Equivariant mappings: a new approach in stochastic simulations

W. Schindler

NWF I—Mathematik, Universität Regensburg, Universitätstr. 31, 93040 Regensburg, Germany

Communicated by Jacob Goodman; submitted 21 July 1993; accepted 3 February 1994

Abstract

Stochastic simulations on manifolds usually are traced back to $\mathbb{R}^n$ via charts. If a group $G$ is acting on a manifold $M$ and if the respective distribution $\nu$ is invariant under this group action then in many cases of practical interest there exists a more convenient approach which uses equivariant mappings. The concept of equivariant mappings will be discussed intensively at the instance of the Grassmann manifold in which case $G$ equals the orthogonal group. Further advantages of this concept will be demonstrated by applying it to a probabilistic problem from the field of combinatorial geometry.

Keywords: Stochastic simulation; Group action; Invariant measure; Grassmann manifold; Chirotope

1. Introduction

Stochastic simulations have become an important tool in applied mathematics and in many technical sciences ([11]). Even in computational geometry it can be used profitably ([2]). Typically, one knows the distributions $\nu_1, \nu_2, \ldots, \nu_s$ of independent random variables $X_1, X_2, \ldots, X_s$ but one is not able to compute the image measure $\nu$ of $Y := \Phi(X_1, X_2, \ldots, X_s)$ for a specific mapping $\Phi$ with analytical or ordinary numerical methods. Loosely speaking, in a stochastic simulation one generates pseudorandom numbers $\bar{X}_{1:p}, \bar{X}_{2:p}, \ldots, \bar{X}_{N:p}$ ($1 \leq p \leq s$) which should have similar statistical properties as "true" realization sequences of independent identically distributed random variables $X_{1:p}, X_{2:p}, \ldots, X_{N:p}$ have with high probability. Computing $\bar{Y}_j := \Phi(\bar{X}_{j;1}, \bar{X}_{j;2}, \ldots, \bar{X}_{j;s})$ for $j \leq N$ one obtains a sequence of pseudorandom numbers with which one simulates the unknown distribution $\eta$. From these data one obtains an approximation for the unknown distribution $\eta$. Usually, one starts with the generation of standard random numbers $\bar{U}_1, \bar{U}_2, \ldots$ which in many aspects behave like...
realization sequences of independent random variables \( U_1, U_2, \ldots \) which are identically equidistributed on \([0, 1)\). The next step is to find an (exact) transformation \( \psi_p \) for each \( p \leq s \) which maps the sequence \( U_1, U_2, \ldots \) onto random variables \( X_{1;p}, X_{2;p}, \ldots \). Using these transformations one computes pseudorandom numbers \( \tilde{X}_{j;p} \) (\( j \leq N, p \leq s \)) from the standard random numbers and finally, as described above, one obtains the wanted pseudorandom numbers, \( \tilde{Y}_1, \tilde{Y}_2, \ldots, \tilde{Y}_N \).

The use of an exact transformation \( \psi \) for simulation purposes depends to a large extent on two criteria. First of all, \( \psi \) should have a simple form which enables a fast computation of pseudorandom numbers. A second criterion is the average number of standard random numbers required per generated pseudorandom number. Usually one favours algorithms for which this average number is small.

To understand the meaning of the second criterion recall that the usefulness and reliability of any stochastic simulation depends to a large extent on the properties of the used standard random numbers. As their name indicates they are not “truly” random but algorithmically generated which sometimes causes unexpected and unpleasant effects. An important criterion is how well the standard random vectors \( \tilde{U}_1, \tilde{U}_2, \ldots, \tilde{U}_n \), \( \tilde{U}_2, \tilde{U}_3, \ldots, \tilde{U}_{n+1} \), \( \ldots \) approximate the \( n \)-dimensional Lebesgue measure on the unit cube for varying dimension \( n \) ([7] and [9, p. 75–113]). As the common standard random number generators deliver periodic sequences, the standard random vectors thin out as \( n \) increases and hence their approximation properties must deteriorate. Clearly, the fewer standard random numbers one needs for generating one pseudorandom number in average the smaller should be the influence of the approximation properties of the high-dimensional standard random vectors on the quality of the whole simulation. We will see in section 2 that the second demand is not absolute. In fact, occasionally it counteracts a third criterion which often is not considered at all, whether \( \psi \) transforms the finite structure of the used standard random vectors in a way which matches with the geometry of the respective space and the symmetry properties of \( \nu \).

For many familiar distributions in \( \mathbb{R} \) or \( \mathbb{R}^n \), respectively, a lot of sophisticated transformations have been published ([6]). These transformations usually are based on purely probabilistic computations or on elementary geometrical considerations. In this article we introduce a new method to simulate a distribution \( \nu \) on a manifold \( M \) provided that \( \nu \) is invariant under the action of a group \( G \). This method exploits equivariant mappings. It catches the geometry of \( M \) and the symmetry properties of \( \nu \) better than ordinary “brute force methods” which trace the essential part of a simulation back to \( \mathbb{R}^n \) by chart mappings.

If the range of the occurring random variables and pseudorandom numbers is not \( \mathbb{R} \) or \( \mathbb{R}^n \) we will call them random elements or pseudorandom elements, respectively. In Section 2 we will briefly discuss effects which may occur when the chosen transformation is not appropriate to the given problem. In the third section we introduce the equivariance concept. Its use and its benefit are discussed in detail at the instance of the Grassmann manifold. Moreover, we sketch further examples and show to which degree this method fulfills the demands on “suitable” transformations formulated
above. In Section 4 we examine the usefulness of the equivariance concept for a particular problem from the field of combinatorial geometry. It reveals some insight in the solution of this probabilistic problem which in turn enables to carry out a simulation in an acceptable amount of time.

2. Transformation problems

At hand of a briefly discussed example we sketch the kind of problems which may arise when using unsuitable transformations. We begin with some definitions which we will need in the remainder.

Definition 2.1. A measure \( \nu \) on a topological space \( M \) will always be positive measure on its Borel \( \sigma \)-algebra \( \mathcal{B}(M) \). Its image measure under a mapping \( \varphi : M_1 \to M_2 \) will be denoted with \( \nu^\varphi \). For each integer \( n \geq 2 \) the term \( S^n \) stands for the \( n \)-sphere \( \{ x \in \mathbb{R}^{n+1} \mid \| x \| = 1 \} \) while \( \mu_{n} \) denotes the probability measure on \( S^n \) which equals the geometric surface measure up to normalization.

We define the mapping

\[
\psi : [0, 1]^2 \to S^2,
\]

\[
\psi(u, v) := (\sqrt{1 - (2v - 1)^2} \cos (2\pi u), \sqrt{1 - (2v - 1)^2} \sin (2\pi u), 2v - 1).
\]

Straight-forward computations verify that the restriction of \( \psi \) to \( (0, 1)^2 \) is a diffeomorphism which transforms the two-dimensional Lebesgue measure on the unit square into \( \mu_{23} \). Compared with other exact transformations the mapping \( \psi \) has two unquestionable advantages: It merely requires the minimal quantity of standard random numbers necessary to generate one pseudorandom element on \( S^2 \) and most of the result concerning the two-dimensional structure of the used standard random vectors can easily be transferred to the generated pseudorandom elements on the sphere. Nevertheless, this transformation also has two grave disadvantages. First of all, it is very slow since one has to compute one square-root and two trigonometric functions for each pseudorandom element on \( S^2 \). This makes it uninteresting for practical use since there exist a lot of faster algorithms to simulate \( \mu_{23} \) ([6, p. 230 f]). From the theoretical point of view another disadvantage is much more serious. If one uses a linear congruential generator, for instance, the pairs \( (\hat{U}_1, \hat{U}_2) \), \( (\hat{U}_2, \hat{U}_3) \), ... form a shifted lattice. The mapping \( \psi \) transforms the edges of this lattice into spiral lines. Near the poles, pseudorandom elements on the same spiral line are situated closely together whereas the stripes between neighbouring spirals are broad and can obviously not be hit by any pseudorandom vector \( \psi(\hat{U}_j, \hat{U}_{j+1}) \) (for details, see [14, p. 30 f]). This effect counteracts the homogeneity of the sphere and the symmetry of \( \mu_{23} \). This is a consequence of the fact that the absolute values of the partial derivatives \( \partial \psi_1(u, v) / \partial u \) and \( \partial \psi_2(u, v) / \partial v \) tend to infinity as vertical components of \((u, v)\) tend to
0 or 1, respectively, whereas the corresponding partial derivatives in \( u \)-direction tend to 0. It is obvious that those unpleasant effects may occur for other generator types, too. Of course, if the used standard number generator has large period length the non-reachable regions are narrow so that we can neglect this irregularity. Nevertheless, this example calls our attention to a more general problem.

