Z. Wahrscheinlichkeitstheorie verw. Gebiete
70, 263–269 (1985)

Zeitschrift für
Wahrscheinlichkeitstheorie
und verwandte Gebiete

No Distribution is Prime

I.Z. Ruzsa [1] and G.J. Székely [2]

[1] Mathematical Institute of the Hungarian Academy of Sciences, Budapest, Hungary
[2] Eötvös Loránd University, Mathematical Institute, Department of Probability Theory, H-1088 Budapest, Hungary

Summary. Let $\mathscr{F}$ denote the convolution semigroup of probability distributions on the real line. We prove that *no element of* $\mathscr{F}$ *is prime* in the sense that given an $F \in \mathscr{F}$ one can always find two distributions $G, H \in \mathscr{F}$ such that F is a convolution factor of $G*H$ but neither of G nor of H. In contrast, $\mathscr{F}$ is known to possess many irreducible elements.

1. Introduction

Let $\mathscr{F}$ denote the convolution semigroup of probability distributions on the real line. For $F, G \in \mathscr{F}$ we write $F|G$ and say that F is a *divisor* or a *factor* of G if $G = F*H$ for some H (which is, in general, not uniquely determined, see e.g. Lukacs [10], p. 104).

Let us restate the customary definition of *irreducible* and *prime* elements for this special case.

(1.1) *Definition.* A distribution F is *irreducible* (indecomposable) if $F = G*H$ implies that either G or H is degenerate, but F itself is not. (Degenerate distributions play the role of units.)

(1.2) *Definition.* A nondegenerate distribution F is *prime* if $F|G*H$ implies $F|G$ or $F|H$.

Note that usually (e.g. in Lukacs [10], and Heyer [6]) the term prime is used for the first named notion. In nice cases (such as the natural numbers) these concepts coincide, but generally they do not. Their coincidence is (roughly) equivalent to the unicity of decomposition (of decomposable elements). The existence of a decomposition is not trivial at all. It is a deep theorem of Hinčin (see e.g. Linnik and Ostrovkii [9]) that every F has a decomposition of the form

$$F = Q*P_1*P_2*\ldots,$$

where $P_1, P_2, \ldots$ are irreducible (there can be a finite or infinite number of them) and Q is "anti-irreducible", i.e. has no irreducible factor at all (usually

called class I_0). Observe that this is not a decomposition in the algebraic sense, as it contains infinite products, which makes sense only if we have also a topology. The anti-irreducible distributions are known to be infinitely divisible. The converse does not hold, but e.g. the normal and Poisson laws are anti-irreducible, by the results of Cramér and Raikov (see e.g. Lukacs [10]).

This fundamental decomposition is known not to be unique; hence we can conclude that not every irreducible distribution is prime. We make a step further in this direction.

Theorem 1. *No element of* $\mathscr{F}$ *is prime in the sense* (1.2).

Remark. In a certain sense our assertion justifies the usual confusion of irreducibility and primary, showing that one of them is void.

2. Primes and Homomorphisms

The existence of primes in $\mathscr{F}$ is closely related to the existence of homomorphisms of $\mathscr{F}$ into the additive group Z of integers, as the following statement shows.

(2.1) **Lemma.** *If* $P\in\mathscr{F}$ *is a prime, then*

$$\varphi(F)=\max\{n: P^{*n}|F\}$$

defines a homomorphism of $\mathscr{F}$ *into* Z.

Proof. First observe that $\varphi(F)$ is finite for every $F\in\mathscr{F}$. If $F_1, F_2\in\mathscr{F}$ *and* $\varphi(F_1)+\varphi(F_2)=n$, then $F_1*F_2=P^{*n}*F$, where $P\nmid F$, thus it is sufficient to show that

$$P^{*(n+1)}\nmid P^{*n}*F \quad \text{if } P\nmid F. \tag{2.2}$$

Suppose indirectly that $P\nmid F$ but

$$P^{*n}*F=P^{*(n+1)}*G \tag{2.3}$$

for some $G\in\mathscr{F}$.

We shall use $\hat{F}$ to denote the characteristic function of any distribution F and write $F\prec G$ if every root of $\hat{F}$ is a root of $\hat{G}$ as well.

(2.3) implies that $\hat{P}^n(\hat{F}-\hat{P}\hat{G})=0$, thus if $P\prec H$, then $\hat{H}(\hat{F}-\hat{P}\hat{G})=0$, $H*F=H*P*G$, hence $P|H*F$. By the assumption $P\nmid F$, P prime we can now conclude $P|H$, i.e. if P is any prime satisfying equation (2.3) and not dividing F, then $P\prec H$ always implies $P|H$.

