_n \sin nt_i + s_n \cos nt_i) = 0.$$

Suppose that $(c_n, s_n) \neq (0,0)$. If we multiply the above equations by c_n and s_n (resp. by $-s_n$ and c_n) and add up, we get after dividing by $c_n^2 + s_n^2$ that

$$\sum_{i=1}^{r} \cos nt_i = 0 \quad \text{and} \quad \sum_{i=1}^{r} \sin nt_i = 0, \tag{6.1}$$

that is, the vectors $(\cos nt_i, \sin nt_i) \in \mathbb{R}^2$, $i \in [r]$, sum up to zero.

If f differs from $1/r$ on a set of positive measure then, for at least one integer $n \geqslant 1$, we have $(c_n, s_n) \neq (0,0)$, and thus (6.1) holds. Conversely, if (6.1) holds for some $n \geqslant 1$, then we can take, for example,

$$f(t) := (1 + \cos nt)/r$$

for $t \in [0, 2\pi)$. This completely describes the set of r-tuples in SO(2) for which the circle $\mathbb{S}^1$ is "fractionally" divisible.

Proposition 6.1. *An r-tuple $(t_1, \ldots, t_r) \in \mathbb{T}^r$ belongs to $\mathcal{F}_r$ if and only if (6.1) holds for at least one integer $n \geqslant 1$.* ■

Let us investigate the sets $\mathcal{B}_r$ and $\mathcal{M}'_r$ for $r \leqslant 4$. As we will see, it holds for each $r \leqslant 4$ that $\mathcal{B}_r = \mathcal{M}'_r$ (and, in particular, this set is also equal to $\mathcal{M}_r$).

Let $(t_1, \ldots, t_r) \in \mathbb{T}^r$. By replacing $(t_1, \ldots, t_r)$ by $(t_1 - t_r, \ldots, t_r - t_r)$, which does not affect divisibility, we can assume for convenience that $t_r = 0$. Since $\mathcal{M}'_r \subseteq \mathcal{F}_r$, assume that (6.1) holds for some $n \geqslant 1$. Let $n \geqslant 1$ be the smallest integer with this property.

Suppose first that $r = 2$. By (6.1) we have $nt_1 = (2k+1)\pi$ for some integer $k \geqslant 0$. Note that n and $2k+1$ are coprime: if an integer $q > 1$ divides both n and $2k+1$ then, for $n' := n/q$, we have $n't_1 = (2k+1)\pi/q$, and thus (6.1) holds for $n' < n$, contradicting the minimality of n. Therefore, the subgroup of $\mathbb{T}$ generated by $t_1 = (2k+1)\pi/n$ is $\{\pi m/n \mid m \in \{0, \ldots, 2n-1\}\}$, which is the additive cyclic group of order $2n$ with t_1 corresponding to an odd multiple of the generator π/n. Since the addition of t_1 swaps odd and even multiples of π/n, we have that

$$A := \left\{\frac{\pi m}{n} \mid m \in \{0, 2, \ldots, 2n-2\}\right\} + \left[0, \frac{\pi}{n}\right)$$

satisfies $t_1 + A = [0, 2\pi) \setminus A$ and shows that $(r_1, 0) \in \mathcal{B}_2$, where for $B, C \subseteq \mathbb{T}$ we denote

$$B + C := \{b + c \mid b \in B, c \in C\}.$$

Thus $\mathcal{B}_2 = \mathcal{M}_2 = \mathcal{M}'_2 = \mathcal{F}_2$, and this set can be equivalently described as consisting of precisely those $(t_1, t_2) \in \mathbb{T}^2$ such that $t_2 - t_1 \in \mathbb{T}$ generates a finite subgroup of even order.

Suppose that $r = 3$. Three vectors on the unit circle sum to $\mathbf{0}$ if and only if they form an equilateral triangle. (Indeed, the sum of any two unit vectors has norm 1 if and only if the angle between the vectors is $2\pi/3$.) Thus, up to swapping t_1 and t_2, we can assume that $nt_1 \equiv 2\pi/3$ and $nt_2 \equiv 4\pi/3$ modulo 2π. Each of $t_1, t_2 \in [0, 2\pi)$ is a (non-zero) integer multiple of $2\pi/(3n)$. Let $k_1, k_2 \in [3n-1]$ satisfy $t_i = 2\pi k_i/(3n)$. By the minimality of n, the greatest common divisor $\gcd(k_1, k_2, n) = 1$. Furthermore, it is impossible that 3 divides both k_1 and k_2, for otherwise by, e.g., $2\pi k_1/(3n) \equiv 2\pi/3 \pmod{2\pi}$ we have that 3 also divides n, a contradiction to $\gcd(k_1, k_2, n) = 1$. Therefore, the subgroup generated by $t_1, t_2 \in \mathbb{T}$ is $\{\frac{2\pi k}{3n} \mid k \in \{0, \dots, 3n-1\}\}$, which is the cyclic group of order $3n$. For $i = 1, 2$, we have $k_i n \equiv in \pmod{3n}$ and thus $k_i \equiv i \pmod 3$. Thus if we take

$$A := \left\{\frac{2\pi m}{3n} \mid m \in \{0, 3, \dots, 3n-3\}\right\} + \left[0, \frac{2\pi}{3n}\right),$$

then $t_1 + A$, $t_2 + A$ and $t_3 + A = A$ partition $[0, 2\pi)$. We conclude that $\mathcal{B}_3 = \mathcal{M}_3 = \mathcal{M}'_3 = \mathcal{F}_3$ and this set can be alternatively described as consisting, up to a permutation of indices, precisely of the triples

$$\left(\frac{2\pi k_1}{3n} + t, \frac{4\pi k_2}{3n} + t, t\right)$$

with $n \geqslant 1$, $k_1, k_2 \in [3n-1]$ and $t \in \mathbb{T}$ such that $\{k_1, k_2\} \equiv \{1, 2\} \pmod 3$ and the greatest common divisor of k_1, k_2 and n is 1.

Suppose that $r = 4$. We need the following geometric claim.

Claim 6.2. *Four vectors $(x_i, y_i) \in \mathbb{S}^1$, $i \in [4]$, have sum $\mathbf{0}$ if and only if they can be split into two pairs of opposite vectors.*

Proof of the claim. The non-trivial direction of the claim can be derived by observing that, up to a permutation of indices, we can assume that $\boldsymbol{v} := (x_1, y_1) + (x_2, y_2)$ is a non-zero vector while, in general, there is at most one way to write $-\boldsymbol{v} \in \mathbb{R}^2 \setminus \{\mathbf{0}\}$ as the unordered sum of two unit vectors. Thus the other two vectors must be $(-x_1, -y_1)$ and $(-x_2, -y_2)$, as desired. ■

Recall that $n \geqslant 1$ is the smallest integer satisfying (6.1). Claim 6.2 applied to $x_i := \cos(nt_i)$ and $y_i := \sin(nt_i)$ for $i \in [4]$ gives that, up to a permutation of indices, $(x_1, y_1) = -(x_2, y_2)$ and $(x_3, y_3) = -(x_4, y_4)$. Thus, by Proposition 6.1, the set $\mathcal{F}_4$ consists precisely of those $(t_1, \dots, t_4)$ such that, for some integer $n \geqslant 1$ and up to a permutation of indices, we have that

$$n(t_1 - t_2) \equiv n(t_3 - t_4) \equiv \pi \pmod{2\pi}. \tag{6.2}$$

Again, let us assume that $t_4 = 0$.

First, let us show that if t_1/π is irrational then $(t_1, \dots, t_4) \notin \mathcal{M}'_4$. By (6.2), we can assume that $t_2 = t_1 + k_2\pi/n$ and $t_3 = k_3\pi/n$ for some odd integers k_2 and k_3. Suppose for a sake of contradiction that for some measurable subset $A \subseteq \mathbb{T}$ we have that $\sum_{i=1}^4 t_i.\mathbb{1}_A = 1$ a.e. Take the Fourier expansion

$$\mathbb{1}_A(t) = \frac{1}{4} + \sum_{m=1}^{\infty} (c_m \cos mt + s_m \sin mt).$$

By the argument leading to (6.1) and Claim 6.2, we see that (c_m, s_m) can be non-zero only if we can split $(mt_1, \dots, mt_4) \in \mathbb{T}^4$ into two pairs, each pair having difference π. Since t_1/π is irrational, these pairs must be (t_1, t_2) and (t_3, t_4) by (6.2). Thus $mk_i\pi/n \equiv \pi \pmod{2\pi}$ for $i = 2, 3$. Clearly, the validity of these two equations is determined by the residue of m modulo n. Since n is minimal, these equations cannot both hold for any $m \in [n-1]$. Thus they can hold only if m is a multiple of n. This means that all non-zero Fourier terms of $\mathbb{1}_A$ have period $2\pi/n$ as functions $\mathbb{T} \to \mathbb{R}$. It follows that $A = (2\pi k/n) + A$ a.e. for every integer k and $\mathbb{1}_A = \frac{1}{n}\sum_{k=0}^{n-1}(2\pi k/n).\mathbb{1}_A$. Thus,

$$\begin{aligned} t_1.\mathbb{1}_A + \mathbb{1}_A &= \frac{1}{n}\sum_{k=0}^{n-1}\big((t_1 + 2\pi k/n).\mathbb{1}_A + (2\pi k/n).\mathbb{1}_A\big) \\ &= \frac{1}{2n}\sum_{k=0}^{n-1}(2\pi k/n).\big(t_1.\mathbb{1}_A + t_2.\mathbb{1}_A + t_3.\mathbb{1}_A + t_4.\mathbb{1}_A\big) = \frac{1}{2} \quad \text{a.e.,} \end{aligned}$$

where we used that $t_1.\mathbb{1}_A + t_2.\mathbb{1}_A + t_3.\mathbb{1}_A + t_4.\mathbb{1}_A = 1$ a.e. by the choice of A. We conclude that the function $2\,\mathbb{1}_A$ demonstrates that $(t_1, 0) \in \mathcal{F}_2$. By the case $r = 2$ that was solved earlier, this contradicts the irrationality of t_1/π.