The simulation of a distribution \( \nu \) on a compact \( n \)-dimensional manifold \( M \) usually is carried out in a two-stage simulation. Therefore one divides \( M \) into finitely many disjoint subsets \( A_1, A_2, \ldots, A_t \). Each \( A_j \) is a subset of an open set \( U_j \subseteq M \) while \( \varphi_j: U_j \rightarrow V_j \subseteq \mathbb{R}^n \) denotes the corresponding chart diffeomorphism. In the first step one chooses an index \( j \leq t \) with respect to the probability vector \((\nu(A_1), \nu(A_2), \ldots, \nu(A_t))\). In the second step one generates a pseudorandom vector \( \tilde{Z} \) on \( \varphi_j(A_j) \) with respect to \( \nu^{\varphi_j}/\nu(A_j) \) and, finally, \( \tilde{X} := \varphi_j^{-1}(\tilde{Z}) \) is the desired pseudorandom element on \( M \). For large dimension \( n \) it may be unfavourable to choose large subsets of maximal charts since near the boundary of \( \varphi_j(U_j) \) the Jacobian matrices \( \varphi_j^{-1}(x) \) and \( \varphi_j^{-1}(y) \) may be rather distinct although \( x \) and \( y \) are close together. Consequently, pseudorandom vectors on \( \varphi_j(A_j) \) which supply an acceptable simulation for \( \nu^{\varphi_j}/\nu(A_j) \) may lead to a bad simulation of \( \nu \) on \( M \). (Of course, the quantitative meaning of the expressions “close” and “near” depend on the distances between neighbouring pseudorandom random elements on \( \varphi_j(A_j) \).) As the standard random vectors thin out as their dimension increases this can also affect generators with large period length and cause defects similar to those discussed above.

Clearly, under those circumstances one cannot trust the results obtained by a stochastic simulation. On the other hand, if one divides \( M \) in many small subsets one should reduce these defects but then \( t \) increases as well as the number of computations (and hence the required time) which are necessary to determine handy expressions for the images \( \varphi_1(A_1), \varphi_2(A_2), \ldots, \varphi_t(A_t) \) and to compute explicit formulas for the distributions \( \nu^{\varphi_1}/\nu(A_1), \nu^{\varphi_2}/\nu(A_2), \ldots, \nu^{\varphi_t}/\nu(A_t) \). In any case, these considerations motivate to search for transformations which exploit the geometry of \( M \) and the symmetry of \( \nu \) and, consequently, avoid or at least reduce problems and defects discussed in this section.

3. The equivariance concept

In this section we introduce a new approach for stochastic simulations on groups and manifolds which uses the calculus of group actions and equivariant mappings in order to avoid problems discussed in the previous section. Its meaning and benefit will immediately become clear by the examples discussed in 3.3. Then we apply Theorem 3.2 to simulate the unique \( O(n) \)-invariant probability measure on the Grassmann manifold. By this, one retracts the essential part of a simulation from the Grassmann manifold to an Euclidean space and, moreover, one has the freedom to simulate any distribution on this Euclidean space provided that it is radial symmetric. In order to emphasize that the underlying mechanism matches with the geometry of the
Grassmann manifold and that it does not depend on a special choice of coordinates we at first prove and formulate the main result coordinate-free. Concrete algorithms (expressed in coordinates) will be deduced directly from the coordinate-free results. We will see that the mapping $p$ defined in Theorem 3.7 fulfills the various demands collected in the introduction to a high degree. Theorem 3.12 tells us how to obtain $O(V)$-invariant probability measures on the $m$ exterior algebra of a finite-dimensional real Hilbert space $V$ which will be needed in Section 4.

**Definition 3.1.** Let $(g, x) \mapsto gx$ denote a continuous action $G \times M \to M$ of a topological group $G$ on a topological space $M$. Equipped with this action we call $M$ a $G$-space. The union $\bigcup_{g \in G} \{gm\}$ is called the orbit of $m \in M$. In case that for every $m_1, m_2 \in M$ there exists a $g \in G$ with $gm_1 = m_2$ we call the action transitive. If $G$ acts transitively on $M$ and if the mapping $g \mapsto gm$ is open for every $m \in M$ then $M$ is a homogeneous space.

A mapping $\pi : M_1 \to M_2$ between two $G$-spaces is called $G$-equivariant if $\pi(gm) = g\pi(m)$ holds for all $(g, m) \in G \times M_1$. A measure $\nu$ on $M$ is $G$-invariant if $\nu(gB) = \nu(\{gx \mid x \in B\}) = \nu(B)$ holds for all $(g, B) \in G \times \mathcal{B}(M)$ and the set of all $G$-invariant probability measures on $M$ is denoted with $\mathcal{M}_1^1(M)$. If $M$ is a Borel subset of a Hilbert space $V'$ and if $G$ equals the orthogonal group $O(V')$ acting on $M$ by left multiplication we also call $\nu$ radial symmetric. Analogously, we call a function $h : M \subseteq V' \to \mathbb{R}$ radial symmetric if there exists an $h' : \mathbb{R} \to \mathbb{R}$ with $h(x) = h'(\|x\|)$ for all $x \in M$.

The restriction of a mapping $\varphi : M_1 \to M_2$ to $E_1 \subseteq M_1$ is denoted with $\varphi|_{E_1}$. For any $E_2 \subseteq M_2$ the term $\varphi^{-1}(E_2)$ stands for the pre-image $\{m_1 \in M_1 \mid \varphi(m_1) \in E_2\}$. If $\varphi$ is invertible then $\varphi^{-1}$ also denotes the inverse mapping of $\varphi$.

Although Theorem 3.2 looks rather elementary it will be crucial for the following considerations. Of particular importance is assertion 3.2 (iii) since it makes the computation of the image measure $\nu^\pi$ unnecessary provided that $\nu$ is $G$-invariant. In other words: To simulate the unique $G$-invariant distribution on $M_2$ one just has to simulate any $G$-invariant distribution on $M_1$ and to map the generated pseudo-random elements to $M_2$ by using the equivariant mapping $\pi$.

**Theorem 3.2.** Let $G$ be a topological group acting continuously on the topological spaces $M_1$ and $M_2$ and let $\pi : M_1 \to M_2$ be a measurable $G$-equivariant mapping.

(i) If $\nu$ is a $G$-invariant measure on $M_1$ then its image measure $\nu^\pi$ is $G$-invariant on $M_2$.

(ii) If $M_2$ is discrete then $\nu^\pi$ has equal mass on any two points of the same orbit.

(iii) If $G$ is a compact group and if $M_2$ is a homogeneous $G$-space then $\pi$ maps all $G$-invariant probability measures on $M_1$ onto the unique $G$-invariant measure on $M_2$.

