Convergence in distribution of the product of random variables from an independent sample on a compact algebraic group

An equivalent condition for the product of elements of an independent random sample on a compact algebraic group converging in distribution to some random variable as the sample size increases is obtained. Namely, a limit distribution exists and is uniform on the support of the parent distribution if a random variable with such a distribution does not belong with the unit probability to any non-trivial coset over an algebraic subgroup that lies in its normalizer; otherwise, it does not exist.

Key words: compact algebraic group, Haar measure, random variable, probability measure, convergence in distribution, uniform distribution.

The notations used

| Expression | Meaning |
|------------|---------|
| $V^*$      | the dual space to a space $V$ |
| $E$        | the identity operator |
| $\text{Spec } A$ | the set of eigenvalues of an operator $A$ |
| $J_m(\lambda)$ | the Jordan cell of size $m$ with eigenvalue $\lambda$ |
| $X^G$      | the subset of fixed points of an action $G: X$ |

Continuation on the next page
Expression | Meaning  
--- | ---  
$G_x$ | the stabilizer of a point $x$ for an action of a group $G$  
$I_Y$ | the indicator function of a subset $Y$  
$\xi \sim D$ | a random variable $\xi$ has distribution law $D$  
$\xi \sim \eta$ | random variables $\xi$ and $\eta$ are identically distributed  
$M\xi$ | the mean of a random variable $\xi$  
$\xrightarrow{P}$ | convergence of random variables in distribution  
a.s. | «almost surely» (with probability 1)  
i. i. d. | «independent identically distributed»  
u. o. s. | «unless otherwise stated»  
In a metric space $(X, \rho)$:  
$\rho(x, Y)$ | $\inf \{ \rho(x, y) : y \in Y \}$ — the distance from a point $x$ to a subset $Y$  
$U_\varepsilon(x)$ | $\{ y : \rho(x, y) < \varepsilon \}$ — the (open) $\varepsilon$-neighborhood of a point $x$  
$\varepsilon$-net | a subset $Y$ such that $\bigcup_{x \in Y} (U_\varepsilon(x)) = X$  

§ 1. Introduction

The papers [1, 2, 3] are devoted to researching various properties of random variables with values in a finite set $G$ on which, (mainly binary) operations are given. Without loss of generality, we can suppose that $G = \{1, \ldots, k\}$, $k \in \mathbb{N}$. In the space $\mathbb{R}^k$, take the standard basis $Q$ and the affine $(k - 1)$-dimensional simplex $S^{(k)} := \text{conv}(Q)$. Then the distribution law of each random variable $\xi$ on $G$ is uniquely defined by the vector $p = p(\xi) \in S^{(k)}$ with coordinates $p_i := P(\xi = i)$ ($i \in G$). A distribution is called uniform if all coordinates of its vector are equal (i.e. are equal to $\frac{1}{k}$).

If a set $\mathcal{F}$ of operations of arbitrary arities is given on $G$, then, one can define a notion of a formula over the set $\mathcal{F}$ depending on finitely many formal variables. The strict definition of a formula is inductive; it is well known in the particular case $k = 2$ for Boolean functions and literally retranslated onto the general one. In some way, a formula over $\mathcal{F}$ represents a finite expression that involves formal variables and applying operations from $\mathcal{F}$ taking the number of arguments into account. The complexity of a formula is defined as the number of applying operations in it, and the depth — as the depth of its circuit of functional elements (i.e. the possibly greatest distance between a root and a leaf). Finally, a formula is called read-once if each formal variable appears in it at most once.

If a formula involves $n$ formal variables $x_1, \ldots, x_n$, then it naturally induces an $n$-ary operation on $G$, i.e. a mapping $f : G^n \to G$. Thus, for arbitrary random variables $\xi_1, \ldots, \xi_n$ on $G$, the random variable $\eta := f(\xi_1, \ldots, \xi_n)$ is defined on $G$. In doing so, in the case of (mutual) independence of the random variables $\xi_1, \ldots, \xi_n$, the distribution vector $p(\eta) \in \mathbb{R}^k$ is uniquely expressed through the vectors $p(\xi_i)$ ($i = 1, \ldots, n$) via an $n$-ary operation $f$ on the
simplex $S^{(k)}$. With one more assumption that the formula is read-once, the replacement in it of all operations from $\mathcal{F}$ with the corresponding operations on $S^{(k)}$ and of the variables $x_i$ with the vectors $p_i \in S^{(k)}$ gives exactly the operation $\hat{f}$.

