ON THE ORIGIN OF THE BOLTZMANN DISTRIBUTION

FEDOR SANDOMIRSKIY

Princeton University

OMER TAMUZ

California Institute of Technology

ABSTRACT. Boltzmann distributions are used in statistical mechanics to describe how the states of a system are distributed at a given temperature. We give a novel characterization of this family as the unique one satisfying independence for uncoupled systems. The theorem boils down to a statement about endomorphisms of the convolution semi-group of finitely supported probability measures on the natural numbers, or, alternatively, about endomorphisms of the multiplicative semi-group of polynomials with non-negative coefficients.

1. INTRODUCTION

In statistical mechanics, a system can be found in various possible states. A state refers to a complete microscopic description of the system which encodes all physically relevant variables, and in particular determines the system's energy.[1] In an equilibrium with a given temperature, the distribution of states is given by the Boltzmann distribution: The probability that the system has energy E is proportional to the number of states with energy E times $\mathrm{e}^{-\beta E}$, where $1/\beta$ is proportional to the temperature of the environment. Formally, if μ is a probability measure on the reals describing the fraction of states with given energy—i.e., for measurable $A \subseteq \mathbb{R}$, the fraction of states with energy in A is $\mu(A)$—then the distribution of energy is given by the measure $\Phi_\beta[\mu]$ where

$$\mathrm{d}\Phi_\beta[\mu](E) = C\mathrm{e}^{-\beta E}\mathrm{d}\mu(E),$$

[1]Statistical mechanics serves only as a motivation for the mathematical question we study. For a brief introduction to the relevant physics concepts, see Section 2.1 of [6]. An uninterested reader may proceed directly to the "Definitions and Results" section.

and C is the normalization constant.

The map Φ_β that assigns to each probability measure μ on $\mathbb{R}$ the measure $\Phi_\beta[\mu]$ has two important properties: First, it preserves the measure class of μ, so that μ and $\Phi_\beta[\mu]$ are mutually absolutely continuous. Second, it commutes with convolution:

$$(1.1) \qquad \Phi_\beta[\mu_1 * \mu_2] = \Phi_\beta[\mu_1] * \Phi_\beta[\mu_2].$$

In terms of the physics, the first property means that the system can only be found at an energy level that corresponds to an existing state, and conversely, any existing state can be attained. The second property involves products of independent systems. Suppose that μ_1 and μ_2 describe the distribution of states in two systems. Form a new system whose set of states is the product of the two sets of states, and whose energy in each state is the sum of the two corresponding energies; this corresponds to no interaction between the two subsystems. Then the convolution $\mu_1 * \mu_2$ describes the new system, and (1.1) follows from the assumption that the joint distribution of states is the product measure of the distributions in the two subsystems, or, differently put, the assumption that there is no correlation between systems that do not interact.

The usual explanation for the Boltzmann distribution is one of maximum entropy [4]. The physics behind this stems from the idea that a system of interest is in contact with the environment—a large "heat bath"—and that the state of the combined system is distributed uniformly over a fixed-energy surface in phase space.

In this paper, we offer an alternative explanation: Our main result is that the members of the family $(\Phi_\beta)_{\beta \in \mathbb{R}}$ are the unique maps that are measure-class-preserving and commute with convolution. Note that Φ_β is not well-defined for every probability measure μ on $\mathbb{R}$, since normalization is impossible when the tails are too thick. We limit ourselves to finitely supported probability measures, and furthermore to measures with support in either the natural numbers, integers or rationals.

The map Φ_β is also the tilting map, whose usefulness in the theory of large deviations stems from the fact that it commutes with convolutions; see, e.g., [1, Lemma 2.6.4]. It is thus natural to ask which maps from measures to measures are like tilting, in the sense that they preserve the measure class and commute with convolution. In this context, our main result is a negative one, stating that none other exist.

Definitions and Results. Given a subset $S \subseteq \mathbb{R}$ closed with respect to addition, denote by $\mathrm{Prob}(S)$ the set of finitely supported probability measures on S. This is a semi-group under the operation of convolution. We say that $\Phi \colon \mathrm{Prob}(S) \to \mathrm{Prob}(S)$ is *support-preserving* if μ and $\Phi[\mu]$ have the same support, or, equivalently, are mutually absolutely continuous, for all $\mu \in \mathrm{Prob}(S)$; note that since these are finitely supported measures, the two notions indeed coincide. We say that Φ is an *endomorphism* if it commutes with convolution, i.e., if $\Phi[\mu_1 * \mu_2] = \Phi[\mu_1] * \Phi[\mu_2]$.

The map $\Phi_\beta \colon \mathrm{Prob}(S) \to \mathrm{Prob}(S)$ given by

$$\Phi_\beta[\mu](s) = \frac{\mu(s)\mathrm{e}^{-\beta s}}{\sum_t \mu(t)\mathrm{e}^{-\beta t}}$$

is easily verified to be a support-preserving endomorphism. Our main result is that these are the unique ones, when S is $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}$ or $\mathbb{Q}$.

Theorem 1. *Suppose that S is either $\mathbb{Z}_{\geq 0}$, $\mathbb{Z}$, or $\mathbb{Q}$. Then, for every support-preserving endomorphism Φ of $\mathrm{Prob}(S)$, there exists a constant $\beta \in \mathbb{R}$ such that $\Phi = \Phi_\beta$.*

For $S = \mathbb{R}$, the corresponding claim is not true, as we discuss below. However, it does hold if we also require Φ to be weakly continuous, as a corollary of the statement for $S = \mathbb{Q}$.

Note that even though Φ is not assumed to be a bijection, this property emerges as a consequence of the assumptions of Theorem 1. Another emergent property is that, up to normalization, Φ is affine, i.e., there is a function $f \colon \mathbb{R} \to \mathbb{R}$ such that $\Phi[\mu](s)$ is proportional to $\mu(s)f(s)$. We do not assume affinity; under such an additional assumption, it is easy to show that f is an exponential.

The bulk of the effort in the proof of Theorem 1 is the case $S = \mathbb{Z}_{\geq 0}$. By considering probability-generating functions, this question can be reduced to a question about polynomials. Denote by $\mathcal{P}$ the polynomials in one variable whose coefficients are non-negative and sum to one:

$$\mathcal{P} = \left\{ p(x) = \sum_{k=0}^n p_k x^k \,\middle|\, p_k \geq 0, \ p(1) = 1 \right\}.$$

These are precisely the probability-generating functions of finitely supported probability measures on $\mathbb{Z}_{\geq 0}$. We note that representing probability measures by probability-generating functions is equivalent to looking at their Fourier transforms. The representation of a probability measure by its probability-generating function carries a trade-off: while simplifying convolution of measures to mere multiplication, this representation makes it harder to handle the support-preserving property.

We say that $\Phi \colon \mathcal{P} \to \mathcal{P}$ is support-preserving if it preserves the set of positive coefficients. That is, if $p' = \Phi[p]$, then $p'_k > 0$ if and only if $p_k > 0$. We say that Φ is multiplicative if $\Phi[p \cdot p'] = \Phi[p] \cdot \Phi[p']$. These two properties, translated back to probability measures, are equivalent to Φ being a support-preserving endomorphism.

Theorem 2. *For every support-preserving multiplicative $\Phi \colon \mathcal{P} \to \mathcal{P}$ there exists a constant $\gamma > 0$ such that $\Phi[p](x) = p(\gamma x)/p(\gamma)$.*

By identifying finitely supported probability measures on $\mathbb{Z}_{\geq 0}$ with their probability-generating functions, this result is equivalent to the case $S = \mathbb{Z}_{\geq 0}$ in Theorem 1.

A corollary of Theorem 2 is that if p is a polynomial with at least two terms—e.g., $p(x) = (x+1)/2$—then Φ is completely determined by $\Phi[p]$: if $\Phi'[p] = \Phi[p]$ for two support-preserving multiplicative maps Φ, Φ', then $\Phi = \Phi'$.

Corollary 1.1. *Suppose that* $\Phi, \Phi' \colon \mathcal{P} \to \mathcal{P}$ *are support-preserving and multiplicative and* $p \in \mathcal{P}$ *is a polynomial with at least two terms. Then* $\Phi[p] = \Phi'[p]$ *implies that* $\Phi = \Phi'$.

Indeed, by Theorem 2 there are $\gamma, \gamma' > 0$ such that $\Phi[p](x) = p(\gamma x)/p(\gamma)$ and $\Phi'[p](x) = p(\gamma' x)/p(\gamma')$. Comparing coefficients at the lowest-degree monomials, we conclude that $\Phi[p] = \Phi'[p]$ implies $\gamma = \gamma'$ and hence $\Phi = \Phi'$.