**Proof.** Let $B \in \mathcal{B}(M_2)$. Due to the equivariance of $\pi$ we obtain the equivalences

\[ (x \in \pi^{-1}(gB)) \iff (\pi(x) \in gB) \iff (\pi(g^{-1}x) = g^{-1}\pi(x) \in B) \]
\[ \iff (g^{-1}x \in \pi^{-1}(B)) \iff (x \in g\pi^{-1}(B)). \]
for all \((g, x) \in G \times M_1\) and hence \(v^n(g B) = v(\pi^{-1}(g B)) = v(g \pi^{-1}(B)) = v(\pi^{-1}(B)) = v(B)\) which proves (i). Assertions (ii) and (iii) are corollaries from (i) and Weyl's theorem ([12, 138]). □

We mention that if a compact group \(G\) acts transitively on a Baire space (e.g., on a locally compact space) \(M\) then \(M\) is a homogeneous \(G\)-space ([4, p. 97]). Of particular practical importance are group actions of \(O(n), SO(n)\) or \(U(n)\). The following examples illustrate the usefulness of the equivariance concept for simulation problems which are likely to arise in computational geometry. They show that one can retract the simulation of specific distributions from manifolds to Euclidean spaces. We point out that Example 3.3(ii) can also be verified with elementary geometrical considerations and, in fact, some known algorithms are based on this idea ([6], p. 225 f.). Notice that the third example fulfills the hypotheses of 3.2(i) but not those of 3.2(iii). Further examples are discussed in [14, p. 124 f].

**Examples 3.3.**

(i) Let \(O(n)\) act on \(\mathbb{R}^n \setminus \{0\}\) and \(S^{n-1}\) by left multiplication while \(q_n : \mathbb{R}^n \setminus \{0\} \to S^{n-1}\) is defined by \(q_n(x) := x / \|x\|\). Then all hypotheses of Theorem 3.2 (iii) are fulfilled and hence the simulation of \(\mu_{n-1}\) can be retracted to the simulation of any radial-symmetric distribution \(v\) on \(\mathbb{R}^n \setminus \{0\}\) (e.g., \(v\) may be a probability measure with radial symmetric Lebesgue density).

(ii) Let \(\text{Pos}(n)\) and \(\text{R}(n)\) denote the set of all symmetric positive definite \((n \times n)\)-matrices and the group of all right upper triangular matrices of rank \(n\) with positive diagonal entries, respectively. Any \(A \in \text{GL}(n)\) can be expressed in a unique fashion as a product \(T_A P_A\) (polar decomposition) or \(T'_A R_A\) (QR-decomposition), respectively, where \(T_A, T'_A \in \text{O}(n), P_A \in \text{Pos}(n)\) and \(R_A \in \text{R}(n)\). The orthogonal group \(O(n)\) acts on \(\text{GL}(n)\) and \(O(n)\) by left multiplication. Let \(\pi_1, \pi_2 : \text{GL}(n) \to O(n)\) be given by \(\pi_1(A) := T_A\) and \(\pi_2(A) = T'_A\). Due to \(\pi_1(TA) = TT'_A\) and \(\pi_2(TA) := TT'_A\) for all \(T \in O(n)\) the mappings \(\pi_1\) and \(\pi_2\) are \(O(n)\)-equivariant and thus Theorem 3.2 can be applied. There is exactly one \(O(n)\)-invariant probability measure on \(O(n)\), namely the Haar probability measure \(\mu_{O(n)}\). Hence for any radial-symmetric probability measure \(v\) on \(\text{GL}(n)\) equations \(v^{\pi_1} = v^{\pi_2} = \mu_{O(n)}\) hold.

(iii) A Lie group is called a torus if it is isomorphic to \((\mathbb{R}/\mathbb{Z})^k\) for a suitable \(k \in \mathbb{N}\). Now let \(G\) be a compact connected Lie group (e.g. \(G = \text{SO}(n)\) or \(G = \text{U}(n)\)) and \(T\) a maximal torus subgroup of \(G\). Then \(G\) acts on \(G/T \times T\) and \(G\) via \(h(gT, t) := (hgT, t)\) and \(h.g := hgh^{-1}\). As \(T\) is abelian the mapping \(q : G/T \times T \to G, q(gT, t) := gtg^{-1}\) is well defined and due to \(q(h(gT, t)) = (hg)(hgh^{-1}) = h.q(gT, t)\) it is \(G\)-equivariant. There exists a unique probability measure \(\mu_{G/T}\) on \(G/T\) which is invariant under the left multiplication with elements of \(G\). Consequently, \(\mu_{G/T} \otimes \tau\) is \(G\)-invariant for each probability measure \(\tau\) on \(T\) and its image measure \((\mu_{G/T} \otimes \tau)^\pi\) is invariant under conjugation ("\(\text{Con-invariant}\)"). Vice versa, one can prove that to any \(\text{Con-invariant}\) probability measure \(v\) on \(G\) there exists a \(\tau_v\) with \(v = (\mu_{G/T} \otimes \tau_v)^\pi\) ([16, Theorem 2.3]). Consequently, one may decompose a simulation of any \(\text{Con-invariant}\) distribution \(v\) on \(G\) into two independent simulation problems on spaces with smaller
dimension. Especially, for $G = \text{SO}(3)$ we may identify $T$ and $\text{SO}(3)/T$ with the interval $[0, 2\pi)$ and $S^2$, respectively. This leads to simulation algorithms for Con-invariant distributions on $\text{SO}(3)$ which are considerably faster than those based on Euler angles (see [16, Section 3]).

We mention that a special case of the second example was published by Stewart ([17]) who exploited specific properties of normally distributed random variables. Moreover, the polar and the QR-decomposition are isomorphisms between $\text{GL}(n)$ and $\text{O}(n) \times \text{Pos}(n)$ or $\text{O}(n) \times \mathbb{R}(n)$, respectively. Using their inverse mappings one can efficiently simulate $\text{O}(n)$-invariant distributions on $\text{GL}(n)$ even if they are neither absolutely continuous with respect to the Haar measure nor discrete ([15]). Roughly speaking, it suffices that their support equals any submanifold which is invariant under the respective $\text{O}(n)$-action. We point out that one can exploit the transformation properties of $\text{O}(n)$-invariant measures on $\text{GL}(n)$ under the polar or the QR-decomposition to simplify and to evaluate particular integrals on $\text{GL}(n)$, respectively ([15]).

We now come to our main object, the simulation of the $\text{O}(n)$-invariant distribution on the Grassmann manifold. To show that simulation algorithms obtained by the equivariance concept match with the geometry of the manifold we at first resign on coordinates.

**Definition 3.4.** In the following $V'$ will always denote a finite-dimensional real Hilbert space with dimension $n'$. The brackets $(\cdot, \cdot)$ denote the scalar products on all Hilbert spaces which occur in this article. We denote the vector space of all homomorphisms between two Hilbert spaces $V_1$ and $V_2$ with $\text{Hom}(V_1, V_2)$ while the group of all invertible or orthogonal endomorphisms on $V'$ are denoted by $\text{GL}(V')$ and $\text{O}(V')$, respectively. These terms are chosen in analogy to the common notations $\text{Mat}(n, m)$, $\text{GL}(n)$ and $\text{O}(n)$ which stand for the vector space of all $(n \times m)$-matrices, for the general linear group or for the orthogonal group of rank $n$, respectively. Moreover, $V_1 \subseteq V_2$ means that $V_1$ is a vector subspace of $V_2$.

The notation $\eta \sim f \cdot \nu$ means that the measure $\eta$ has $\nu$-density $f$ while $\lambda$ stands for the standard Lebesgue measure on $\mathbb{R}^n$ as well as for a Haar measure on a finite-dimensional real Hilbert space.

The letter $W$ denotes an $m$-dimensional subspace of an $n$-dimensional Hilbert space $V$ while $\text{Hom}(W, V)$ stands for the set of all injective homomorphisms from $W$ to $V$. In the following these spaces are assumed to be arbitrary but fixed. We begin with a construction of a coordinate-free pendant to the Grassmann manifold.