This gives that $\mathcal{M}'_4$ is strictly smaller than $\mathcal{F}_4$: for example, $(a, a+\pi, \pi, 0)$ belongs to $\mathcal{F}_4 \setminus \mathcal{M}'_4$ if a/π is irrational.

Now, suppose that t_1/π is rational. Let Γ be the subgroup of $\mathbb{T}$ that is generated by t_1, t_2 and t_3. (There is no need to add t_4 as it is 0.) By (6.2) and the rationality of t_1/π, the group Γ is finite. Of course, if 4 does not divide its order $|\Gamma|$ then there is no $\boldsymbol{t}$-division even if a null set can be removed. So suppose that $|\Gamma| = 4m$ for some integer m, i.e., that Γ is the cyclic group of order $4m$. For $i \in [4]$, let $k_i \in \{0, \dots, 4m-1\}$ satisfy that $t_i = \frac{\pi k_i}{2m}$. Let $\boldsymbol{k} := (k_1, \dots, k_4)$. Let us say that the cyclic group $\mathbb{Z}_{4m}$, that consists of integer residues modulo $4m$, is *$\boldsymbol{k}$-divisible* if there is a subset $A \subseteq \mathbb{Z}_{4m}$ such that the sets $k_i + A$, $i \in [4]$, partition $\mathbb{Z}_{4m}$. Of course, such a set A must have exactly m elements.

The following claim implies in particular that $\mathcal{B}_4 = \mathcal{M}_4 = \mathcal{M}'_4$.

Claim 6.3. *If* $\mathbb{Z}_{4m}$ *is* $\boldsymbol{k}$*-divisible then* $\boldsymbol{t} \in \mathcal{B}_4$*; otherwise,* $\boldsymbol{t} \notin \mathcal{M}'_4$*.*

Proof of the claim. Suppose first that a subset $A \subseteq \mathbb{Z}_{4m}$ witnesses the $(k_1, \ldots, k_4)$-divisibility of $\mathbb{Z}_{4m}$. It corresponds to an m-subset $B \subseteq [0, 2\pi)$ such that its translates by $t_1, \ldots, t_4$ partition the subgroup $\Gamma \subseteq \mathbb{T}$. Now the Borel set $C := B + [0, \frac{\pi}{2m})$ exhibits the $\boldsymbol{t}$-divisibility of $\mathbb{T}$.

Conversely, suppose that $\mathbb{Z}_{4m}$ is not $\boldsymbol{k}$-divisible. Take any measurable set $C \subseteq [0, 2\pi)$ such that its translates by $t_1, \ldots, t_4$ are pairwise disjoint. Take any coset $X := t + \Gamma \subseteq \mathbb{T}$ of Γ. Define A to consist of those $k \in \mathbb{Z}_{4m}$ such that $t + \frac{\pi k}{2m} \in C$ (that is, A encodes the intersection of C with the Γ-coset X). The translates of A by $k_1, \ldots, k_4$ in $\mathbb{Z}_{4m}$ (which correspond to the intersections $(t_i + C) \cap X$, $i \in [4]$) are pairwise disjoint and, by our assumption, omit at least one element of $\mathbb{Z}_{4m}$. Thus every coset of Γ in $\mathbb{T}$ contains at least one element of $B := \mathbb{T} \setminus (\{t_1, \ldots, t_4\} + C)$. It follows that B has measure at least $2\pi/(4m)$ (as its translates by $\frac{\pi k}{2m}$ for $k \in \{0, \ldots, 4m-1\}$ cover $\mathbb{T}$). This implies that $\boldsymbol{t} \notin \mathcal{M}'_4$. ∎

Unfortunately, an explicit characterization of the set $\mathcal{B}_4 = \mathcal{M}_4 = \mathcal{M}'_4$ for general n seems to be rather messy, although it reduces to a finite case analysis for any given $\boldsymbol{t} \in \mathbb{T}^4$ by Claim 6.3. So we will restrict ourselves to the special cases $n = 1$ and $n = 2$, just to illustrate that the measurable $\boldsymbol{t}$-divisibility is not determined by the order $4m$ of the group Γ alone (which happens already for $n = 2$).

First, assume that $n = 1$. By (6.2), we have up to a permutation that

$$(t_1, t_2, t_3) \equiv (a, a + \pi, \pi) \pmod{2\pi}$$

with $a \notin \{0, \pi\}$. Thus, working inside $\mathbb{Z}_{4m}$ (that is, modulo $4m$), we have that $k_2 = k_1 + 2m$ and $k_3 = 2m$. Since $k_1, k_1 + 2m, 2m$ generate $\mathbb{Z}_{4m}$, we have that k_1 and $2m$ are coprime; in particular k_1 is odd. As it is easy to see $A := \{2i \mid i \in \{0, \ldots, m-1\}\}$ witnesses the $\boldsymbol{k}$-divisibility of $\mathbb{Z}_{4m}$. Thus $\boldsymbol{t} \in \mathcal{B}_4$ by Claim 6.3.

Now, assume that $n = 2$. By (6.2), we have that each of the differences $k_1 - k_2$ and $k_3 - k_4$ modulo $4m$ is either m or $3m$. We can assume that $k_3 = m$ (by negating all k_i's if necessary) and that $k_2 = k_1 + m$ (by swapping k_1 and k_2 if necessary). Note that these operations do not affect the $\boldsymbol{k}$-divisibility of $\mathbb{Z}_{4m}$ and thus the conclusion of Claim 6.3 is also unaffected. Let $k := k_1$. Thus,

$$\boldsymbol{k} = (k, k + m, m, 0).$$

First, let us show that if $m = 2s$ is even then $\mathbb{Z}_{4m}$ is $\boldsymbol{k}$-divisible (and thus $\boldsymbol{t} \in \mathcal{B}_4$ by Claim 6.3). It is enough to find an s-set $S \subseteq \{0, \ldots, m-1\}$ such that, modulo m, the sets S and $k + S$ partition $\mathbb{Z}_m$ (because then $A := S \cup (2m + S)$ as a subset of $\mathbb{Z}_{4m}$ witnesses the $\boldsymbol{k}$-divisibility of $\mathbb{Z}_{4m}$). Note that $S := \{2ik \mid i \in \{0, \ldots, s-1\}\}$ works.

(Indeed, by $\gcd(k, m) = 1$ each residue modulo m appears exactly once as ik with $i \in \{0, \ldots, m-1\}$ and we have included every second multiple of k into the set S.)

Finally, suppose that m is odd. Recall that $\gcd(k, m) = 1$. We claim that $\mathbb{Z}_{4m}$ is $\boldsymbol{k}$-divisible if and only if $k \equiv 2 \pmod 4$.

First, suppose that an m-set $A \subseteq \mathbb{Z}_{4m}$ witnesses the $\boldsymbol{k}$-divisibility. Since m is odd, some residue i modulo m appears an odd number of times in A. This multiplicity cannot be larger than 2 since otherwise the translates $k_1 + A, \ldots, k_4 + A$ would cover the four points

$$i,\ i+m,\ i+2m,\ i+3m \in \mathbb{Z}_{4m}$$

at least six times. Thus the multiplicity of i in A modulo m is exactly 1. By the commutativity of $\mathbb{Z}_{4m}$, we can replace A by any its translate. Thus assume that A contains 0 but none of m, $2m$ and $3m$. Thus, by $(k_3, k_4) = (m, 0)$, the set $(k_3 + A) \cup (k_4 + A)$ covers 0 and m but not $2m$ nor $3m$. Since $2m \notin A$, the only way to consistently cover $2m$ and $3m$ is that $2m - k \in A$. Now, $\{k_1, \ldots, k_4\} + \{0, 2m - k\}$ contains $2m - k$ and $3m - k$ but not $-k$ nor $m - k$. None of the last two elements can be covered by $k_3 + A$ or $k_4 + A$ (as then A modulo m would contain $-k \pmod m$ at least twice but then the four elements $0, m, 2m, 3m$ would be covered at least six times, with the extra multiplicity coming from 0 and m being covered by $0 \in A$ when translated by k_3 and k_4). Thus the only way to consistently cover $-k$ and $m - k$ is that $-2k \in A$. One can continue to argue in this manner, showing that for each $i \in \{0, 1, \ldots\}$ we have $-2ik \in A$ and $-(2i+1)k + 2m \in A$. As the first m of these elements of A are pairwise distinct (in fact, they have pairwise distinct residues modulo m) and m is odd, it must hold that the m-th element, $-mk + 2m$, belongs to A. Since A does not contain any of m, $2m$ and $3m$, we necessarily have that $-mk + 2m \equiv 0 \pmod{4m}$. This equation has m solutions, namely, all $k \in \mathbb{Z}_{4m}$ with $k \equiv 2 \pmod 4$, giving the claim.

