ARITHMETIC PROPERTIES OF BERNOULLI CONVOLUTIONS[1]

BY

ADRIANO M. GARSIA

Introduction and historical remarks. Let $A(x)$ denote the distribution function of a random variable which takes the values ± 1 with equal probability, and let

$$r = (r_1, r_2, \cdots, r_n, \cdots) \tag{I.1}$$

denote a sequence of positive real numbers.

It is well known[2] that the infinite convolution

$$F(x, r) = A\left(\frac{x}{r_1}\right) * A\left(\frac{x}{r_2}\right) * \cdots * A\left(\frac{x}{r_n}\right) * \cdots \tag{I.2}$$

converges to a distribution function if and only if

$$\sum_{n=1}^{\infty} r_n^2 < \infty. \tag{I.3}$$

Here and in the following we shall suppose that this condition is satisfied.

It is easy to show that $F(x, r)$ is continuous. Since it can be shown (see [4]) that it is always "pure," i.e. either absolutely continuous or purely singular, the question arises for which sequences r, $F(x, r)$ enjoys the former or the latter property.

Under the sole condition (I.3), very little is known to this date. There are some conditions (cf. [8]) on the speed of convergence of $\sum_{n=1}^{\infty} r_n^2$ which assure that $F(x, r)$ is infinitely many times differentiable. These conditions are of the type $n^{-\gamma}/n^{\sigma} \leqq r_n \leqq n^{\gamma}/n^{\sigma}$ (for $n \geqq n_{\sigma,\gamma}$) for some $\sigma > 1/2$ and all $\gamma > 0$. More recently Kahane and Salem (cf. [5]) have found a condition of arithmetical nature which, when applicable, assures not only that $F(x, r)$ is absolutely continuous but that its Fourier transform is square integrable. Their result can be so described. Let

$$\Lambda(u, r) = \int_{-\infty}^{+\infty} e^{iux} dF(x, r) \tag{I.4}$$

and M_n denote the number of solutions to the inequality

Presented to the Society, June 17, 1960; received by the editors April 6, 1961.

(1) This work was carried out while the author was supported by the U. S. Air Force Office of Scientific Research (Contract No. Af 49(638)-857).

(2) See footnote (3), p. 411.

$$(I.5)\quad |(\pm r_1 \pm r_2 \pm \cdots \pm r_n) - (\pm r_1 \pm r_2 \pm \cdots \pm r_n)| < \left(\sum_{k=n+1}^{\infty} r_k^2\right)^{1/2}.$$

Then any of the following conditions

$$(I.6)\quad \text{(a)}\quad \Lambda(u, r) \in L_2(-\infty, +\infty),$$

$$\text{(b)}\ \liminf_{n\to\infty} \frac{M_n}{4^n\left(\sum_{k=n+1}^{\infty} r_k^2\right)^{1/2}} < \infty, \qquad \text{(c)}\ \limsup_{n\to\infty} \frac{M_n}{4^n\left(\sum_{k=n+1}^{\infty} r_k^2\right)^{1/2}} < \infty,$$

implies the remaining ones.

Some additional information is available when the sequence r satisfies the more restrictive condition

$$(I.7)\quad \sum_{n=1}^{\infty} r_n < \infty.$$

Since a simultaneous change of scale in the r_n does not affect the smoothness of $F(x, r)$, when (I.7) is satisfied, we can actually assume

$$(I.8)\quad \sum_{n=1}^{\infty} r_n \leqq 1.$$

In this case $F(x, r)$ has an interesting probabilistic interpretation.

We introduce the quantities

$$(I.9)\quad \xi_n = \frac{1 - (r_1 + r_2 + \cdots + r_n)}{1 - (r_1 + r_2 + \cdots + r_{n-1})}.$$

Clearly

$$(I.10)\quad 0 < \xi_n < 1$$

and

$$(I.11)\quad r_n = \xi_1\xi_2 \cdots \xi_{n-1}(1 - \xi_n).$$

Vice versa, given any sequence $(\xi_1, \xi_2, \cdots, \xi_n, \cdots) \in I \times I \times \cdots \times I \times \cdots$ in the infinite product of the interval $I = (0, 1)$ with itself and defining r_n by means of (I.11) we obtain a sequence r satisfying (I.8).