Let $H_m := \{v_1, v_2, \ldots, v_m\} \subseteq V \times V \times \cdots \times V | v_1, v_2, \ldots, v_m$ are linearly independent}. Further, we define $G(W, V) := \{W' \subseteq V | W'$ is isomorphic to $W\}$ and $q: H_m \to G(W, V)$ maps each $m$-tuple $(v_1, v_2, \ldots, v_m) \in H_m$ onto its linear span. If we equip $G(W, V)$ with the quotient topology (relative to $q$) then $(\varphi, W') \mapsto \varphi(W')$ for all $(\varphi, W') \in \text{O}(V) \times G(W, V)$ defines a transitive group action of $\text{O}(V)$ on $G(W, V)$. Hence $G(W, V)$ is a homogeneous $\text{O}(V)$-space ([4, p. 97]) and the isotropy group of
$W \in G(W, V)$ is given by $O_w(V) := \{ \varphi \in O(V) | \varphi(W) = W \}$. Indeed, $G(W, V)$ is isomorphic to the Grassmann manifold $\mathcal{G}_{n,m}^\mathbb{R}$ whose points are $m$-dimensional subspaces of $\mathbb{R}^n$. Consequently, we have

$$\mathcal{G}_{n,m}^\mathbb{R} \cong G(W, V) \cong O(V)/O_w(V) \cong \frac{O(n)}{O(m) \times O(n-m)}.$$ (1)

**Lemma 3.5.** Let $V_1$ and $V_2$ be two finite dimensional Hilbert spaces with dimension $n_1$ and $n_2$, respectively. Then

$$(\cdot, \cdot): \text{Hom}(V_1, V_2) \times \text{Hom}(V_1, V_2) \to \mathbb{R}, \quad (\varphi, \psi) := \frac{1}{n_1} \text{tr}(\varphi' \psi)$$

defines a scalar product on $\text{Hom}(V_1, V_2)$. Equipped with this scalar product $\text{Hom}(V_1, V_2)$ is a Hilbert space.

(ii) Let $p: \mathbb{R}^k \to \mathbb{R}$ be a polynomial. If $p \neq 0$ the zero-set of $p$ has Lebesgue measure 0.

(iii) For $m \leq n$ let $\text{Mat}(n, m)$ denote the set of all $(n \times m)$-matrices with rank $m$. Then

$$\lambda(\text{Mat}(n, m) \setminus \text{Mat}(n, m)_*) = 0$$

(iv) Let $\nu$ be a measure on a $O(V')$-saturated Borel set $N \subseteq V'$ (i.e. $\varphi(N) \subseteq N$ for all $\varphi \in O(V')$) with radial symmetric Lebesgue density $h$. Then $\nu$ is radial symmetric.

**Proof.** Assertions (i) and (ii) are well known and their proofs are straightforward (see e.g. [14, p. 163f.]) and (iii) is an immediate corollary from (ii). For any $B \in \mathcal{B}(N)$ and $\varphi \in O(V')$ the transformation theorem for integrals yields $\nu(\varphi(B)) = \int_{\varphi(B)} h(y) \lambda(dy) = \int_{\nu(\varphi(N))} \lambda(dy) = \int_{\nu(h(x))} \lambda(dx) = \nu(B)$ which proves (iv).

**Theorem 3.6.** (i) The mapping

$$\Gamma_w: O(V) \to O(\text{Hom}(W, V)), \quad \Gamma_w(\varphi)(x) := \varphi x \text{ for all } x \in \text{Hom}(W, V)$$

is a group homomorphism. Moreover, $\Gamma_w(\varphi)(\text{Hom}(W, V)_*) \subseteq \text{Hom}(W, V)_*$ for all $\varphi \in O(V)$.

(ii) $O(V)$ acts on $\text{Hom}(W, V)_*$ and $G(W, V)$ by left multiplication. The mapping

$$\pi: \text{Hom}(W, V)_* \to G(W, V), \quad \pi(\varphi) := \varphi(W)$$

is $O(V)$-equivariant. For each $\nu \in \mathcal{M}^1_{O(V)}(\text{Hom}(W, V)_*)$ the image measure $\nu^\pi$ equals the unique $O(V)$-invariant probability measure $\mu_{G(W, V)}$ on $G(W, V)$.

(iii) Let $\eta$ be any radial symmetric probability on $\text{Hom}(W, V)$ with $\eta(\text{Hom}(W, V)_*) = 1$. If $\tilde{\pi}: \text{Hom}(W, V) \to G(W, V)$ is any measurable extension of $\pi$ then $\eta^\pi = \mu$.

**Proof.** The proof of (i) is straight-forward using the definition of the scalar product on $\text{Hom}(V_1, V_2)$. Assertion (i) verifies the first assertion of (ii) and since $\psi \pi(\varphi) = \psi \varphi(W) = (\psi \varphi) W = \pi(\psi \varphi)$ holds for all $\psi \in O(V)$ the mapping $\pi$ is equivariant. Hence (ii) follows from 3.2 (iii) while (iii) is an immediate consequence from 3.5 (iv) and (ii).
Up to now our results were formulated coordinate-free. For a concrete simulation we yet can not resign on coordinates. We denote the standard basis of \( \mathbb{R}^n \) with \( \{ e_1, e_2, \ldots, e_n \} \) and define \( W := \operatorname{span}\{ e_1, e_2, \ldots, e_n \} \), the vector space spanned by \( \{ e_1, e_2, \ldots, e_n \} \). We equip \( \operatorname{Mat}(n, m) \) with the scalar product \( (A, B) := \frac{\operatorname{tr}(A'B)}{m} \). As we can canonically identify \( A \in \operatorname{Mat}(n, m) \) with the linear mapping \( \kappa_A : \mathbb{R}^n \to \mathbb{R}^m \) which maps the \( j \)-th unit vector of \( \mathbb{R}^n \) onto the \( j \)-th column vector \( a_j \) of \( A \) Theorem 3.7 is an immediate consequence from 3.6 (iii) whereas Corollary 3.8 follows from 3.5 (iii) and 3.7.

**Theorem 3.7.** Let \( \mu_{n,m} \) denote the unique \( O(n) \)-invariant probability measure on \( \mathcal{G}_{n,m}^\mathbb{R} \) (as above, \( (T, W') \mapsto T(W') \)). Further, let \( \tilde{\mu} : \operatorname{Mat}(n, m) \to \mathcal{G}_{n,m}^\mathbb{R} \),

\[
\tilde{\mu}(A) := \begin{cases} p(A) := \operatorname{span}\{ a_1, a_2, \ldots, a_m \} & \text{if } A \in \operatorname{Mat}(n, m) \\ \operatorname{span}\{ e_1, e_2, \ldots, e_n \} & \text{else} \end{cases}
\]

while \( X \) denotes a random element with range \( \operatorname{Mat}(n, m) \) and image measure \( \nu \in \mathcal{M}_{1,0}(\operatorname{Mat}(n, m)) \). If \( \nu(\operatorname{Mat}(n, m)_*) = 1 \) then \( \tilde{\mu}(X) \) is \( \mu_{n,m} \)-distributed.  

**Corollary 3.8.** Let the random variables \( X_{11}, X_{12}, \ldots, X_{nm} \) be independent and identically \( N(0, 1) \)-distributed. Then

\[
X = \begin{pmatrix} X_{11} & X_{12} & \cdots & X_{1m} \\ X_{21} & X_{22} & \cdots & X_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ X_{n1} & X_{n2} & \cdots & X_{nm} \end{pmatrix}
\]

fulfills the hypotheses of Theorem 3.7.

