Decomposition of balls into congruent pieces

Gergely Kiss and Miklós Laczkovich

July 13, 2010

Abstract

We prove that if $3 \mid d$, then the d-dimensional balls are m-divisible for every m large enough. In particular, the 3-dimensional balls are m-divisible for every $m \geq 22$.

1 Introduction and main results

We say that a subset of $\mathbb{R}^d$ is *m-divisible,* if it can be decomposed into m pairwise disjoint congruent pieces. A set is called *divisible,* if it is m-divisible for some $2 \leq m < \infty$. Investigations of divisible sets started in 1949, when van der Waerden noticed that the disc is not 2-divisible, and posed this fact as an exercise in *Elemente der Mathematik.* Van der Waerden's observation prompted the question, still unsolved, whether or not the disc is divisible, or even m-divisible for every $m \geq 3$. As for higher dimensions, it was proved by S. Wagon in 1983 that the d-dimensional balls are not m-divisible if $m \leq d$ [8]. Wagon's result, again, motivated the question whether or not d-dimensional balls are divisible. In this paper we give a partial answer by proving the following.

Theorem 1.1. *For every d divisible by three there is an m_d such that the d-dimensional balls (either open or closed) are m-divisible for every $m \geq m_d$.*

In particular, for $d = 3$ we have the following result.

[1]**Keywords:** m-divisibility of balls in Euclidean spaces
[2]**MSC 2010 classification:** 52A15, 52A20, 51F20

Theorem 1.2. *The three dimensional balls (either open or closed) are m-divisible for every $m \geq 22$.*

We remark that in infinite dimensional spaces the situation is different. It was shown by M. Edelstein that in infinite dimensional strictly convex Banach spaces the closed unit ball is not divisible [2, Theorem 6]. (On the other hand, the unit balls of the Banach spaces c_0 and $C[0,1]$ are m-divisible for every $m \geq 2$; see [2, Theorem 1]. For further results concerning divisibility in infinite dimensional spaces, we refer to [7].)

Returning to finite dimensional Euclidean spaces, recently it was proved by C. Richter that in $\mathbb{R}^d$ most of the convex bodies (that is, convex compact sets with nonempty interior) are not divisible. More precisely, Richter proved that the set of divisible convex bodies is of first category in an appropriate space of all convex bodies [6]. Motivated by this result Richter formulated the conjecture that no convex body is divisible in $\mathbb{R}^d$ [6, p. 131]. Our Theorem 1.1 disproves this conjecture if $3 \mid d$. We also have the following simple consequence of Theorem 1.2.

Corollary 1.3. *For every $d \geq 3$ there exist convex bodies in $\mathbb{R}^d$ which are m-divisible for every $m \geq 22$.*

Indeed, if B_3 denotes the three dimensional unit ball then, by Theorem 1.2, $A \times B_3$ is m-divisible for every $m \geq 22$ and for every $A \subset \mathbb{R}^{d-3}$; and if A is a convex body in $\mathbb{R}^{d-3}$ then so is $A \times B_3$ in $\mathbb{R}^d$. Perhaps we can modify Richter's conjecture as follows: is it true that if a convex body $C \subset \mathbb{R}^d$ is divisible, then C is congruent to a set of form $A \times B$, where $A \subset \mathbb{R}^n$ is a convex body, $0 \leq n < d$, and $B \subset \mathbb{R}^{d-n}$ is a ball?

In the next section we present a general sufficient condition for m-divisibility of sets under a transformation group. (The condition was motivated by [4, Lemma 1].) Then we prove Theorems 1.1 and 1.2 by showing that this condition can be realized by isometries. This part of the proof is based on the fact that the action of SO_3 is locally commutative on $\mathbb{R}^3 \setminus \{0\}$; that is, if two elements of SO_3 have a common nonzero fixed point then they commute. We shall work with a set of rotations and a translation generating a free group. The main observation, also motivated by [4], is that under local commutativity the graph generated by the transformations has the property that whenever two cycles have a nonzero common vertex then the cycles coincide (see Lemma 4.1).

The proof of Theorems 1.2 and 1.1 will be given in sections 4 and 5. In the last section we make some comments on the limits of our method concerning possible generalizations to other dimensions, and on the number of pieces in the decompositions.

2 A lemma on decompositions

Let X be a set, and let $f_1, \dots, f_n$ be maps from subsets of X into X. Our aim is to find a sufficient condition for the existence of a decomposition $X = A_0 \cup A_1 \cup \ldots \cup A_n$ such that $f_i(A_0) = A_i$ for every $i = 1, \dots, n$.

Suppose that f_i is defined on $D_i \subset X$ $(i = 1, \dots, n)$, and put $D = \bigcap_{i=1}^n D_i$. We say that the point x is a core point, if $x \in D$, and the points $x, f_1(x), \dots, f_n(x)$ are distinct. By the image of a core point x we mean the set $\{f_1(x), \dots, f_n(x)\}$.

We define a graph Γ on the set X as follows: we connect the distinct points $x, y \in X$ by an edge if there is an $i \in \{1, \dots, n\}$ such that $f_i(x) = y$ or $f_i(y) = x$. Then Γ will be called the graph generated by the functions $f_1, \dots, f_n$.

Lemma 2.1. *Let X, $f_1, \dots, f_n$, D, and Γ be as above, and suppose that the graph Γ has the property that whenever two cycles C_1 and C_2 in Γ share a common edge, then the sets of vertices of C_1 and C_2 coincide.*

Suppose that there is a point $x_0 \in X$ satisfying the following conditions.

(i) *x_0 is in the image of at least one core point;*

(ii) *every $x \in X \setminus \{x_0\}$ is in the image of at least three core points.*

Then there is a decomposition $X = A_0 \cup A_1 \cup \ldots \cup A_n$ such that $A_0 \subset D$, and $f_i(A_0) = A_i$ for every $i = 1, \dots, n$.

Proof. We shall prove that whenever E is the set of vertices of a connected component of Γ, then E can be decomposed into disjoint sets $E_0, E_1, \dots, E_n$ such that $E_0 \subset D$, and $f_i(E_0) = E_i$ for every $i = 1, \dots, n$. Clearly, this will prove the statement of the lemma.

For every core point x we shall denote the set $\{x, f_1(x), \dots, f_n(x)\}$ by $U(x)$.

Let E be a given connected component of Γ. Clearly, if x is a core point and $U(x) \cap E \neq \emptyset$, then $x \in E$. Also, if $x \in E$ is a core point, then $U(x) \subset E$.

By (i), there is a core point u_0 such that x_0 is in the image of u_0. It is easy to check, using Zorn's lemma, that there exists a maximal subset C of E such that every element of C is a core point, if $x_0 \in E$ then $u_0 \in C$, the sets $U(x)$ $(x \in C)$ are pairwise disjoint, and the subgraph of E spanned by the set $V = \bigcup\{U(x) : x \in C\}$ is connected. Note that $x_0 \in U(u_0)$, and thus we have either $x_0 \notin E$ or $x_0 \in V$.

We prove that $V = E$. Suppose this is not true. Since E is connected, there are points $x \in E \setminus V$ and $y \in V$ such that x and y are connected by an edge. Then $x \neq x_0$, and thus it follows from condition (ii) that there are distinct core points p, q, r such that x belongs to the image of each of p, q, r. Then p, q, r, x are distinct. Also, at least two of the points p, q, r are different from y. We may assume that $p \neq y$ and $q \neq y$, and thus the points x, y, p, q are distinct.

Now $V \cup U(p)$ is connected, since $U(p)$ is connected, $x \in U(p)$, and x is connected to $y \in V$ by an edge. Thus, by the maximality of the set C, we have $U(p) \cap V \neq \emptyset$. Therefore, we have either $p \in V$, or $p \notin V$ and $f_i(p) \in V$ for a suitable $i \in \{1, \ldots, n\}$. Similarly, we have either $q \in V$, or $q \notin V$ and $f_j(q) \in V$ for a suitable $j \in \{1, \ldots, n\}$.

First suppose $p \in V$ and $q \in V$. Since V is connected, there is a path $p = y_0, y_1, \ldots, y_s = y$ in V. (Note that $s \geq 1$.) Then $C_1 = \{y_0, y_1, \ldots, y_s, x\}$ is a cycle containing the edge (y, x) and the vertex p. By a similar argument we find another cycle containing (y, x) and q. Since both of these cycles contain the edge (y, x), it follows that the vertex sets of these cycles coincide, and thus $q = y_r$ for some $0 < r < s$. Then $\{q = y_r, \ldots, y_s, x\}$ is another cycle having the edge (y, x), but not containing the vertex p. Therefore, the vertex set of this cycle is different from that of C_1, which is impossible.

Next suppose that $p \in V$, $q \notin V$, and $f_j(q) \in V$ for some $j \in \{1, \ldots, n\}$. As in the previous case, we can find a cycle C_1 containing the edge (y, x) such that $C_1 \subset V \cup \{x\}$. Let $f_j(q) = z_0, z_1, \ldots, z_t = y$ be a path in V. (Here $t = 0$ is not excluded; this is the case if $f_j(q) = y$.) Then $C_2 = \{z_0, z_1, \ldots, z_t = y, x, q\}$ is a cycle containing the edge (y, x). Since $q \notin C_1$, the vertex sets of the cycles C_1 and C_2 are different, a contradiction.