This corollary may be a priori surprising since it is not clear how the multiplicative and support-preserving properties of Φ imply that fixing $\Phi[(x+1)/2]$ constrains $\Phi[q]$ for any q that is not a power of $(x+1)/2$. Indeed, one could have imagined that any choice of $\Phi[(x+1)/2]$ and, say, $\Phi[(x^2 + x^{17})/2]$ that is support-preserving could be extended to a support-preserving and multiplicative Φ. Nevertheless, this is generally impossible, as a consequence of Theorem 2. The underlying reason is that $\mathcal{P}$ is not a unique factorization domain.

Say that $p \in \mathcal{P}$ is irreducible if it cannot be written as a product $p = q_1 \cdot q_2$, for $q_1, q_2 \in \mathcal{P}$ such that $q_1, q_2 \neq 1$. It is easy to see that every $p \in \mathcal{P}$ can be written as a product of irreducibles. But importantly, this decomposition is not always unique. Hence, if $p = q_1 \cdot q_2 = r_1 \cdot r_2$, then $\Phi[q_1] \cdot \Phi[q_2] = \Phi[r_1] \cdot \Phi[r_2]$, providing additional constraints on Φ. As it turns out, there are sufficiently many such constraints for $\Phi[(x+1)/2]$ to fix Φ.

Proof techniques. The main tool in the proof of Theorem 2 is the extension of a support-preserving multiplicative Φ to the larger domain

$$\mathcal{M} = \left\{ p(x) = \sum_{k=0}^{d} p_k x^k \ \middle| \ p(x) > 0 \text{ for all } x > 0, \ p(1) = 1 \right\}.$$

These are the polynomials that are positive for positive x and whose coefficients sum to 1. Equivalently, these are the generating functions of signed, finitely supported, unit mass measures on $\mathbb{Z}_{\geq 0}$ that have a positive moment generating function.[2]

The fact that Φ can be extended to a multiplicative map on $\mathcal{M}$ follows from the following classical result due to Poincaré [12].

Lemma 1.2 (Poincaré). *For every* $p \in \mathcal{M}$ *there is an* $r \in \mathcal{P}$ *such that* $p \cdot r \in \mathcal{P}$.

---

[2]In statistical mechanics terms, these measures describe systems that have *anti-states*—a negative number of states at some energies—but still have a positive partition function. It is unclear if these have a meaningful physical interpretation.

Using this, we can extend the domain of any support-preserving multiplicative Φ to $\mathcal{M}$ by choosing for $p \in \mathcal{M}$ an $r \in \mathcal{P}$ such that $p \cdot r \in \mathcal{P}$ and setting

$$\Phi[p] = \frac{\Phi[p \cdot r]}{\Phi[r]}.$$

As we show, this is well-defined, i.e., independent of the choice of r. However, $\Phi[p]$ could now be a rational function. The first part of our proof is dedicated to showing that the image of this extension of Φ is, in fact, in $\mathcal{M}$.

The advantage of $\mathcal{M}$ is that it is a unique factorization domain: This set consists of the polynomials p with $p(1) = 1$ that have no positive roots, and hence, by the fundamental theorem of algebra, each $p \in \mathcal{M}$ can be written as a product of linear terms with non-positive roots and quadratic terms without real roots, all in $\mathcal{M}$, and this decomposition is unique. Since Φ commutes with multiplication, in order to show that $\Phi[p] = \Phi_\beta[p]$ for all $p \in \mathcal{M}$, it suffices to show that this holds for linear and quadratic p. This is what the remainder of our effort is dedicated to.

Polynomials with rational coefficients. Recall that, in the physics interpretation, a measure μ represents the fraction of states at each energy level. In quantum mechanical settings, there are often only finitely many states at each energy level. In this case, the measure μ will have rational probabilities, and the corresponding probability-generating function will be a polynomial with rational coefficients. Indeed, if there are k_i states with energy E_i and the total number of states is $k = \sum_i k_i$, then μ has an atom of weight k_i/k at E_i. This motivates the pursuit of the same questions, but in a rational setting. Let

$$\mathcal{P}_\mathbb{Q} = \left\{ p(x) = \sum_{k=0}^d p_k x^k \,\middle|\, p_k \in \mathbb{Q}_{\geq 0}, \;\; p(1) = 1 \right\}$$

be the set of polynomials with non-negative rational coefficients that sum to one. The next result shows that Theorem 2 still holds in this setting.

Theorem 3. *For every support-preserving multiplicative $\Phi \colon \mathcal{P}_\mathbb{Q} \to \mathcal{P}$ there exists a constant $\gamma > 0$ such that $\Phi[p](x) = p(\gamma x)/p(\gamma)$.*

If the image of Φ is further restricted to belong to $\mathcal{P}_\mathbb{Q}$, then the resulting parameter γ will also belong to $\mathbb{Q}$.

The proof of Theorem 3 requires additional arguments beyond those of Theorem 2.[3] The main difficulty is that the rationality of the coefficients leads to more (and more

---

[3]The same proof technique shows that a version of Theorem 3 holds for any subfield of $\mathbb{R}$ instead of $\mathbb{Q}$. We focus on the case of $\mathbb{Q}$ since other subfields do not result in a clear physical interpretation.

complicated) irreducible polynomials. We circumvent this issue by using the arguments from the proof of Theorem 2 to show a similar statement for a dense sub-semi-group that does have simple irreducibles, and then proving the following automatic continuity type result.

We say that a set P of polynomials is rich if P contains $q(x) = x$ and, with each polynomial of the form $p(x) = x^m \cdot r(x)$ contained in P, the polynomial $r(x)$ is also contained in P. We endow $\mathcal{M}$ with the topology of simultaneous convergence of the coefficients and the degree.

Proposition 1.3. *Let $M \subset M'$ be rich dense sub-semi-groups of $\mathcal{M}$. Suppose $\Phi \colon M' \to \mathcal{M}$ is multiplicative and degree-preserving, $\Phi[p] \in \mathcal{P}$ for $p \in M' \cap \mathcal{P}$, and the restriction of Φ to M is the identity map. Then Φ is the identity map.*

Here, "degree-preserving" means that q and $\Phi[q]$ are polynomials of the same degree.

Open questions.

Probability measures over the reals. Endow the set $\mathrm{Prob}(\mathbb{R})$ of finitely supported probability measures on $\mathbb{R}$ with the topology defined by $\mu_n \to \mu$ if $\int f \, d\mu_n \to \int f \, d\mu$ for all continuous $f \colon \mathbb{R} \to \mathbb{R}$. Then $\mathrm{Prob}(\mathbb{Q})$ is a dense subset of $\mathrm{Prob}(\mathbb{R})$, and so any continuous support-preserving endomorphism of $\mathrm{Prob}(\mathbb{R})$ is of the form Φ_β.

There are many other support-preserving endomorphisms of $\mathrm{Prob}(\mathbb{R})$. Indeed, if $\pi \colon \mathbb{R} \to \mathbb{R}$ is any non-continuous solution to the Cauchy equation $\pi(x + y) = \pi(x) + \pi(y)$, then

$$\Phi[\mu](x) = \frac{\mu(x)\mathrm{e}^{-\pi(x)}}{\sum_y \mu(y)\mathrm{e}^{-\pi(y)}}$$

is a support-preserving endomorphism. Of course, this is non-constructive, since the existence of non-continuous solutions of the Cauchy equation requires an application of some axiom of choice (e.g., any axiom that is strong enough to guarantee a Hamel basis of $\mathbb{R}$ over $\mathbb{Q}$). A natural conjecture is that any support-preserving endomorphism on $\mathrm{Prob}(\mathbb{R})$ that is not continuous (equivalently, not of the form Φ_β) is not measurable.

The same conjecture can be made about support-preserving endomorphisms of the set of compactly supported (rather than finitely supported) probability measures on the reals. In this case, we suspect that the conjecture follows from automatic continuity results for Polish groups, such as the Banach-Pettis Theorem (see Theorem 2.2 in [14]).