**Proof.** The image measure of \( X \) has radial symmetric Lebesgue density

\[
h(A) = \prod_{i=1}^n \prod_{j=1}^m c e^{-\frac{1}{2} a_{ij}^2} = c^{nm} e^{-\frac{1}{2} \sum_{i=1}^n \sum_{j=1}^m a_{ij}^2} = c^{nm} e^{-\frac{1}{2} \| A \|^2}.
\]

We point out that nearly any algorithm which is based on Theorem 3.7 should be suitable for simulation purposes. In fact, the mapping \( \tilde{\mu} \) retracts the essential part of a simulation of \( \mu_{n,m} \) from \( \mathcal{G}_{n,m}^\mathbb{R} \) to the well-known vector space \( \operatorname{Mat}(n, m) \cong \mathbb{R}^{n \times m} \). There are no problems with chart boundaries and \( \tilde{\mu} \) does not distinguish any direction or region of \( \mathbb{R}^{nm} \) besides a single point (the origin). Corollary 3.8 is of immense practical meaning since it decomposes a high-dimensional simulation problem into \( nm \) independent identical one-dimensional simulation problems for which many
well-tried exact transformations are known ([6]). Due to (1) we have \( \dim \mathcal{B}_{n,m}^R = \dim O(n) - \dim O(m) - \dim O(n-m) = m(n-m) \). Clearly, for any simulation algorithm the average number of standard random numbers required to generate one pseudorandom element on \( \mathcal{B}_{n,m}^R \) can not be smaller than \( \dim \mathcal{B}_{n,m}^R \). If we simulate the one-dimensional normal distributions with Marsaglia’s method ([6, p. 235f.]), for instance, the algorithm proposed by 3.8 requires about \( 1.27nm \) standard random numbers to generate one pseudorandom element \( \bar{X} \) on \( \text{Mat}(n, m) \) in average. This is very acceptable since acceptance-rejection algorithms in high dimensions usually are much less efficient (unless the distribution and the area of interest fulfill strong regularity conditions). A further advantage of Theorem 3.8 is that one can choose any radial symmetric distribution on \( \text{Mat}(n, m)_* \). Remark 3.9 gives two further \( O(n) \)-invariant distributions on \( \text{Mat}(n, m)_* \).

We point out that although \( \text{Prob}(X \notin \text{Mat}(n, m)_*) = 0 \) the set \( \text{Mat}(n, m) \setminus \text{Mat}(n, m)_* \) may be hit by some pseudorandom elements. In a concrete simulation we recommend to reject these pseudorandom elements as it is usual practice in similar situations.

**Remark 3.9.** (i) Let \( Y \) be a random element with range \( \text{Mat}(n, m)_* \) whose columns can be viewed as independent \( \mu_{n-1} \)-distributed random vectors on \( S^{n-1} \). Then \( Y \) fulfills the hypotheses of Theorem 3.7.

(ii) Let \( K_1(0) \) denote the unit ball in \( \text{Mat}(n, m) \) and \( \eta = f \cdot \lambda \) with \( f \equiv 1/\lambda(K_1(0)) \) on \( K_1(0) \) and \( f \equiv 0 \) elsewhere. Then \( \eta \) fulfills the hypotheses of Theorem 3.7.

**Proof.** The mapping \( \vartheta : \text{Mat}(n, m) \to \text{Mat}(n, m) \) which divides each column of \( A \in \text{Mat}(n, m)_* \) by its Euclidean norm and maps \( A \notin \text{Mat}(n, m)_* \) onto itself, is \( O(n) \)-equivariant. If \( X \) is distributed as in Corollary 3.8 then \( \vartheta(X) \) has the same distribution as \( Y \) (due to \( P(X \in \text{Mat}(n, m)_*) = 1 \) and 3.3 (i)). This proves (i) while (ii) is an immediate consequence from 3.5 (iv).

Although we have already reached the declared aim of this section, an efficient algorithm to simulate \( \mu_{n,m} \), we continue applying the calculus of equivariant mappings to construct \( O(V) \)-invariant measures on the \( m \)th exterior algebra of \( V \). Lemma 3.11 collects some important properties of the \( m \)th exterior power which will be needed in the proofs of Theorems 3.12 and 4.4.

**Definition 3.10.** An \( m \)-linear skew-symmetric mapping \( \wedge^m : V \times V \times \cdots \times V \to \wedge^m(V) \) has universal property if for each \( m \)-linear skew-symmetric mapping \( \psi \) from \( V \times V \times \cdots \times V \) to an arbitrary vector space \( H \) there exists a unique linear mapping \( f : \wedge^m(V) \to H \) with \( \psi = f \circ \wedge^m \). If \( \wedge^m \) has the universal property we call the vector space \( \wedge^m(V) \) the \( m \)th exterior algebra of \( V \) and the pair \( (\wedge^m, \wedge^m(V)) \) the \( m \)th exterior power of \( V \). For all \( v_1, v_2, \ldots, v_m \in V \) we define \( v_1 \wedge v_2 \wedge \cdots \wedge v_m :\)
Lemma 3.11. (i) Equation \( v_1 \wedge v_2 \wedge \cdots \wedge v_m = 0 \) holds iff \( v_1, v_2, \ldots, v_m \in V \) are linearly dependent.

(ii) \( \bigwedge^m(V) \) becomes a Hilbert space via
\[
(v_1 \wedge v_2 \wedge \cdots \wedge v_m, w_1 \wedge w_2 \wedge \cdots \wedge w_m) := \det((v_j, w_k))_{1 \leq j, k \leq m}
\]
where \((v_j, w_k)\) denotes the scalar product of \( v_j \) and \( w_k \) on \( V \). For any orthonormal basis \( e_1, e_2, \ldots, e_n \) of \( V \) the set \( \{v_{j_1} \wedge v_{j_2} \wedge \cdots \wedge v_{j_m} \mid 1 \leq j_1 < j_2 < \cdots < j_m \leq n\} \) is an orthonormal basis of \( \bigwedge^m(V) \).

(iii) Let \( v_1, v_2, \ldots, v_m \) and \( w_1, w_2, \ldots, w_m \), resp., be linearly independent vectors in \( V \). Then the following conditions are equivalent.

(a) \( (v_1 \wedge v_2 \wedge \cdots \wedge v_m) = r(w_1 \wedge w_2 \wedge \cdots \wedge w_m) \) for a suitable scalar \( r \in \mathbb{R} \setminus \{0\} \).

(b) The vectors \( v_1, v_2, \ldots, v_m \) and \( w_1, w_2, \ldots, w_m \), resp., span, resp., the same \( m \)-dimensional subspace of \( V \).

Assertions (i), (ii) and (iii) are proved in [8, p. 100, p. 107] and in [14, p. 164f]. Theorem 3.12 is crucial for the following. The universal property implies that for each \( \varphi \in \text{Hom}(V, V) \) there exists a unique linear mapping \( \Gamma_\varphi : \bigwedge^m(V) \to \bigwedge^m(V) \) with
\[
\Gamma_\varphi(v_1 \wedge v_2 \wedge \cdots \wedge v_m) = (\varphi(v_1) \wedge \varphi(v_2) \wedge \cdots \wedge \varphi(v_m))
\]
for all \( v_1, v_2, \ldots, v_m \in V \). More precisely, since the operator \( \wedge^m \) is a functor from the category of finite-dimensional vector spaces into itself ([10, p. 589]) this induces a group homomorphism \( \Gamma_\varphi : \text{GL}(V) \to \text{GL}(\bigwedge^m(V)) \). It may be noteworthy that this homomorphism is injective for odd \( m < n \) and has kernel \( \{\text{id}, -\text{id}\} \) if \( m < n \) is even ([14, p. 131f]).