Now if $\hat{P}$ has no root, then (2.3) obviously yields $F=G*P$, a contradiction to the assumption $P\nmid F$, thus we may suppose that P has at least one root. Write

$$c=\min\{t: t>0, \hat{P}(t)=0\}.$$

Let $T_a(a>0)$ be the distribution whose characteristic function is the "triangle function": $1-|t|/a$ for $t<a$ and 0 otherwise. Let further $T_{a,b}$ $(b>a>0)$ be the distribution whose characteristic function is $1-|t|/a$ for $|t|<a$, 0 for $t\in[a,b]$

and periodic with period $a+b$. If $b>a>c$, then $P \prec T_a * T_{c,b}$, which implies (by the above considerations) that $P \mid T_a * T_{c,b}$, thus $P \mid T_a$ or $P \mid T_{c,b}$. But $P \nmid T_a$ if $a>c$, since $\hat{T}_a(c) \neq 0 = \hat{P}(c)$, and $P \nmid T_{c,b}$ if $|\hat{P}(c+b)| < 1 = \hat{T}_{c,b}(c+b)$, which can be achieved by a suitable choice of b.

By this lemma our Theorem 1 follows from the next assertion.

Theorem 2. *There is no nontrivial homomorphism of $\mathscr{F}$ into Z.*

Remark 1. Lemma (2.1) sounds so natural that at first we did not realize that it needs to be proved at all. There are, however, semigroups where this function φ is always finite but is not always a homomorphism.

Remark 2. In the multiplicative semigroup of integers there are many primes (even a unique factorization), but there is no homomorphism into Z because of the zero-element. In fact this phenomenon occurs even in cancellative semigroups. Let $A \subset R^2$ consist of pairs (x, y) such that $x \geqq 0$ and if $x=0$, then y is a nonnegative integer, the operation being the addition. Here the element $(0, 1)$ is prime and the reader can easily check that the only homomorphism of A into Z is the trivial one.

It would be interesting to obtain a result in the reverse direction. Of course, from a single homomorphism we cannot conclude anything, but perhaps the existence of "many" nonnegative-valued homomorphisms may have some consequence on the arithmetical structure.

Remark 3. We proved (Ruzsa-Székely [12]) that there are nontrivial homomorphisms of $\mathscr{F}$ into R, the additive group of reals; moreover, a homomorphism can coincide with the expectation for all distributions for which it is finite; the crucial point is that Z is not divisible.

G. Halász proved that there is no nontrivial continuous homomorphism of $\mathscr{F}$ endowed with the weak topology into R endowed with the usual topology (or into any topological group; unpublished, oral communication).

3. The Quotient Group of $\mathscr{F}$

The problem of existence of a homomorphism from a semigroup can be reduced to the problem of homomorphisms between groups. Let S be a commutative semigroup; a group G_0 and a homomorphism $\kappa: S \to G_0$ can be constructed so that if G is an arbitrary Abelian group and $\varphi: S \to G$ a homomorphism, then $\varphi = \varphi_0 \circ \kappa$ for some homomorphism $\varphi_0: G_0 \to G$. If we impose the natural requirement that $\kappa(S)$ generates G_0, then G_0 is unique up to an isomorphism: if (G_0', κ') is another such system, then $\kappa' = \iota \circ \kappa$ with an isomorphism $\iota: G_0 \to G_0'$.

This G_0 is called the quotient group of S; in case of a cancellative semigroup it reduces to the ordinary quotient group (cf. Chevalley [2], Ch. 2, Th. 20 or Lang [8], I §9.). Since we need not only the existence but some particular properties of this group, we briefly describe its construction.

(3.1) *Definition.* Call two element $s_1, s_2 \in S$ *sisters* and write $s_1 \sim s_2$ if there is an $s \in S$ such that $ss_1 = ss_2$.

If s_1, s_2 are sisters and φ is any homomorphism of S into a group (or cancellative semigroup), then, of course, $\varphi(s_1)=\varphi(s_2)$. Hence it is natural to consider the factor semigroup $S_0=S/\sim$ ($\sim$ is evidently a congruence relation). It is easy to see that S_0 is cancellative, thus it can be embedded into its (ordinary) quotient group G_0, which will do also for our purposes.