For read-once formulas of i.i.d. random variables, the question of convergence of distribution to the uniform one as the complexity and (or) the depth increases is actively studied. Present one important result in this direction.

**Definition.** A set with a binary operation on it is called a *quasigroup* if left and right multiplications by all elements in it are bijective.

**Theorem 1** (see Theorem 1 in [1, § 3]). Let $*$ be a quasigroup operation on the set $G = \{1, \ldots, k\}$ and $p \in S^{(k)}$ a vector with more than $\frac{k}{2}$ non-zero coordinates. Then the distribution of the random variable obtained by substitution of independent random variables with distribution $p$ to a read-once formula over the set $\{\cdot\}$, as its depth increases, converges exponentially to the uniform one.

Thus, Theorem 1 states that, unless the above-mentioned convergence holds for i.i.d. random variables, each of them with probability 1 takes a value in some subset $B \subset G$ of order at most $\frac{|G|}{2}$.

In this paper, similar properties of random variables on compact algebraic groups are researched. Consider a fixed probability space $(\Omega, \mathcal{A}, P)$. A *random variable* on a set $X$ with a $\sigma$-algebra $\mathcal{B}$ of its subsets is an $(\mathcal{A}, \mathcal{B})$-measurable mapping $\xi: \Omega \to X$; its distribution law is uniquely defined by the probability measure $\mu_\xi: \mathcal{B} \to [0; 1]$, $B \to P(\xi \in B)$. Now let $X$ be a topological space. Then, we will consider random variables on $X$ with respect to the corresponding Borel $\sigma$-algebra and define convergence in distribution $\xi_n \xrightarrow{F} \xi$ as the convergence $M(f(\xi_n)) \xrightarrow{n \to \infty} M(f(\xi))$ for any continuous bounded function $f: X \to \mathbb{R}$. If, in addition, $X$ is a compact set, then the condition of boundedness of the function can be omitted since it follows from continuity.

U.o.s., assume that, on all finite-dimensional real linear spaces and algebraic groups, the real topology is given.

Let $(G, \cdot)$ be a compact algebraic group. One can define on it the Borel $\sigma$-algebra $\mathcal{B}$ and, also, the *Haar measure* $\mu: \mathcal{B} \to [0; 1]$ invariant under left and right multiplications and satisfying the normalization condition $\mu(G) = 1$. Subgroups of the group $G$ will, u.o.s., be supposed to be algebraic. If a random variable $\xi$ on $G$ satisfies the condition $\mu_\xi \equiv \mu$, then its distribution law will be called *uniform* and denoted by $R(G)$.

Each read-once formula of complexity $n - 1$ ($n \in \mathbb{N}$) over the set $\{\cdot\}$ induces the $n$-ary operation $G^n \to G$, $(g_1, \ldots, g_n) \to g_{\tau(1)} \cdots g_{\tau(n)}$, $\tau \in S_n$. Substitution to it of independent random variables $\xi_1, \ldots, \xi_n$ with common distribution law $D$ gives a random variable with the distribution law of $\xi_1 \cdot \cdots \cdot \xi_n$; this law is uniquely defined by $D$ and $n$ while does not depend on $\tau$.

Due to compactness of $G$, each non-empty family of its subgroups has a minimal element by inclusion. Let $\xi$ be an arbitrary random variable on $G$. The family of all subgroups
$H \subset G$ such that $\xi \in H$ a.s. is closed under intersection. Hence, there exists the least of such subgroups by inclusion that will be called the support of $\xi$ (not. supp $\xi$).

The main result of the paper is the following theorem.