Theorem 3.12. (i) The restriction of \( \Gamma_\varphi \) on \( O(V) \) induces a group homomorphism \( \Gamma_\varphi : O(V) \to O(\bigwedge^m(V)) \). Especially, \( (\varphi, v_\wedge) \mapsto \Gamma_\varphi(v_\wedge) \) for all \( (\varphi, v_\wedge) \in O(V) \times \bigwedge^m(V) \) defines an \( O(V) \)-action on \( \bigwedge^m(V) \).

(ii) If \( O(V) \) acts on \( V \times V \times \cdots \times V \) via
\[
(\varphi, (v_1, v_2, \ldots, v_m)) \mapsto (\varphi(v_1), \varphi(v_2), \ldots, \varphi(v_m))
\]
the mapping \( \wedge^m : V \times V \times \cdots \times V \to \bigwedge^m(V) \) is \( O(V) \)-equivariant.

(iii) For every basis \( B = \{b_1, b_2, \ldots, b_m\} \) of \( W \) the mapping
\[
\hat{\pi}_B : \text{Hom}(W, V) \to V \times V \times \cdots \times V, \quad \hat{\pi}_B(\psi) = (\psi(b_1), \psi(b_2), \ldots, \psi(b_m))
\]
is an \( O(V) \)-equivariant linear isomorphism. Consequently, \( \wedge^m \circ \hat{\pi}_B : \text{Hom}(W, V) \to \bigwedge^m(V) \) and its restriction \( \wedge^m \circ \hat{\pi}_B|_{\text{Hom}(W, V)} \) are \( O(V) \)-equivariant mappings.

Proof. Using the definition of the scalar product in \( \bigwedge^m(V) \) one easily verifies
\[
(\Gamma_\varphi(v_1 \wedge v_2 \wedge \cdots \wedge v_m), \ \Gamma_\varphi(w_1 \wedge w_2 \wedge \cdots \wedge w_m)) = (v_1 \wedge v_2 \wedge \cdots \wedge v_m, w_1 \wedge w_2 \wedge \cdots \wedge w_m)
\]
for all \( \varphi \in O(V) \) and every choice of \( v_1, v_2, \ldots, v_m, w_1, w_2, \ldots, w_m \in V \). As \( \Gamma_\varphi \) is linear this proves its orthogonality. Hence \( \Gamma_\varphi(O(V)) \) is a subgroup of \( O(\bigwedge^m(V)) \) and the remainder of the theorem is obvious. \( \square \)
4. Chirotopes: An application of the equivariance concept

In this section we utilize the concept of equivariant mappings to obtain a handy simulation problem with which one can refute or confirm a conjecture of Goodman and Pollack concerning chirotopes. Numerical results of stochastic simulations confirming a special case of this conjecture were published in [2]. In that paper the probabilistic background receded into the background in favour of geometrical and combinatorical aspects. A comprehensive treatment of the following can be found in [14, p. 133–158]. We begin with some definitions which are necessary to formulate Theorem 4.4.

**Definition 4.1.** For \( A \in \text{Mat}(n, m) \) let \( [j_1, j_2, \ldots, j_m]_A \) denote the determinant of that \((m \times m)\)-matrix \( A_{j_1, \ldots, j_m} \) whose \( i \)th row equals the \( j_i \)th row of \( A \). As in the preceding section the unique \( O(n) \)-invariant probability measure on \( \mathbb{R}^n_+ \) is denoted with \( \mu_{n,m} \), while \( NI(0, 1)^n \) stands for the image measure of the random element \( X \) defined in corollary 3.8. Further, \( E = \{e_1, e_2, \ldots, e_n\} \) denotes the standard vector basis of \( \mathbb{R}^n \), \( GF(3) \) the Galois field over \( \{-1, 0, 1\} \), \( \mathbb{R}^* \) the multiplicative group \( \mathbb{R} \setminus \{0\} \) and, finally, \( \mathbb{P}^k \) and \( \mathbb{PGF}(3)^k \) the projective spaces \( (\mathbb{P}^k \setminus \{0\})/\mathbb{R}^* \) and \( (\mathbb{PGF}(3)^k \setminus \{0\})/\{1, -1\} \).

The following lemma motivates the definition of chirotopes. Its proof can be found in [3, p. 10f].

**Lemma 4.2.** Let \( j_1, j_2, \ldots, j_{m+1} \) and \( k_1, k_2, \ldots, k_{m-1} \) denote increasing sequences of integers with \( 1 \leq j_1, k_1 \) and \( j_{m+1}, k_{m-1} \leq n \). Then the Grassmann–Plücker relation

\[
\sum_{i=1}^{m+1} (-1)^i[j_1, j_2, \ldots, j_i, j_{i+1}, \ldots, j_{m+1}]_A[j_i, k_1, k_2, \ldots, k_{m-1}]_A = 0
\]

holds for each \( A \in \text{Mat}(n \times m) \).

**Definition 4.3.** Let \( F = \{1, 2, \ldots, n\} \). A skew-symmetric mapping \( \chi: F^m \to \{-1, 0, 1\} \) is called a chirotope if for all increasing sequences \( j_1, j_2, \ldots, j_{m+1} \in F \) and \( k_1, k_2, \ldots, k_{m-1} \in F \) the set

\[
\{\chi(j_2, j_3, \ldots, j_{m+1}) \chi(j_1, k_1, \ldots, k_{m-1}) - \chi(j_1, j_3, \ldots, j_{m+1}) \chi(j_2, k_1, \ldots, k_{m-1})
\]

either equals \( \{0\} \) or a superset of \( \{-1, 1\} \). Due to (2) the mapping

\[
\chi_A: F^m \to \{-1, 0, 1\}, \quad \chi_A(j_1, j_2, \ldots, j_m) = \text{sgn}[j_1, j_2, \ldots, j_m]_A
\]

is a chirotope for each \( A \in \text{Mat}(n, m) \). A chirotope \( \chi \) is realizable if there exists an \( A \in \text{Mat}(n, m) \) with \( \chi = \chi_A \). An \( m \)-tuple \( (j_1, j_2, \ldots, j_m) \in F^m \) is ordered if \( j_1 < j_2 < \cdots < j_m \) holds. We denote the set of all ordered \( m \)-tuples in \( F^m \) with \( \Lambda(F, m) \).
and call a chirotope $\chi$ simplicial if $\chi(J) \in \{1, -1\}$ for all $J \in \Lambda(F, m)$. The set of all realizable chirotopes is denoted by $\text{Re}_x(n, m)$ while $\text{Si}_x(n, m)$ denotes the set of all simplicial chirotopes. As usually, $\text{sgn}: \mathbb{R} \to \{1, 0, -1\}$ denotes the signum function.

Since a chirotope is a skew-symmetric function it is completely determined by its restriction to $\Lambda(F, m)$. Hence we will identify the chirotope $\chi$ with the $(\binom{n}{m})$-tuple

$$(\chi(1, 2, \ldots, m), \chi(1, \ldots, m - 1, m + 1), \ldots, \chi(n - m + 1, \ldots, n)) \in \text{GF}(3)^{(\binom{n}{m})}.$$ 

As we will presently see one can canonically map the $m$-dimensional subspaces $\mathbb{R}^m$ onto pairs of chirotopes, or equivalently, onto elements in $\text{PGF}(3)^{(\binom{n}{m})}$. This mapping induces an image measure $P_X$ of $\mu_{n,m}$ on this projective space. The aim of [2] was to determine those elements where $P_X$ attains its maximum.