Starting with the ξ_n we define the following random walk. We let $x_0 = 0$, then, inductively, for each $n \geqq 1$, with equal probability we let x_n stay at x_{n-1} or go to the point z_n, where z_n divides the interval $(x_{n-1}, 1)$ in the ratio $(1-\xi_n)/\xi_n$.

It is easy to show that

$$(I.12)\quad x_n = x_{n-1} + a_n\xi_1\xi_2 \cdots \xi_{n-1}(1 - \xi_n)$$

where $a_n = 1$ or 0 with equal probability. We thus get

$$x_N = \sum_{k=1}^{N} a_k r_k. \tag{I.13}$$

Setting $a_k = (1+\phi_k)/2$, where the ϕ_k are independent random variables taking the values ± 1 with equal probability and letting

$$y_N = \sum_{n=1}^{N} \phi_n r_n, \qquad y = \sum_{n=1}^{\infty} \phi_n r_n, \qquad F_n(x, r) = \text{Prob}\{y_n \leqq x\}$$

we obtain that

$$x_N = \frac{1}{2}\sum_{n=1}^{N} r_n + \frac{1}{2} y_N \tag{I.14}$$

and

$$F_N(x, r) \to F(x, r)(^3). \tag{I.15}$$

In other words

$$F(x, r) = \text{Prob}\{y \leqq x\}. \tag{I.16}$$

Under this setup the first criterion one finds is rather elementary. In fact, if $\xi_n < 1/2$ for all n or equivalently if

$$r_n > \sum_{l=n+1}^{\infty} r_k \tag{I.17}$$

the random walk x_n is contained in a nowhere dense set E whose measure is given by

$$m(E) = \lim_{n\to\infty} 2^n \sum_{k=n+1}^{\infty} r_k = \lim_{n\to\infty} 2^n \xi_1, \xi_2 \cdots \xi_n(^4).$$

Then clearly if $m(E)=0$, $F(x, r)$ must be singular. On the other hand if $m(E)>0$ it can be shown (cf. [4]) that $F(x, r)$ is absolutely continuous. Since the smoothness of $F(x, r)$ depends only on the tail of r, similar results hold when (I.17) is satisfied from some time on.

The real difficulties arise when (I.17) is never satisfied or only occasionally satisfied. In the former case it can be shown that the range of y is the full interval (0, 1), and such simple considerations do not apply. Nevertheless, since in the space $I \times I \times I \times \cdots$ (5) of all random sequences $(\xi_1, \xi_2, \cdots, \xi_n, \cdots)$ $0 < \xi_i < 1$ the event

"$F(x, r)$ absolutely continuous"

---

(3) Actually, for this relation (I.7) is not needed. In fact $y = \sum_{n=1}^{\infty} \pm r_n$ is defined for almost all changes of sign if and only if $\sum r_n^2 < \infty$.

(4) (I.17) assures the existence of this limit.

(5) With a probability measure defined by the product Lebesgue measure.

is a tail event, the function $F(x, r)$ must be either almost surely absolutely continuous or almost surely singular. It is quite likely that it is almost surely absolutely continuous; however, no such result is available.

However, it is worth pointing out that Kahane and Salem (cf. [5]) were able to show that if r is defined by (I.11) and

$$\xi_n = a_n + \eta_n(b_n - a_n), \qquad b_n > a_n, \qquad 0 \leqq \eta_n \leqq 1, \tag{1}$$

$$\liminf(a_1 a_2 \cdots a_n)^{1/n} > 1/2, \tag{2}$$

$$b_n - a_n \geqq e^{-o(n)}, \tag{3}$$

then in the space $I \times I \times I \times \cdots$ of all random sequences

$$\eta = (\eta_1, \eta_2, \cdots, \eta_n, \cdots) \qquad 0 \leqq \eta_i \leqq 1$$

the Fourier transform $\Lambda(u, r)$ of $F(x, r)$ is almost surely in $L_2(-\infty, +\infty)$.

Other scattered results of this nature are available (for further references cf. [3]), and all seem to point out that the singularity of $F(x, r)$ is more the exception than the rule. Nonetheless, examples are easily constructed (even when $\xi_n > 1/2$ for all n) to illustrate that $F(x, r)$ may also be singular.

A most interesting particular case of the general problem is obtained by setting $r_n = (1-\beta)\beta^{n-1}$ $(0 < \beta < 1)$ or equivalently $\xi_1 = \xi_2 = \cdots = \xi_n = \beta$. It follows then from the above considerations that $F(x, \beta)$([6]) is purely singular when $\beta < 1/2$.