**Theorem 2.** Let $\xi$ be a random variable on $G$ with support $\overline{G}$ and $\xi_n \sim \xi$ ($n \in \mathbb{N}$) independent random variables. Then the following conditions are equivalent:

1) $\xi_1 \ldots \xi_n \xrightarrow{F} \eta$ for some random variable $\eta$ on $G$;

2) $\xi_1 \ldots \xi_n \xrightarrow{F} \eta$ where $\eta \sim \mathcal{R}(\overline{G})$;

3) for each subgroup $H \subset \overline{G}$ and coset $Z \in (N(H))/H$ such that $\xi \in Z$ a.s., we have $H = \overline{G}$;

4) for each subgroup $H \subset G$ and coset $Z \in (N(H))/H$ such that $\xi \in Z$ a.s., we have $Z = H$.

The implication 2) $\Rightarrow$ 1) is obvious. Besides, if 4) holds, then 3) also holds: for each subgroup $H \subset \overline{G}$ and coset $Z \in (N(H))/H$ such that $\xi \in Z$ a.s., we have $Z = H$, and, hence, $\xi \in H$ a.s. that implies $H \supset (\text{supp } \xi) = \overline{G} \supset H$, $H = \overline{G}$. It remains to prove the implications 1) $\Rightarrow$ 4) and 3) $\Rightarrow$ 2) that is done further in the paper.

---

**§ 2. Auxiliary facts**

This section contains a number of auxiliary statements.

**Statement 1.** If $m \in \mathbb{N}$, $\lambda \in \mathbb{C}$, and $|\lambda| < 1$, then $(J_m(\lambda))^n \xrightarrow{n \to \infty} 0$.

□ As $n \to \infty$, we have

$$\forall k \geq 0 \quad C_n^k \lambda^{n-k} \sim \frac{n^k \lambda^{n-k}}{k!} \to 0$$

that gives $(J_m(\lambda))^n = \sum_{0 \leq k < m} \left( C_n^k \lambda^{n-k}(J_m(0))^k \right) \to 0$. □

Let $G$ be a topological space and $\mathbb{F}$ a field $\mathbb{R}$ or $\mathbb{C}$. Denote by $C_\mathbb{F}(G)$ the Banach space (over $\mathbb{F}$) of all continuous bounded functions $G \to \mathbb{F}$ with the uniform norm. Fix random variables $\eta$ and $\eta_n$ ($n \in \mathbb{N}$) on $G$.

For an arbitrary finite-dimensional space $W$ over $\mathbb{F}$, all continuous bounded functions $f : G \to W$ such that $M(f(\eta_n)) \xrightarrow{n \to \infty} M(f(\eta))$ form a space (again over $\mathbb{F}$) that will be denoted by $L_W(G)$. In particular, $L_\mathbb{F}(G) \subset C_\mathbb{F}(G)$. 


Proposition 1. For any finite-dimensional spaces $W_{1,2}$ over $\mathbb{F}$, operator $A: W_1 \to W_2$ and function $f \in L_{W_1}(G)$, we have $(A \circ f) \in L_{W_2}(G)$. □

Preserving continuity and boundedness is obvious. Besides, if $\xi$ is an arbitrary random variable on $G$, then $M((A \circ f)(\xi)) = A(M(f(\xi)))$. ■

Corollary 1. Any finite-dimensional space $W$ over $\mathbb{F}$ and function $f: G \to W$ satisfy the relation $(f \in L_W(G)) \Leftrightarrow (\forall \alpha \in W^* (\alpha \circ f) \in L_{\mathbb{F}}(G))$. □

The operator $E \in \text{Hom}_\mathbb{F}(W, W) = W \otimes_\mathbb{F} W^*$ has form $\sum_{i=1}^m (A_i \circ \alpha_i)$ ($\alpha_i \in W^*$, $A_i \in \text{Hom}_\mathbb{F}(\mathbb{F}, W)$), and, thus, $f = \sum_{i=1}^m (A_i \circ (\alpha_i \circ f))$. It remains to use Proposition 1. ■

Statement 2. For any function $f \in C_\mathbb{F}(G)$ and random variable $\xi$ on $G$, there holds $|M(f(\xi))| \leq \|f\|$. □

If $c := \|f\|$, then $|f| \leq c$, $|f(\xi)| \leq c$, $|M(f(\xi))| \leq M|f(\xi)| \leq M(c) = c$. ■

Lemma 1. The subspace $L_\mathbb{F}(G) \subset C_\mathbb{F}(G)$ is closed. □

Suppose that $f_m \in L_\mathbb{F}(G)$ ($m \in \mathbb{N}$), $f_\infty \in C_\mathbb{F}(G)$ and, also, $f_m \Rightarrow f_\infty$ on $G$, i.e. $c_m := \|f_m - f_\infty\| \xrightarrow{m\to\infty} 0$. We need to prove that $f_\infty \in L_\mathbb{F}(G)$.