The same argument applies if $p \notin V$, $f_i(p) \in V$ for some i, and $q \in V$.

Finally, suppose that $p \notin V$, $f_i(p) \in V$, and $q \notin V$, $f_j(q) \in V$ for some $i, j \in \{1, \ldots, n\}$. As in the previous case, we can find a cycle C_2 containing the edge (y, x) such that $C_2 \subset V \cup \{x, q\}$. Similarly, there exists a cycle C_3 containing (y, x) such that $C_3 \subset V \cup \{x, p\}$. Since $q \notin C_3$, the vertex sets of the cycles C_2 and C_3 are different, which is a contradiction.

We have proved that $V = \bigcup\{U(x) : x \in C\} = E$. Let $E_0 = C$, and $E_i = f_i(C)$ for every $i = 1, \ldots, n$. Since the sets $U(x)$ $(x \in C)$ are pairwise disjoint, it follows that $E_0 \cup E_1 \cup \ldots \cup E_n$ is a decomposition of E, which completes the proof. □

3 Lemmas on isometries of $\mathbb{R}^3$

By a rational parametrization of SO_d we mean an open subset Ω of a Euclidean space $\mathbb{R}^D$ and rational functions with integer coefficients a_{ij} of the real variables $x_1, \ldots, x_D$ $(i, j = 1, \ldots, d)$ such that the denominators of a_{ij} do not vanish on Ω, and the map $v \mapsto (a_{ij}(v))_1^d$ $(v \in \Omega)$ is a surjection from Ω onto SO_d.

The existence of a rational parametrization of SO_d follows, e.g., from the Cayley-transformation [5, IV.22.1]. Another (elementary) way of constructing such a parametrization is the following. It is well-known (and easy to see) that every orthogonal transformation $A \in O_d$ can be obtained as the product (i.e., composition) of at most d reflections about a hyperplane containing the origin. Since the determinant of a reflection is -1, it follows that every $A \in SO_d$ can be obtained as the product of at most d' reflections, where $d' = d$ if d is even, and $d' = d - 1$ if d is odd. Now the number of reflections in the representation must be even, and then we can find representations containing exactly d' reflections by extending the given representation by a suitable even number of factors that equal the same reflection. Therefore, SO_d equals the set of compositions of d' reflections. Let $x = (x_1, \ldots, x_d) \in \mathbb{R}^d, x \neq 0$, and let R_x denote the matrix of the reflection about the hyperplane perpendicular to x. It is easy to check that the entries of the matrix of R_x are rational functions of $x_1, \ldots, x_d$ with integer coefficients and with denominator $x_1^2 + \ldots + x_d^2$. Now we put $D = d \cdot d'$ and $\Omega = \left(\mathbb{R}^d \setminus \{0\}\right)^{d'}$. If $v = (v_1, \ldots, v_{d'})$, where $v_1, \ldots, v_{d'} \in \mathbb{R}^d \setminus \{0\}$, then we define a_{ij} as the (i, j)'s entry of the matrix of $R_{v_1} \cdots R_{v_{d'}}$ for every $i, j = 1, \ldots, d$. Then a_{ij} is a rational function of the coordinates of $v \in \mathbb{R}^D$. Moreover, if $v = (x_1, \ldots, x_D)$, then the denominator of a_{ij} equals $(x_1^2 + \ldots + x_d^2) \cdots (x_{D-d+1}^2 + \ldots + x_D^2)$, which does not vanish in Ω.

In the sequel we fix a rational parametrization of SO_3. If $v \in \Omega \subset \mathbb{R}^6$, then we shall denote by O_v the image of the parametrization; both as a matrix and as a linear transformation of $\mathbb{R}^3$. Then $v \mapsto O_v$ is a surjection from Ω onto SO_3, and every entry of the matrix of O_v is a rational function with integer coefficients of the coordinates of v.

If $b \in \mathbb{R}^3$ then we shall denote by T_b the translation by b.

Lemma 3.1. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ are algebraically independent over the rationals, and let $b \in \mathbb{R}^3$ be an arbitrary vector. If H denotes the group generated by the transformations $O_{v_1}, \ldots, O_{v_N}$ and $P = T_b O_{v_0}$, then H is freely generated by $O_{v_1}, \ldots, O_{v_N}$ and P.*

Proof. If the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ are algebraically independent over the rationals, then the matrices $O_{v_0}, \ldots, O_{v_N}$ generate a free subgroup of SO_3. Indeed, suppose that w is a nonempty reduced word on the alphabet $O_{v_0}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$. Then the entries of the matrix w are rational functions with integer coefficients of the coordinates of $v_0, \ldots, v_N$. If w is the identity matrix, then, by the algebraic independence of the coordinates, the entries of the diagonal of w are identically 1, and the other entries of w are identically zero. Thus, for every $u_0, \ldots, u_N \in \Omega$, by replacing O_{v_i} by O_{u_i} in w we always obtain the identity matrix. However, SO_3 contains $N+1$ matrices generating a free group (see [9]). Therefore, we may choose $u_0, \ldots, u_N \in \Omega$ such that $O_{u_0}, \ldots, O_{u_N}$ generate a free group and then, substituting them into w we cannot get the identity matrix. This contradiction shows that w is not the identity.

Now let w be a nonempty reduced word on the alphabet $O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$ and $P^{\pm 1}$, and let $\overline{w}$ be the word obtained from w by substituting P by O_{v_0}. Let W and $\overline{W}$ denote the transformations defined by w and $\overline{w}$. It is easy to see that $W(x) = \overline{W}(x) + c$ for every $x \in \mathbb{R}^3$, where and c is a suitable vector of $\mathbb{R}^3$. Since $\overline{w}$ is a nonempty reduced word on the alphabet $O_{v_0}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$, it follows that $\overline{W}$ is not the identity map, and then W is not the identity either. $\square$

Lemma 3.2. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and of $b \in \mathbb{R}^3$ are algebraically independent over the rationals. Let w be* *a nonempty reduced word on the alphabet $O_{v_0}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$ and T_b. Suppose that the transformation defined by w has a fixed point. Then, if we replace $O_{v_0}, \ldots, O_{v_N}$ by arbitrary elements of SO_3, and replace T_b by an arbitrary translation in the word w, then the transformation obtained is either a translation or has a fixed point.*

Proof. First we introduce the following notation: if V is a 3×3 matrix and $c \in \mathbb{R}^3$, then we denote by $[V; c]$ the matrix obtained from the matrix of U extended by c as a fourth column.

We show that if $U \in SO_3$ and U is not the identity, then the map $T_c U$ has a fixed point if and only if the rank of the matrix $[I - U; c]$ equals 2. Indeed, $T_c U$ has a fixed point if and only if the equation $(I - U)x = c$ has a solution if and only if the rank of $I - U$ equals the rank of $[I - U; c]$. Now the kernel of $I - U$ consist of the fixed points of U; that is, the points of the axis of U, and thus the kernel of $I - U$ has dimension 1. Thus the dimension of the image space of $I - U$ is two; that is, the rank of $[I - U]$ equals two, which proves the statement.

Let w be a nonempty reduced word on the alphabet $O_{v_0}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$ and $(T_b)^{\pm 1}$, and let W be the transformation defined by w. Note that $(T_b)^{-1} = T_{-b}$. Therefore, if we apply the identities $AT_d = T_{Ad}A$ and $T_d T_e = T_{d+e}$ successively, we find that w has the form $T_c U$, where

(i) U is defined by the word $\overline{w}$ obtained from w by deleting the letters $T_b^{\pm 1}$, and

(ii) $c = Cb$, where C is a finite sum of transformations $\pm W_i$, where each W_i is defined by a word on the alphabet $O_{v_0}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$.

Let u_{ij} and c_{ij} denote the entries of the matrices of U and C $(i, j = 1, 2, 3)$. It follows from (i) and (ii) that each of u_{ij} and c_{ij} is a rational function with integer coefficients of the coordinates of $v_0, \ldots, v_N$. Also, by (ii) we find that the coordinates c_1, c_2, c_3 of the vector c are rational functions with integer coefficients of the coordinates of $v_0, \ldots, v_N$ and b.

By Lemma 3.1, $W = T_c U$ is not the identity map. Since W has a fixed point by assumption, it follows that W is not a translation, and thus U is not the identity. As we saw above, this implies that $W = T_c U$ has a fixed point if and only if the rank of the matrix $[I - U; c]$ equals two. Now the rank of $I - U$ equals two, and thus this condition holds if and only if each of the 3×3 subdeterminants of $[I - U; c]$ vanishes. Each of these determinants are rational functions with integer coefficients of the coordinates of $v_0, \dots, v_N$ and b. If these are zero, then they must be identically zero.