A mystery surrounds the case $\beta > 1/2$. It was repeatedly conjectured that $F(x, \beta)$ ought to be absolutely continuous for $\beta > 1/2$. However, already in 1939 Erdös (cf. [1]) showed that when β is the reciprocal of a Pisot-Vijayaraghavan number [9], then not only $F(x, \beta)$ is not absolutely continuous but actually $\Lambda(u, \beta)$ does not even tend to zero at infinity. Perhaps we should recall that an algebraic integer α is called a Pisot-Vijayaraghavan number when all its conjugates are in absolute value less than one. Erdös then exhibited the solution of $\beta^2 + \beta - 1 = 0$ and $\beta^3 + \beta^2 - 1 = 0$ as examples of $\beta > 1/2$ for which $F(x, \beta)$ is singular. Siegel (in [14]) showed later that the positive solution of $\alpha^3 - \alpha - 1 = 0$ is the smallest P.V. number, and Pisot and Dufresnoy [10] showed that the solution of $\alpha^2 - \alpha - 1 = 0$ is the smallest limit point of such numbers. Salem in [13] showed that $\Lambda(u, \beta)$ does not tend to zero only if β is the reciprocal of a Pisot-Vijayaraghavan number. Thus after $\beta > \beta_0$ $(\beta_0^3 + \beta_0^2 - 1 = 0)$ the function $\Lambda(u, \beta)$ tends to zero as $u \to \infty$.

Erdös [2] has shown that for almost all β in the interval $1/2 \leqq \beta \leqq 1/2^{1/2}$ we have

$$|\Lambda(u, \beta)| = O(1/|u|^{\gamma}) \tag{I.18}$$

for a constant $\gamma > 0$ independent of β. From his method it is actually possible

([6]) Here and in the following, when $r = (\beta, \beta^2, \cdots, \beta^n, \cdots)$ in our formulas we shall replace r by β.

to show that for any β_1, β_2 $(0<\beta_1<\beta_2<1)$ there exists a constant $\gamma(\beta_1, \beta_2)$ for which (I.18) holds for almost all $\beta\in(\beta_1, \beta_2)$. Erdös used the result (I.18) to show that there exists a sequence of numbers $\beta_k\to 1$ such that $F(x, \beta)$ has k derivatives for almost all $\beta\in(\beta_k, 1)$. This result can be easily obtained from (I.18) and the identity

$$\Lambda(u, \beta) = \Lambda(u, \beta^n)\Lambda(u\beta, \beta^n)\cdots\Lambda(u\beta^{n-1}, \beta^n) \tag{I.19}$$

valid for all integers n.

It is worth while to point out that from Vieta's identity

$$\Lambda(u, 1/2) = \frac{\sin u}{u},$$

thus in view of (I.19) it follows that $F(x, (1/2)^{1/n})$ has n derivatives.

This together with the stated results would seem to suggest that perhaps $F(x, \beta)$ is absolutely continuous for almost all $1/2<\beta<1/2^{1/2}$, differentiable for almost all $1/2^{1/2}<\beta<1/3\cdot 2^{1/2}$, etc. No such results are available.

The nature of the set of β for which $F(x, \beta)$ is singular is still unknown. The results of our investigations seem to suggest that the singularity of $F(x, \beta)$ may only occur when β is algebraic and satisfies a polynomial equation with coefficients ± 1 or 0. This conjecture we have been unable to prove or disprove. If false, an example to the contrary would be very valuable for further investigations.

Perhaps it is worth while to mention, before closing this introduction, that the random variable $y=\sum_{n=1}^{\infty}(\pm 1)\beta^n$ as well as its distribution $F(x, \beta)$ have recently arisen in connection with some psychological experiments (for further references see [7] and [6]) and in some problems of data transmission (see for instance [12]).

The main results of this paper are some criteria which assure the absolute continuity of $F(x, r)$ and some criteria which assure its singularity. These criteria are far from being necessary, but they appear to be fruitful in some special cases. In each case we illustrate our results with examples.

1. **Criteria for the absolute continuity of $F(x, r)$.** 1.1. Our first result depends upon a rather intuitive lemma on the theory of distribution functions.