Theorem 3. *The quotient group of $\mathscr{F}$ is a divisible torsionfree group of cardinality continuum (and therefore it is isomorphic to the additive group of real numbers).*

Theorem 3 obviously implies Theorem 2: from a divisible group no nontrivial homomorphism goes into Z. Two distribution functions F_1 and F_2 are sisters if and only if their characteristic functions $\hat{F}_1$ and $\hat{F}_2$ coincide in a neighbourhood of 0. Namely if $F_1 * F = F_2 * F$, then $\hat{F}_1\hat{F}=\hat{F}_2\hat{F}$ and hence $\hat{F}_1(t)=\hat{F}_2(t)$ whenever $\hat{F}(t)\neq 0$, which surely holds for small t. On the other hand, if $\hat{F}_1(t)=\hat{F}_2(t)$ for $|t|<a$, then $F_1 * T_a = F_1 * T_a$ with the same distribution T_a as in Sect. 2.

It is easy to see that the distributions of bounded variables are "only children" i.e. they have no sisters (the characteristic function is analytic, and if two analytic functions coincide on an interval, they are identic, i.e. the $\sim$ equivalence classes of these distributions have cardinality 1).

Concerning Theorem 3 we note that it is evident that this quotient group is torsionfree and of cardinality continuum; its divisibility will be proved in the next section. That these assertions imply isomorphism to the additive group of reals follows from the structure theorem of divisible groups, see e.g. Fuchs [5], Ch. 3, § 19.

4. The Divisibility of $\mathscr{F}$ and a Wiener-Lévy Type Theorem

To prove the divisibility of the quotient group of $\mathscr{F}$ means, according to the considerations at the end of the previous section, that for any characteristic function $\hat{F}$ and natural number n two characteristic functions $\hat{F}_1$ and $\hat{F}_2$ can be found such that

$$\hat{F}(t)=(\hat{F}_1(t)/\hat{F}_2(t))^n \tag{4.1}$$

in a neighbourhood of 0. We shall obtain a bit more general result.

Theorem 4. *Let $\hat{F}$ be a characteristic function and f a function, analytic in a neighbourhood of 1 and satisfying $f(1)=1$. Then one can find two characteristic functions $\hat{F}_1$ and $\hat{F}_2$ such that*

$$f(\hat{F}(t))=\hat{F}_1(t)/\hat{F}_2(t) \tag{4.2}$$

holds in a neighbourhood of 0.

(4.1) follows by setting $f(x)=x^{1/n}$. Our main tool is

(4.3) **Lemma.** *Let χ be a Fourier-transform of a function from $L_1(-\infty,\infty)$ and f a function, analytic in a neighbourhood of $\chi(0)$. Then there is another $h\in L_1$ whose Fourier-transform ψ coincides with $f(\chi(t))$ in a neighbourhood of 0.*

This is a Wiener-Lévy type theorem due to Ditkin [4]. For a proof, history and generalizations see Reiter [11], p. 7 or Ahiyezer [1].

We need the following lemma.

(4.4) **Lemma.** *Suppose* $h \in L_1$, $\int_{-\infty}^{\infty} h(t)dt > 0$. *One can find a nonnegative* $g \in L_1$, $g \not\equiv 0$ *such that* $h * g$ *is also nonnegative.*

(Note that in the usual inaccurate way we use the same symbol $*$ to form the density function of a sum from density functions and to form the distribution from distributions, though formally they are two different operations on real functions.)

We could not decide whether this lemma has been known (several mathematicians asserted to have seen it, but we could not get any exact reference). A more general version is proved in Ruzsa-Székely [13].

Proof of Theorem 4. Let

$$\eta(t) = \begin{cases} 0 & \text{for } |t| \geqq 2, \\ 1 & \text{for } |t| \leqq 1, \\ 2-t & \text{for } 1 \leqq |t| \leqq 2. \end{cases}$$

η is a Fourier-transform of a function from L_1, therefore so is $\chi\eta$. Applying Lemma (4.3) we obtain a $h \in L_1$ whose Fourier-transform ψ satisfies

$$\psi(t) = f(\chi(t)\eta(t)) = f(\chi(t))$$

for small t. This h satisfies the requirement of Lemma (4.4), since

$$\int_{-\infty}^{\infty} h(t)dt = \psi(0) = f(\chi(0)) = 1.$$

Lemma (4.4) provides us a nonnegative g; we may assume it is a density function, since this can be achieved by a constant factor, and then

$$\int (h * g) = (\int h)(\int g) = 1,$$

thus so is $g_1 = h * g$.

Denoting the Fourier-transform of g and g_1 by $\hat{F}_2$ and $\hat{F}_1$, for small values of t we have

$$\hat{F}_2(t) f(\hat{F}(t)) = \hat{F}_2(t)\psi(t) = \hat{F}_1(t)$$

as wanted.

5. Further Problems

(i) *Squarefree distributions.* Call a distribution F *squarefree* if $F | G^{*2}$ implies $F | G$. (This concept is often called "weak prime"; however, for integers this is the well-known notion of a squarefree number, thus we considered this name to be more appropriate.) Are there nondegenerate squarefree distributions at all? A negative answer would be, of course, stronger than the nonexistence of

primes. From Theorem 3 one can easily deduce that the distribution of a bounded variable cannot be squarefree.