Support-preserving endomorphisms of $\mathrm{Prob}(\mathbb{Z}^d)$ and beyond. Our techniques do not extend beyond $d = 1$ in a straightforward way, as multivariate polynomials do not generally decompose into a product of simple factors, such as the quadratic polynomials in the one-dimensional case. We thus offer the following question: Is

there, for every support-preserving endomorphism $\Phi\colon \mathrm{Prob}(\mathbb{Z}^d) \to \mathrm{Prob}(\mathbb{Z}^d)$, a vector $\beta = (\beta_1, \ldots, \beta_d)$ such that

$$\Phi[\mu](x) = \frac{\mu(x)\mathrm{e}^{-\beta \cdot x}}{\sum_y \mu(y)\mathrm{e}^{-\beta \cdot y}}?$$

More generally, given a semi-group G, does there always exist a homomorphism $\pi\colon G \to \mathbb{R}$ such that every support-preserving $\Phi\colon \mathrm{Prob}(G) \to \mathrm{Prob}(G)$ is of the form

$$\Phi[\mu](x) = \frac{\mu(x)\mathrm{e}^{-\pi(x)}}{\sum_y \mu(y)\mathrm{e}^{-\pi(y)}}?$$

Weakening the support-preserving requirement. For $S \subset \mathbb{R}$, say that $\Psi\colon \mathrm{Prob}(S) \to \mathrm{Prob}(S)$ is *weakly support-preserving* if $\Psi[\mu]$ is absolutely continuous with respect to μ, i.e., the support of $\Psi[\mu]$ is a subset of the support of μ. Clearly, every support-preserving Φ is also weakly support-preserving, and so the class of support-preserving endomorphisms of, say, $\mathrm{Prob}(\mathbb{Z}_{\geq 0})$ is contained in the weakly support-preserving ones. We conjecture that the set of all weakly support-preserving endomorphisms is exhausted by Φ_β and the two limiting cases $\Phi_{+\infty} = \lim_{\beta \to +\infty} \Phi_\beta$ and $\Phi_{-\infty} = \lim_{\beta \to -\infty} \Phi_\beta$, which correspond to putting a point mass on the minimal or maximal point of the support, respectively.

Related literature. This paper is related to other work on polynomials with non-negative coefficients. This literature consists of two lines of research.

The line closest to our analysis originated from the classical works of Poincaré [12] and Pólya [13], exploring the relation of non-negativity of a polynomial p and the possibility of finding a factor r such that $r \cdot p$ has non-negative coefficients under various assumptions on r; see a recent contribution by Michelen and Sahasrabudhe [9] for a survey.

A related strain of research explores the connection between the coefficients and the distribution of zeros. Since polynomials with non-negative coefficients are moment-generating functions of finitely-supported distributions, this direction is tightly related to non-classical limit theorems of probability theory; see the series of papers by Michelen and Sahasrabudhe for recent progress [7, 8, 10].

The algebra of the semi-group of probability measures on the reals under convolutions is well studied, including its homomorphisms to $\mathbb{R}$, $\mathbb{Z}$ and $\mathbb{C}$; see "Algebraic Probability Theory," a book by Ruzsa and Székely [15], as well as more recent work [2, 11]. Homomorphisms into general groups were considered by Mattner [5].

2. Preliminaries

Recall that $\mathcal{P}$ is the set of polynomials $p(x) = \sum_{k=0}^{d} p_k x^k$ such that $p_k \geq 0$ and $p(1) = \sum_k p_k = 1$. We denote by $\deg(p)$ the degree of p. The set $\mathcal{P}$ is contained in $\mathcal{M}$, the set of polynomials p such that $p(1) = 1$ and $p(x) > 0$ for all $x > 0$. Note that the latter condition can be equivalently changed to $p(x) \neq 0$ for all $x > 0$, so that $\mathcal{M}$ consists of the polynomials p with no positive roots such that $p(1) = 1$.

For notational convenience, we will sometimes omit normalization constants, often writing these polynomials in monic form. For example, $p(x) = (x+1)/2 \in \mathcal{P}$ will be written as $p(x) = x + 1$. Similarly, an expression of the form $\Phi[(x+1)/2] = (x+2)/3$ will be written more succinctly as $\Phi[x+1] = x+2$. Since every polynomial with non-positive roots can be normalized to a unique $p \in \mathcal{M}$, and since normalization preserves the support and commutes with multiplication, this will introduce no ambiguity.

For $\gamma > 0$, let $\Psi_\gamma \colon \mathcal{M} \to \mathcal{M}$ be given by

$$\Psi_\gamma \colon \mathcal{M} \to \mathcal{M}$$
(2.1)
$$p(x) \mapsto p(x/\gamma).$$

Note that we omit normalization constants, as explained above; the normalized form is $\Psi_\gamma[p] = p(x/\gamma)/p(1/\gamma)$. In terms of probability measures, Ψ_γ corresponds to the map Φ_β from the introduction, for $\beta = \log \gamma$. In particular, it is easy to verify that Ψ_γ is support-preserving and multiplicative, and—importantly—that it maps $\mathcal{P}$ to $\mathcal{P}$.

The following lemma is a strengthening of Lemma 1.2.

Lemma 2.1 (Bálinth). *For every $q \in \mathcal{M}$ it holds for all n large enough that $q(x) \cdot (x+1)^n \in \mathcal{P}$.*

Note that we here again drop the normalization constant and write $(x+1)^n$ rather than $2^{-n}(x+1)^n$. This result is a consequence of Pólya's Positivstellensatz [13], a more general statement about multivariate polynomials; see also Theorem 56 in [3]. In the univariate setting, a version of this result was obtained by Bálinth; see a footnote on the first page of [13].

We will need a slight strengthening of this lemma.

Lemma 2.2. *For every $q \in \mathcal{M}$ and all $\gamma > 0$ it holds for all n large enough that $q(x)(x+\gamma)^n \in \mathcal{P}$.*

Proof. Note that Ψ_γ maps $x+1$ to $x+\gamma$ (omitting normalization). Fix $q \in \mathcal{M}$. By Lemma 2.1, we know that $\Psi_{\gamma^{-1}}[q](x) \cdot (x+1)^n$ is in $\mathcal{P}$ for all n large enough. Since Ψ_γ is multiplicative,

$$\Psi_\gamma\big[\Psi_{\gamma^{-1}}[q](x) \cdot (x+1)^n\big] = q(x) \cdot \Psi_\gamma[(x+1)^n] = q(x)(x+\gamma)^n,$$

and since Ψ_γ maps $\mathcal{P}$ to $\mathcal{P}$, it follows that $q(x)(x+\gamma)^n$ is also in $\mathcal{P}$ for all n large enough. $\qquad\square$

3. Support-preserving multiplicative maps of polynomials with non-negative coefficients

In this section, we prepare the ingredients for proofs of Theorems 1, 2, and 3 and then prove the theorems. The first ingredient is extending a multiplicative support-preserving Φ from the set of polynomials with non-negative coefficients $\mathcal{P}$ to the set $\mathcal{M}$ of polynomials without positive roots.

3.1. Extending the domain of Φ. In this section we prove the following result.

Proposition 3.1. *Every support-preserving multiplicative $\Phi\colon \mathcal{P} \to \mathcal{P}$ can be (uniquely) extended to a degree-preserving multiplicative $\Phi\colon \mathcal{M} \to \mathcal{M}$.*

Let

$$\mathcal{F}(\mathbb{Z}_{\geq 0}) = \left\{ \frac{p'}{p} \ : \ p, p' \in \mathcal{P} \right\}.$$

The first step towards proving Proposition 3.1 is to extend a support-preserving multiplicative $\Phi\colon \mathcal{P} \to \mathcal{P}$ to a multiplicative $\Phi\colon \mathcal{M} \to \mathcal{F}(\mathbb{Z}_{\geq 0})$.

To this end, given $q \in \mathcal{M}$, there is, by Lemma 1.2, $p, r \in \mathcal{P}$ such that $q \cdot p = r$. Define the extension of Φ to $\mathcal{M}$ by

$$(3.1) \qquad\qquad \Phi[q] = \frac{\Phi[r]}{\Phi[p]}.$$

To see that this is well defined, suppose that $q \cdot p' = r'$ for some $p', r' \in \mathcal{P}$, and note that $q \cdot p \cdot p' \in \mathcal{P}$. Thus

$$\Phi[r] \cdot \Phi[p'] = \Phi[q \cdot p] \cdot \Phi[p'] = \Phi[q \cdot p \cdot p'] = \Phi[q \cdot p'] \cdot \Phi[p] = \Phi[r'] \cdot \Phi[p],$$

and so

$$\frac{\Phi[r]}{\Phi[p]} = \frac{\Phi[r']}{\Phi[p']}.$$

To see that Φ is multiplicative, i.e., that $\Phi[q \cdot q'] = \Phi[q] \cdot \Phi[q']$ for all $q, q' \in \mathcal{M}$, suppose that $q \cdot p$ and $q' \cdot p'$ belong to $\mathcal{P}$. Thus $q \cdot q' \cdot p \cdot p' \in \mathcal{P}$. Hence,

$$\Phi[q \cdot q'] = \frac{\Phi[q \cdot q' \cdot p \cdot p']}{\Phi[p \cdot p']} = \frac{\Phi[q \cdot p]}{\Phi[p]} \frac{\Phi[q' \cdot p']}{\Phi[p']} = \Phi[q] \cdot \Phi[q'].$$

We note that the extension defined by (3.1) is unique, since any extension that satisfies $\Phi[q \cdot q'] = \Phi[q] \cdot \Phi[q']$ must satisfy (3.1) whenever $q \cdot p = r$.