LEMMA 1.1. *Let y_n be a sequence of random variables with respective distributions $F_n(x)$. Let y be a random variable with a continuous distribution $F(x)$. Suppose that the random variables*

$$z_n = y - y_n$$

tend to zero in probability, which implies that for all x

$$\lim_{n\to\infty} F_n(x) = F(x).$$

If, in addition, each y_n assumes only a finite number of values

$$y_n^{1}, y_n^{2}, \cdots, y_n^{k_n}$$

and for each j, n

$$\Pr\{y_n = y_n^{j}\} \leqq A \inf_{i \neq j} |y_n^{i} - y_n^{j}| \tag{1.11}$$

then $F(x)$ is absolutely continuous with a derivative bounded by A.

Proof. For a given interval $(a, b]$ suppose that the values of y_n in $(a, b]$ are

$$a < y_n^{i_1} < y_n^{i_2} < \cdots < y_n^{i_\nu} \leqq b.$$

In view of (1.11) we shall have

$$\begin{aligned} A(b-a) &> A[y_n^{i_\nu} - y_n^{i_{\nu-1}} + y_n^{i_{\nu-1}} - y_n^{i_{\nu-2}} + \cdots + y_n^{i_2} - y_n^{i_1}] \\ &\geqq \Pr\{y_n = y_n^{i_\nu}\} + \Pr\{y_n = y_n^{i_{\nu-1}}\} + \cdots + \Pr\{y_n = y_n^{i_2}\} \\ &= F_n(b) - F_n(a) - \Pr\{y_n = y_n^{i_1}\}. \end{aligned}$$

However, since

$$\Pr\{y_n = y_n^{i}\} \leqq \Pr\{|y - y_n^{i}| \leqq \epsilon\} + \Pr\{|z_n| > \epsilon\},$$

as $n \to \infty$ we shall have

$$F(b) - F(a) \leqq A(b-a).$$

This proves the assertion.

1.2. We can now establish our first criterion. Let $r = (r_1, r_2, \cdots, r_n, \cdots)$ be a sequence of positive numbers such that

$$\sum_{n=1}^{\infty} r_n^{2} < \infty. \tag{1.21}$$

Let A_n indicate the set of all n-tuples

$$\alpha = (a_1, a_2, \cdots, a_n)$$

with $a_i = \pm 1, 0$ $(i = 1, 2, \cdots, n)$, and $|a_1| + |a_2| + \cdots + |a_n| \neq 0$. Let

$$m_n(r) = \min_{\alpha \in A_n} |a_1 r_1 + a_2 r_2 + \cdots + a_n r_n|.$$

Finally let $E^p r$ for every positive integer p indicate the sequence

$$(r_{p+1}, r_{p+2}, \cdots, r_{p+n}, \cdots).$$

We shall have the following

THEOREM 1.2. *If the sequence r is such that there exists a p for which*

$$\liminf_{n \to \infty} 2^n m_n(E^p r) > 0$$

then the function $F(x, r)$ is absolutely continuous with a bounded derivative.

Proof. The assumptions imply that there exist p, n_0 and a constant $\sigma>0$ such that

$$m_n(E^p r) > \sigma/2^n \tag{1.22}$$

for $n \geqq n_0$. Since $m_n(E^p r)$ does not increase with n, (1.22) implies that $m_n(E^p r)>0$ for all n and therefore there must exist a (maybe smaller) constant σ such that (1.22) becomes true for all n.

To prove the theorem it is sufficient to show that the function $F(x, E^p r)$ is absolutely continuous with a bounded derivative. In fact, we have

$$F(x, r) = F_p(x, r) * F(x, E^p r)$$

where $F_p(x, r)$ denotes the distribution function of $y_p = \pm r_1 \pm r_2 \pm \cdots \pm r_n$ and the star denotes convolution product.

For convenience of notation we might as well suppose $p=0$ and assume that

$$2^n m_n(r) > \sigma/2 > 0 \qquad \text{for all } n.$$

However, this implies that the values $y_n = \pm r_1 \pm r_2 \pm \cdots \pm r_n$ are all distinct and that if y_n', y_n'' come from two different sign distributions, we have

$$| y_n' - y_n'' | \geqq \sigma/2^n = \sigma \Pr\{y_n = y_n'\} = \sigma \Pr\{y_n = y_n''\}.$$

Thus the theorem is an immediate consequence of Lemma 1.1.