Let $u_0, \dots, u_N \in \Omega$ and $b' \in \mathbb{R}^3$ be arbitrary, and let w' denote the word obtained from w by substituting $O_{v_i}^{\pm 1}$ by $O_{u_i}^{\pm 1}$ for every $i = 0, \dots, N$, and $(T_b)^{\pm 1}$ by $(T_{b'})^{\pm 1}$. It is easy to see that the transformation W' defined by w' is the form $T_{c'}U'$, where the entries u'_{ij} of U' are obtained from u_{ij} by substituting $v_0, \dots, v_N$ by $u_0, \dots, u_N$. Similarly, the coordinates c'_i of the vector c' are obtained from c_i by substituting $v_0, \dots, v_N$ by $u_0, \dots, u_N$ and substituting the coordinates of b by those of b'. This implies that the 3×3 subdeterminants of $[I - U'; c']$ are obtained from the 3×3 subdeterminants of $[I - U; c]$ by the same substitutions. As we proved above, if W has a fixed point, then all these determinants, as rational functions of the variables listed, are identically zero. Therefore, in that case the 3×3 subdeterminants of $[I - U'; c']$ are zero, and thus the rank of $[I - U'; c']$ is at most two. If U' is not the identity, then the rank is exactly two, and thus $W' = T_{c'}U'$ has a fixed point. If U' is the identity, then $W' = T_{c'}$ is a translation.

Since the rational parametrization O_v maps Ω onto SO_3, the transformations $O_{u_0}, \dots, O_{u_N}$ can be arbitrary elements of SO_3, which proves the statement of the lemma. □

The next lemma is essentially due to de Groot [3] (see also [9, Theorem 5.7]). Considering that de Groot's formulation is somewhat different and that the formula on [9, p. 59] contains a misprint, we sketch the proof.

Lemma 3.3. *Let A and B be the rotations in SO_3 given by the matrices*

$$\begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \textit{and} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix},$$

respectively, where the common rotation angle θ is such that $\cos\theta$ is transcendental. If the integers $n_1, m_1, \dots, n_s, m_s$ are nonzero, then the matrix of the transformation $A^{n_1}B^{m_1}\cdots A^{n_s}B^{m_s}$ equals

$$2^{t-2s} \cdot \begin{bmatrix} p_{t-1} & -\mathrm{sgn}\,(n_1) \cdot q_{t-1} \cdot \sin\theta & -\mathrm{sgn}\,(n_1 m_s) \cdot q_t \\ p_{t-2} \cdot \sin\theta & q_t & -\mathrm{sgn}\,(m_s) \cdot q_{t-1} \cdot \sin\theta \\ p_{t-1} & p_{t-2} \cdot \sin\theta & p_{t-1} \end{bmatrix}, \qquad (1)$$

where $t = |n_1| + |m_1| + \ldots + |n_s| + |m_s|$, p_d stands for a polynomial in $\cos\theta$ (possibly different in each entry) with rational coefficients and of degree at *most d, and q_d stands for a monic polynomial in $\cos\theta$ (possibly different in each entry) with rational coefficients and of degree exactly d.*

Proof. It is easy to check by induction on n that

$$A^n = 2^{n-1} \cdot \begin{bmatrix} q_n & -q_{n-1} \cdot \sin\theta & 0 \\ q_{n-1} \cdot \sin\theta & q_n & 0 \\ 0 & 0 & 2^{1-n} \end{bmatrix}$$

for every $n = 1, 2, \ldots$. Since A^n is orthogonal, A^{-n} equals the transpose of A^n, and thus we have

$$A^n = 2^{|n|-1} \cdot \begin{bmatrix} q_{|n|} & -\operatorname{sgn}(n) \cdot q_{|n|-1} \cdot \sin\theta & 0 \\ \operatorname{sgn}(n) \cdot q_{|n|-1} \cdot \sin\theta & q_{|n|} & 0 \\ 0 & 0 & 2^{1-|n|} \end{bmatrix} \tag{2}$$

for every $n \neq 0$. We find, in the same way, that

$$B^m = 2^{|m|-1} \cdot \begin{bmatrix} 2^{1-|m|} & 0 & 0 \\ 0 & q_{|m|} & -\operatorname{sgn}(m) \cdot q_{|m|-1} \cdot \sin\theta \\ 0 & \operatorname{sgn}(m) \cdot q_{|m|-1} \cdot \sin\theta & q_{|m|} \end{bmatrix} \tag{3}$$

for every $m \neq 0$. Multiplying (2) and (3) we can see that (1) is true for $s = 1$. Then it is easy to check by induction on s that (1) is true for every $s \geq 1$. □

Lemma 3.4. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and of $b \in \mathbb{R}^3$ are algebraically independent over the rationals. Put $P = T_b O_{v_0}$, and let w be a nonempty reduced word on the alphabet $O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$ and $P^{\pm 1}$. If the first letter of w is one of $O_{v_i}^{\pm 1}$ $(i = 1, \ldots, N)$ and the last letter of w is $P^{\pm 1}$, then the transformation W defined by w has no fixed point.*

Proof. Let A and B be the transformations (matrices) as in Lemma 3.3. Let p be a positive integer to be fixed later. We shall replace O_{v_i} by $AB^{2^i}A$ for every $i = 1, \ldots, N$, O_{v_0} by A^p, and the vector b by $k = (0, 0, 1)$. By Lemma 3.2, it is enough to show that for a suitable choice of p, under this replacement, w is transformed to a word representing a transformation which is not a translation and has no fixed point.

Let K denote the set of words of the form $A^{n_1}B^{m_1} \cdots A^{n_s}B^{m_s}$, where $s \geq 1$ and $n_1, m_1, \ldots, n_s, m_s$ are nonzero integers. The integer n_1 will be called the *first exponent* of the word $A^{n_1}B^{m_1} \cdots A^{n_s}B^{m_s}$.

It is easy to see that if v is a nonempty reduced word on the alphabet $O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$, then, under the substitution considered, v becomes a word of the form $DA^{\pm 1}$, where $D \in K$, and the first exponent of D equals ± 1. Therefore, under this substitution w becomes a word of the form

$$C = D_1 A^{\varepsilon_1} (T_k A^p)^{r_1} \ldots D_u A^{\varepsilon_u} (T_k A^p)^{r_u},$$

where $D_1, \ldots, D_u \in K$, each of $\varepsilon_1, \ldots, \varepsilon_u$ equals ± 1, and $r_1, \ldots, r_u$ are nonzero integers. Note that in this expression the transformations $D_1, \ldots, D_u$ and the integers ε_i and r_i only depend on w; that is, they do not depend on p.

For every r we have $(T_k A^p)^r = T_{rk} A^{rp}$, since T_k and A commute. Therefore,

$$C = D_1 T_{r_1 k} A^{\varepsilon_1 + r_1 p} D_2 T_{r_2 k} A^{\varepsilon_2 + r_2 p} D_3 T_{r_3 k} \ldots D_u T_{r_u k} A^{\varepsilon_u + r_u p}.$$

We define $E_i = A^{\varepsilon_{i-1} + r_{i-1} p} D_i$ for every $i = 1, \ldots, u$, where we put $r_0 = r_u$. We can choose p so large that $E_i \in K$, and the first exponent of E_i has the same sign as r_{i-1} for every $i = 1, \ldots, u$.

We prove that C is not a translation and has no fixed point. Suppose this is not true. Then $F = A^{\varepsilon_u + r_u p} C A^{-\varepsilon_u - r_u p}$ is a translation or has a fixed point. We have

$$F = E_1 T_{r_1 k} E_2 T_{r_2 k} \ldots E_u T_{r_u k}.$$

Since $M T_d = T_{Md} M$ for every linear transformation M and for every vector d, is follows that $F = T_c E$, where $c = E_1(r_1 k) + E_1 E_2 (r_2 k) + \ldots + E_1 E_2 \ldots E_u (r_u k)$ and $E = E_1 \ldots E_u$. The rotation E is not the identity, since $E_i \in K$ for every i, and A, B generate a free group. Thus F is not a translation.

In order to prove that F has no fixed point, we shall apply the argument of the proof of [9, Theorem 5.7, p. 60]. Let a be a unit vector in the direction of the axis of E; that is, a fixed point of E of unit length. Let ξ denote the angle of rotation of E "looking from the direction of a". (This means that if x is a nonzero vector perpendicular to a, then the orientation of the vectors x, Ex, a is positive.) Since E^2 is not the identity, ξ is not an integer multiple of π, and $\sin \xi \neq 0$.

It is easy to see that the image space of $I - E$ is the plane perpendicular to a. If c does not belong to this plane; that is, if c is not perpendicular to a, then the rank of the matrix $[I - E; c]$ is three, and thus $T_c E$ has no fixed point.

Therefore, it is enough to show that the scalar product $\langle c, a\rangle$ is nonzero. Let $E_1 \ldots E_i = F_i$ for every $i = 1, \ldots, u$. (Thus $F_u = E$.) Then we have

$$\langle c, a\rangle = \sum_{i=1}^{u} r_i \cdot \langle F_i(k), a\rangle. \tag{4}$$

Since F_i is orthogonal, we have $F_i^T = F_i^{-1}$, and thus $\langle F_i(k), a\rangle = \langle k, F_i^{-1}(a)\rangle$.

Note that $F_i^{-1}(a)$ is a unit vector and a fixed point of $F_i^{-1}EF_i$. In other words, $F_i^{-1}(a)$ is a unit vector in the direction of the axis of $F_i^{-1}EF_i$. One can check that the angle of rotation of $F_i^{-1}EF_i$ looking from the direction of $F_i^{-1}(a)$ equals ξ.