To prove Proposition 3.1, we need to show that the image of this extension is, in fact, in the polynomials. To this end, for $0 < a < b$, let[4]

$$q^{a,b}(x) = x^2 - ax + ab.$$

Note that $q^{a,b} \in \mathcal{M}$.

Then

$$q^{a,b}(x) \cdot (x + t) = (x^2 - ax + ab) \cdot (x + t) = x^3 + (t - a)x^2 + a(b - t)x + abt,$$

and in particular

$$q^{a,b}(x) \cdot (x + a) = x^3 + a(b - a)x + a^2 b$$
$$q^{a,b}(x) \cdot (x + b) = x^3 + (b - a)x^2 + ab^2.$$

are both in $\mathcal{P}$. Importantly, they have different supports. By (3.1),

$$\Phi[q^{a,b}] = \frac{\Phi[q^{a,b}(x) \cdot (x + a)]}{\Phi[x + a]} = \frac{\Phi[q^{a,b}(x) \cdot (x + b)]}{\Phi[x + b]}.$$

Now, because $q^{a,b}(x) \cdot (x + a)$ and $q^{a,b}(x) \cdot (x + b)$ have different supports, it follows from the support-preserving property of Φ that

$$\Phi[q^{a,b}(x) \cdot (x + a)] \neq \Phi[q^{a,b}(x) \cdot (x + b)].$$

Hence $\Phi[x + a] \neq \Phi[x + b]$. We have thus proved the following claim:[5]

Claim 3.2. *Suppose that Φ is support-preserving and multiplicative. Then $\Phi[x+a] \neq \Phi[x + b]$ for $a \neq b$.*

With this claim, we are ready to prove our proposition.

Proof of Proposition 3.1. Let $\Phi \colon \mathcal{P} \to \mathcal{P}$ be support-preserving and multiplicative. Extend it to $\Phi \colon \mathcal{P} \to \mathcal{F}(\mathbb{Z}_{\geq 0})$ using (3.1). Choose any $a, b > 0$, $a \neq b$, and fix $q \in \mathcal{M}$. By Lemma 2.2, there is n large enough so that both $q(x)(x + a)^n$ and $q(x)(x + b)^n$ are in $\mathcal{P}$. We thus have that

$$\Phi[q] = \frac{\Phi[q(x) \cdot (x + a)^n]}{\Phi[(x + a)^n]} = \frac{\Phi[q(x) \cdot (x + b)^n]}{\Phi[(x + b)^n]}.$$

By Claim 3.2 and the support-preserving property, we know that there are some $c \neq d$ such that $\Phi[x + a] = x + c$ and $\Phi[x + b] = x + d$. Hence,

$$\frac{\Phi[q(x) \cdot (x + a)^n]}{(x + c)^n} = \frac{\Phi[q(x) \cdot (x + b)^n]}{(x + d)^n},$$

---

[4]As discussed in §2, we omit a normalizing constant and write $q^{a,b}(x)$ as above, rather than $(x^2 - ax + ab)/(1 - a + ab)$.

[5]Again, we omit normalization constants as discussed in §2. With these constants the claim would be that $a \neq b$ implies $\Phi[(x + a)/(1 + a)] \neq \Phi[(x + b)/(1 + b)]$.

and rearranging we get

$$\Phi[q(x) \cdot (x + a)^n](x + d)^n = \Phi[q(x) \cdot (x + b)^n] \cdot (x + c)^n.$$

Both sides are polynomials and have the same roots. Of these roots, at least n are equal to $-c$, since the right-hand side includes the term $(x + c)^n$. The left-hand side thus also has at least n roots which are equal to $-c$. Since $c \neq d$, $\Phi[q(x) \cdot (x + a)^n]$ has at least n roots equal to $-c$. It follows that

$$\Phi[q] = \frac{\Phi[q(x) \cdot (x + a)^n]}{(x + c)^n}$$

is a polynomial. Furthermore, it is in $\mathcal{M}$, since it does not have positive roots. Finally, by the support-preserving property of Φ,

$$\deg(\Phi[q(x) \cdot (x + a)^n]) = \deg(q(x) \cdot (x + a)^n) = \deg(q) + n.$$

On the other hand, since Φ is a multiplicative,

$$\deg(\Phi[q(x) \cdot (x + a)^n]) = \deg(\Phi[q] \cdot \Phi[(x + a)^n]) = \deg(\Phi[q]) + n,$$

and so $\deg(\Phi[q]) = \deg(q)$. $\square$

3.2. **Linear polynomials and some quadratic polynomials.** In this section, we prove the following proposition.

Proposition 3.3. *Let $\Phi \colon \mathcal{P} \to \mathcal{P}$ be support-preserving and multiplicative. Then there exists a constant $\gamma > 0$ such that $\Phi[x + a] = x + \gamma a$ for all $a > 0$.*

Let $\Phi \colon \mathcal{P} \to \mathcal{P}$ be support-preserving and multiplicative. Consider $\varphi \colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ given by $\Phi[x + t] = x + \varphi(t)$. We will show that $\varphi(a) = \gamma a$, thus proving Proposition 3.3. As a byproduct, we also show that $\Phi[x^2 - ax + ab] = x^2 - \gamma ax + \gamma^2 ab$ for all $0 < a < b$ (Corollary 3.6).

As above, let $q^{a,b}(x) = x^2 - ax + ab$, for $0 < a < b$. Then

$$q^{a,b}(x) \cdot (x + t) = (x^2 - ax + ab) \cdot (x + t) = x^3 + (t - a)x^2 + a(b - t)x + abt$$

is in $\mathcal{P}$ for any $t \in [a, b]$. By Proposition 3.1,

(3.2) $\qquad \Phi[q^{a,b}] = \dfrac{\Phi[q^{a,b}(x) \cdot (x + t)]}{\Phi[x + t]} = \dfrac{\Phi[x^3 + (t - a)x^2 + a(b - t)x + abt]}{x + \varphi(t)}$

is a polynomial for all $0 < a < b$ and $t \in [a, b]$. In particular, for $t = a$ we get that

$$\Phi[q^{a,b}] = \frac{\Phi[x^3 + a(b - a)x + a^2 b]}{x + \varphi(a)}$$

is a polynomial. Using the support-preserving property of Φ, we can write the numerator as $\Phi(x^3 + a(b-a)x + a^2b) = x^3 + cx + d$, which must have $x + \varphi(a)$ as a factor. Factoring $x + \varphi(a)$ from this polynomial yields that

$$(3.3) \qquad \Phi[q^{a,b}] = x^2 - \varphi(a)x + \varphi(a)^2 + c.$$

Similarly, substituting $t = b$ into (3.2) we get

$$\Phi[q^{a,b}] = \frac{\Phi(x^3 + (b-a)x^2 + ab^2)}{x + \varphi(b)}.$$

Writing the numerator as $\Phi[x^3 + (b-a)x + ab^2] = x^3 + ex^2 + f$, and since $x + \varphi(b)$ is a factor of this polynomial, we get that

$$(3.4) \qquad \Phi[q^{a,b}] = x^2 - (\varphi(b) - e)x + \varphi(b)^2 - e\varphi(b).$$

Equating (3.3) and (3.4), we get that $\varphi(a) = \varphi(b) - e$. This then yields that

$$(3.5) \qquad \Phi[q^{a,b}] = x^2 - \varphi(a)x + \varphi(a)\varphi(b).$$

Now, choose $t \in (a, b)$. Then $q^{a,b}(x) \cdot (x + t)$ is a cubic polynomial with positive coefficients and, by the above,

$$\Phi[q^{a,b}(x) \cdot (x + t)] = (x^2 - \varphi(a)x + \varphi(a)\varphi(b))(x + \varphi(t))$$
$$= x^3 + (\varphi(t) - \varphi(a))x^2 + \cdots.$$

By the support-preserving property of Φ, the coefficient of x^2 must be positive, and so we have shown that φ is strictly monotone increasing:

Claim 3.4. *If $0 < a < b$, then $\varphi(a) < \varphi(b)$.*

We are now ready to prove the main result of this section.