1.3. To understand the strength of the assumption in Theorem 1.2 we should point out that (1.21) implies that

$$\limsup_{n\to\infty} 2^n m_n(r) < \infty.$$

In fact, there will exist a large constant M and a suitable integer n_0 such that for all $n \geqq n_0$ for more than half of the possible sign distributions the numbers

$$\pm r_1 \pm r_2 \pm \cdots \pm r_n$$

will fall in the interval $[-M, M]$. But such an interval contains only 2^{n-1} intervals of amplitude $4M/2^n$.

1.4. Nevertheless, Theorem 1.2 affords an easy way to construct sequences r for which $F(x, r)$ is Lipschitzian(7). If $r=(\beta, \beta^2, \cdots, \beta^n, \cdots)$ for some $1/2<\beta<1$, in general it is quite difficult to verify whether Theorem 1.2 applies. In fact, for such a sequence $m_n(r)$ is the same as

$$m_n(\beta) = \min | P^n(\beta) | \tag{1.41}$$

where the minimum is taken over all nonidentically vanishing polynomials of the type

(7) For instance if $r_n=a_n/2^n$ where $\{a_n\}$ is any sequence such that $a_{n-1} \geqq a_n \geqq a>0$ then Theorem 1.2 applies.

$$P^n(x) = a_1x + a_2x^2 + \cdots + a_nx^n$$

where $a_i = \pm 1, 0$. The condition $m_n(\beta) \neq 0$ for all n translates into the condition that β should not be a root of any polynomials with coefficients $\pm 1, 0$. The condition

$$\liminf_{n\to\infty} 2^n m_n(\beta) > 0 \tag{1.42}$$

expresses the fact that β should be far from such roots in a rather strong sense. The observations of 1.3 make it seem quite unlikely that the β's in (1/2, 1) which satisfy (1.42) could fill more than a set of zero Lebesgue measure.

We do not know of any rationals in (1/2, 1) which satisfy (1.42); as a matter of fact it is not even clear, given integers p, q which are relatively prime, whether or not for each n we must necessarily have

$$\min_{\alpha\in A_n} \left| a_1p^{n-1} + a_2p^{n-2}q + \cdots + a_nq^{n-1} \right| > 1.$$

1.5. We shall now present a few lemmas which help in the characterization of a family of algebraic numbers $\beta\in(1/2, 1)$ for which (1.42) is fulfilled.

LEMMA 1.51. *Let α be an algebraic integer greater than one*([8]). *Let $\alpha_1, \alpha_2, \cdots, \alpha_s$ denote the conjugates of α and σ denote the number of i such that $|\alpha_i| = 1$. If $A(x)$ is a polynomial with integer coefficients and height M of degree at most n for which $A(\alpha) \neq 0$; then*

$$|A(\alpha)| \geqq \frac{\prod_{|\alpha_i|\neq 1} \big||\alpha_i| - 1\big|}{(n+1)^{\sigma}\left(\prod_{|\alpha_i|>1} |\alpha_i|\right)^{n+1} M^s}. \tag{1.51}$$

Proof. Such a result is quite standard, but for sake of completeness we shall include its proof. In view of the hypothesis we necessarily have

$$|A(\alpha)A(\alpha_1)\cdots A(\alpha_s)| \geqq 1. \tag{1.52}$$

But in any case

$$|A(\alpha_i)| \leqq M(1 + |\alpha_i| + \cdots + |\alpha_i|^n) \leqq \begin{cases} \dfrac{M}{1 - |\alpha_i|} & \text{if } |\alpha_i| < 1, \\ (n+1)M & \text{if } |\alpha_i| = 1, \\ \dfrac{M|\alpha_i|^{n+1}}{|\alpha_i| - 1} & \text{if } |\alpha_i| > 1. \end{cases}$$

([8]) We recall that an algebraic integer is defined as a root of a polynomial with integer coefficients and leading coefficient plus or minus one.

Combining these inequalities with (1.52) the lemma follows.

LEMMA 1.52. *If $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_s$ and σ are defined as in the previous lemma and in addition α does not satisfy any polynomial with integer coefficients and height 1, then setting $\beta = 1/\alpha$ we necessarily have*

$$m_n(\beta) \geqq \frac{\prod_{|\alpha_i| \neq 1} ||\alpha_i| - 1|}{n^{\sigma}\left(\alpha \prod_{|\alpha_i|>1} |\alpha_i|\right)^n}. \tag{1.53}$$

Proof. For any nontrivial polynomial over the integers of height one of the type $A(x) = a_1 x + \cdots + a_n x^n$ we shall have

$$A(\beta) = (1/\alpha^n) A^*(\alpha)$$

where $A^*(x)$ is a similar polynomial of degree $n-1$ at most. The assumptions imply that $A^*(\alpha)$ is different from zero; thus Lemma 1.51 applies with $M = 1$, and (1.53) necessarily holds.