Conversely, if $k \equiv 2 \pmod 4$, then the set A consisting of elements $-2ik$ for $i \in \{0, \ldots, (m-1)/2\}$ and $-(2i+1)k + 2m$ for $i \in \{0, \ldots, (m-3)/2\}$ shows the $\boldsymbol{k}$-divisibility of $\mathbb{Z}_{4m}$. Indeed, note that $|A| = m$ (as its elements have different residues modulo m by $\gcd(k, m) = 1$) and that if we keep increasing the index i beyond the stated ranges then we just repeat the elements of A since $-mk + 2m \equiv 0 \pmod{4m}$. By "reverse engineering" the proof of the forward implication, we see that the translates of A by $k_1, \ldots, k_4$ are pairwise disjoint and thus partition $\mathbb{Z}_{4m}$, as required.

In the initial version of the manuscript, we conjectured that if $(t_1, \ldots, t_r) \in \mathcal{M}'_r$ then $(t_i - t_j)/\pi$ is rational for every $i, j \in [r]$. This conjecture was subsequently proved by Grebík, Greenfeld, Rozhoň and Tao [9]. This implies that $\mathcal{B}_r = \mathcal{M}_r = \mathcal{M}'_r$ for every r (by an argument similar to that of Proposition 1.6) and reduces the question if any given $\boldsymbol{t} \in \mathbb{T}^r$ belongs to this set to some finite case analysis.

7. Proof of Proposition 1.2

In order to prove Proposition 1.2, we need some auxiliary results first.

Lemma 7.1. *The kernels of real $n_i \times n$ matrices A_i, $i \in [k]$, contain a common non-zero vector $\boldsymbol{x} \in \mathbb{R}^n \setminus \{\boldsymbol{0}\}$ if and only if the $n \times n$ matrix $M := \sum_{i=1}^{k} A_i^T A_i$ has zero determinant.*

Proof. If some non-zero $\boldsymbol{x} \in \mathbb{R}^n$ satisfies $A_i \boldsymbol{x} = \boldsymbol{0}$ for every $i \in [k]$, then

$$M\boldsymbol{x} = \sum_{i=1}^{k} A_i^T (A_i \boldsymbol{x}) = \boldsymbol{0},$$

so the determinant of M is zero.

Conversely, suppose that M is singular. Choose a non-zero vector $\boldsymbol{x} \in \mathbb{R}^n$ with $M\boldsymbol{x} = \boldsymbol{0}$. Then

$$0 = \boldsymbol{x} \cdot M\boldsymbol{x} = \sum_{i=1}^{k} \boldsymbol{x} \cdot (A_i^T A_i \boldsymbol{x}) = \sum_{i=1}^{k} (A_i \boldsymbol{x}) \cdot (A_i \boldsymbol{x}) = \sum_{i=1}^{k} \|A_i \boldsymbol{x}\|_2^2$$

and each $A_i \boldsymbol{x}$ must be the zero vector, giving the required. ■

The results of Dekker [6], Deligne and Sullivan [8], and Borel [3] (see [23, Theorem 6.4] and the historical discussion preceding it) give the following.

Lemma 7.2. *For every $d \geqslant 2$ and $r \geqslant 2$ there is a choice of rotations $\beta_1, \dots, \beta_r \in$ $\mathrm{SO}(d)$ that generate the free rank-r group F_r such that its action on $\mathbb{S}^{d-1}$ is free for even d and* locally commutative *for odd d (meaning that every two elements of F_r that have a common fixed element on $\mathbb{S}^{d-1}$ commute).* ■

Note that the above result is usually stated in the special case $r = 2$ as the general case easily follows by taking any subgroup of F_2 isomorphic to F_r.

Lemma 7.3. *If $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$ is generic, then the rotations $\gamma_1, \dots, \gamma_r$ generate the free rank-r group F_r and the corresponding action of F_r on $\mathbb{S}^{d-1}$ is free for even d and locally commutative for odd d.*

Proof. For a non-trivial reduced word w in F_r and $\boldsymbol{\beta} = (\beta_1, \dots, \beta_r) \in \mathrm{SO}(d)^r$, the relation $w(\boldsymbol{\beta}) = I_d$ amounts to d^2 polynomial equations, with $p_{ij}(\boldsymbol{\beta}) = 0$ stating that the (i, j)-th entry of the corresponding product of the matrices of β_i's and their transposes (which are equal to their inverses) is $\mathbb{1}_{i=j}$, where $\mathbb{1}_{i=j}$ is 1 if $i = j$, and 0 otherwise. Each of these polynomials p_{ij} has rational coefficients. Moreover, the r-tuple of matrices $\boldsymbol{\beta}$ returned by Lemma 7.2 (which, in particular, generates the free subgroup) gives a point where at least one of these polynomials is non-zero, say $p_{ij}(\boldsymbol{\beta}) \neq 0$. The polynomial p_{ij} has to be non-zero also at the generic point $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$, and so $w(\boldsymbol{\gamma}) \neq I_d$. Since w was an arbitrary non-trivial word, the rotations $\gamma_1, \dots, \gamma_r$ indeed generate the free group.

Let us show the second part in the case of odd d (with the case of even d being similar). Suppose on the contrary that we have two reduced non-commuting words w_1 and w_2 in F_r such that the corresponding elements $w_1(\boldsymbol{\gamma})$ and $w_2(\boldsymbol{\gamma})$ have a common fixed point $\boldsymbol{x} \in \mathbb{S}^{d-1}$. Thus the matrices

$$A_1 := w_1(\boldsymbol{\gamma}) - I_d \quad \text{and} \quad A_2 := w_2(\boldsymbol{\gamma}) - I_d$$

have $\boldsymbol{x} \neq \mathbf{0}$ as a common zero eigenvector. By Lemma 7.1, this property is equivalent to $\det(A_1^T A_1 + A_2^T A_2) = 0$, which is a polynomial equation in $\boldsymbol{\gamma}$ with rational coefficients. For the special r-tuple of matrices $\boldsymbol{\beta}$ returned by Lemma 7.2, the matrices

$$B_1 := w_1(\boldsymbol{\beta}) - I_d \quad \text{and} \quad B_2 := w_2(\boldsymbol{\beta}) - I_d$$

cannot have a common zero eigenvector as it would give a common fixed point for the non-commuting elements $w_1(\boldsymbol{\beta})$ and $w_2(\boldsymbol{\beta})$. Thus, we have by Lemma 7.1 that

$$\det(B_1^T B_1 + B_2^T B_2) \neq 0.$$

We have found a polynomial equality with rational coefficients that holds for $\boldsymbol{\gamma}$ but not for $\boldsymbol{\beta} \in \mathrm{SO}(d)^r$. This contradicts our assumptions that $\boldsymbol{\gamma} \in \mathrm{SO}(d)^r$ is generic. ■

Also, we will need the following result of Conley, Marks and Unger that directly follows (as a rather special case) from [4, Lemmas 3.4 and 3.6].

Theorem 7.4 (Conley, Marks and Unger [4]). *Let F_r be the free group of rank r with generators $\gamma_1, \dots, \gamma_r$ and let $a\colon F_r \curvearrowright X$ be a free Borel action on a Polish space X. Then there is a Borel subset $A \subseteq X$ such that $\gamma_1.A, \dots, \gamma_r.A$ are disjoint and $X \setminus \cup_{i=1}^r \gamma_i.A$ is meager.* ■

Proof of Proposition 1.2. We have to show that if an r-tuple $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_r) \in \mathrm{SO}(d)^r$ is generic then there is a $\boldsymbol{\gamma}$-division of $\mathbb{S}^{d-1}$ with pieces that have the property of Baire.

By Lemma 7.3, the elements $\gamma_1, \dots, \gamma_r \in \mathrm{SO}(d)$ generate a free (resp. locally commutative) action a of the free group F_r on the sphere $\mathbb{S}^{d-1}$ when d is even (resp. odd). The more general [23, Corollary 5.12] (which is attributed in [23] to Dekker [6,7]) directly gives that $\mathbb{S}^{d-1}$ is $\boldsymbol{\gamma}$-divisible, that is, there is a subset $B \subseteq \mathbb{S}^{d-1}$ with $\gamma_1.B, \dots, \gamma_r.B$ partitioning the sphere.

For every $\gamma \in \mathrm{SO}(d) \setminus \{I_d\}$, the set of its fixed points on $\mathbb{S}^{d-1}$ is closed (as the pre-image of $\mathbf{0}$ under the continuous map that sends $\boldsymbol{x} \in \mathbb{S}^{d-1}$ to $\gamma.\boldsymbol{x} - \boldsymbol{x} \in \mathbb{R}^d$) and has empty relative interior (for otherwise one can choose d linearly independent vectors fixed by γ, contradicting $\gamma \neq I_d$). In particular, this set is meager. Since the group F_r is countable, the *free part* X of the action a (which consists of $\boldsymbol{x} \in \mathbb{S}^{d-1}$ such that $w.\boldsymbol{x} \neq \boldsymbol{x}$ for each non-trivial $w \in F_r$) is co-meager. Also, it is easy to show that the free part X is a Borel subset of the sphere (see, e.g., [21, Lemma 4.4]).