Now we use the fact that if x is a unit vector in the direction of the axis of an orthogonal transformation U and ξ is the angle of rotation (looking from the direction of x), then $(2\sin\xi)\cdot x = (a_{32} - a_{23}, a_{13} - a_{31}, a_{21} - a_{12})$, where (a_{ij}) is the matrix of U. (See [9, Theorem A.6, p. 226].) Therefore, if (a_{ij}) is the matrix of $F_i^{-1}EF_i$, then $(2\sin\xi)\cdot F_i^{-1}(a) = (a_{32}-a_{23}, a_{13}-a_{31}, a_{21}-a_{12})$. Since $k = (0, 0, 1)$, it follows that $\langle k, F_i^{-1}(a)\rangle = (2\sin\xi)^{-1}\cdot(a_{21} - a_{12})$.

Since $F_i^{-1}EF_i = E_{i+1}E_{i+2}\ldots E_uE_1, \ldots, E_i$, it follows from Lemma 3.3, that the matrix of $F_i^{-1}EF_i$ is given by (1). We obtain

$$\langle k, F_i^{-1}(a)\rangle = (2\sin\xi)^{-1}\cdot(a_{21} - a_{12}) = 2^{t-2s}\cdot(2\sin\xi)^{-1}\cdot \operatorname{sgn}(n_1)\cdot q_{t-1}\cdot\sin\theta.$$

Note that the value of t and s is the same for every $i = 1, \ldots, u$, and that n_1 stands for the first exponent of E_{i+1}. By the choice of p, this first exponent has the same sign as r_i. Therefore, we find that $r_i\cdot\langle F_i(k), a\rangle$ is of the form $(\sin\theta/\sin\xi)\cdot Q_{t-1}$, where Q_{t-1} is a polynomial of $\cos\theta$ with rational coefficients, of degree $t-1$, and having a positive leading coefficient. Then, by (4), $\langle c, a\rangle$ has the same form. Since $\cos\theta$ is transcendental, this gives $\langle c, a\rangle \neq 0$, which completes the proof. $\square$

Let H be a group of bijections mapping a set X onto itself. By the conjugates of an element $f \in H$ we mean the elements $g^{-1}fg$, where $g \in H$. It is easy to see that a map $f \in H$ has a fixed point if and only if each of its conjugates has a fixed point.

Lemma 3.5. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and $b \in \mathbb{R}^3$ are algebraically independent over the rationals. Let G denote the group generated by the transformations $O_{v_1}, \ldots, O_{v_N}$, and let H denote* *the group generated by the transformations $O_{v_1}, \dots, O_{v_N}$ and P, where $P = T_b O_{v_0}$. Then a map $W \in H$ has a fixed point if and only if it is a conjugate of an element of G.*

Proof. The 'if' part of the statement is obvious: if $g \in G$, then 0 is a fixed point of g, and thus every conjugate of g has a fixed point.

In order to prove the 'only if' part, suppose that $W \in H$ has a fixed point, but W is not a conjugate of any element of G. Let W be such an element represented by a word w on the alphabet $O_{v_0}^{\pm 1}, \dots, O_{v_N}^{\pm 1}, P$ of minimal length. Then w contains one of the letters $P^{\pm 1}$, since otherwise $W \in G$. We show that w is not a power of P. First note that $P = T_b O_{v_0}$ does not have a fixed point, because the rank of the matrix $[I - O_{v_0}; b]$ equals three (this follows from the condition that the coordinates of v_0 and b are algebraically independent over the rationals). Since P does not change orientation, it follows that P is a screw motion with a nonzero translation part. If $n \neq 0$, then P^n is also a screw motion with a nonzero translation part, and hence P^n has no fixed point either.

Therefore, w must contain letters of the form $O_{v_i}^{\pm 1}$ $(i = 1, \dots, N)$ as well. Since W has a fixed point, it follows from Lemma 3.4, that either the first letter of w is one of $P^{\pm 1}$, or the last letter of w is one of $O_{v_i}^{\pm 1}$ $(i = 1, \dots, N)$. Thus $w = uv$, where u ends with one of the letters $P^{\pm 1}$, and u starts with one of the letters $O_i^{\pm 1}$ $(i = 1, \dots, N)$. Then vu is a conjugate of W, and the word vu is not longer then w. Since $w = uv$ has a fixed point, so does vu, and thus its length cannot be shorter than that of w. Thus vu has the same length as w. Consequently, there is no cancellation in vu, and thus vu ends with one of the letters $P^{\pm 1}$, and starts with one of the letters $O_i^{\pm 1}$ $(i = 1, \dots, N)$. Then, by Lemma 3.4, the transformation defined by vu does not have a fixed point. This contradiction completes the proof. □

4 Proof of Theorem 1.2

Let B_3 denote the three dimensional unit ball (either closed or open). We shall prove Theorem 1.2 by finding isometries that satisfy the conditions of Lemma 2.1 with $X = B_3$. Our aim is to prove that the transformations $O_{v_1}, \dots, O_{v_N}$ (restricted to B_3) and $P = T_b O_{v_0}$ (restricted to $B_3 \cap P^{-1}(B_3)$) satisfy these conditions for suitable vectors $v_0, v_1, \dots, v_N \in \Omega$ and $b \in \mathbb{R}^3$.

First we check that the condition on the graph generated by the isometries can be satisfied.

Lemma 4.1. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and $b \in \mathbb{R}^3$ are algebraically independent over the rationals, and let Γ denote the graph on $\mathbb{R}^3$ generated by the transformations $O_{v_1}, \ldots, O_{v_N}$ and $P = T_b O_{v_0}$. Then the graph Γ has the property that whenever two cycles C_1 and C_2 in Γ share a common edge, then the sets of vertices of C_1 and C_2 coincide.*

Proof. We shall prove more: we show that if two cycles have a common nonzero vertex, then they coincide. Let $C = \{x_0, x_1, \ldots, x_n = x_0\}$ be a cycle in Γ. Then, by the definition of Γ, for every $i = 1, \ldots, n$ there is a map $R_i \in \{O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}, P^{\pm 1}\}$ such that $x_i = R_i(x_{i-1})$.

In the word $w = R_n \cdots R_2 R_1$ there is no cancellation, since $R_{i+1} = R_i^{-1}$ would imply $x_{i+1} = R_{i+1}(x_i) = R_i^{-1}(x_i)$, $x_i = R_i(x_{i-1})$ and $x_{i-1} = R_i^{-1}(x_i) = x_{i+1}$, which is impossible. For the same reason, $R_n \neq R_1^{-1}$. Indeed, $R_n = R_1^{-1}$ would imply $x_n = R_n(x_{n-1}) = R_1^{-1}(x_{n-1})$, $x_1 = R_1(x_0) = R_1(x_n)$ and $x_1 = x_{n-1}$, which is impossible. Let W denote the transformation defined by w. Note that x_0 is a fixed point of W.

We claim that $W \in G$, where G denotes the group generated by the transformations $O_{v_1}, \ldots, O_{v_N}$. Since x_0 is a fixed point of W, it follows from Lemma 3.5 that W is a conjugate of an element of G. Then we have $w = v^{-1}uv$, where the word u does not contain the letters $P^{\pm 1}$. If $W \notin G$, then v must contain at least one of the letters $P^{\pm 1}$, and thus v can be written in the form xy, where x does not contain the letters $P^{\pm 1}$, y is reduced, and the first letter of y is one of $P^{\pm 1}$. Then $w = y^{-1}x^{-1}uxy$. Let z denote the reduced form of $x^{-1}vx$. Then z does not contain the letters $P^{\pm 1}$, and thus in the word $y^{-1}zy$ there is no cancellation. Let R denote the last letter of y. Then $w = y^{-1}zy$ implies that the first letter of w equals R^{-1}, and the last letter of w equals R. But, as we proved above, this is impossible, which gives $W \in G$. Therefore, each of the letters of w is one of $O_i^{\pm 1}$ $(i = 1, \ldots, N)$. In particular, $W \in SO_3$.

Now suppose that $C' = \{x'_0, \ldots, x'_m\}$ is another cycle of Γ such that C and C' have a common nonzero vertex. We may assume that $x_0 = x'_0 \neq 0$. Let $x'_i = R'_i(x_{i-1})$ for every $i = 1, \ldots, m$. If $w' = R'_m \cdots R'_2 R'_1$ and W' denotes the transformation defined by w' then, repeating the argument above, we find that w' is reduced, the first letter of w' is not the inverse of the last letter of w', $W' \in G$ and thus $W' \in SO_3$.

Since W and W' have a common fixed point different from the origin, it follows that they have the same axis of rotation, and thus they commute. Therefore, we have $w = z^i$ and $w' = z^j$ for some word z and nonzero integers i, j. Indeed, since G is free, it follows that each subgroup of G is free. Thus the subgroup generated by W and W' is free. But this subgroup is commutative, and thus it must be cyclic. If z is its generator, then we have $w = z^i$ and $w' = z^j$ for some nonzero i and j. Replacing w by w^{-1} (or w' by $(w')^{-1}$) if necessary, we may assume that $i, j > 0$.