Set $a_{m,n} := M(f_m(\eta_n))$ and $a_m := M(f_m(\eta))$ ($m \in \mathbb{N} \cup \{\infty\}$, $n \in \mathbb{N}$). For any random variable $\xi$ on $G$ and number $m \in \mathbb{N}$, we have

$$|M(f_m(\xi)) - M(f_\infty(\xi))| = |M((f_m - f_\infty)(\xi))| \leq \|f_m - f_\infty\| = c_m.$$ 

In particular, $|a_{m,n} - a_{\infty,n}| \leq c_m$ and $|a_m - a_{\infty}| \leq c_m$ ($m, n \in \mathbb{N}$). Recall that $c_n \xrightarrow{n\to\infty} 0$.

Hence, $a_m \xrightarrow{m\to\infty} a_{\infty}$ and $a_{m,n} \xrightarrow{m\to\infty} a_{\infty,n}$ uniformly by $n \in \mathbb{N}$. Meanwhile, $a_{m,n} \xrightarrow{n\to\infty} a_{m_n}$ ($m \in \mathbb{N}$). Therefore, $a_{m,n} \xrightarrow{n\to\infty} a_{\infty,n}$, i.e. $f_\infty \in L_\mathbb{F}(G)$. ■

It is obvious that the subspaces $C_C(G)$ and $L_C(G)$ are complexifications of the subspaces $C_\mathbb{R}(G)$ and $L_\mathbb{R}(G)$ respectively. It follows that

$$(\eta_n \xrightarrow{n\to\infty} \eta) \Leftrightarrow (L_\mathbb{R}(G) = C_\mathbb{R}(G)) \Leftrightarrow (L_C(G) = C_C(G)). \quad (1)$$

From now, we will additionally assume that the topological space $G$ is in fact a compact algebraic group; for its Borel $\sigma$-algebra and Haar measure, save the earlier notations $B$ and $\mu$ respectively.

Definition. Matrix coefficients of the group $G$ are any functions of type $(\alpha \circ \varphi): G \to \mathbb{C}$, where $\varphi: G \to \text{GL}(V)$ is an irreducible complex representation and $\alpha$ is a linear function $\text{End}(V) \to \mathbb{C}$. 

5
The following theorem is known as «part I» of the Peter–Weyl theorem (see, for instance, [4, § I.5], Theorem 1.12 and Remark after its statement).

**Theorem 3.** The linear span of matrix coefficients of the group $G$ is dense in $C_c(G)$.

**Theorem 4.** The following conditions are equivalent:

1) $\eta_n \xrightarrow{F} \eta$;

2) for arbitrary irreducible complex representation $\varphi: G \to \text{GL}(V)$ and linear function $\alpha: \text{End}(V) \to \mathbb{C}$, we have $(\alpha \circ \varphi) \in L_c(G)$;

3) for any irreducible complex representation $\varphi: G \to \text{GL}(V)$, there holds

$$M(\varphi(\eta_n)) \xrightarrow{n \to \infty} M(\varphi(\eta)).$$

□ The equivalence 1) $\Leftrightarrow$ 2) follows from Equation (1), Lemma 1 and Theorem 3, and the equivalence 2) $\Leftrightarrow$ 3) — from Corollary 1.

Let $\varphi: G \to \text{GL}(V)$ be a complex representation.

For any independent random variables $\xi_1, \ldots, \xi_n$ on $G$, the random variables $\varphi(\xi_i)$ ($i = 1, \ldots, n$) on the space $\text{End}(V)$ are also independent that implies

$$M(\varphi(\xi_1, \ldots, \xi_n)) = M(\varphi(\xi_1)) \cdot \ldots \cdot M(\varphi(\xi_n)).$$

Consequently, for arbitrary element $g \in G$ and random variable $\eta$ on $G$, we have

$$M(\varphi(\eta g)) = (M(\varphi(g))) \cdot (M(\varphi(\eta))).$$

§ 3. Proofs of the results

In this section, Theorem 2 is proved.