Theorem 7.4, when applied to the free action of F_r on X, gives a Borel set $A \subseteq X$ with its translates $\gamma_1.A, \ldots, \gamma_r.A$ being disjoint and $Z := \mathbb{S}^{d-1} \setminus \cup_{i=1}^{r} \gamma_i.A$ being meager. We can additionally assume that Z is a-invariant: its saturation $[Z] := \cup_{w \in F_r} w.Z$ is still meager (since the countable group F_r acts by homeomorphisms) so we can replace A by $A \setminus [Z]$ without violating the conclusion of Theorem 7.4.

Now, we can combine the Borel $\boldsymbol{\gamma}$-division of $\mathbb{S}^{d-1} \setminus Z$ given by Conley, Marks and Unger [4] with the $\boldsymbol{\gamma}$-division of Dekker [6, 7] restricted to Z. Formally, take $C := A \cup (B \cap Z)$. The set C, as the union of a Borel set and a meager set, has the property of Baire while its translates $\gamma_1.C, \ldots, \gamma_r.C$ partition $\mathbb{S}^{d-1}$ by the invariance of Z. ∎

8. Proof of Lemmas 1.3 and 1.4

This section is dedicated to proving Lemmas 1.3 and 1.4. Their proofs are rather technical; this is why we postponed them until the very end.

8.1. Some definitions and results from algebraic geometry. In this section we present some definitions and results from algebraic geometry that we need. We will follow the notation from the book by Hassett [12] to which we refer for missing details (and for a nice concrete introduction to most results needed here).

A field extension $K \hookrightarrow L$ is called *algebraic* if every $x \in L$ is *algebraic* over K, that is, satisfies a non-trivial polynomial equation with coefficients in K. Some easy but very useful facts ([12, Proposition A.16]) are that, for an arbitrary field extension $K \hookrightarrow L$,

(8.1) the elements of L that are algebraic over K form a field

and, for another field extension $L \hookrightarrow M$,

(8.2) if $K \hookrightarrow L$ and $L \hookrightarrow M$ are both algebraic then $K \hookrightarrow M$ is algebraic.

Let us fix a field K.

By a *variety* we mean a subset X of some affine space K^n which is closed in the *Zariski topology*, that is, X is equal to

$$V_K(\mathcal{F}) := \{\boldsymbol{x} \in K^n \mid \forall\, f \in \mathcal{F},\ f(\boldsymbol{x}) = 0\}$$

for some family $\mathcal{F} \subseteq K[\boldsymbol{x}]$ of polynomials where $\boldsymbol{x} := (x_1, \ldots, x_n)$. Then the *coordinate ring* of X is $K[X] := K[\boldsymbol{x}]/I(X)$, where

$$I(X) := \{f \in K[\boldsymbol{x}] \mid \forall\, \boldsymbol{x} \in X,\, f(\boldsymbol{x}) = 0\}$$

denotes the *ideal* of the variety $X \subseteq K^n$.

We call a variety $X \subseteq K^n$ *irreducible* if we cannot write $X = X_1 \cup X_2$ for some varieties $X_1, X_2 \subsetneq X$. This is equivalent to the statement that the ideal $I(X) \subseteq K[\boldsymbol{x}]$ is prime ([12, Theorem 6.5]). Then $K[X]$ is a domain so we can define its fraction field, which is called the *function field* of X and is denoted by $K(X)$. Elements of $K[X]$ (resp. $K(X)$) can be viewed as the restrictions of polynomial (resp. rational) functions to X modulo identifying functions that coincide on X.

The *dimension* $\dim X$ of an irreducible variety X is the cardinality of a *transcendence basis* for the field extension $K \hookrightarrow K(X)$, which is a collection of algebraically independent (over K) elements $z_1, \ldots, z_k \in K(X)$ such that $K(X)$ is algebraic over $K(z_1, \ldots, z_k)$, the smallest subfield of $K(X)$ containing $K \cup \{z_1, \ldots, z_k\}$. By [12, Proposition 7.15], a transcendence basis exists and every two transcendence bases have the same cardinality.

Every variety X can be written as a finite union $X_1 \cup \ldots \cup X_m$ of irreducible varieties ([12, Theorem 6.4]). (In fact, this decomposition, if irredundant, is unique up to a permutation of indices.) Then the *dimension* of X is defined as $\dim X := \max\{\dim X_i \mid i \in [m]\}$. By [5, Corollary 2.68], one can equivalently define

$$\dim X := \max\{k \mid \exists \text{ irreducible varieties } Y_1, \ldots, Y_k \text{ with } \emptyset \subsetneq Y_1 \subsetneq \ldots \subsetneq Y_k \subseteq X\}. \tag{8.3}$$

We will also need the following easy result.

Lemma 8.1. *If $X_1, \ldots, X_n$ are infinite subsets of a field K and a polynomial $f \in K[x_1, \ldots, x_n]$ vanishes on each element of $X_1 \times \cdots \times X_n$, then f is the zero polynomial.*

Proof. We use induction on n. The base case $n = 1$ can be proved by induction on the degree of the univariate polynomial $f(x_1)$ by factoring out a linear factor corresponding to a root of f.

Let $n \geqslant 2$. Expand

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{m} c_i x_n^i,$$

with $c_i \in K[x_1, \ldots, x_{n-1}]$ and $c_m \neq 0$. By induction, there is $(a_1, \ldots, a_{n-1})$ in $X_1 \times \cdots \times X_{n-1}$ with $c_m(a_1, \ldots, a_{n-1}) \neq 0$. Thus, $f(a_1, \ldots, a_{n-1}, x_n)$ is a non-zero polynomial of x_n so it cannot vanish on X_n by the base case $n = 1$. ∎

8.2. Variety $\mathrm{SO}(d;K)^r$. In this section we show in particular that $\mathrm{SO}(d)^r$, as a variety in $\mathbb{R}^{d^2r}$, is irreducible and that the set of entries above the diagonals forms a transcendence basis; in particular, the dimension of $\mathrm{SO}(d)^r$ is $\binom{d}{2}r$. In fact, we will need an extension of this result, where the underlying field can be different from $\mathbb{R}$, for the proof of Lemma 1.4 (even though the statement of Lemma 1.4 deals only with the real case).

Let $d \geqslant 1$ be an integer and K be a field. Consider the affine space $K^{d\times d}$ of all $d \times d$ matrices with entries in K, writing its elements as $\gamma = (\gamma_{i,j})_{i,j\in[d]}$. Let the *special orthogonal variety* over K be the variety $\mathrm{SO}(d;K) := V_K(I_{\mathrm{SO}}) \subseteq K^{d\times d}$ defined by the ideal

$$(8.4)\qquad I_{\mathrm{SO}} := \langle (u_i)_{i\in[d]}, (f_{ij})_{1\leqslant i<j\leqslant d}, \det(\gamma) - 1\rangle \subseteq K[\gamma],$$

where $u_i := \gamma_{i,1}^2 + \cdots + \gamma_{i,d}^2 - 1$ encodes the fact that each row is a unit vector (when $K \subseteq \mathbb{R}$), $f_{i,j} := \gamma_{i,1}\gamma_{j,1} + \cdots + \gamma_{i,d}\gamma_{j,d}$ encodes the orthogonality of the i-th and j-th rows while the last constraint states that the determinant of γ is 1. Note that the "orthonormality" constraints force γ to have determinant -1 or 1, which follows from

$$(8.5)\quad (\det(\gamma))^2 = \det(\gamma^T\gamma) \equiv \det(I_d) = 1 \pmod{\langle (u_i)_{i\in[d]}, (f_{ij})_{1\leqslant i<j\leqslant d}\rangle}.$$

The matrix multiplication makes $\mathrm{SO}(d;K)$ a group. If $K = \mathbb{R}$ then we get the familiar group $\mathrm{SO}(d)$ of special orthogonal real $d \times d$ matrices (and the shorthand $\mathrm{SO}(d)$ will always be reserved for the real variety $\mathrm{SO}(d;\mathbb{R})$).

Take any integer $r \geqslant 1$. The r-th power $\mathrm{SO}(d;K)^r = \mathrm{SO}(d;K) \times \cdots \times \mathrm{SO}(d;K)$ is a variety in K^{d^2r} since a product of Zariski closed sets is Zariski closed (or since one can write the explicit equations defining $\mathrm{SO}(d;K)^r$).

For $(\gamma_1, \ldots, \gamma_r) \in \mathrm{SO}(d;K)^r$, let

$$\gamma_U := \big((\gamma_s)_{i,j} \mid s \in [r], 1 \leqslant i < j \leqslant d\big),$$

be the sequence of the $\binom{d}{2}r$ entries strictly above the diagonals. We call these entries *upper*. For notational convenience, we fix an ordering of the coordinates of K^{d^2r} so that all *non-upper* entries (that is, those on or below the diagonals) come before all upper ones; thus when we write a vector of length d^2r as $(\boldsymbol{x}, \boldsymbol{y})$ then we mean that $\boldsymbol{y}$ is the upper part.