(ii) *Prime Ideals.* Another possible generalization of prime elements is the notion of prime ideal. $\mathcal{I} \subset \mathcal{F}$ is an *ideal* if for every $F \in \mathcal{F}$ and $G \in \mathcal{I}$ we have $F * G \in \mathcal{I}$; it is a *prime ideal* if its complementer forms a semigroup.

Problem. Characterize the prime ideals of $\mathcal{F}$. In these terms the famous theorems of Cramér and Raikov (see e.g. Lukacs [10]) state that the set of non-normal, resp. the set of non-Poisson distributions are prime ideals. Another class of prime ideals is obtained by regarding those distributions whose characteristic function vanishes at a given real number. (Our Theorem 1 shows that there is no principal prime ideal.)

(iii) *Decomposition of* $\mathcal{F}$. Take the factor semigroup $\mathcal{F}^*$ of $\mathcal{F}$ with respect to the set $\mathcal{F}_0$ of degenerate distribution (i.e. we identify distributions which are translates of each other). Is this semigroup simple? We think it is; the simplicity would evidently imply the nonexistence of primes. (Our result quoted at the end of Sect. 2 shows that $\mathcal{F}$ is the direct product of $\mathcal{F}_0$ and $\mathcal{F}^*$.)

(iv) *Coprime Distributions.* Call two distributions F and G *coprime* if $F|H$, $G|H$ implies $F * G|H$. Are there nondegenerate coprime distributions at all? We can prove that distributions of two bounded variables cannot be coprime.

(v) *Generalizations.* Analogous problems can be investigated concerning the semigroup of distributions on a commutative topological group, or even more generally, a Borel group. In this generality unexpected difficulties may arise, e.g. the convolution of two distributions may not exist. This can be avoided by restricting ourselves to measures which are in some sense regular, cf. Csiszár [3].

Among the distributions over some commutative groups there can be primes. The complete list of prime distributions on locally compact (Hausdorff) Abelian groups will be published in Ruzsa-Székely [14].

Finally we note that Hinčin's theorem can be extended to Delphic semigroups (see Kendall [7]) thus the existence of primes in these semigroups may also be interesting. We plan to return to such generalizations in another paper.

References

1. Ahiyezer, N.I.: Lectures on approximation theory (in Russian). Moscow-Leningrad: Gostehizdat 1947
2. Chevalley, Cl.: Fundamental concepts of algebra. New York: Academic Press 1956
3. Csiszár, I.: Some problems concerning measures on topological spaces and convolutions of measures on topological groups. In: Coll. Internat. du CNRS, Clermond-Ferrand 1969. Les probabilités sur les structures algébriques. Paris 1970
4. Ditkin, V.A.: Investigations concerning the structure of ideals in certain normed rings (in Russian) Učen. Zap. Mosk. Gos. Univ. Ser. Matem. **30**, 93–130 (1939)
5. Fuchs, L.: Abelian Groups. Budapest: Akadémiai Kiadó 1966
6. Heyer, H.: Probability measures on locally compact groups. Berlin-Heidelberg-New York: Springer 1977

7. Kendall, D.G.: Delphic semigroups, infinitely divisible regenerative phenomena and the arithmetic of p-functions, Z. Wahrscheinlichkeitstheor. verw. Geb. **9**, 163–195 (1968)
8. Lang, S.: Algebra. Reading: Addison-Wesley 1965.
9. Linnik, Yu.V., Ostrovskiĭ, I.V.: Decomposition of random variables and vectors. Transl. of Mathem. Monographs 48. Providence: Amer. Math. Soc. 1977
10. Lukacs, E.: Characteristic functions. London: Ch; Griffin and Co. 1970
11. Reiter, H.: Classical harmonic analysis and locally compact groups. Oxford: Clarendon 1968
12. Ruzsa, I.Z., Székely, G.J.: An extension of expactation. Z. Wahrscheinlichkeitstheor. verw. Gebiete **53**, 17–19 (1980)
13. Ruzsa, I.Z., Székely, G.J.: Convolution quotients of nonnegative functions. Monatsh. Math. **95**, 235–239 (1983)
14. Ruzsa, I.Z., Székely, G.J.: Irreducible and prime distributions. In: Proc. of the Conf. "Probability Measures on Groups", Oberwolfach 1981. Lecture Notes in Math. **928**, pp. 354–361. Berlin-Heidelberg-New York: Springer 1983

Received January 12, 1982; in revised form February 10, 1985