1.6. A comparison of (1.53) with (1.42) suggests that we should look for algebraic integers $\alpha > 1$ which do not satisfy any polynomial equation of height one and for which either

$$\text{(a) } \sigma \neq 0 \quad \text{and} \quad H = \alpha \prod_{|\alpha_i|>1} |\alpha_i| < 2 \tag{1.61}$$

or

$$\text{(b) } \sigma = 0 \quad \text{and} \quad H = \alpha \prod_{|\alpha_i|>1} |\alpha_i| \leqq 2. \tag{1.62}$$

The considerations of 1.3 clearly exclude case (a) and leave as the only possibility the equality sign for the inequality in (b).

As a matter of fact, the following lemma holds:

LEMMA 1.6. *If $\alpha > 1$ is an algebraic integer, $\alpha_1, \alpha_2, \cdots, \alpha_s$ indicate its conjugates and $H = \alpha \prod_{|\alpha_i|>1} |\alpha_i|$, then α satisfies polynomial equations with integer coefficients and height less than or equal to H.*

Proof. Let $P(x) = b_0 + b_1 x + \cdots + b_n x^n$ indicate a polynomial with nonnegative integer coefficients of degree at most n and height M. If $P'(x)$ is another polynomial of the same type, we have

$$P(1/\alpha) - P'(1/\alpha) = A(1/\alpha),$$

where $A(x)$ is a nontrivial polynomial with integer coefficients and height M. If α is not a root of any polynomial with integer coefficients and height M, Lemma 1.51 applies so that necessarily

$$(1.63) \qquad |P(1/\alpha) - P'(1/\alpha)| \geqq \frac{1}{(n+1)^{\sigma} H^{n+1}} \frac{\prod_{|\alpha_i| \neq 1} ||\alpha_i| - 1|}{M^{s}}.$$

On the other hand, if the $(M+1)^{n+1}$ values

$$0 \leqq P(1/\alpha) = b_0 + b_1/\alpha + \cdots + b_n/\alpha^n < M \frac{1}{1 - 1/\alpha},$$

we obtain by varying $b_0, b_1, \cdots, b_n$ in all possible ways are all distinct, there must be a couple of polynomials $P(x)$ and $P'(x)$ for which

$$|P(1/\alpha) - P'(1/\alpha)| \leqq \frac{M\alpha/(\alpha - 1)}{(M+1)^{n+1} - 1}.$$

This inequality combined with (1.63) leads to a contradiction unless

$$M + 1 \leqq H.$$

1.7. We shall then search for algebraic integers for which $\sigma = 0$ and $H = \alpha \prod_{|\alpha_i|>1} |\alpha_i| = 2$. To simplify our exposition we shall introduce the following terminology:

A polynomial $P(x)$ with integer coefficients and leading coefficient one will be said of "*type* A," if $\alpha, \alpha_1, \cdots, \alpha_s$ being its roots we have

$$1 < \alpha < 2, \qquad \alpha \prod_{|\alpha_i|>1} |\alpha_i| = 2.$$

A polynomial $P(x)$ will be said of "*type* B," if it is of type A and in addition it is irreducible.

We note that a polynomial of type A must have a constant term equal to ± 2. In fact, it is clear that if $P(x)$ is of type A, then $P(0) = \pm 2$ or ± 1. The latter case was excluded by E. Rodemich by the observation that $P(0) = \pm 1$ implies

$$(1.71) \qquad \prod_{|\alpha_i|<1} \alpha_i = \pm 1/2.$$

For we must always have

$$\alpha \prod_{|\alpha_i|>1} \alpha_i = \pm \alpha \prod_{|\alpha_i|>1} |\alpha_i| = \pm 2.$$

However, (1.71) is absurd since 1/2 is not an algebraic integer.

We can finally establish the following

LEMMA 1.7. *If $1 < \alpha < 2$ is a root of a polynomial $P(x)$ of type* A, *then α is also a root of a polynomial of type* B. *In addition all the conjugates of α are outside the unit circle and therefore α is not a root of a polynomial with coefficients ± 1 or* 0.