Lemma 8.2. *For every subfield $K \subseteq \mathbb{C}$, the variety $X := (\mathrm{SO}(d;K))^r \subseteq K^{rd^2}$ is irreducible, has dimension $\binom{d}{2}r$ and the set of upper coordinates forms a transcendence basis of the function field $K(X)$ over K.*

Proof. First, let us show that X is irreducible. The proof of this in the case $r = 1$ (for an arbitrary field with $2 \neq 0$) can be found in [2, Proposition 5-2.3]. We adapt the argument from [2] to work for any $r \geqslant 1$. (Note that products need not preserve the irreducibility when the underlying field is not algebraically closed.)

For $\boldsymbol{x} \in K^d$ with $\boldsymbol{x} \cdot \boldsymbol{x} := \sum_{i=1}^{d} x_i^2$ non-zero, the map $\rho_{\boldsymbol{x}}\colon K^d \to K^d$ that is defined by

$$\rho_{\boldsymbol{x}}(\boldsymbol{y}) := \boldsymbol{y} - 2\,\frac{\boldsymbol{y}\cdot\boldsymbol{x}}{\boldsymbol{x}\cdot\boldsymbol{x}}\boldsymbol{x} \quad \text{for } \boldsymbol{y} \in K^d,$$

can be thought of as the reflection of K^d around the hyperplane orthogonal to $\boldsymbol{x}$, so we call $\rho_{\boldsymbol{x}}$ a *reflection*. Each $\gamma \in \mathrm{SO}(d;K)$ can be written as a product of an even number of reflections, see [2, Proposition 1-9.4] (and, conversely, every such product is in $\mathrm{SO}(d;K)$). In fact, the proof in [2], which proceeds by induction on d, shows that at most $m := 2d$ reflections are needed. By inserting the trivial composition $\rho_{\boldsymbol{x}}\rho_{\boldsymbol{x}} = I_d$ for some $\boldsymbol{x} \in K^d$ with $\boldsymbol{x}\cdot\boldsymbol{x} \neq 0$ we can write each $\gamma \in \mathrm{SO}(d;K)$ as the product of exactly m reflections.

Let $U := \{\boldsymbol{z} \in K^d \mid \boldsymbol{z}\cdot\boldsymbol{z} \neq 0\}$ and define $f\colon U^m \to \mathrm{SO}(d;K)$ by

$$f(\boldsymbol{z}_1,\ldots,\boldsymbol{z}_m) := \rho_{\boldsymbol{z}_1}\ldots\rho_{\boldsymbol{z}_m} \in \mathrm{SO}(d;K) \quad \text{for } (\boldsymbol{z}_1,\ldots,\boldsymbol{z}_m) \in U^m.$$

Consider the product map $f^r\colon (U^m)^r \to \mathrm{SO}(d;K)^r$ that applies f in each of the r coordinates. As the complement $V := K^{dm} \setminus U^m$ is Zariski closed (as the finite union over $i \in [m]$ of the sets of $(\boldsymbol{z}_1,\ldots,\boldsymbol{z}_m) \in K^{dm}$ satisfying the polynomial equation $\boldsymbol{z}_i \cdot \boldsymbol{z}_i = 0$), the complement $W := K^{dmr} \setminus U^{mr}$ is also Zariski closed as the finite union over $i \in [r]$ of the closed sets $K^{dm(i-1)} \times V \times K^{dm(r-i)}$. Clearly, f^r is a rational map defined everywhere on U^{mr} and thus continuous in the Zariski topology on $U^{mr} \subseteq K^{dmr}$. Also, the image of f^r is exactly $X = \mathrm{SO}(d;K)^r$ with the surjectivity following from the choice of m. It follows from [2, Lemma 5-2.1] that X is irreducible. (In brief, if X can be written as a union of two proper closed subsets $X_1 \cup X_2$, then K^{dmr} is a union of two proper closed sets $f^{-1}(X_1) \cup W$ and $f^{-1}(X_2) \cup W$, contradicting the irreducibility of K^{dmr} since its ideal $I(K^{dmr})$, which is $\{0\}$ by, e.g., Lemma 8.1, is trivially prime.) Thus X is indeed irreducible.

It remains to show that the set of upper coordinates γ_U (that is, all entries above the diagonals) is a transcendence basis for the function field $K(X)$ over K. This claim is made of the following two parts.

First, let us show that the field extension $K(\gamma_U) \hookrightarrow K(X)$ is algebraic. By (8.1) and (8.2), it is enough to represent this field extension as a composition of field extensions where, at each step, every added non-upper coordinate is algebraic over the previously added coordinates and the upper coordinates in the same matrix. Thus we consider just one matrix in $\mathrm{SO}(d;K)$, which we denote as $\gamma = (\gamma_{i,j})_{i,j\in[d]}$. We add the non-upper coordinates by whole rows in the natural order (with Row 1 added first, then Row 2, and so on). Take any Row m and a non-upper pair (m,j) (i.e., with $j \leqslant m$). The following argument works for every index $j \in [m]$ so we pick $j = m$ for notational convenience. Thus we have to show that $z := \gamma_{m,m}$, as an element of $K(X)$, is algebraic over

$$K\big(\{\gamma_{i,j} : i \in [m-1], j \in [d]\} \cup \{\gamma_{m,j} \mid j \in \{m+1, \dots, d\}\}\big).$$

Let the vector $\boldsymbol{x} := (\gamma_{m,1}, \dots, \gamma_{m,m-1})$ consist of the other non-upper entries of Row m and let $M := (\gamma_{i,j})_{i,j\in[m-1]}$ be the square submatrix of γ which lies above $\boldsymbol{x}$. The orthogonality of Row m to the previous rows gives a system of $m-1$ linear equations, namely,

$$M\boldsymbol{x}^T = \boldsymbol{f}^T,$$

where $\boldsymbol{f} := (f_1, \dots, f_{m-1})$ with

$$f_i := -\gamma_{i,m} z - \sum_{j=m+1}^{d} \gamma_{i,j}\gamma_{m,j} \quad \text{for } i \in [m-1].$$

By Cramer's rule, we have $\det(M)\boldsymbol{x}^T = \mathrm{Ad}(M)\boldsymbol{f}^T$, where $\mathrm{Ad}(M)$ denotes the *adjoint matrix* of M (whose (i,j)-th entry is $(-1)^{i+j}$ times the determinant of M with Row j and Column i removed). Take the unit "norm" relation $\sum_{i=1}^{d} \gamma_{m,i}^2 = 1$ for Row m, multiply it by $(\det(M))^2$ and replace each $(\det(M))^2 x_i^2$ by its value from Cramer's rule. We get a polynomial equation having no $\boldsymbol{x}$, namely,

$$(\det(M))^2 z^2 + \sum_{i=1}^{m-1} \left(\sum_{j=1}^{m-1} \mathrm{Ad}(M)_{ij} f_j \right)^2 + (\det(M))^2 \sum_{i=m+1}^{d} \gamma_{m,i}^2 = (\det(M))^2. \tag{8.6}$$

Let us show that the coefficient at z^2 in this equation is non-zero. This coefficient is some polynomial in the upper entries and the previous entries. If we take the identity matrix I_d for γ, then the column above z is all zero and the matrix M is invertible (namely, it is the $(m-1)\times(m-1)$ identity matrix I_{m-1}). Then $\boldsymbol{f}$ does not depend on z at all and the coefficient at z^2 is $(\det(M))^2 = 1$, which is non-zero. So the coefficient at z^2 in (8.6) is a non-zero polynomial, that is, z is algebraic over all previous entries, as desired. We conclude (by (8.1) and (8.2)) that all entries on or below the diagonals are algebraic over $K(\gamma_U)$ and thus the field extension $K(\gamma_U) \hookrightarrow K(X)$ is indeed algebraic.

Thus in order to show that the coordinates γ_U form a transcendence basis, it remains to prove that these $\binom{d}{2}r$ coordinates, as elements of the function field $K(X)$, are algebraically independent over K. It is enough to prove this for $K = \mathbb{C}$. Indeed, we assumed that $K \subseteq \mathbb{C}$. A non-trivial algebraic relation over K between the upper coordinates means that the ideal that defines $\mathrm{SO}(d; K)^r$ (which, in the case $r = 1$, is the ideal I_{SO} in (8.4)) contains a non-zero polynomial g that does not depend on non-upper coordinates. The same polynomial g, when viewed as a polynomial in $\mathbb{C}[\boldsymbol{\gamma}]$, then witnesses that the upper coordinates are algebraically dependent over $\mathbb{C}$.

Thus let us assume that $K = \mathbb{C}$. We need an easy auxiliary claim first from which we will derive that every choice of sufficiently small in absolute value upper entries can be extended to a matrix in $\mathrm{SO}(d;\mathbb{C})$. For $m \in [d]$ and an $m \times d$ matrix $\gamma = (\gamma_{i,j})$, let the property $\mathcal{P}_m$ state that for all $i \in [m]$, we have

$$\sum_{j=1}^{d} \gamma_{i,j}\gamma_{m,j} = \mathbb{1}_{i=m}.$$

(Recall that $\mathbb{1}_{i=m}$ is 1 if $i = m$, and 0 otherwise.) In other words, $\mathcal{P}_m$ states that Row m has unit "norm" and is orthogonal to all previous rows.