Proof of Proposition 3.3. Note that

$$q^{a,b}(x) \cdot (x + 2b)^2 = (x^2 - ax + ab) \cdot (x + 2b)^2$$
$$= x^4 + (4b - a)x^3 + b(4b - 3a)x^2 + 4ab^3.$$

is in $\mathcal{P}$. Since

$$\Phi[q^{a,b}(x)] \cdot \Phi[(x + 2b)^2] = (x^2 - \varphi(a)x + \varphi(a)\varphi(b)) \cdot (x + \varphi(2b))^2$$
$$= \cdots + (2\varphi(a)\varphi(b)\varphi(2b) - \varphi(a)\varphi(2b)^2)x + \cdots,$$

it follows from the support-preserving property of Φ that

$$2\varphi(a)\varphi(b)\varphi(2b) - \varphi(a)\varphi(2b)^2 = 0$$

or

$$\varphi(2b) = 2\varphi(b).$$

Likewise,

$$q^{a,b}(x) \cdot (x+3b)^3 = (x^2 - ax + ab) \cdot (x+3b)^3$$
$$= x^5 + (9b-a)x^4 + b(27b-8a)x^3 + b^2(27b-18a)x^2 + 27ab^4.$$

is in $\mathcal{P}$ for $b > a$. Since

$$\Phi[q^{a,b}(x)] \cdot \Phi[(x+3b)^3] = (x^2 - \varphi(a)x + \varphi(a)\varphi(b)) \cdot (x + \varphi(3b))^3$$
$$= \cdots + (3\varphi(a)\varphi(b)\varphi(3b)^2 - \varphi(a)\varphi(3b)^3)x + \cdots ,$$

again applying the support-preserving property of Φ yields that

$$3\varphi(a)\varphi(b)\varphi(3b)^2 - \varphi(a)\varphi(3b)^3 = 0,$$

or

$$\varphi(3b) = 3\varphi(b).$$

It thus follows from Lemma 3.5 below that there exists a constant $\gamma > 0$ such that $\varphi(b) = \gamma b$. $\qquad\square$

Lemma 3.5. *Suppose that $f \colon \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is strictly monotone increasing, and satisfies $f(2x) = 2f(x)$ and $f(3x) = 3f(x)$. Then there exists a constant $c > 0$ such that $f(x) = cx$.*

Proof. Since 2 and 3 are coprime, the set $X = \{2^m 3^n : m, n \in \mathbb{Z}\}$ is dense in $\mathbb{R}_{>0}$. Since $f(2x) = 2f(x)$ and $f(3x) = 3f(x)$, we obtain that $f(x) = xf(1)$ for all $x \in X$. Given any $y \in \mathbb{R}_{>0}$, choose a sequence $(x_n^+)_n$ in X that converges to y from above, and likewise $(x_n^-)_n$ that converges to y from below. Then, by the monotonicity of f,

$$yf(1) = \lim_n x_n^+ f(1) = \lim_n f(x_n^+) \geq f(y) \geq \lim_n f(x_n^-) = \lim_n x_n^- f(1) = yf(1).$$

In particular, $f(y) = f(1)y$. $\qquad\square$

We end this section with the following result which is a corollary of Proposition 3.3 and identity (3.5):

Corollary 3.6. *Consider an extension of a support-preserving and multiplicative $\Phi \colon \mathcal{P} \to \mathcal{P}$ to $\mathcal{M}$ and define γ by $\Phi[x+1] = x + \gamma$. Then $\Phi[x^2 - ax + ba] = x^2 - \gamma ax + \gamma^2 ab$ for all $0 < a < b$.*

3.3. **Quadratic polynomials.** Consider a polynomial of the form $q^a(x) = x^2 - ax + 1$. For q^a to be in $\mathcal{M}$, the discriminant must be negative, i.e., $a < 2$.

Claim 3.7. *Suppose that Φ is support-preserving and multiplicative, and $\Phi[x+1] = x + 1$. Then $\Phi[q^a] = q^a$ for all $a \in [-1, 1] \setminus \{0\}$.*

Proof. For $a \in (0, 1)$, we know from Corollary 3.6 that $\Phi[q^a] = q^a$, by choosing $b = 1/a$. We next demonstrate that $\Phi[q^a] = q^a$ for $a = 1$. Let $\Phi[x^2 - x + 1] = x^2 - a'x + b'$. Note that

$$(x^2 - x + 1)(x + 1) = x^3 + 1.$$

Hence, by the support-preserving property of Φ, in the expression

$$\Phi[(x^2 - x + 1)(x + 1)] = (x^2 - a'x + b')(x + 1) = x^3 + (1 - a')x^2 + (b' - a')x + b'$$

the coefficients of x and x^2 must vanish. We obtain $1 - a' = 0$ and $b' - a' = 0$. Thus $a' = b' = 1$ and so $\Phi[q^a] = q^a$ for $a = 1$.

Now suppose $a \in [-1, 0)$. Then $q^a \in \mathcal{P}$ so $\Phi(q^a) = x^2 + a'x + b'$ for some $a', b' > 0$. Then

$$\begin{aligned}
\Phi[q^{-a} \cdot q^a] &= \Phi[q^{-a}] \cdot \Phi[q^a] \\
&= (x^2 - ax + 1) \cdot (x^2 + a'x + b') \\
&= x^4 + (a' - a)x^3 + (1 + b' - aa')x^2 + (a' - ab')x + b'.
\end{aligned}$$

Now,

$$q^a(x) \cdot q^{-a}(x) = (x^2 - ax + 1) \cdot (x^2 + ax + 1) = x^4 + (2 - a^2)x^2 + 1,$$

and so, by the support-preserving property of Φ, we have that $a' - a = 0$ and $a' - ab' = 0$. Hence, $a' = a$ and $b' = 1$. We conclude that $\Phi[q^a] = q^a$ for $a \in [-1, 1] \setminus \{0\}$. $\square$

Define $\pi \colon \mathcal{M} \to \mathcal{M}$ to be the map $q(x) \mapsto q(x^2)$. Let $\Phi^\pi = \pi^{-1} \circ \Phi \circ \pi$, so that

$$\Phi^\pi[q_0 + q_1 x + q_2 x^2 + \cdots + q_d x^d] = r_0 + r_1 x + r_2 x^2 + \cdots + r_d x^d$$

whenever

$$\Phi[q_0 + q_1 x^2 + q_2 x^4 + \cdots + q_d x^{2d}] = r_0 + r_1 x^2 + r_2 x^4 + \cdots + r_d x^{2d}.$$

It is easy to verify that $\Phi^\pi \colon \mathcal{P} \to \mathcal{P}$ is support-preserving and multiplicative if Φ is. By Proposition 3.1, Φ^π admits a unique extension to a degree-preserving multiplicative map $\mathcal{M} \to \mathcal{M}$.

Claim 3.8. *Suppose that Φ is support-preserving and multiplicative, and $\Phi[x + 1] = x + 1$. Then for all $a \in [-1, 1]$ it holds that $\Phi[q^a] = q^a$.*

Proof. The case of $a \neq 0$ was shown in Claim 3.7. It remains to be shown that $\Phi[x^2 + 1] = x^2 + 1$, or equivalently that $\Phi^\pi[x + 1] = x + 1$. Since Φ^π is support-preserving and multiplicative, by Proposition 3.3 there is a constant $\gamma > 0$ such that $\Phi^\pi[x + a] = x + \gamma a$.

Define $\Phi' = \Psi_{1/\gamma} \circ \Phi^\pi$, where we recall that $\Psi_{1/\gamma} \colon p(x) \to p(\gamma x)$. Hence, Φ' is support-preserving and multiplicative and satisfies $\Phi'[x + 1] = x + 1$. Therefore, by Claim 3.7, $\Phi'[x^2 - a + 1] = x^2 - ax + 1$ for all $a \in [-1, 1] \setminus \{0\}$. Since $\Phi^\pi = \Psi_\gamma \circ \Phi'$, we get $\Phi^\pi[q^a(x)] = x^2 - \gamma ax + \gamma^2$ for all $a \in [-1, 1] \setminus \{0\}$.

Let us show that $\gamma = 1$. Observe that for $a = -1$

$$q^a(x^2) = x^4 + x^2 + 1 = (x^2 + x + 1) \cdot (x^2 - x + 1) = q^a(x) \cdot q^{-a}(x).$$

Hence,

$$\Phi[q^a(x^2)] = \Phi[q^a(x)] \cdot \Phi[q^{-a}(x)] = (x^2 + x + 1)(x^2 - x + 1) = x^4 + x^2 + 1.$$

On the other hand,

$$\Phi[q^a(x^2)] = \Phi^\pi[q^a](x^2) = x^4 - \gamma a x^2 + \gamma^2.$$

Thus $\gamma = 1$, which completes the proof. $\qquad\square$

Claim 3.9. *Let A be a subset of $(-2, 2)$. Suppose that $\Phi^\pi[q^a] = q^a$ for all $a \in A$. Then $\Phi[q^a] = q^a$ for all a such that $a^2 - 2 \in A$.*

Proof. Note that

$$q^a(x) \cdot q^{-a}(x) = (x^2 - ax + 1) \cdot (x^2 + ax + 1) = x^4 + (2 - a^2)x^2 + 1.$$

By the claim hypothesis $\Phi^\pi[x^2 + (2 - a^2)x + 1] = x^2 + (2 - a^2)x + 1$. It follows that

$$\Phi[q^a] \cdot \Phi[q^{-a}] = x^4 + (2 - a^2)x^2 + 1.$$

Without loss of generality, we can assume that $a \geq 0$. By Proposition 3.1, the left-hand side is the product of two quadratic polynomials; moreover, $\Phi[q^{-a}]$ has non-negative coefficients. The polynomial $x^4 + (2 - a^2)x^2 + 1$ on the right-hand side has two pairs of complex-conjugate roots. Hence, there is a unique way to represent it as a product of two quadratic monic polynomials with real coefficients:

$$x^4 + (2 - a^2)x^2 + 1 = (x^2 - ax + 1) \cdot (x^2 + ax + 1).$$

Only one of these quadratic factors has non-negative coefficients and thus

$$\Phi[q^a] = x^2 - ax + 1 \qquad \text{and} \qquad \Phi[q^{-a}] = x^2 + ax + 1$$

completing the proof. $\qquad\square$

Claim 3.10. *If a support-preserving multiplicative Φ satisfies $\Phi[x + 1] = x + 1$, then $\Phi[q^a] = q^a$ for all a in $(-2, 2)$.*

Proof. Let A^* be the set of all $a \in (-2, 2)$ such that $\Phi'[q^a] = q^a$ for all support-preserving multiplicative maps Φ' such that $\Phi'[x + 1] = x + 1$. By Claim 3.8, $[-1, 1] \subseteq A^*$.