Recall that 2) $\Rightarrow$ 1) and 4) $\Rightarrow$ 3) (see § 1). It remains to prove that 1) $\Rightarrow$ 4) and 3) $\Rightarrow$ 2).

Take arbitrary random variables $\xi$ and $\xi_n$ ($n \in \mathbb{N}$) from the statement of Theorem 2. Set $\eta_n := \xi_1 \cdot \ldots \cdot \xi_n$ ($n \in \mathbb{N}$).

1) $\Rightarrow$ 4).

Take any random variable $\eta$ on $G$, subgroup $H \subset G$ and element $b \in N(H)$ such that $\eta_n \xrightarrow{F} \eta$ and $\xi \in bH$ a.s. It is required to prove that $b \in H$.

In the compact algebraic group $G$, there exists metrics $\rho$ invariant under left and right multiplications and inducing the standard real topology.

Choose an arbitrary number $\varepsilon > 0$.

Since $G$ is a compact group, it has a finite $\varepsilon$-net $Y$, and, hence, for some neighborhood $U$ of type $U_\varepsilon(a)$ ($a \in Y$), there holds

$$M(I_U(\eta_n)) = P(\eta \in U) > 0.$$
The function $f : G \to \mathbb{R}$, $g \to \max\{2\varepsilon - \rho(a, g); 0\}$ is continuous and satisfies $0 \leq f \leq 2\varepsilon$ (so, is bounded). Thus,

\begin{align*}
\forall g \in U & \quad \rho(a, g) < \varepsilon, \quad f(g) > \varepsilon; \\
f \geq \varepsilon I_U; & \quad f(\eta) \geq \varepsilon \cdot I_U(\eta); \\
M(f(\eta_n)) & \xrightarrow{n \to \infty} M(f(\eta)) \geq \varepsilon \cdot M(I_U(\eta)) > 0;
\end{align*}

$\exists n_0 \in \mathbb{N}$ \quad $\forall n \geq n_0$ \quad $M(f(\eta_n)) > 0$.

(3)

Take an arbitrary positive integer $n \geq n_0$. Note that $\eta_n \in b^n H$ a.s. If $f|_{b^n H} \equiv 0$, then $f(\eta_n) = 0$ a.s. that contradicts (3). Hence, for some elements $h_n \in H$ and $g_n := b^n h_n$, we have $f(g_n) \neq 0$, i.e. $\rho(a, g_n) < 2\varepsilon$.

If $n := n_0$, then $n, n+1 \geq n_0$, and, therefore, $\rho(a, g_n), \rho(a, g_{n+1}) < 2\varepsilon$, $\rho(g_{n+1}, g_n) < 4\varepsilon$;

$\rho(b, H) \leq \rho(b, h_n b_{n+1}) = \rho(b^n b h_{n+1}, b^n h_{n+1}) = \rho(g_{n+1}, g_n) < 4\varepsilon$.

Since the number $\varepsilon$ is chosen arbitrarily and the subgroup $H \subset G$ is closed, then $b \in H$.

So, the implication 1) $\Rightarrow$ 4) is completely proved.

3) $\Rightarrow$ 2).

The subgroup $\overline{G} = \text{supp} \xi \subset G$ with probability 1 contains all random variables $\xi, \xi_n$ and $\eta_n$ ($n \in \mathbb{N}$). Therefore, while proving the implication 3) $\Rightarrow$ 2), we can, without loss of generality, assume that $\overline{G} = G$.

Suppose that, for each subgroup $H \subset G$ and coset $Z \in (N(H))/H$ such that $\xi \in Z$ a.s., there holds $H = G$. We need to prove that $\eta_n \xrightarrow{F \cdot n \to \infty} \eta$ where $\eta \sim R(G)$.

The measure $\mu_\eta$ on $G$ coincides with $\mu$ that implies

$\forall g \in G$ \quad $\forall B \in \mathcal{B}$ \quad $\mu_\eta(B) = P(\eta \in B) = P(\eta \in g^{-1} B) = \mu_\eta(B)$;

$\forall g \in G$ \quad $\mu_{g\eta} \equiv \mu \equiv \mu_\eta$, \quad $\eta \sim g\eta$.