Claim 8.3. *For every $m \in [d]$ and $\delta > 0$ there is $\varepsilon = \varepsilon_m(\delta) > 0$ such that the following holds. Take any complex numbers $(\gamma_{i,j})_{(i,j)\in S}$, where*

$$S := \big([m-1] \times [d]\big) \cup \{(m, j) \mid m < j \leqslant d\},$$

such that $\mathcal{P}_1, \ldots, \mathcal{P}_{m-1}$ hold and $|\gamma_{i,j} - \mathbb{1}_{i=j}| \leqslant \varepsilon$ for any $(i, j) \in S$. Then there is a choice of $\gamma_{m,1}, \ldots, \gamma_{m,m} \in \mathbb{C}$ such that $|\gamma_{m,j} - \mathbb{1}_{m=j}| \leqslant \delta$ for each $j \in [m]$ and $\mathcal{P}_m$ holds. Moreover, if $\gamma_{i,j}$ for each $(i, j) \in S$ is real then $\gamma_{m,1}, \ldots, \gamma_{m,m}$ can additionally be chosen to be real.

Proof of the claim. Suppose that the claim fails for some $m \in [d]$ and $\delta > 0$. Let real ε tend to 0 from above and let $\gamma \in \mathbb{C}^S$ be a partial assignment violating the claim. Let us use the notation that was introduced around (8.6). By our choice of γ, we have that each entry of M is within additive $\varepsilon = o(1)$ from the corresponding entry of the identity matrix and thus $\det(M) = 1 + o(1)$ is non-zero. Of the two roots of the quadratic equation (8.6), which now reads $z^2 - 1 = o(1 + |z|^2)$, choose $z = 1 + o(1)$. In fact, (8.6) gives not only the entry $z = \gamma_{m,m}$ but the consistent remainder of Row m by $\boldsymbol{x}^T := (\det(M))^{-1}\,\mathrm{Ad}(M)\,\boldsymbol{f}^T$, satisfying $\mathcal{P}_m$. By the continuity of the all involved functions (and $\det(M) = 1 + o(1)$), we have $\|\boldsymbol{x}\|_\infty = o(1)$, a contradiction to $\delta > 0$ being fixed.

Let us show how to adapt this argument to establish the second part of the claim. Suppose additionally that the given $\gamma_{i,j}$'s are reals. In the above notation, the quadratic equation (8.6) has all real coefficients and, as before, states that $z^2 - 1 = o(1 + |z^2|)$. Its left-hand side as a function of $z \in \mathbb{R}$ changes sign at $z = 1$ with its derivative $2z$ being bounded away from 0 around $z = 1$. Hence, we can choose a real root $z = 1 + o(1)$. Then M is a real matrix and the rest of Row m, namely $\boldsymbol{x}^T := (\det(M))^{-1}\,\mathrm{Ad}(M)\,\boldsymbol{f}^T$ is also real. ■

Consider the projection $\pi\colon \mathrm{SO}(d;\mathbb{C})^r \to \mathbb{C}^m$ on the $m := \binom{d}{2}r$ upper coordinates, which maps $(\boldsymbol{x},\boldsymbol{y})$ to $\boldsymbol{y}$. In particular, the r-tuple of the identity matrices projects to the zero vector $\mathbf{0} \in \mathbb{C}^m$. The image of π contains some Euclidean open ball

$$\mathrm{Ball}_\varepsilon(\mathbf{0}) := \{z \in \mathbb{C}^m \mid \|z\|_1 < \varepsilon\}$$

of radius $\varepsilon > 0$ around the origin. Namely, we can take its radius to be

$$\varepsilon := \varepsilon_d(\varepsilon_{d-1}(\dots\varepsilon_1(1/(2^d\, d!))\dots)) > 0, \tag{8.7}$$

where $\varepsilon_1,\dots,\varepsilon_d$ are the functions returned by Claim 8.3. Indeed, by the choice of the constants we know that for every $\boldsymbol{y} \in \mathrm{Ball}_\varepsilon(\mathbf{0})$, we can construct a $d \times d$ matrix γ row by row so that γ projects to $\boldsymbol{y}$ and satisfies all properties $\mathcal{P}_1,\dots,\mathcal{P}_d$ while it also holds that

$$\|\gamma - I_d\|_\infty < 1/(2^d\, d!).$$

The last inequality gives, rather roughly, that $|\det(\gamma) - 1| < 1$. Thus, $\det(\gamma) = 1$ because $\det(\gamma)$ is either -1 or 1 by (8.5). So indeed $\pi(\mathrm{SO}(d;\mathbb{C}))$ contains $\pi(\gamma) = \boldsymbol{y}$.

Now, suppose on the contrary that there is a non-trivial polynomial relation between the upper coordinates. Thus there is a non-zero polynomial g which does not depend on the non-upper coordinates and belongs to the ideal generated by the polynomials that define $\mathrm{SO}(d;\mathbb{C})^r$ (with those for $r = 1$ being listed in (8.4)). The polynomial g, as a function of the m upper coordinates, vanishes on $\pi(X) \subseteq \mathbb{C}^m$. This contradicts Lemma 8.1 as $\pi(X)$ contains a non-empty open set, namely the open ball of radius ε around the origin, and thus $\pi(X)$ contains a product of m infinite sets. ■

Now we are ready to show that the set $\mathcal{N}$ of non-generic points in $\mathrm{SO}(d)^r$ is "small".

Proof of Lemma 1.3. As before, when we identify an r-tuple of $d \times d$ matrices over a field K with an element of $K^{d^2 r}$, let us order the $d^2 r$ coordinates so that the $m := \binom{d}{2}r$ upper entries (i.e., those above the diagonals) come at the end. Thus if we write an element of $K^{d^2 r}$ as $(\boldsymbol{x},\boldsymbol{y})$ then $\boldsymbol{y}$ corresponds to the m upper entries. Also, we use the standard topology on $\mathbb{S}^{d-1}$ (the one which is inherited from the Euclidean space $\mathbb{R}^d$).

There are countably many polynomials in $\mathbb{Q}[\boldsymbol{x},\boldsymbol{y}]$ so enumerate those that are non-zero on at least one element of $\mathrm{SO}(d)^r$ as $f_1, f_2, \dots$. By definition, if a point $(\boldsymbol{a},\boldsymbol{b}) \in \mathrm{SO}(d;\mathbb{R})^r$ is not generic then some f_i vanishes on $(\boldsymbol{a},\boldsymbol{b})$. Thus $\mathcal{N}$ is a subset of the countable union $\cup_{i=1}^\infty Z_i$, where

$$Z_i := \{(\boldsymbol{a},\boldsymbol{b}) \in \mathrm{SO}(d)^r \mid f_i(\boldsymbol{a},\boldsymbol{b}) = 0\}. \tag{8.8}$$

Since each polynomial f_i is continuous as a function $\mathbb{R}^{d^2 r} \to \mathbb{R}$, each set Z_i is closed.

Let us turn to part (i) where we have to show that the Haar measure ν assigns measure 0 to $\mathcal{N}$. By the countable additivity, it is enough to show that each set Z_i, defined by (8.8), has ν-measure zero.

First, let us recall how the Haar measure can be constructed for the group $\Gamma := \mathrm{SO}(n)^r$ (and, in fact, for any real Lie group), following the presentation in [17, Sections VIII.1–2]. Namely, choose some linear basis for the Lie algebra $(\mathfrak{so}(d))^r$ viewed as the tangent space $T_{(I_d,\dots,I_d)}$ at the identity $(I_d,\dots,I_d) \in \mathrm{SO}(d)^r$ and, using the translations of these vectors, turn them into left-invariant vector fields $X_1,\dots,X_m$. (Note the Lie algebra $(\mathfrak{so}(d))^r$, that consists of all r-tuples of skew-symmetric matrices, has dimension $m = \binom{d}{2}r$ as a vector space.) For each $\boldsymbol{\gamma} \in \Gamma$, let $e_1(\boldsymbol{\gamma}),\dots,e_m(\boldsymbol{\gamma}) \in T^*_{\boldsymbol{\gamma}}$ be the dual basis to $(X_1(\boldsymbol{\gamma}),\dots,X_m(\boldsymbol{\gamma}))$. Then $\omega = e_1 \wedge \dots \wedge e_m$ (the skew-symmetric product) is a smooth m-form on Γ, which is positive and left-invariant and thus defines a Borel left-invariant non-zero measure on Γ ([17, Theorem 8.21]). By the uniqueness, this has to be a multiple of the Haar measure ν. In particular, any smooth submanifold of Γ of dimension (as a manifold) less than m has zero Haar measure ([17, Equation (8.25)]).

The set $Z_i \subsetneq \mathrm{SO}(d)^r$, as an algebraic variety, has dimension smaller than m which follows from the definition of the dimension via nested chains of irreducible varieties (that is, by (8.3)) and from the irreducibility of the variety $\mathrm{SO}(d)^r$ (that is, by Lemma 8.2). Some standard results in the theory of (semi-)algebraic sets give that every bounded variety in some $\mathbb{R}^n$ admits a triangulation into simplices each of which is a smooth submanifold of $\mathbb{R}^n$; see, e.g., [1, Theorem 5.43]. Apply this result to every irreducible component $Z \subseteq Z_i$. The dimension k of each obtained simplex S (as a manifold) is at most $\dim Z$. Indeed, pick a point $\boldsymbol{s} \in S$ and the projection from S on some k coordinates which is a homeomorphism around $\boldsymbol{s}$. Observe that these k coordinates are algebraically independent in the function field $\mathbb{R}(Z)$ because no non-zero polynomial on $\mathbb{R}^k$ can vanish on a non-empty open set by Lemma 8.1.