Proof. The polynomial $P(x)$ will factor in the form

$$P(x) = P^*(x)\chi(x)$$

where $P^*(x)$ is irreducible and $P^*(\alpha)=0$. First of all we observe that

$$P^*(0)\cdot\chi(0) = P(0) = \pm 2.$$

However, $P^*(x)$ has a root greater than one and no roots inside the unit circle; thus

$$P^*(0) = \pm 2. \tag{1.72}$$

Thus, $P^*(x)$ is of type B.

But $P^*(x)$ has no roots on the unit circle. In fact, if ϵ were such a root, we would have

$$P^*(\epsilon) = P^*(1/\epsilon) = 0.$$

Then, the polynomials $P^*(x)$ and $Q(x)=x^nP^*(1/x)$ (n degree of $P^*(x)$) have a root in common; but this is excluded by (1.72) and the assumption that $P^*(x)$ is irreducible.

The last assertion of the lemma is also a consequence of the irreducibility of $P^*(x)$.

REMARK. Perhaps we should note that from this proof it also follows that all the roots of $\chi(x)$ (if any) must be roots of unity. For, because of (1.72), they must all lie on the unit circle. But then if $\epsilon_1, \epsilon_2, \cdots, \epsilon_m$ denote all the roots of an irreducible factor of $\chi(x)$ the numbers $a_\nu=\epsilon_1^\nu+\epsilon_2^\nu+\cdots+\epsilon_m^\nu$ are all integers and $|a_\gamma| \leqq m$ for all ν. Since they satisfy a difference equation, they necessarily form a periodic sequence(9). But this implies that the ϵ_i's are roots of unity.

1.8. As a consequence of Theorem 1.2 and Lemmas 1.52, 1.7, we obtain the following

THEOREM 1.8. *If α is a real root of a polynomial of type* A *and $\alpha_1, \alpha_2, \cdots, \alpha_s$ are its conjugates, the function $F(x, 1/|\alpha|)$ is absolutely continuous and has a derivative bounded by*

$$\frac{2}{\prod_{i=1}^{s}(|\alpha_i| - 1)}.$$

Trivial examples of such α are the roots of 2. The most general examples in view of Lemma 1.7 are to be found among the roots of polynomials with integer coefficients, leading coefficient one and constant coefficient ± 2 whose roots lie all outside the unit circle. Such are for instance the polynomials

(9) In a block of $(2m+1)^m+1$ consecutive a_ν's there must be at least 2 distinct blocks of length m with the same entries.

$$P(x) = x^{p+n} - x^n - 2$$

where n and p are positive integers and $\max(p, n) \geqq 2$.

E. Rodemich has investigated all polynomials of type B up to the fifth degree and found some forty of them. Here are a few samples:

$$x^3 + x^2 - x - 2, \quad x^3 - x - 2, \quad x^3 - 2x - 2, \quad x^3 - x^2 + x - 2,$$
$$x^3 - x^2 - 2, \quad x^3 - 2x^2 + 2x - 2, \quad x^4 - x^2 + x - 2.$$

1.9. We shall now show another criterion for the absolute continuity of $F(x, r)$ which seems of some interest. To this end we introduce a notation.

Let $\sigma_n = (\sum_{\nu=n+1}^{\infty} r_\nu^2)^{1/2}$ and let $M_{k,n}$ for any integers k, n denote the number of sign distributions for which

$$\pm r_1 \pm r_2 \pm \cdots \pm r_n \in (k\sigma_n, k\sigma_n + \sigma_n].$$

Then the following holds:

THEOREM 1.9. *A necessary and sufficient condition for $F(x, r)$ to be absolutely continuous with a derivative in L_p for some $p > 1$ is that*

$$\limsup_{n\to\infty} (\text{or } \inf) \frac{1}{2^n \sigma_n^{(p-1)/p}} \left(\sum_{k=-\infty}^{+\infty} M_{k,n}^p \right)^{1/p} < \infty. \tag{1.91}$$

It is easy to deduce from this theorem both the criterion of Salem-Kahane and our Theorem 1.2.