Let $f(x) = x^2 - 2$, and denote by $f^{(n)}$ the n-fold composition of f with itself. We claim that for any $x \in (1, 2)$ there is a number n such that $f^{(n)}(x) \in [-1, 1]$. Since the image of $(1, 2)$ under f is $(-1, 2)$, it is enough to show that there is no $x_0 \in (1, 2)$ such that $x_n = f^{(n)}(x_0)$ stays in $(1, 2)$ for all n. Towards a contradiction, suppose that such x_0 exists. For $x \in (1, 2)$, we have that $f(x) < 3x - 4$, since $f(1) = -1$, $f(2) = 2$ and f is strictly convex. In particular, $f(x) - x < 2x - 4 < 0$ for all $x \in [1, 2)$, so

that $f(x) < x$. Thus the sequence x_n is decreasing. Denote $x_\infty = \lim_n x_n \in [1, 2)$. By continuity of f, we get $f(x_\infty) = x_\infty$. But $f(x) < x$ for all $x \in [1, 2)$. This contradiction implies that for any $x \in (1, 2)$, there is n such that $f^{(n)}(x) \in (-1, 1)$. The same argument applies to $x \in (-2, -1)$, since $f(-x) = f(x)$.

By Claim 3.9, if $f(a) \in A^*$ then $a \in A^*$. It follows that if $f^{(n)}(a) \in A^*$, then $a \in A^*$. Since $[-1, 1] \subseteq A^*$, we conclude that $(-2, 2) \subseteq A^*$. Thus $A^* = (-2, 2)$.
□

We are now ready to show that if $\Phi[x + 1] = x + 1$, then $\Phi[q] = q$ for all quadratic $q \in \mathcal{M}$ that have no real roots. Note that any such q is (up to normalization) of the form $q(x) = x^2 - a\gamma x + \gamma^2$ for some $a \in (-2, 2)$ and $\gamma > 0$.

Proposition 3.11. *If a support-preserving multiplicative Φ satisfies $\Phi[x+1] = x+1$, then $\Phi[x^2 - a\gamma x + \gamma^2] = x^2 - a\gamma x + \gamma^2$ for all $a \in (-2, 2)$ and all $\gamma > 0$.*

Proof. Recall that Ψ_γ maps $p(x)$ to $p(x/\gamma)$. Consider $\Phi' = \Psi_{1/\gamma} \circ \Phi \circ \Psi_\gamma$. Then Φ' is support-preserving and multiplicative, and $\Phi'[x + 1] = x + 1$. By Claim 3.9, $\Phi'[q^a] = q^a$ for all $a \in (-2, 2)$. Equivalently, $\Psi_{1/\gamma} \circ \Phi \circ \Psi_\gamma[q_a] = q_a$. Applying Ψ_γ on both sides of this identity, we get $\Phi[\Psi_\gamma[q_a]] = \Psi_\gamma[q_a]$. Since $\Psi_\gamma[q_a](x) = x^2 - a\gamma x + \gamma^2$, the proof is complete.
□

3.4. **Proofs of Theorems 1 and 2.**

Proof of Theorem 2. We first claim that to prove the theorem, it suffices to show that a support-preserving and multiplicative Φ such $\Phi[x + 1] = x + 1$ is the identity map. To see that this statement implies the theorem, let Φ be support-preserving and multiplicative. Define $\gamma > 0$ by $\Phi[x+1] = x+\gamma$. Recall from (2.1) that $\Psi_\gamma \colon \mathcal{P} \to \mathcal{P}$ is the map that takes $p(x)$ to $p(x/\gamma)/p(1/\gamma)$. Hence $\Phi' = \Psi_\gamma^{-1} \circ \Phi$ is support-preserving and multiplicative, and furthermore satisfies $\Phi'[x + 1] = x + 1$. Hence, if we show that Φ' is the identity map, then we have shown that $\Phi = \Psi_\gamma$.

We now show that a support-preserving and multiplicative $\Phi \colon \mathcal{P} \to \mathcal{P}$ such that $\Phi[x + 1] = x + 1$ is the identity map.

Fix $p \in \mathcal{P}$. By the fundamental theorem of algebra, we can write it as a product of polynomials

$$p(x) = \prod_i r^i(x) \prod_j q^j(x),$$

where each r^i is linear and each q^j is quadratic with no real roots.

Since $p \in \mathcal{P}$ has no positive roots, each linear term r^i is of the form $r^i(x) = x + b_i$ for some $b_i \geq 0$. Since each quadratic term has no real roots, it is of the form $q^j(x) = x^2 - a_j\gamma_j x + \gamma_j^2$ for some $\gamma_j > 0$ and $a_j \in (-2, -2)$.

By Proposition 3.1, we can extend Φ to a multiplicative map $\Phi\colon \mathcal{M} \to \mathcal{M}$. Hence,

$$\Phi[p] = \prod_i \Phi[r^i] \prod_j \Phi[q^j].$$

By Proposition 3.3, $\Phi[r^i] = r^i$. And by Proposition 3.11, $\Phi[q^j] = q^j$. We conclude that $\Phi[p] = p$, and so Φ is the identity map. By the remark at the beginning of the proof, this implies the theorem statement. $\square$

Proof of Theorem 1. The case $S = \mathbb{Z}_{\geq 0}$ follows immediately from Theorem 2 by translating from probability-generating functions back to probability measures.

Consider now $S = \mathbb{Z}$, and let $\Phi\colon \mathrm{Prob}(\mathbb{Z}) \to \mathrm{Prob}(\mathbb{Z})$ be a support-preserving endomorphism. Then its restriction to $\mathrm{Prob}(\mathbb{Z}_{\geq 0})$ is equal to some Φ_β. Given $\mu \in \mathrm{Prob}(\mathbb{Z})$, there is some $z \in \mathbb{Z}$ such that $\mu * \delta_z \in \mathrm{Prob}(\mathbb{Z}_{\geq 0})$. Hence

$$\Phi[\mu * \delta_z] = \Phi_\beta[\mu * \delta_z] = \Phi_\beta[\mu] * \Phi_\beta[\delta_z] = \Phi_\beta[\mu] * \delta_z,$$

since Φ_β is a support-preserving endomorphism. On the other hand,

$$\Phi[\mu * \delta_z] = \Phi[\mu] * \Phi[\delta_z] = \Phi[\mu] * \delta_z,$$

since Φ is a support-preserving endomorphism. Hence

$$\Phi[\mu] * \delta_z = \Phi_\beta[\mu] * \delta_z$$

and so $\Phi[\mu] = \Phi_\beta[\mu]$.

Finally, consider the case $S = \mathbb{Q}$, and let $\Phi\colon \mathrm{Prob}(\mathbb{Q}) \to \mathrm{Prob}(\mathbb{Q})$ be a support-preserving endomorphism. For each $n \in \mathbb{Z}_{>0}$, the semi-group $\mathrm{Prob}(\mathbb{Z}/n)$ is isomorphic to $\mathrm{Prob}(\mathbb{Z})$, and thus there is some β_n such that the restriction of Φ to $\mathrm{Prob}(\mathbb{Z}/n)$ is equal to Φ_{β_n}. But since $\mathbb{Z}/n$ and $\mathbb{Z}/m$ are both contained in $\mathbb{Z}/(nm)$, $\beta_n = \beta_m = \beta$. Finally, $\mathrm{Prob}(\mathbb{Q}) = \cup_n \mathrm{Prob}(\mathbb{Z}/n)$, and so $\Phi = \Phi_\beta$. $\square$

3.5. **Proof of Theorem 3.** The proof of Theorem 3 initially follows the argument of the proof of Theorem 2. We first analogously extend Φ to a map from $\mathcal{M}_\mathbb{Q}$ to $\mathcal{M}$ where

$$\mathcal{M}_\mathbb{Q} = \left\{ p(x) = \sum_{k=1}^d p_k x^k \,\middle|\, p_k \in \mathbb{Q}, \ \ p(x) > 0 \text{ for all } x > 0, \ \ p(1) = 1 \right\}.$$

The same argument as in the proof of Proposition 3.1 shows that there exists a multiplicative extension that preserves the degree. Note that instead of Poincaré's Lemma (Lemma 1.2), one can use Pólya's Lemma (Lemma 2.1) to ensure that for every $p \in \mathcal{M}_\mathbb{Q}$ there exists an $r \in \mathcal{P}_\mathbb{Q}$ such that $p \cdot r \in \mathcal{P}_\mathbb{Q}$.