Let $\varphi : G \to \text{GL}(V)$ be any irreducible complex representation. Prove the relation (2).

The subspace $V^G \subset V$, being $G$-invariant, equals 0 or $V$. If $V^G = V$, then $\varphi(G) = \{E\}$, $\varphi(\eta_n) = \varphi(\eta) = \mu = \text{const}$, that obviously implies (2). So, assume from now that $V^G = 0$.

For each $g \in G$, we have $\eta \sim g\eta$, $M(\varphi(\eta_n)) = M(\varphi(\eta)) = (\varphi(g)) \cdot \left(M(\varphi(\eta))\right)$. Therefore, $M(\varphi(\eta)) \subset V^G = 0$, $M(\varphi(\eta)) = 0$. Set $T := M(\varphi(\xi))$. Then, $M(\varphi(\eta_n)) = T^n$ ($n \in \mathbb{N}$).

The space $V$ has a $G$-invariant positively definite Hermitian form $(\cdot, \cdot)$; denote by $\|\cdot\|$ the corresponding norm.

Suppose that the operator $T$ has an eigenvalue $\lambda$ with $|\lambda| \geq 1$. In this case, there exists a vector $v \in V \setminus \{0\}$ such that $Tv = \lambda v$. Note that

$$
\|\xi v - \lambda v\|^2 = \|\xi v\|^2 + \|\lambda v\|^2 - 2\Re(\xi v, \lambda v) = \|v\|^2 + \|\lambda v\|^2 - 2\Re(\xi v, \lambda v)
$$

and $M(\xi v, \lambda v) = (Tv, \lambda v) = (\lambda v, \lambda v) = \|\lambda v\|^2$; hence,

$$
M(\|\xi v - \lambda v\|^2) = \|v\|^2 + \|\lambda v\|^2 - 2\Re(\|\lambda v\|^2) = \|v\|^2 - \|\lambda v\|^2 = (1 - |\lambda|^2) \cdot \|v\|^2 \leq 0.
$$
Therefore, $\xi v = \lambda v$ a.s. Denote by $G_{(v)}$ the subgroup of all elements of $G$ preserving the line $\langle v \rangle = \mathbb{C}v$. Obviously, the kernel of the homomorphism $G_{(v)} \to \text{GL}(\langle v \rangle)$, $g \to g_{(v)}$ is $G_v$. So, $G_v < G_{(v)}$. All elements of $G$ taking $v$ to $\lambda v$ form a coset $gG_v$ ($g \in G_{(v)} \subset N(G_v)$), and $\xi \in gG_v$ a.s. By assumption, $G_v = G$, $v \in V^G = 0$, that contradicts the choice of $v$.

Hence, $|\lambda| < 1$ for all $\lambda \in \text{Spec } T$. By Statement 1, each cell $J$ of the Jordan form of the operator $T$ satisfies $J^n \xrightarrow{n \to \infty} 0$. Therefore, $T^n \xrightarrow{n \to \infty} 0$, i.e. $M(\varphi(\eta_n)) \xrightarrow{n \to \infty} M(\varphi(\eta))$.

So, we obtained that any irreducible complex representation $\varphi: G \to \text{GL}(V)$ satisfies (2).

By Theorem 4, $\eta_n \xrightarrow{n \to \infty} \eta$.

It completely proves the implication 3) $\Rightarrow$ 2) and, thus, the whole Theorem 2.

Acknowledgements

The author is grateful to Prof. E. B. Vinberg for exciting interest to algebra.

The author dedicates the article to E. N. Troshina.

References

[1] Yashunskii A. D. On transformations of probability distributions by read-once quasigroup formulae // Discr. Math. Appl. 2013. Vol. 23. № 2. Pp. 211–223.

[2] Yashunskii A. D. On read-once transformations of random variables over finite fields // Discr. Math. Appl. 2015. Vol. 25. № 5. Pp. 311–321.

[3] Yashunskii A. D. Convex algebras of probability distributions induced by finite associative rings // Discr. Math. Appl. 2021. Vol. 31. № 3. Pp. 223–230.

[4] Knapp A. W. Representation theory of semisimple groups. Princeton Univ. Press, 1986, 773 p.

ISBN: 0-691-09089-0.