Thus we covered Z_i by finitely many manifolds of dimension less than m, each having zero Haar measure as it was observed earlier (by [17, Equation (8.25)]). We conclude that the Haar measure of Z_i is indeed zero.

Let us show part (ii). Recall that the sets $Z_1, Z_2, \dots$ were defined in (8.8). Clearly, each set Z_i is closed. Thus it is enough to show that the relative interior of each $Z_i \subseteq \mathrm{SO}(d)^r$ is empty. Suppose on the contrary that the relative interior U of some Z_i is non-empty. Since the compact group $\mathrm{SO}(d)^r$ acts transitively on itself by homeomorphisms, finitely many translates of U cover the whole group. As the Haar measure is ν is invariant under this action, we have that $\nu(U) > 0$. However, this contradicts part (i) that we have already proved.

This finishes the proof of Lemma 1.3. ∎

8.3. Proof of Lemma 1.4. Our proof of the reverse (harder) implication of Lemma 1.4 needs Lemma 8.4 below. Since we could not find this rather natural statement anywhere in the literature we present a proof whose main idea (to use dimension) was suggested to us by Miles Reid. In fact, Miles Reid came up with a full proof of some initial version of the lemma. Since his proof relies on the so-called *universal domain* of K while we would like to have this paper as elementary as possible, we present a proof that avoids universal domains.

Given a field extension $K \hookrightarrow L$ and a variety $X \subseteq L^n$ (over the field L), we say that an element $\boldsymbol{a} \in X$ is K-*generic* for X if every polynomial $p \in K[x_1, \dots, x_n]$ with $p(\boldsymbol{a}) = 0$ vanishes on every element of X. (Here as well as in the rest of this paper, each evaluation mixing elements of some two fields $K \hookrightarrow L$ is done in the larger field L.) In the special case when $K := \mathbb{Q}$, $L := \mathbb{R}$, $X := \mathrm{SO}(d)^r$ we get exactly the definition of a generic r-tuple of rotations from the introduction.

Lemma 8.4. *Let $K \hookrightarrow L$ be a field extension, with L being algebraically closed. Let $\mathcal{P} \subseteq K[\boldsymbol{x}, \boldsymbol{y}]$ be some family of polynomials over K, where we abbreviate $\boldsymbol{x} := (x_1, \dots, x_m)$ and $\boldsymbol{y} := (y_1, \dots, y_n)$. Suppose that*

$$X := \{(\boldsymbol{x}, \boldsymbol{y}) \in L^{m+n} \mid \forall\, f \in \mathcal{P}, f(\boldsymbol{x}, \boldsymbol{y}) = 0\},$$

as a variety over L, is irreducible and has dimension n with $y_1, \dots, y_n$ forming a transcendence basis for the function field $L(X)$ over L.

Then every $p = (\boldsymbol{a}, \boldsymbol{b}) \in X$ with the n-tuple $\boldsymbol{b} \in L^n$ being algebraically independent over K is a K-generic point of X.

Proof. Let the ideal $I_p \subseteq K[\boldsymbol{x}, \boldsymbol{y}]$ consist of those polynomials over K that vanish on p. Let

$$Z := V_L(I_p) = \{(\boldsymbol{x}, \boldsymbol{y}) \in L^{m+n} \mid \forall\, f \in I_p, f(\boldsymbol{x}, \boldsymbol{y}) = 0\}.$$

As $\mathcal{P} \subseteq I_p$, we trivially have that $Z \subseteq X$. We have to show that $Z = X$, which by the definition of $Z = V_L(I_p)$ will give the required result (namely, that every $f \in I_p$ vanishes on X).

Let $Z = Z_1 \cup \ldots \cup Z_t$ be a decomposition of Z into irreducible varieties ([12, Theorem 6.4]).

Suppose first that there is $i \in [t]$ such that the n-tuple $\boldsymbol{y}$, with each y_j viewed as an element of the function field $L(Z_i)$, is algebraically independent over L. This means that the dimension of the irreducible variety $Z_i \subseteq L^{m+n}$ is at least n. Recall that $Z_i \subseteq Z \subseteq X$. By the definition of the dimension via nested chains of irreducible subvarieties (that is, by (8.3)), we cannot have $Z_i \subsetneq X$ for otherwise any chain for Z_i

extends to a strictly larger chain for X which gives that $\dim X - 1 \geqslant \dim Z_i \geqslant n$, contradicting our assumption. Thus, $Z_i = Z = X$, as desired.

Thus we can assume that for every $i \in [t]$ there is a non-zero $g_i \in L[\boldsymbol{y}] \cap I(Z_i)$. Since $Z = \cup_{i=1}^t Z_i$, we have by [12, Proposition 3.12] that $I(Z) = \cap_{i=1}^t I(Z_i)$. (Recall that, for example, the ideal $I(Z)$ of $Z \subseteq L^{m+n}$ consists of those $p \in L[\boldsymbol{x}, \boldsymbol{y}]$ that vanish on Z.) Thus the product $g_1 \dots g_t \in L[\boldsymbol{y}]$, which trivially belongs to each $I(Z_i)$, also belongs to $I(Z)$.

Let I_p^L be the ideal in $L[\boldsymbol{x}, \boldsymbol{y}]$ generated by $I_p \subseteq K[\boldsymbol{x}, \boldsymbol{y}] \subseteq L[\boldsymbol{x}, \boldsymbol{y}]$. In other words,

$$I_p^L := \left\{ \sum_{i=1}^m h_i(\boldsymbol{x}, \boldsymbol{y}) f_i(\boldsymbol{x}, \boldsymbol{y}) \mid m \geqslant 0, h_1, \dots, h_m \in L[\boldsymbol{x}, \boldsymbol{y}], f_1, \dots, f_m \in I_p \right\},$$

from which it easily follows that $V_L(I_p^L) = V_L(I_p) = Z$. Since L is algebraically closed, we have by Hilbert's Nullstellensatz ([12, Theorem 7.3]) that $I(Z)$ is equal to

$$\sqrt{I_p^L} := \{ f \in L[\boldsymbol{x}, \boldsymbol{y}] \mid \exists N \ f^N \in I_p^L \},$$

the *radical* of I_p^L. Thus there is some integer $N \geqslant 1$ such that $g := (g_1 \dots g_t)^N$ belongs to I_p^L.

In other words, we have shown that I_p^L contains a non-zero polynomial g that does not depend on $\boldsymbol{x}$, that is,

$$I_p^L \cap L[\boldsymbol{y}] \neq \{0\}. \tag{8.9}$$

We claim that, in fact, $I_p \cap K[\boldsymbol{y}] \neq \{0\}$. In order to show this, we analyse how a known algorithm for eliminating variables works, arguing that we can run two instances of the algorithm, one for $I_p^L \cap L[\boldsymbol{y}]$ and the other for $I_p \cap K[\boldsymbol{y}]$, to produce the same generating set of polynomials in each case.

Since all following steps are fairly standard, we will be rather brief, referring the reader to [12] for a detailed exposition. First, by the Hilbert Basis theorem ([12, Corollary 2.22]), there is a finite set $\mathcal{F} \subseteq K[\boldsymbol{x}, \boldsymbol{y}]$ that generates I_p. Of course, the same set $\mathcal{F}$, as a subset of $L[\boldsymbol{x}, \boldsymbol{y}]$, generates I_p^L. We fix any monomial order $\prec$ for $(\boldsymbol{x}, \boldsymbol{y})$ which is an elimination order for $\boldsymbol{x}$ ([12, Definition 4.6]) and apply Buchberger's algorithm ([12, Corollary 2.29]) to find a $\prec$-Gröbner basis $\mathcal{G}$ for I_p^L using $\mathcal{F}$ as its input. At a very low level, each step of the algorithm is to pick some two previous non-zero polynomials h_1 and h_2, take the coefficients c_1 and c_2 at their $\prec$-highest monomials and add $h_1 - (c_1/c_2)hh_2$ for some monomial h to the current pool of polynomials. Thus all encountered polynomials have coefficients in K; in particular, the obtained Gröbner basis $\mathcal{G}$ is a subset of $K[\boldsymbol{x}, \boldsymbol{y}]$. By the Elimination theorem ([12, Theorem 4.8]) and our choice of the monomial order $\prec$, the ideal $I_p^L \cap L[\boldsymbol{y}]$ is generated by $\mathcal{G} \cap L[\boldsymbol{y}]$, that is, by those polynomials in $\mathcal{G}$ that do not depend on $\boldsymbol{x}$. Moreover, if we apply Buchberger's algorithm to find the intersection of $I_p = \langle \mathcal{F} \rangle \subseteq K[\boldsymbol{x}, \boldsymbol{y}]$ and $K[\boldsymbol{y}]$, we obtain the very same generating set $\mathcal{G} \cap K[\boldsymbol{y}]$ (because the choice of h_1, h_2 and h at each low-level step of the algorithm depends only on the $\prec$-highest monomials of the previous polynomials).