As in the proof of Theorem 2, we first consider linear polynomials with rational coefficients and note that the same argument of Proposition 3.3 shows that the analogous statement holds in the rational setting.

Proposition 3.12. *For any support-preserving multiplicative $\Phi: \mathcal{P}_\mathbb{Q} \to \mathcal{P}$, there exists a constant $\gamma > 0$ such that $\Phi[x + a] = x + \gamma a$ for all $a \in \mathbb{Q}_{>0}$.*

We next study quadratic polynomials with rational coefficients. The argument of Proposition 3.11 still applies.

Proposition 3.13. *Let $\Phi: \mathcal{P}_\mathbb{Q} \to \mathcal{P}$ be support-preserving and multiplicative, and $\Phi[x + 1] = x + 1$. Then its extension to $\mathcal{M}_\mathbb{Q}$ satisfies $\Phi[p] = p$ for any polynomial p of the form $p(x) = x^2 - a\gamma x + \gamma^2$ with $a \in (-2, 2) \cap \mathbb{Q}$ and $\gamma \in \mathbb{Q}_{>0}$.*

Note that this does not apply to all rational quadratic polynomials, since the free coefficient is a square of a rational.

Accordingly, let $\mathcal{M}'_\mathbb{Q} \subset \mathcal{M}_\mathbb{Q}$ be the set of polynomials with rational coefficients which are products of linear rational polynomials ($x + a$ for $a \in \mathbb{Q}_{\geq 0}$) and quadratic polynomials of the form considered in Proposition 3.12 ($x^2 - a\gamma x + \gamma^2$ for $a \in (-2, 2) \cap \mathbb{Q}$ and $\gamma \in \mathbb{Q}_{>0}$). Then the same proof of Theorem 2 yields the following:

Proposition 3.14. *Let Φ be an extension of a support-preserving multiplicative map from $\mathcal{P}_\mathbb{Q}$ to $\mathcal{M}_\mathbb{Q}$. Then there exists a constant $\gamma > 0$ such that $\Phi[p](x) = p(\gamma x)/p(\gamma)$ for any $p \in \mathcal{M}'_\mathbb{Q}$.*

Consider the topology on $\mathcal{M}$ given by $\lim_t p^{(t)} = p$ if $\lim_t \deg(p^{(t)}) = \deg(p)$ and $\lim_t p_k^{(t)} = p_k$ for all k. Then $\mathcal{M}'_\mathbb{Q}$ is a rich dense sub-semi-group of $\mathcal{M}_\mathbb{Q}$, which is dense in $\mathcal{M}$. Thus, automatic continuity (Proposition 1.3) together with Proposition 3.14 yield Theorem 3.

Proof of Theorem 3. Let $\Phi: \mathcal{P}_\mathbb{Q} \to \mathcal{P}$ be support-preserving and multiplicative. Define γ by $\Phi[x + 1] = x + \gamma$, and let $\Phi' = \Psi_\gamma^{-1} \circ \Phi$. Then Φ' is support-preserving, multiplicative, and satisfies $\Phi'[x + 1] = x + 1$. Extend it to a multiplicative, degree-preserving $\Phi': \mathcal{M}_\mathbb{Q} \to \mathcal{M}$. By Proposition 3.14, the restriction of Φ' to $\mathcal{M}'_\mathbb{Q}$ is of the form $\Psi_{\gamma'}$, and since $\Phi'[x + 1] = x + 1$, we get $\gamma' = 1$. Therefore, Φ' restricted to $\mathcal{M}'_\mathbb{Q}$ is the identity map. Hence, by Proposition 1.3, Φ' is the identity map on the whole domain $\mathcal{M}_\mathbb{Q}$. Thus $\Phi = \Psi_\gamma$. $\qquad\square$

3.6. **Proof of Proposition 1.3.** Recall that Poincaré's Lemma (Lemma 1.2) shows that for every $q \in \mathcal{M}$ there is a polynomial $p \in \mathcal{P}$ such that $q \cdot p \in \mathcal{P}$. Towards proving Proposition 1.3, we investigate a related question: Given $p \in \mathcal{P}$, for which $q \in \mathcal{M}$ does it holds that $q \cdot p \in \mathcal{P}$?

Given $p \in \mathcal{P}$, denote by $S_p \subseteq \mathcal{M}$ the set of polynomials q such that $q \cdot p \in \mathcal{P}$:

$$S_p = \{q \in \mathcal{M} : q \cdot p \in \mathcal{P}\}.$$

A natural question is to understand when $S_p \subseteq S_{p'}$. For example, if $p'(x) = p^2(x)$ then clearly $S_p \subseteq S_{p'}$. The next lemma shows that if we further require that $\deg(p') \leq \deg(p)$ (and $p_0 \neq 0$), then the containment $S_p \subseteq S_{p'}$ is only possible when $p = p'$.

Lemma 3.15. *Consider $p, p' \in \mathcal{P}$ such that $\deg(p') \leq \deg(p)$ and $p_0 \neq 0$. Then $p = p'$ if and only if $S_p \subseteq S_{p'}$.*

Proof. Only one direction is non-trivial: proving the existence of $q \in S_p \setminus S_{p'}$ if $p \neq p'$.

Denote $n = \deg(p)$. We claim that we can assume without loss of generality that $p_k > 0$ for $k = 0, \ldots, n$. Otherwise, replace p and p' by $p \cdot r$ and $p' \cdot r$ with $r(x) = (x+1)^n$. If we can find q such that $q \cdot p \cdot r \in \mathcal{P}$ but $q \cdot p' \cdot r \notin \mathcal{P}$ then $q \cdot r \in S_p \setminus S_{p'}$.

The first step is to show the existence of a polynomial $s(x) = \sum_{k=0}^{n+1} s_k x^k$ with $\deg(s) = n+1$ such that all the coefficients $(p \cdot s)_k$ are non-negative for $k = 0, \ldots, n+1$ but $(p' \cdot s)_{n+1} \leq -1$. These requirements are equivalent to a system of linear inequalities on coefficients of s:

$$(3.6) \qquad A\vec{s} \geq \vec{b}, \qquad \text{where}$$

$$A = \begin{pmatrix} p_0 & 0 & \cdots & \cdots & 0 \\ p_1 & p_0 & 0 & \ddots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 \\ p_n & p_{n-1} & \cdots & p_0 & 0 \\ 0 & p_n & p_{n-1} & \cdots & p_0 \\ 0 & -p'_n & -p'_{n-1} & \cdots & -p'_0 \end{pmatrix}, \qquad \vec{s} = \begin{pmatrix} s_0 \\ s_1 \\ \vdots \\ s_{n+1} \end{pmatrix}, \qquad \vec{b} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

By the Farkas Lemma, (3.6) has a solution if and only if there is no way to combine the inequalities with non-negative coefficients to get the contradictory inequality $0 \geq 1$. Formally, there must be no $(\lambda_0, \ldots, \lambda_{n+2}) \in \mathbb{R}_{\geq 0}^{n+2}$ such that

$$(3.7) \qquad \begin{cases} A^T \vec{\lambda} &= \vec{0} \\ \langle \vec{b}, \vec{\lambda} \rangle &= 1. \end{cases}$$

Here $\lambda_l \geq 0$ is interpreted as the weight of the inequality l in the original system, and A^T denotes the transposed matrix A. Let us write down the equations (3.7) explicitly:

$$\begin{cases} p_0 \lambda_0 + \ldots + p_n \lambda_n &= 0 \\ (p_0 \lambda_k + \ldots + p_{n-k} \lambda_n) + p_{n-k+1} \lambda_{n+1} - p'_{n-k+1} \lambda_{n+2} &= 0, \quad k = 1, \ldots, n+1 \\ \lambda_{n+2} &= 1 \end{cases}$$

Since all coefficients of p are assumed to be positive and $\lambda_k \geq 0$ for all k, the first equation implies $\lambda_0 = \lambda_1 = \ldots = \lambda_n = 0$. Hence, the second family of equations gives $p_{n-k+1} \lambda_{n+1} - p'_{n-k+1} \lambda_{n+2} = 0$ for $k = 1, \ldots, n+1$. Since p and p' are non-zero and not equal, these identities can only hold if $\lambda_{n+1} = \lambda_{n+2} = 0$. Since $\lambda_{n+2} = 1$ by the last equation, we conclude that the system (3.7) does not have a solution. Thus the system (3.6) has a solution and the polynomial $s(x)$ exists.