**Theorem 4.4.** Let

$$\Psi: \text{Mat}(n, m) \to \mathbb{R}^{\binom{n}{m}},$$

$$\Psi(A) = ([1, 2, \ldots, m], [1, 2, \ldots, m - 1, m + 1], \ldots, [n - m + 1, n - m + 2, \ldots, n]).$$

(The subdeterminants are ordered lexicographically.) Moreover, let $p: \mathbb{R}^{\binom{n}{m}} \to \mathbb{R}^{\binom{m}{m}}$ be given by $p(x) = x^{\mathbb{R}^*}$ and $p$ be defined as in 3.7. Then the following assertions hold:

(i) The orthogonal group $O(n)$ acts on $\text{Mat}(n, m)_\ast$ and on $\mathbb{R}^{\binom{n}{m}}$ by left multiplication. For each $H \in O(n)$ there exists a unique orthogonal matrix $\Gamma_x(H) \in O(\binom{n}{m})$ with $\Gamma_x(H)(\Psi(A)) = \Psi(HA)$ for all $A \in \text{Mat}(n, m)$. The orthogonal group $O(n)$ acts on $\mathbb{R}^{\binom{n}{m}} \setminus \{0\}$ via $(H, x) \mapsto \Gamma_x(H)x$ for all $(H, x) \in O(n) \times (\mathbb{R}^{\binom{n}{m}} \setminus \{0\})$. Moreover, $(H, x^{\mathbb{R}^*}) \mapsto Hx^{\mathbb{R}^*} := (\Gamma_x(H)x)^{\mathbb{R}^*}$ defines an $O(n)$-action on $\mathbb{R}^{\binom{m}{m}}$.

(ii) Let $\Psi: \mathbb{R}^{\binom{n}{m}} \to \mathbb{R}^{\binom{m}{m}}$ be given by $\Psi(W) := \Psi(w_1, w_2, \ldots, w_m)^{\mathbb{R}^*}$ for $W \in \mathbb{R}^{\binom{n}{m}}$ where $w_1, w_2, \ldots, w_m$ is any basis of $W$. Then $\Psi$ is a (well-defined) injective mapping. With respect to the $O(n)$-actions defined above the mappings $p, \Psi, \Psi$ and $p$ are $O(n)$-equivariant.

(iii) Let the mappings $\gamma: \mathbb{R}^{\binom{n}{m}} \setminus \{0\} \to \text{GF}(3)^{(\binom{n}{m})} \setminus \{0\}$, $\bar{\gamma}: \mathbb{R}^{\binom{m}{m}} \to \text{PGF}(3)^{(\binom{m}{m})}$ and $\gamma: \text{GF}(3)^{(\binom{n}{m})} \setminus \{0\} \to \text{PGF}(3)^{(\binom{m}{m})}$ be given by $\gamma(x_1, x_2, \ldots, x_{\binom{n}{m}}) := (\text{sgn}(x_1), \text{sgn}(x_2), \ldots, \text{sgn}(x_{\binom{n}{m}}))$, $\bar{\gamma}(x^{\mathbb{R}^*}) := \gamma(x)^{\mathbb{R}^*}$ and $p_{\gamma}(q) := \{q, -q\}$ where $(x_1, x_2, \ldots, x_{\binom{n}{m}}), x$ and $q$ denote elements of the respective domains. Then the following diagram is commutative.

$$\begin{array}{c}
\text{Mat}(n, m)_\ast \\
\downarrow \Psi \\
\mathbb{R}^{\binom{n}{m}} \setminus \{0\} \\
\downarrow \gamma \\
\text{GF}(3)^{(\binom{n}{m})} \setminus \{0\}
\end{array} \rightarrow 
\begin{array}{c}
\mathbb{R}^{\binom{m}{m}} \\
\downarrow p \\
\mathbb{R}^{\binom{m}{m}} \\
\downarrow \bar{\gamma} \\
\text{PGF}(3)^{(\binom{m}{m})}
\end{array}$$

(iv) Let $P_X := (\mu_{n,m})^{\gamma, \Psi}$. For any $v \in \mathcal{M}_0(\text{Mat}(n, m)_\ast)$ the equations $v_{\Psi, p} = v_{\Psi, p}$ hold.
(v) Let $v_1, v_2 \in \mathcal{M}_{\text{O}(n)}(\text{Mat}(n, m)_*)$. Then $v^T_1(y^{-1}(\{q, -q\})) = v^T_2(y^{-1}(\{q, -q\}))$ holds for all $q \in GF(3)^2 \setminus \{0\}$.

(vi)

$$P_x(\{q, -q\}) = \begin{cases} > 0 & \text{if } \{q, -q\} \in (\text{Re}_x(n, m) \cap \text{Si}_x(n, m)) \cdot \{1, -1\}, \\ 0 & \text{else} \end{cases}$$

Proof. The first and second assertion of (i) have already been proved in Section 3. Let $(\wedge^n, [\mathbb{R}^m])$ have universal property and let the linear isomorphism $\pi_E: \text{Mat}(n, m) \to \mathbb{R}^n \times \mathbb{R}^n \times \cdots \times \mathbb{R}^n$ be defined as in 3.12 (iii). Then there exists a linear endomorphism $f$ on $[\mathbb{R}^m]$ with $\Psi \circ \pi_E^{-1} = f \circ \wedge^m$. Since the image of $\mathcal{E} := \{(e_i, e_j, \ldots, e_m) \mid 1 \leq i < j_2 < \cdots < j_\ell \leq n\}$ under $\Psi \circ \pi_E^{-1}$ is the standard vector basis of $[\mathbb{R}^m]$, $f$ must be an isomorphism. Thus the pair $(\Psi \circ \pi_E^{-1}, [\mathbb{R}^m])$ has itself universal property and hence Theorem 3.12 and 3.11(i) guarantee uniqueness and existence of a linear $O(n)$-action on $[\mathbb{R}^m] \setminus \{0\}$ with the properties claimed in (i). The last assertion of (i) follows from the linearity of $\Gamma_\chi(H)$. Due to 3.11(iii) the mapping $\Psi$ is well defined and injective while the $O(n)$-equivariance of $p, \Psi$ and $pr$ is either already proved (3.7, 3.12) or it follows immediately from definition. Let $A \in \text{Mat}(n, m)_*$ with $p(A) = W'$. Then $\Psi(p(A)) = pr(\Psi(A))$ follows immediately from definition of $pr$. It leads to

$$\Psi(HW') = \Psi(Hp(A)) = \Psi(p(HA)) = pr \circ \Psi(HA) = H \cdot (pr \circ \Psi(A)) = H \cdot (\Psi(W'))$$

for all $H \in O(n)$. This proves (ii). The validity of (iii) follows from the preceding and from the definition of $\Psi, \Psi$ and $pr$. As $y^{-1}(\{q, -q\}) = pr^{-1} \circ \Psi^{-1}(\{q, -q\})$ holds for all $q \in GF(3)^2 \setminus \{0\}$ assertion (v) follows from (iv) which itself is an immediate consequence from (iii). Let $v_N$ stand for the restriction of $N\mathbb{I}(0, 1)^m_*$ to $\text{Mat}(n, m)_*$, let $q \in \text{Re}_x(n, m) \cap \text{Si}_x(n, m)$ and $A \in \text{Mat}(n, m)_*$ with $\Psi(A) = q$. Due to the continuity of $\Psi$ there exists an $\varepsilon > 0$ with $\Psi(A') = q$ for all $A' \in \text{Mat}(n, m)_*$ with $\|A - A'\| < \varepsilon$. Since $v_N$ has positive Lebesgue density this proves first part of (vi) while the second part is an easy consequence from 3.5(ii) applied to the particular subdeterminant functions.

Remark 4.5. (i) Chirotopes are a useful tool to describe the combinatorial structure of geometrical configurations. If we identify the row vectors of an $(n \times m)$-matrix $A$ with points $Q_1, Q_2, \ldots, Q_m \in \mathbb{R}^m$ then $\chi_A(j_1, j_2, \ldots, j_m)$ equals the orientation of $Q_{j_1}, Q_{j_2}, \ldots, Q_{j_m}$.