We have $w^j = (w')^i$. Since the first and last letter of w are not the inverses of each other, in the power w^j there are no cancellations. The same is true for $(w')^i$, and thus the words w^j and $(w')^i$ are formally equal. By symmetry, we may assume that n (the length of w) is not greater than m (the length of w'). Then we have $R'_i = R_i$ for every $i = 1, \ldots, n$. Thus

$$x'_i = R'_i R'_{i-1} \ldots R'_1(x'_0) = R_i R_{i-1} \ldots R_1(x_0) = x_i$$

for every $i = 1, \ldots, n$. Since $x_n = x_0$, this implies that $m = n$, and $C' = C$. This completes the proof. □

Let $v_1, \ldots, v_N \in \Omega$ be fixed, and put $\ell_i = \{x \in \mathbb{R}^3 : O_{v_i}(x) = x\}$ and $\ell_{i,j} = \{x \in \mathbb{R}^3 : O_{v_i}^{-1} O_{v_j}(x) = x\}$ for every $i, j = 1, \ldots, N,\ i \neq j$. Then ℓ_i is the axis of rotation of O_{v_i}, and $\ell_{i,j}$ is the axis of rotation of $O_{v_i}^{-1} O_{v_j}$. Note that $\ell_{i,j} = \ell_{j,i}$ for every $i \neq j$. Let L denote the union of the sets ℓ_i and $\ell_{i,j}$ ($i, j = 1, \ldots, N,\ i \neq j$). Note that if $x \notin L$, then the points $x, O_{v_1}(x), \ldots, O_{v_N}(x)$ are distinct. We put $I_x = \{i \in \{1, \ldots, N\} : O_{v_i}^{-1}(x) \in L\}$ for every x.

Lemma 4.2. *Suppose that the coordinates of the vectors $v_1, \ldots, v_N \in \Omega$ are algebraically independent over the rationals. Then*

(i) *if $i \neq j,\ k \neq n$ and $\{i, j\} \neq \{k, n\}$, then $\ell_{i,j} \cap \ell_{k,n} = \{0\}$;*

(ii) *if $x \neq 0$ and $x \in \ell_{i,j}$ for some $1 \leq i < j \leq N$, then $I_x = \emptyset$;*

(iii) *I_x contains at most two indices for every $x \neq 0$.*

Proof. (i) Suppose $x \in \ell_{i,j} \cap \ell_{k,n}$ and $x \neq 0$. Thus x is a common fixed point of $O_{v_i}^{-1} O_{v_j}$ and $O_{v_k}^{-1} O_{v_n}$. Then these rotations must commute, since their axis of rotation coincides. However, it is easy to check that if $\{i, j\} \neq \{k, n\}$, then the words $O_{v_i}^{-1} O_{v_j}$ and $O_{v_k}^{-1} O_{v_n}$ do not commute. Since the transformations O_{v_i} ($i = 1, \ldots, N$) generate a free group by Lemma 3.1, this is a contradiction.

(ii) Suppose that $i \neq j$, $x \in \ell_{i,j} \setminus \{0\}$, and $k \in I_x$. If $O_{v_k}^{-1}(x) \in \ell_m$, then x is a common fixed point of $O_{v_i}^{-1}O_{v_j}$ and $O_{v_k}O_{v_m}O_{v_k}^{-1}$. Therefore, they must commute. However, it is easy to check that if $i \neq j$ then the words $O_{v_i}^{-1}O_{v_j}$ and $O_{v_k}O_{v_m}O_{v_k}^{-1}$ do not commute for any choice of k and m, which is a contradiction.

Next suppose that $O_{v_k}^{-1}(x) \in \ell_{n,m}$, where $n \neq m$. Then x is a common fixed point of $O_{v_i}^{-1}O_{v_j}$ and $O_{v_k}O_{v_n}^{-1}O_{v_m}O_{v_k}^{-1}$. Therefore, they must commute. However, it is easy to check that if $i \neq j$ and $n \neq m$ then these words do not commute for any choice of k, which is a contradiction.

(iii) Suppose that $x \neq 0$ and $k, n \in I_x$, where $k \neq n$. We prove that in this case $O_{v_k}^{-1}(x)$ belongs to $\ell_{k,n}$. There are several cases to consider.

I. Suppose that $O_{v_k}^{-1}(x) \in \ell_i$, and $O_{v_n}^{-1}(x) \in \ell_j$. Then x is a common fixed point of $O_{v_k}O_{v_i}O_{v_k}^{-1}$ and $O_{v_n}O_{v_j}O_{v_n}^{-1}$. Then these rotations must commute. Now the word $u = O_{v_k}O_{v_i}O_{v_k}^{-1}$ is either reduced (if $i \neq k$) or equals O_{v_k} (if $i = k$). Similarly, the word $v = O_{v_n}O_{v_j}O_{v_n}^{-1}$ is either reduced or equals O_{v_n}. It is easy to check that in each of these cases we have $uv \neq vu$, which is impossible.

II. Suppose that $O_{v_k}^{-1}(x) \in \ell_i$, and $O_{v_n}^{-1}(x) \in \ell_{j,m}$, where $j \neq m$. Then x is a common fixed point of $O_{v_k}O_{v_i}O_{v_k}^{-1}$ and $O_{v_k}O_{v_j}^{-1}O_{v_m}O_{v_n}^{-1}$.

The word $u = O_{v_k}O_{v_i}O_{v_k}^{-1}$ is either reduced or equals O_{v_k}. On the other hand, the word $v = O_{v_n}O_{v_j}^{-1}O_{v_m}O_{v_n}^{-1}$ is either reduced, or equals $O_{v_m}O_{v_n}^{-1}$ where $m \neq n$, or $O_{v_n}O_{v_j}^{-1}$ with $j \neq n$. (Note that at least one of j and m is different from n, as $j \neq m$.) It is easy to check that in each of these cases we have $uv \neq vu$, and thus this case cannot occur either.

III. The case when $O_{v_k}^{-1}(x) \in \ell_{j,m}$ $(j \neq m)$ and $O_{v_n}^{-1}(x) \in \ell_i$ is similar to II.

IV. Finally, we suppose $O_{v_k}^{-1}(x) \in \ell_{i,j}$ $(i \neq j)$ and $O_{v_n}^{-1}(x) \in \ell_{m,p}$ $(m \neq p)$. Then x is a common fixed point of $O_{v_k}O_{v_i}^{-1}O_{v_j}O_{v_k}^{-1}$ and $O_{v_n}O_{v_m}^{-1}O_{v_p}O_{v_n}^{-1}$.

The word $u = O_{v_k}O_{v_i}^{-1}O_{v_j}O_{v_k}^{-1}$ is either reduced or equals $O_{v_k}O_{v_i}^{-1}$ where $i \neq k$, or $O_{v_j}O_{v_k}^{-1}$ with $j \neq k$. Similarly, the word $v = O_{v_n}O_{v_m}^{-1}O_{v_p}O_{v_n}^{-1}$ is either reduced or equals $O_{v_n}O_{v_m}^{-1}$ where $m \neq n$, or $O_{v_p}O_{v_n}^{-1}$ with $p \neq n$. It is easy to check, by inspecting each of the 9 cases, that the condition $uv = vu$ is satisfied only if $\{i, j\} = \{m, p\} = \{k, n\}$. Therefore, we have $O_{v_k}^{-1}(x) \in \ell_{k,n}$.

We have proved the following: if $x \neq 0$ and n, k are different elements of

I_x, then $O_{v_k}^{-1}(x) \in \ell_{k,n}$. Suppose that k, n, p are distinct elements of I_x. Then we have $O_{v_k}^{-1}(x) \in \ell_{k,n} \cap \ell_{k,p}$, which contradicts (i). Thus I_x cannot have more than two elements. $\square$

For every isometry f we shall denote by f^* the restriction of f to the set $B_3 \cap f^{-1}(B_3)$. Thus f^* maps a subset of B_3 into B_3. (If $f \in SO_3$ then f^* is the restriction of f to B_3.)

Lemma 4.3. *Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and $b \in \mathbb{R}^3$ are algebraically independent over the rationals. Suppose further that $\|O_{v_0} - I\| < 0.01$ (I denotes the identity), and that $b = (b_1, b_2, b_3)$, where $0.09 < b_1 < 0.1$ and $0 < b_2, b_3 < 0.001$. Let Γ^* denote the graph on B_3 generated by the transformations $O_{v_1}^*, \ldots, O_{v_N}^*$ and P^*, where $P = T_b O_{v_0}$.*

If $x \in B_3 \setminus L$ and $P(x) \in B_3$, then x is a core point. In particular, if $x = (x_1, x_2, x_3) \in B_3 \setminus L$ and $x_1 < -0.29$, then x is a core point.

Proof. Since $x \notin L$, the points $x, O_{v_1}(x), \ldots, O_{v_N}(x)$ are distinct. The transformations P and $PO_{v_i}^{-1}$ $(i = 1, \ldots, N)$ have no fixed points by Lemma 3.5, and thus $P(x)$ is different from each of the points $x, O_{v_1}(x), \ldots, O_{v_N}(x)$. If $P(x) \in B_3$, then x belongs to the domain of P^* and clearly to each of $O_{v_1}^*$, and thus x is a core point.