We now argue that the polynomial $q \in \mathcal{M}$ defined (up to normalization) by

$$q(x) = s(x) + C \cdot x^{n+2}$$

has the desired properties for a large enough constant $C > 0$. Indeed, the coefficients of x^k with $k = 0, \ldots, n+1$ in the products $p \cdot q$ and $p' \cdot q$ are the same as in $p \cdot s$ and $p' \cdot s$. Hence, $(p' \cdot q)_{n+1} \leq -1$ and so $p' \cdot q \notin \mathcal{P}$. It remains to be shown that we can always choose C so that $(p \cdot q)_k \geq 0$ for $k = n+2, \ldots 2n+2$. For such k, we get

$$(p \cdot q)_k = (p \cdot s)_k + C \cdot p_{k-(n+2)}$$

Since all the coefficients of p are strictly positive, choosing

$$C = \max_{k=n+2,\ldots 2n+2} \frac{(p \cdot s)_k}{p_{k-(n+2)}}$$

ensures that $p \cdot q \in \mathcal{P}$. As $p \cdot q \in \mathcal{P}$ and $p \in \mathcal{P}$, we conclude that the constructed polynomial q belongs to $\mathcal{M}$ and complete the proof. $\qquad\square$

The next lemma strengthens the previous, again considering p, p' such that $\deg(p') \leq \deg(p)$ and $p_0 \neq 0$. It shows that when $p \neq p'$, then not only is S_p not contained in $S_{p'}$, but moreover, the interior of S_p is not contained in $S_{p'}$. Recall that our topology is the one under which $\lim_t p^{(t)} = p$ if $\lim_t \deg(p^{(t)}) = \deg(p)$ and $\lim_t p_k^{(t)} = p_k$ for all k. Note that S_p trivially has a non-empty interior because, for any p, it contains $\mathcal{P}$, which has a non-empty interior. The lemma implies that the interior of S_p extends non-trivially beyond that.

Lemma 3.16. *Consider $p, p' \in \mathcal{P}$ such that $\deg(p') \leq \deg(p)$ and $p_0 \neq 0$. Then $p = p'$ if and only if the interior of S_p is contained in $S_{p'}$.*

Proof. One direction is again immediate. For the other direction, we need to show that if M is a dense subset of $\mathcal{M}$, then $p \neq p'$ implies that there is an element of M in $S_p \setminus S_{p'}$.

Fix $p \neq p'$ with $p_0 \neq 0$ and $\deg(p') \leq \deg(p)$. By Lemma 3.15, there is $q \in \mathcal{M}$ such that $q \in S_p \setminus S_{p'}$, i.e., $p \cdot q$ has non-negative coefficients, but $p' \cdot q$ has a negative coefficient.

Denote by m the degree of q and consider $r(x) = (x+1)^m$. For $\varepsilon > 0$, define $q^\varepsilon = q + \varepsilon \cdot r$. Note that $p \cdot q^\varepsilon$ has strictly positive coefficients. Since the coefficients of a product depend continuously on the multiplicands, we can choose small $\varepsilon > 0$ such that $p' \cdot q^\varepsilon$ has a negative coefficient.

Let $q^{(t)} \in M$, $t = 1, 2, \ldots$, be a sequence of polynomials of degree m such that $q_k^{(t)} \to q_k^\varepsilon$ as $t \to \infty$ for all $k = 0, 1, \ldots, m$. Using the continuity of the product again, we conclude that, for large enough t, all the coefficients of $p \cdot q^{(t)}$ are strictly positive, but $p' \cdot q^{(t)}$ has a negative coefficient. $\qquad\square$

Proof of Proposition 1.3. We first consider a polynomial $p \in M' \cap \mathcal{P}$, prove that $\Phi[p] = p$, and then extend the conclusion to all $p \in M'$.

We assume without loss of generality that $p_0 \neq 0$. Indeed, if $p(x) = x^m \cdot r(x)$ for some r with $r_0 \neq 0$, then, by the richness hypothesis, x is contained in M and r is contained in M'. Hence, $\Phi[p] = \Phi[x]^m \cdot \Phi[r] = x^m \cdot \Phi[r]$ and proving $\Phi[r] = r$ would imply $\Phi[p] = p$.

Towards a contradiction, assume that $p \neq \Phi[p]$ and denote $p' = \Phi[p]$. As Φ is degree-preserving, $\deg(p') = \deg(p)$. By Lemma 3.16, there is a polynomial $q \in M$ such that $q \in S_p$ and $q \notin S_{p'}$. In other words, $p \cdot q$ has non-negative coefficients, and $p' \cdot q$ has a negative coefficient.

Since $q \in M$, by the proposition hypothesis, $\Phi[q] = q$ and thus

$$p' \cdot q = \Phi[p] \cdot \Phi[q] = \Phi[p \cdot q].$$

Since $p \cdot q$ has non-negative coefficients, so does $\Phi[p \cdot q]$ because Φ maps $M' \cap \mathcal{P}$ to $\mathcal{P}$. We get that $p' \cdot q$ has no negative coefficients and reach a contradiction. Thus $p' = p$ or, equivalently, $\Phi[p] = p$ for $p \in M' \cap \mathcal{P}$.

It remains to show that $\Phi[p] = p$ for $p \in M' \setminus \mathcal{P}$. By the density of M, there is a constant $a > 0$ such that $q(x) = x + a$ belongs to M. By Pólya's Lemma (Lemma 2.2), $p(x) \cdot (x + a)^n$ has non-negative coefficients for some n large enough. Denote $q(x) = (x + a)^n$. Both multiplicands in $p \cdot q$ belong to M', so the product also does. Hence, $p \cdot q \in M' \cap \mathcal{P}$. By the already proved statement, $\Phi[p \cdot q] = p \cdot q$. On the other hand, $\Phi[p \cdot q] = \Phi[p] \cdot \Phi[q]$. Since $q \in M$, we get $\Phi[q] = q$ and conclude that $\Phi[p] = p$. $\qquad\square$

References

[1] Rick Durrett, *Probability: theory and examples*, Vol. 49, Cambridge university press, 2019.

[2] Tobias Fritz, Xiaosheng Mu, and Omer Tamuz, *Monotone homomorphisms on convolution semigroups*, arXiv preprint arXiv:1912.01733 (2019).

[3] Godfrey Harold Hardy, John Edensor Littlewood, and George Pólya, *Inequalities*, Cambridge university press, 1952.

[4] Edwin T Jaynes, *Information theory and statistical mechanics*, Physical review **106** (1957), no. 4, 620.

[5] Lutz Mattner, *Cumulants are universal homomorphisms into Hausdorff groups*, Probab. Theory Related Fields **130** (2004), no. 2, 151–166.

[6] Marc Mezard and Andrea Montanari, *Information, physics, and computation*, Oxford University Press, 2009.

[7] Marcus Michelen and Julian Sahasrabudhe, *Central limit theorems and the geometry of polynomials*, arXiv preprint arXiv:1908.09020 (2019).

[8] _____, *Central limit theorems from the roots of probability generating functions*, Advances in Mathematics **358** (2019), 106840.

[9] _____, *A characterization of polynomials whose high powers have non-negative coefficients*, Discrete Anal. (2020), Paper No. 20, 16.

[10] _____ , *Anti-concentration of random variables from zero-free regions*, Discrete Anal. (2022), Paper No. 13, 29.

[11] Xiaosheng Mu, Luciano Pomatto, Philipp Strack, and Omer Tamuz, *Monotone additive statistics*, Econometrica **92** (2024), no. 4, 995–1031.

[12] Henri Poincaré, *Sur les équations algébriques*, C. R. Acad. Sci. Paris **93** (1883), 1418–1419; Reprinted in *Oeuvres de Henri Poincaré*, Vol. 5 (1950), 81–82.

[13] George Pólya, *Über positive Darstellung von Polynomen*, Vierteljahrsschrift der Naturforschenden Gesellschaft in Zürich, 1928, pp. 141–145; Reprinted in *Collected Papers of George Pólya*, Vol. 2 (1974) 309–313.

[14] Christian Rosendal, *Automatic continuity of group homomorphisms*, Bulletin of Symbolic Logic **15** (2009), no. 2, 184–214.

[15] Imre Ruzsa and Gábor J Székely, *Algebraic probability theory*, John Wiley & Sons Inc, 1988.