(ii) In fact, $P_x$ determines the random combinatorial structure of $n$ points randomly (= $\mu_{m-1}$-distributed) and independently thrown on an $m$-sphere. As in the proof of Remark 3.9(i) this result can immediately be deduced from Corollary 3.8. (The key is that the multiplication of any row of $A \in \text{Mat}(n, m)$ with a positive scalar leads to a matrix $A'$ with $\chi_{A'} = \chi_A = \Psi^o(\Psi(A))$.)

(iii) Definitions and objects from classical geometry can be transferred and generalized to chirotopes. Their combinatorial properties can be used to give alternate
proofs for well-known theorems from elementary geometry. Further, one can identity chirotopes with oriented matroids. (see e.g. [13], [14, p. 134f.], [11], [5]).

On the basis of geometrical considerations Goodman and Pollack conjectured that \( P_x \) attains maximum at \( \{(1,1,...,1), (-1,-1,...,-1)\} \) in \( \text{PGF}(3)^{23} \). To investigate this conjecture Theorem 4.4 suggests to simulate any distribution \( \nu \in \mathcal{M}_{\text{ind}}(\text{Mat}(n,m)) \) and to map the generated pseudorandom elements with \( \text{pr}_3 \circ \Psi \) into \( \text{PGF}(3)^{23} \). Doing so, one avoids time-consuming numerical operations on a manifold and on real projective space. Moreover, due to 4.4(vi) one may restrict his attention to \( \text{supp } P_x = (\text{Re}_x(n,m) \cap \text{Si}_x(n,m)) \cdot \{1, -1\} \). Nevertheless, this is not enough for \( (n,m) = (8,4) \) which is a case of particular interest ([2]). In fact, we have \( |\text{supp } P_x| \approx 12 \cdot 10^9 \) in this case which is gigantic. Without further informations we hence have no chance that relative frequencies obtained by a stochastic simulation converge to the true values.

Therefore we will exploit Theorem 3.2 once again. Since there do not exist \( \text{O}(n) \)-actions on \( \text{GF}(3)^{23} \setminus \{0\} \) and \( \text{PGF}(3)^{23} \) which supply further information on \( P_x \) we have to search for a further group which acts on all spaces occurring in diagram (3).

**Definition 4.6.** A matrix \( M \in \text{O}(k) \) is called *monoidal* if it maps the set \( \{ \pm e_1, \pm e_2, ..., \pm e_k \} \) bijectively onto itself. The set of all monoidal matrices of rank \( k \) is denoted by \( \text{Man}(k) \).

**Theorem 4.7.** (i) \( \text{Mon}(n) \leq \text{O}(n) \).

(ii) \( \Gamma_\wedge (\text{Mon}(n)) \leq \text{Mon}((\wedge n)) \).

(iii) The spaces \( \text{GF}(3)^{23} \setminus \{0\} \) and \( \text{PGF}(3)^{23} \) become \( \text{Mon}(n) \)-spaces via

\[
(M, q) \rightarrow M \cdot q := \gamma(M_\wedge) \quad \text{and} \quad (M, \{q, -q\}) \rightarrow \text{pr}_3(M \cdot q)
\]

for all \( (M, q) \in \text{Mon}(n) \times (\text{GF}(3)^{23} \setminus \{0\}) \) and \( x_q \in \gamma^{-1}(\{q\}) \).

(iv) Diagram (3) is commutative and all mappings are \( \text{Mon}(n) \)-equivariant.

(v) The \( \text{Mon}(n) \)-action divides \( \text{PGF}(3)^{23} \) into orbits ("reorientation classes"). The probability measure \( P_x \) has equal mass on any two elements contained in the same orbit. Especially, these assertions also hold for

\( \text{supp } P_x = (\text{Re}_x(n,m) \cap \text{Si}_x(n,m)) \cdot \{1, -1\} \) instead of \( \text{PGF}(3)^{23} \).

**Proof.** Let \( \mathcal{E} \) be defined as in the proof of Theorem 4.4 and let \( \wedge^m := \Psi \circ \pi_F^{-1} \). As \( M \) is monoidal

\[
\Gamma_\wedge (M)(\wedge^m(e_{j_1}, e_{j_2}, ..., e_{j_m})) = \wedge^m(Me_{j_1}, Me_{j_2}, ....)
\]

holds for each \( m \)-tuple \( (j_1, j_2, ..., j_m) \) in \( \Lambda(F, m) \). By this and since \( \Gamma_\wedge (M) \) is invertible

\[
\Gamma_\wedge (M)(\{ \pm \wedge^m(e_j) | e_j \in \mathcal{E} \}) = \{ \pm \wedge^m(e_j) | e_j \in \mathcal{E} \}.
\]
Hence $M \in \text{Mon}(\binom{p}{2})$ and (ii) is proved. As a left multiplication with $\Gamma \cdot (M)$ maps the set of pre-images $\{Y^{-1}(q) : q \in \text{GF}(3)^{\binom{p}{2}} \setminus \{0\}\}$ bijectively onto itself the $\text{Mon}(n)$-actions given in (4) are well defined. We already know that Diagram (3) is commutative and that its upper part is $O(n)$- and hence $\text{Mon}(n)$-equivariant. Together with (iii) this proves (iv). Assertion (i) follows immediately from definition and Theorem 3.2 (ii) proves (v). $\Box$

Theorem 4.7 is a decisive improvement of 4.4 since it reduces the cardinality of the simulation problem considerably. We just have to determine the cardinality of the reorientation classes $K_1, K_2, \ldots, K_s \subseteq (\text{Re}_x(n, m) \cap \text{Si}_x(n, m)) \cdot \{1, -1\}$ which is a pure combinatorial problem. Then we have to generate pseudorandom elements on $\text{Mat}(n, m)_*$ to obtain estimators for $P_x(K_1), \ldots, P_x(K_s)$. For $(n, m) = (8, 4)$ we have $s = 2604$. Hence the reduction factor $|\text{supp } P_x|/s \approx 5 \cdot 10^6$ in this case. Several stochastic simulations using various exact transformations gave a very serious indication that Goodman and Pollack’s conjecture concerning the location of the maximum of $P_x$ is true for $(n, m) = (8, 4)$ (see [2], [14, p. 149–158]).

**Remark 4.8.** (i) Altogether we simulated 1200000 pseudorandom elements on $\text{PGF}(3)^{\binom{p}{2}}$. These simulations led to the estimate

$$P_x(\{(1, 1, \ldots, 1), (-1, -1, \ldots, -1)\}) \approx 7 \cdot 10^{-10}.$$  

Considerations concerning the reliability of the results of simulation are given in [14, p. 151 f].

(ii) Exploiting specific properties of normally distributed random variables and Theorem 3.2 of [17] one can find a coset $T'$ of an $(m(n - m))$-dimensional vector subspace $T$ of $\text{Mat}(n, m)$ and a probability measure $\tau$ on $T$ with $\tau^X\cdot \{q, -q\} = \nu_X(\{q, -q\})$ where $\nu_X$ again denotes the restriction of $NI(0, 1)^{\binom{p}{2}}$ to $\text{Mat}(n, m)_*$. We point out that $\tau$ is not $O(n)$-invariant but its simulation yet requires less standard random numbers than that of $\nu_X$. As this does not belong to the thematic of this article we refer the interested reader to [14, p. 145f.] or [2] for a detailed treatment of this topic.

We conclude this article pointing out the advantages of the equivariance concept in this specific simulation problem: Above all we could trace the essential part of a stochastic simulation from a $\mathcal{U}_{n,m}$ back to an Euclidean space. Thereby we avoided problems which were discussed in section 2. We further had the freedom to choose an appropriate distribution on $\text{Mat}(n, m)_*$. Moreover, Theorems 4.4 and 4.7 gave us additional information about $P_x$. This led to a considerable reduction of the cardinality of the simulation problem on $\text{PGF}(3)^{\binom{p}{2}}$ which made a stochastic simulation for the (8, 4)-case practicable.
References