In order to finish the proof we have to show that if $x_1 < -0.29$, then $P(x) \in B_3$.

Let $O_{v_0}(x) = y = (y_1, y_2, y_3)$. Since $\|O_{v_0} - I\| < 0.01$, we have $|y - x| < 0.01$, and thus $y_1 < -0.28$. We have to show that $y + b = T_b(y) \in B_3$. Let $b' = (b_1, 0, 0)$. Then $|b - b'| \le |b_2| + |b_3| < 0.01$. Also, we have

$$|y + b'|^2 = (y_1 + b_1)^2 + y_2^2 + y_3^2 \le (y_1 + b_1)^2 + 1 - y_1^2 = b_1(2y_1 + b_1) + 1 <$$
$$< 0.09 \cdot (-0.56 + 0.1) + 1 < 0.96$$

and $|y + b| \le |y + b'| + |b - b'| < \sqrt{0.96} + 0.01 < 1$, which proves $y + b \in B_3$. $\square$

We shall denote by S_2 the unit sphere $\{x \in \mathbb{R}^3 : |x| = 1\}$.

Lemma 4.4. *There are rotations $A_1, A_2, A_3, A_4 \in SO_3$ with the following property: for every $x \in S_2$ there is an $i \in \{1, 2, 3, 4\}$ such that the first coordinate of $A_i(x)$ is at most $-1/3$.*

Proof. The points $p_1 = (-1,0,0)$, $p_2 = (1/3, \sqrt{8}/3, 0)$, $p_3 = (1/3, -\sqrt{2}/3, \sqrt{2/3})$ and $p_4 = (1/3, -\sqrt{2}/3, -\sqrt{2/3})$ are the vertices of a regular tetrahedron inscribed in S_2. It is easy to see that for every $i = 1,2,3,4$ there is a rotation $A_i \in SO_3$ such that $A_i(p_i) = p_1$. We show that $A_1, \ldots, A_4$ satisfy the requirement.

First we prove that for every $x \in S_2$ there is an $i \in \{1,2,3,4\}$ such that $|x - p_i| \le 2/\sqrt{3}$. The function $d(x) = \min_{1 \le i \le 4} |x - p_i|$ is continuous, and thus it attains its maximum on S_2. If $d(x)$ is maximal at a point $x \in S_2$, then $|x - p_i| = d(x)$ is satisfied for at least three of the indices $i = 1, \ldots, 4$, because otherwise the value of $d(x)$ could be increased by moving x in an appropriate direction on S_2. Therefore, the maximum of d is attained at four points, and one of them is $(1,0,0)$. Easy computation shows that for $x = (1,0,0)$ we have $d(x) = 2/\sqrt{3}$.

Let $x \in S_2$ be arbitrary, and let $i \in \{1,2,3,4\}$ be such that $|x - p_i| \le 2/\sqrt{3}$. Then the distance between the points $A_i(x)$ and $A_i(p_i) = p_1$ is at most $2/\sqrt{3}$. It is easy to check that if $y \in S_2$ and $|y - p_1| \le 2/\sqrt{3}$, then the first coordinate of the point y is at most $-1/3$. □

Lemma 4.5. *Let $A_1, A_2, A_3, A_4 \in SO_3$ be as in the previous lemma. Suppose that the coordinates of the vectors $v_0, v_1, \ldots, v_N \in \Omega$ and $b \in \mathbb{R}^3$ are algebraically independent over the rationals. Suppose further that*

(i) $\|O_{v_0} - I\| < 0.01$;

(ii) *for every $i = 1,2,3,4$ there are at least five indices $1 \le j \le N$ such that $\|O_{v_j} - A_i^{-1}\| < 0.01$;*

(iii) $b = (b_1, b_2, b_3)$, *where* $0.09 < b_1 < 0.091$ *and* $0 < b_2, b_3 < 0.001$.

Then there is a set $E \subset B_3$ such that the sets $E, T_b O_{v_0}(E)$, $O_{v_j}(E)$ $(j = 1, \ldots, N)$ constitute a partition of B_3. In particular, B_3 is $N+2$-divisible.

Proof. We check that the conditions of Lemma 2.1 are satisfied for the transformations $O^*_{v_1}, \ldots, O^*_{v_N}$ and P^*, where $P = T_b O_{v_0}$.

The condition on the cycles of the graph is satisfied by Lemma 4.1. Indeed, the graph Γ^* generated by the transformations $O^*_{v_1}, \ldots, O^*_{v_N}$ and P^* is a subgraph of the graph Γ generated by $O_{v_1}, \ldots, O_{v_N}$ and P. If two cycles of Γ^* share a common edge then they also share an edge in Γ and then, by Lemma 4.1, they have the same set of vertices.

We show that conditions (i) and (ii) of Lemma 2.1 are satisfied with $x_0 = 0$. In order to check (i) it is enough to show that $P^{-1}(0)$ is a core point. It is clear that $P^{-1}(0) \in B_3$. Therefore, it is enough to prove that the points $P^{-1}(0)$ and $O_{v_i}P^{-1}(0)$ $(i = 1, \ldots, N)$ are distinct (nonzero) elements of B_3.

Suppose that $P^{-1}(0) = O_{v_i}P^{-1}(0)$ for some $1 \le i \le N$. Then, by $P^{-1} = O_{v_0}^{-1}T_{-b}$, we have $-O_{v_0}^{-1}(b) = -O_{v_i}O_{v_0}^{-1}(b)$. Since the coordinates of v_0, v_i and b are algebraically independent over the rationals, this must be an identity in the sense that whenever $U, V \in SO_3$ and $c \in \mathbb{R}^3$, then $U^{-1}(c) = VU^{-1}(c)$, which is clearly impossible.

Next suppose that $O_{v_i}P^{-1}(0) = O_{v_j}P^{-1}(0)$ for some $i \neq j$. Then $-O_{v_i}O_{v_0}^{-1}(b) = -O_{v_j}O_{v_0}^{-1}(b)$, and we obtain a contradiction in the same way.

Now we check that condition (ii) of Lemma 2.1 is satisfied. We have to prove that every $x \in B_3 \setminus \{0\}$ is in the image of at least three core points. By Lemma 4.3, it is enough to show that x is the image of at least three points $y \in B_3 \setminus L$ such that $P(y) \in B_3$.

Let $x \in B_3 \setminus \{0\}$ be arbitrary. We show that there are at least $N - 2$ indices $1 \le i \le N$ such that the corresponding elements $O_{v_i}^{-1}(x)$ are distinct and are not in L. First suppose that $x \in \ell_{k,n}$ for some $1 \le k < n \le N$. Then, by (ii) of Lemma 4.2, $O_{v_j}^{-1}(x) \notin L$ for every $j = 1, \ldots, N$. If $O_{v_i}^{-1}(x) = O_{v_j}^{-1}(x)$ for some $i \neq j$, then $x \in \ell_{i,j}$, and thus we have $\{i, j\} = \{k, n\}$ by (i) of Lemma 4.2. This means that the points $O_{v_i}^{-1}(x)$ $(1 \le i \le N,\ i \neq k)$ are distinct and are not in L.

Next suppose that $x \notin \ell_{i,j}$ for every $i \neq j$. Then the elements $O_{v_i}^{-1}(x)$ $(i = 1, \ldots, N)$ are distinct. By (iii) of Lemma 4.2, at least $N-2$ of these elements are outside L, proving the statement.

If $|x| \le 0.9$, then $|O_{v_i}^{-1}(x)| \le 0.9$ and $PO_{v_i}^{-1}(x) \in B_3$ for every $i = 1, \ldots, N$ by $|b| < 0.1$. According to the previous remarks, this implies that there are at least $N-2$ indices $1 \le j \le N$ for which $O_{v_j}^{-1}(x)$ is a core point. Therefore, in this case condition (ii) of Lemma 2.1 is satisfied.

Suppose that $|x| > 0.9$. By Lemma 4.4, there is an $i \in \{1, 2, 3, 4\}$ such that the first coordinate of $A_i(x)$ is at most $(-1/3) \cdot |x| < -(1/3) \cdot 0.9 < -0.3$. By assumption, there are five indices $1 \le j \le N$ such that $\|O_{v_j}^{-1} - A_i\| < 0.01$. If j is such an index, then the first coordinate of $O_{v_j}^{-1}(x)$ is less than -0.29.