However, we know that $I_p \cap K[\boldsymbol{y}] = \{0\}$ because no non-zero polynomial in $K[\boldsymbol{y}]$ can vanish on p by our assumption that $\boldsymbol{y}$ is algebraically independent over K. Thus,

$$\mathcal{G} \cap L[\boldsymbol{y}] = \mathcal{G} \cap K[\boldsymbol{y}]$$

can contain only the zero polynomial. This means that $I_p^L \cap L[\boldsymbol{y}] = \{0\}$, contradicting (8.9) and proving the lemma. ∎

Now we are ready to prove Lemma 1.4 that gives an alternative characterisation of $\mathbb{Q}$-generic points of $\mathrm{SO}(d)^r$.

Proof of Lemma 1.4. As before, the $m := \binom{d}{2} r$ upper entries of $\mathrm{SO}(d)^r \subseteq \mathbb{R}^{d^2 r}$ come at the end and if we write an element of $K^{d^2 r}$ as $(\boldsymbol{x}, \boldsymbol{y})$ then $\boldsymbol{y}$ corresponds to the m upper entries.

The forward implication of the lemma is easy. Take any $(\boldsymbol{a}, \boldsymbol{b}) \in SO(d; \mathbb{R})^r$ such that $f(\boldsymbol{b}) = 0$ for some non-zero polynomial f with rational coefficients. Take any vector $\boldsymbol{b}' \in \mathbb{R}^m$ whose L^∞-norm is at most the expression in (8.7) with entries algebraically independent over $\mathbb{Q}$. By Claim 8.3, there is a choice of a real vector $\boldsymbol{a}'$ with $(\boldsymbol{a}', \boldsymbol{b}') \in \mathrm{SO}(d)^r$, that is, we can extent the vector $\boldsymbol{b}'$ of upper entries to an r-tuple of real special orthogonal matrices. Since the polynomial f with rational coefficients cannot vanish on $\boldsymbol{b}'$, the polynomial map $(\boldsymbol{x}, \boldsymbol{y}) \mapsto f(\boldsymbol{y})$ shows that $(\boldsymbol{a}, \boldsymbol{b})$ is not a generic point.

Let us show the converse implication. Let $(\boldsymbol{a}, \boldsymbol{b}) \in SO(d; \mathbb{R})^r$ be any point with the m-tuple $\boldsymbol{b} \in \mathbb{R}^m$ of reals being algebraically independent over $\mathbb{Q}$.

By Lemma 8.2, the complex variety $X := \mathrm{SO}(d; \mathbb{C})^r \subseteq \mathbb{C}^{d^2 r}$ is irreducible and the upper coordinates $\boldsymbol{y}$ form a transcendence basis for the function field $\mathbb{C}(X)$. Now, Lemma 8.4 (which requires that the field L is algebraically closed) applies with $K := \mathbb{Q}$, $L := \mathbb{C}$ and $\mathcal{P} \subseteq \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ consisting of the polynomials that define the variety $\mathrm{SO}(d; \mathbb{R})^r$ (with the ones in (8.4) corresponding to the case $r = 1$). The lemma gives that $(\boldsymbol{a}, \boldsymbol{b}) \in \mathrm{SO}(d; \mathbb{R})^r \subseteq \mathrm{SO}(d; \mathbb{C})^r$ is a $\mathbb{Q}$-generic point of $\mathrm{SO}(d; \mathbb{C})^r$. Of course, this trivially implies that $(\boldsymbol{a}, \boldsymbol{b})$ is a $\mathbb{Q}$-generic point also of $\mathrm{SO}(d; \mathbb{R})^r$ (as every polynomial $p \in \mathbb{Q}[\boldsymbol{x}, \boldsymbol{y}]$ that vanishes on $(\boldsymbol{a}, \boldsymbol{b})$ has to vanish on $\mathrm{SO}(d; \mathbb{C})^r \supseteq \mathrm{SO}(d; \mathbb{R})^r$), as desired.

This finishes the proof of Lemma 1.4. ∎

Acknowledgements. The authors would like to thank Miles Reid for the very useful discussions and for sharing his proof of some initial version of Lemma 8.4. Also, the authors thank the anonymous referee for helpful comments.

Funding. Clinton T. Conley was supported by NSF Grant DMS-1855579. Jan Grebík was supported by Leverhulme Research Project Grant RPG-2018-424. Oleg Pikhurko was supported by ERC Advanced Grant 101020255 and Leverhulme Research Project Grant RPG-2018-424.

References

[1] S. Basu, R. Pollack and M.-F. Roy, *Algorithms in real algebraic geometry*. Second edn., Algorithms Comput. Math. 10, Springer, Berlin, 2006. Zbl 1102.14041 MR 2248869

[2] M. Boij and D. Laksov, An introduction to algebra and geometry via matrix groups. Lecture notes, KTH, 2008.

[3] A. Borel, On free subgroups of semisimple groups. *Enseign. Math. (2)* **29** (1983), no. 1–2, 151–164. Zbl 0533.22009 MR 702738

[4] C. T. Conley, A. S. Marks and S. T. Unger, Measurable realizations of abstract systems of congruences. *Forum Math. Sigma* **8** (2020), article no. e10. Zbl 07178124 MR 4068762

[5] S. D. Cutkosky, *Introduction to algebraic geometry*. Grad. Stud. Math. 188, American Mathematical Society, Providence, RI, 2018. Zbl 1396.14001 MR 3791837

[6] T. J. Dekker, Decompositions of sets and spaces. I, II. *Indag. Math.* **18** (1956), 581–589, 590–595. Zbl 0074.28103 MR 92135

[7] — *Paradoxical decompositions of sets and spaces*. Drukkerij Wed. G. van Soest, Amsterdam, 1958. Zbl 0082.04404 MR 121696

[8] P. Deligne and D. Sullivan, Division algebras and the Hausdorff–Banach–Tarski paradox. *Enseign. Math. (2)* **29** (1983), no. 1–2, 145–150. Zbl 0521.57035 MR 702737

[9] J. Grebík, R. Greenfeld, V. Rozhoň and T. Tao, Measurable tilings by abelian group actions. *Int. Math. Res. Not. IMRN* (2023), no. 23, 20211–20251. MR 4675070

[10] H. Groemer, *Geometric applications of Fourier series and spherical harmonics*. Encyclopedia Math. Appl. 61, Cambridge University Press, Cambridge, 1996. Zbl 0877.52002 MR 1412143

[11] B. Grünbaum, *Convex polytopes*. Second edn., Grad. Texts in Math. 221, Springer, New York, 2003. Zbl 1024.52001 MR 1976856

[12] B. Hassett, *Introduction to algebraic geometry*. Cambridge University Press, Cambridge, 2007. Zbl 1118.14002 MR 2324354

[13] F. Hausdorff, Bemerkung über den Inhalt von Punktmengen. *Math. Ann.* **75** (1914), no. 3, 428–433. Zbl 45.0128.05 MR 1511802

[14] R. A. Horn and C. R. Johnson, *Matrix analysis*. Second edn., Cambridge University Press, Cambridge, 2013. Zbl 1267.15001 MR 2978290

[15] A. S. Kechris, *Classical descriptive set theory*. Grad. Texts in Math. 156, Springer, New York, 1995. Zbl 0819.04002 MR 1321597

[16] A. S. Kechris and A. S. Marks, Descriptive graph combinatorics. Unpublished manuscript, 2020, https://pma.caltech.edu/documents/5616/combinatorics20book.pdf, visited on 5 February 2024

[17] A. W. Knapp, *Lie groups beyond an introduction*. Second edn., Progr. Math. 140, Birkhäuser, Boston, MA, 2002. Zbl 1075.22501 MR 1920389

[18] J. Mycielski, On the paradox of the sphere. *Fund. Math.* **42** (1955), 348–355. Zbl 0068.04402 MR 80899

[19] — On the decomposition of a segment into congruent sets and related problems. *Colloq. Math.* **5** (1957), no. 1, 24–27. Zbl 0082.04603 MR 100821

[20] — Problem 166. *Colloq. Math.* **4** (1957), no. 2, 240.

[21] O. Pikhurko, Borel combinatorics of locally finite graphs. In *Surveys in combinatorics 2021*, pp. 267–319, London Math. Soc. Lecture Note Ser. 470, Cambridge University Press, Cambridge, 2021. Zbl 1504.03027 MR 4273433

[22] R. M. Robinson, On the decomposition of spheres. *Fund. Math.* **34** (1947), 246–260. Zbl 0032.40303 MR 26093

[23] G. Tomkowicz and S. Wagon, *The Banach–Tarski paradox*. Second edn., Encyclopedia Math. Appl. 163, Cambridge University Press, New York, 2016. Zbl 1372.43001 MR 3616119

[24] S. Wagon, *The Banach–Tarski paradox*. Cambridge University Press, Cambridge, 1993. Zbl 0569.43001 MR 1251963

[25] S. H. Weintraub, *Fundamentals of algebraic topology*. Grad. Texts in Math. 270, Springer, New York, 2014. Zbl 1305.55001 MR 3243764

(Reçu le 9 décembre 2020)

Clinton T. Conley, Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA 15213, USA; *e-mail:* clintonc@andrew.cmu.edu

Jan Grebík, UCLA Mathematics, 520 Portola Plaza, Los Angeles, CA 90095, USA; and Faculty of Informatics, Masaryk University, Botanicka 68A, 602 00 Brno, Czech Republic; *e-mail:* grebikj@math.ucla.edu

Oleg Pikhurko, Mathematics Institute and DIMAP, University of Warwick, Coventry CV4 7AL, UK; *e-mail:* o.pikhurko@warwick.ac.uk