By Lemma 4.3, $O_{v_j}^{-1}(x)$ will be a core point provided it is not an element of L. We have seen that with the exception of two indices, the points $O_{v_j}^{-1}(x)$ are distinct and are not elements of L. Therefore, there are at least three indices j such that $O_{v_j}^{-1}(x)$ is a core point; that is, condition (ii) of Lemma 2.1 is satisfied in this case as well, which completes the proof. $\square$

Proof of Theorem 1.2. Let $m \geq 22$ be arbitrary, and put $N = m - 2$. Then we have $N \geq 20$. It is well-known that there is an everywhere dense subset of $\mathbb{R}$ whose elements are algebraically independent over the rationals. Since the map $v \mapsto O_v$ is a continuous surjection from Ω onto SO_3, we can find vectors $v_0, \ldots, v_N, b \in \mathbb{R}^3$ such that the conditions of Lemma 4.5 are satisfied. Thus B_3 is m-divisible. $\square$

5 Proof of Theorem 1.1

Let $d = 3s$, and let B_d denote the d dimensional unit ball (either closed or open). Let $\eta = 1/(100s^2)$. We can find a finite subset F of the sphere $S_2 = \{x \in \mathbb{R}^3 : |x| = 1\}$ such that $\operatorname{dist}(x, F) < \eta$ for every $x \in S_2$. For every $x \in F$ let $O_x \in SO_3$ be a rotation such that $O_x(x) = (-1, 0, 0)$, and put $\mathcal{A} = \{O_x : x \in F\}$. It is clear that $\mathcal{A}$ has the following property: for every $x \in B_3$ there exists an $O \in \mathcal{A}$ such that $O(x) = (x_1, x_2, x_3)$, where $x_1 \leq 0$ and $|x_2|, |x_3| < \eta$. Let $\{A_1, \ldots, A_n\}$ be an enumeration of the elements of $\mathcal{A}$.

We shall prove that B_d is m-divisible for every $m \geq 5n^s + 2$. Suppose that $m = N + 2$, where $N \geq 5n^2$. Using the facts that the parametrization $v \mapsto O_v$ is a continuous function of v, and that there exists an everywhere dense subset of $\mathbb{R}$ whose elements are algebriacally independent over $\mathbb{Q}$, we can find a system of vectors $v_j^k \in \Omega$ $(k = 0, \ldots, N,\ j = 1, \ldots, s)$ and $b = (b_1, \ldots, b_d) \in \mathbb{R}^d$ with the following properties.

(i) The coordinates of v_j^k and of c are algebriacally independent over $\mathbb{Q}$.

(ii) We have $\|O_{v_j^0} - I\| < \eta$ for every $j = 1, \ldots, s$.

(iii) For every $1 \leq i_1, \ldots, i_s \leq n$ there are at least five indices $1 \leq k \leq N$ such that $\|O_{v_j^k} - A_{i_j}^{-1}\| < \eta$ for every $j = 1, \ldots, s$.

(iv) $1/(8s) < b_i < 1/(4s)$ for every $i = 1, \ldots, d$.

We represent $\mathbb{R}^d$ as $V_1 \times \ldots \times V_s$, where $V_j = \{(x_1, \ldots, x_d) : x_i = 0$ for every $i \neq 3j-2, 3j-1, 3j\}$ $(j = 1, \ldots, s)$. We shall identify V_j with $\mathbb{R}^3$ for every $j = 1, \ldots, s$. For every $k = 0, \ldots, N$ there is a transformation $O_k \in SO_d$ such that $O_k(x) = O_{v_j^k}(x)$ for every $x \in V_j$ $(j = 1, \ldots, s)$. Our aim is to prove that the transformations $O_1, \ldots, O_N$ (restricted to B_d) and $Q = T_b O_0$ (restricted to $B_d \cap Q^{-1}(B_d)$) satisfy the conditions of Lemma 2.1 with $X = B_d$ and $x_0 = 0$.

First we check that the condition on the graph Γ generated by the isometries $O_1, \ldots, O_N$ and Q is satisfied. It is clear that the transformations $O_1, \ldots, O_N$ and Q generate a free group. We show that whenever two cycles C and C' in Γ share a common nonzero vertex, then the cycles C and C' coincide.

Let $C = \{y_0, y_1, \ldots, y_p = y_0\}$ and $C = \{y'_0, y'_1, \ldots, y'_q = y'_0\}$ be two cycles in Γ such that $0 \neq y_0 = y'_0$. Then, by the definition of Γ, for every $i = 1, \ldots, p$ there is a map $R_i \in \{O_1^{\pm 1}, \ldots, O_N^{\pm 1}, Q^{\pm 1}\}$ such that $y_i = R_i(y_{i-1})$, and for every $i = 1, \ldots, q$ there is a map $R'_i \in \{O_1^{\pm 1}, \ldots, O_N^{\pm 1}, Q^{\pm 1}\}$ such that $y'_i = R_i(y'_{i-1})$.

As we saw in the proof of Lemma 4.1, in the words $w = R_p \cdots R_2 R_1$ and $w' = R'_q \cdots R'_2 R'_1$ there is no cancellation, moreover, $R_p \neq R_1^{-1}$ and $R'_q \neq (R'_1)^{-1}$. Let W and W' denote the transformations defined by w and w'. Then $y_0 = y'_0$ is a common fixed point of W and W'.

Let π_j denote the projection of $\mathbb{R}^d$ onto V_j $(j = 1, \ldots, s)$. Since $y_0 \neq 0$, we can fix a j such that $\pi_j(y_0) \neq 0$. Let $P_j \in SO_3$ be defined by

$$P_j = T_{(c_{3j-2}, c_{3j-1}, c_{3j})} O_{v_j^0}.$$

We denote by $\overline{w}$ denote the word obtained from w by replacing the letter $O_k^{\pm 1}$ by $O_{v_j^k}^{\pm 1}$ and Q by P_j. Let $\overline{W}$ be the transformation defined by $\overline{w}$. It is easy to see that for every $x \in \mathbb{R}^d$ we have

$$\overline{W}(\pi_j(x)) = \pi_j\left(W(x)\right)$$

and, similarly,

$$\overline{W'}(\pi_j(x)) = \pi_j\left(W'(x)\right).$$

Since $\overline{W}$ and $\overline{W'}$ have a common nonzero fixed point (namely, $\pi_j(y_0)$), it follows from the argument of the proof of Lemma 4.1, that we have either

$\overline{W} = \overline{W'}$ or $\overline{W} = \overline{W'}^{-1}$. This implies that we have either $R = R'$ or $R = (R')^{-1}$, and thus the cycles C and C' coincide.

Next we show that for every $x \in B_d$ there are five indices $k \in \{1, \ldots, N\}$ such that $QO_k^{-1}(x) \in B_d$. Let $x \in B_d$ be fixed. By the choice of the rotations $A_1, \ldots, A_n$, there are indices $i_1, \ldots, i_s$ such that for every $j = 1, \ldots, s$, the first coordinate of $A_{i_j}(\pi_j(x))$ is nonpositive, and the absolute value of the other two coordinates of $A_{i_j}(\pi_j(x))$ is less than η. Then it follows from (ii) and (iii) above that there are five indices $k \in \{1, \ldots, N\}$ such that the vector $y = O_0 O_k^{-1}(x)$ has the following property: if $y = (y_1, \ldots, y_d)$, then $y_{3j-2} < 2\eta$ and $|y_{3j-1}|, |y_{3j}| < 2\eta$ for every $j = 1, \ldots, s$. We show that $QO_k(x) \in B_d$ for all such k.

It is enough to prove that $|Q(y)| < 1$. Let $z = (z_1, \ldots, z_d)$, where $z_{3j-2} = \min(y_{3j-2}, 0)$ and $z_{3j-1} = z_{3j} = 0$ for every $j = 1, \ldots, s$. Then $|y - z| < 6s\eta$, and thus $|Q(y) - Q(z)| < 6s\eta$. It is enough to show that $|Q(z)| < 1 - 6s\eta$. We have

$$\sum_{j=1}^{s} z_{3j-2} b_{3j-2} \le \frac{1}{8s} \sum_{j=1}^{s} z_{3j-2} \le -\frac{1}{8s} \sum_{j=1}^{s} z_{3j-2}^2 = -\frac{|z|^2}{8s}.$$

Since $Q(z) = (z_1 + b_1, \ldots, z_d + b_d)$, this implies

$$\begin{aligned} |Q(z)|^2 &= |z + b|^2 = \\ &= \sum_{j=1}^{s} (z_{3j-2}^2 + 2 z_{3j-2} b_{3j-2} + b_{3j-2}^2) + \sum_{j=1}^{s} (b_{3j-1}^2 + b_{3j}^2) \le \\ &\le |z|^2 - \frac{|z|^2}{4s} + 3s \cdot \frac{1}{16s^2} = |z|^2 \cdot \left(1 - \frac{1}{4s}\right) + \frac{3}{16s} \le \\ &\le 1 - \frac{1}{4s} + \frac{3}{16s} = 1 - \frac{1}{16s} < 1 - 6s\eta, \end{aligned}$$

since $\eta < 1/(96s^2)$. This proves the statement.

Now we prove that the conditions (i) and (ii) of Lemma 2.1 are satisfied with $x_0 = 0$. Note that for every j, the coordinates of $v_j^0, \ldots, v_j^N$ and of $(c_{3j-2}, c_{3j-1}, c_{3j})$ are algebraically independent over $\mathbb{Q}$. By the argument of the proof of Theorem 1.2, for every j, the points $P_j^{-1}(0)$ and $O_{v_j^k} P_j^{-1}(0)$ ($k = 1, \ldots, N$) are distinct nonzero elements of B_3. Since $P_j^{-1}(0) = \pi_j(Q^{-1}(0))$ and $O_{v_j^i} P_j^{-1}(0) = \pi_j(O_k Q^{-1}(0))$ for every $k = 1, \ldots, N$, it follows that the points $Q^{-1}(0)$ and $O_k Q^{-1}(0)$ $(k = 1, \dots, N)$ are distinct nonzero elements of B_d. Thus $Q^{-1}(0)$ is a core point; that is, (i) of Lemma 2.1 is satisfied.

Let $x \in B_d$, $x \neq 0$ be arbitrary. Then there is a j such that $\pi_j(x) \neq 0$. In the proof of Theorem 1.2 it was shown that there are at least $N-2$ indices k for which the points $O_{v_j^k}^{-1}(\pi_j(x))$ are distinct, and are core points with respect to the graph generated by the transformations $O_{v_j^i}$ $(i = 1, \dots, N)$ and P_j. In particular, for each of these indices k, the points $O_{v_j^i} O_{v_j^k}^{-1}(\pi_j(x))$ $(i = 1, \dots, N)$ and $P_j O_{v_j^k}^{-1}(\pi_j(x))$ are distinct. Then it follows that for each of these indices k, the points

$$O_k^{-1}(x), \quad QO_k^{-1}(x) \quad \text{and} \quad O_i O_k^{-1}(x) \qquad (i = 1, \dots, N) \tag{5}$$

are distinct. As we proved above, there are five indices k for which the points listed in (5) belong to B_d. Therefore, at least three of these indices k have the property that the points listed in (5) are distinct and belong to B_d. Therefore, these points are distinct core points, and thus the condition (ii) of Lemma 2.1 is satisfied. □

6 Concluding remarks

Since the transformation group O_2 does not contain noncommutative free subgroups, our method cannot say anything about the divisibility of discs. As for $d = 3$, the question whether or not B_3 is m-divisible for $4 \leq m \leq 21$ also remains open. There are several obstacles in the way of improving the bound 22. One of them is the condition of Lemma 2.1 which requires that every point $x \neq x_0$ be in the image of at least three core points. This condition cannot be relaxed; in fact, Lemma 2.1 is sharp, as the following example shows.

Example 6.1. *For every $n \geq 2$ there exists a set X and there are maps $f_1, \dots, f_n$ from subsets of X into X with the following properties.*

(i) *Every point of X is in the image of at least two core points.*

(ii) *The graph generated by the maps $f_1, \dots, f_n$ only contains one cycle.*

(iii) *There is no decomposition $X = A_0 \cup A_1 \cup \ldots \cup A_n$ such that $f_1, \dots, f_n$ are defined on A_0, and $f_i(A_0) = A_i$ for every $i = 1, \dots, n$.*

First we sketch the construction for $n = 2$. We define a graph Γ as follows. Let $P_0, \dots, P_5$ be distinct points, and let V_0, V_2, V_4 be pairwise disjoint countably infinite sets not containing the points $P_0, \dots, P_5$. The vertex set of the graph Γ will be $X = V_0 \cup V_2 \cup V_4 \cup \{P_0, \dots, P_5\}$. For every $i = 0, 2, 4$ let T_i be a tree on the set $V_i \cup \{P_i\}$ such that the degree of the point P_i is two, and the degree of each point $x \in V_i$ is four. Let Γ be the union of the trees T_0, T_2, T_4 together with the edges (P_i, P_{i+1}) $(i = 0, \dots, 5)$, where $P_6 = P_0$. Then the graph Γ only contains one cycle, namely the hexagon $(P_0, \dots, P_5)$.

Now we direct the edges of Γ in such a way that for each of $i = 1, 3, 5$ the two edges meeting at P_i are directed towards P_i, and at every other point $x \in X$, two of the four edges meeting at x are directed outwards, and the other two are directed towards x. It is easy to see that this is possible. Then we 'colour' the directed edges by the 'colours' f_1 and f_2 as follows. The directed edges $\overrightarrow{P_0P_1}$, $\overrightarrow{P_2P_3}$, $\overrightarrow{P_4P_0}$ have colour f_1, and the directed edges $\overrightarrow{P_2P_1}$, $\overrightarrow{P_4P_3}$, $\overrightarrow{P_0P_5}$, have colour f_2. Every other edge will be coloured in such a way that, for every $x \in X \setminus \{P_1, P_3, P_5\}$, one of the two outgoing edges has colour f_1, the other has colour f_2, one of the two edges directed towards x has colour f_1, and the other has colour f_2. Again, it is easy to check that this is possible.

Then we define f_1 and f_2 on the set $D = X \setminus \{P_1, P_3, P_5\}$ as follows. If $x \in D$, then let $f_i(x) = y$, if the edge (x, y) is directed towards y and has colour f_i $(i = 1, 2)$. It is clear that f_1, f_2 are defined on D, they map D onto X, every point of D is a core point, and that (i) is satisfied. We prove (iii). Suppose that $X = A_0 \cup A_1 \cup A_2$ is a decomposition such that f_1 and f_2 are defined on A_0, $f_1(A_0) = A_1$ and $f_2(A_0) = A_2$. Since f_1, f_2 are not defined at P_1, we have $P_1 \notin A_0$. If A_0 does not contain any of the points P_0, P_2 then $P_1 \notin A_1 \cup A_2$ which is impossible. If $P_0 \in A_0$, then A_0 cannot contain any of the points P_2 and P_4, because otherwise A_1 and A_2 would not be disjoint. Thus $P_2, P_4 \notin A_2$, and then $P_3 \notin A_0 \cup A_1 \cup A_2$ which is absurd. We get a similar contradiction if $P_2 \in A_0$.

If $n > 2$, then the construction is similar, but we have to start with 6 trees, $T_0, \dots, T_5$, such that for $i = 0, 2, 4$ the degree of P_i equals $2n - 2$, for $i = 1, 3, 5$ the degree of P_i equals $2n - 4$, and the degree of every point $x \neq P_0, \dots, P_5$ is $2n$. We omit the details.

Now we turn to the questions concerning higher dimensions. In the proof of Theorem 1.1 we showed that if $m \geq m_d = 5n^s + 2$, then B_d is m-divisible. Here $d = 3s$, and n is the size of the smallest subset F of the sphere S_2

such that $\text{dist}\,(x, F) < 1/(100s^2)$ for every $x \in S_2$. It is easy to see that $n \geq c \cdot s^4$ with an absolute positive constant c, and thus $m_d \geq \exp\,(c_1 d \log d)$. It would be desirable to improve this bound, especially because a substantial improvement would need new ideas.

The most important question is whether or not B_d is divisible for every $d \geq 3$. It is very likely that the answer is affirmative; however, our proof does not seem to work in the general case. The crucial step in the proof of Theorems 1.1 and 1.2 is Lemma 4.1 which states that the condition of Lemma 2.1 on the graph generated by the isometries considered is satisfied. The proof of Lemma 4.1 is based on the fact that if $O_0, \ldots, O_N \in SO_3$ are 'generic' rotations, $b \in \mathbb{R}^3$ is a 'generic' vector and $P = T_b O_0$, then a nonempty reduced word on the alphabet $O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$ and P has a fixed point only if the word is a conjugate of a word on the alphabet $O_{v_1}^{\pm 1}, \ldots, O_{v_N}^{\pm 1}$. (See Lemma 3.5 for the precise statement.) Unfortunately, this statement does not generalize for other dimensions. For example, if $d = 4$, then a 'generic' rotation $O \in SO_4$ has no fixed point other than the origin. Thus $T_b O$ has a fixed point for *every* vector $b \in \mathbb{R}^4$, since $I - O$ is invertible, and $(I - O)^{-1}(b)$ is a fixed point of $T_b O$. Still, we conjecture that the statement of Lemma 4.1 is true for every dimension $d \geq 3$. It would be interesting to see if the methods applied in [1] can be used in this context.

References

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

[2] M. Edelstein, Isometric decompositions, *J. London Math. Soc.* (2) **37** (1988), 158-163.

[3] J. de Groot, Orthogonal isomorphic representation of free groups, *Canad. J. Math.* **8** (1956), 256-262.

[4] M. Laczkovich, Paradoxical decompositions using Lipschitz functions, *Mathematika* **39** (1992), 216-222.

[5] V. V. Prasolov: *Problems and theorems in linear algebra.* Translations of Mathematical Monographs, 134. American Mathematical Society, Providence, RI, 1994.

[6] C. Richter, Most convex bodies are isometrically indivisible, *J. Geom.* **89** (2008), 130-137.

[7] C. Richter, Affine divisibility of convex sets, *Bull. Lond. Math. Soc.* **41** (2009), no. 4, 757-768.

[8] S. Wagon, Partitioning intervals, spheres and balls into congruent pieces, *Canad. Math. Bull.* **26** (1983), no. 3, 337-340.

[9] S. Wagon: *The Banach-Tarski paradox.* Second edition, Cambridge Univ. Press, 1986. First paperback edition, 1993.

Department of Analysis

Eötvös Loránd University

Budapest, Pázmány Péter sétány 1/C

1117 Hungary (G. Kiss and M. Laczkovich)

and

Department of Mathematics

University College London

Gower Street, London, WC1E 6BT

England. (M. Laczkovich)

e-mail: kisss@cs.elte.hu (G. Kiss)

e-mail: laczk@cs.elte.hu (M. Laczkovich)