In fact, let as before M_n denote the number of sign distributions such that

$$\left| (\pm r_1 \pm r_2 \pm \cdots \pm r_n) - (\pm r_1 \pm r_2 \pm \cdots \pm r_n) \right| < \sigma_n. \tag{1.92}$$

Then we necessarily have

$$(1/3) M_n \leqq \sum_{k=-\infty}^{+\infty} M_{k,n}^2 \leqq M_n. \tag{1.93}$$

For, if two numbers $\pm r_1 \pm r_2 \pm \cdots \pm r_n$ fall in the same interval $(k\sigma_n, k\sigma_n + \sigma_n]$, their difference satisfies (1.92). On the other hand, a given value $\pm r_1 \pm r_2 \pm \cdots \pm r_n$ must lie in some interval $(k\sigma_n, k\sigma_n + \sigma_n]$ and any other value $\pm r_1 \pm r_2 \pm \cdots \pm r_n$ which with the former satisfies (1.92) must necessarily lie in $(k\sigma_n, k\sigma_n + \sigma_n]$ or in one of the two adjacent intervals. Thus the criterion of Salem-Kahane is obtained from this theorem for $p = 2$.

Suppose now that $m_n(r) > A/2^n$.[10] In that case in an interval of amplitude σ_n there cannot fall more than $2^n \sigma_n / A$ numbers of the type $\pm r_1 \pm r_2 \pm \cdots \pm r_n$. This means that

$$\frac{1}{2^n \sigma_n} \operatorname{Max} M_{k,n} \leqq 1/A.$$

---

[10] See §1.2 for the definition of $m_n(r)$.

And this implies (1.91) for $p=\infty$. Thus also Theorem 1.2 follows from this theorem.

1.10. Theorem 1.9 is a corollary of a more general theorem concerning distribution functions. In fact, let as before y and y_n denote random variables with distributions $F(x)$ and $F_n(x)$ respectively, with $F(x)$ continuous. Assume in addition that the random variable $z_n=y-y_n$ is independent of y_n and that

$$E(z_n^2)\to 0 \quad \text{as} \quad n\to\infty.$$

In other words, assume that y_n converges to y in the square mean. Then the following theorem holds:

THEOREM 1.10. *If A_n is an arbitrary sequence of positive numbers decreasing to zero, then for a given $p>1$ the condition*

$$\liminf_{n\to\infty} \frac{1}{A_n^{1-1/p}}\left(\sum_{k=-\infty}^{+\infty}[F_n(kA_n+A_n)-F_n(kA_n)]^p\right)^{1/p} \leqq M < \infty \tag{1.101}$$

is sufficient to guarantee that $F(x)$ is absolutely continuous with a derivative in L_p. If in addition we know that

$$\liminf_{n\to\infty} \frac{A_n^2}{E(z_n^2)} > 0, \tag{1.102}$$

then the condition

$$\limsup_{n\to\infty} \frac{1}{A_n^{1-1/p}}\left(\sum_{k=-\infty}^{+\infty}[F_n(kA_n+A_n)-F_n(kA_n)]^p\right)^{1/p} \leqq M < \infty \tag{1.103}$$

is also necessary for $F(x)$ to be absolutely continuous with a derivative in L_p.

Proof. Suppose first that (1.101) is satisfied for some sequence A_n and $p<\infty$. There is no loss in generality to assume that also (1.103) holds([11]).

Let $\phi(x)$ be a C^1 function with compact support. We then necessarily have

$$\lim_{n\to\infty} \sum_{k=-\infty}^{+\infty} \phi(kA_n)\Delta F_n(k, A_n) = \int_{-\infty}^{+\infty} \phi(x)dF(x)([12]). \tag{1.104}$$

In fact, it is readily seen that

$$\sum_{k=-\infty}^{+\infty} \phi(kA_n)\Delta F_n(k, A_n) = \int_{-\infty}^{+\infty} \phi(x)dF(x) + \sum_{k=-\infty}^{+\infty} \int_{kA_n-A_n}^{kA_n} \phi'(x)[F(x)-F_n(kA_n)]dx.$$

([11]) Replacing the sequence y_n by a suitable subsequence.

([12]) Here and in the following the symbol $\Delta G(k, \sigma)$ for a distribution $G(x)$, any real k and a $\sigma>0$ is to represent the increment $G(k\sigma+\sigma)-G(k\sigma)$.

Thus (1.104) follows from the uniform continuity of $F(x)$ together with the uniform convergence of $F_n(x)$ to $F(x)$. On the other hand, from Hölder's inequality we obtain

$$\left|\sum_{k=-\infty}^{+\infty}\phi(kA_n)\Delta F_n(k, A_n)\right| \leqq \left(\sum_{k=-\infty}^{+\infty}|\phi(kA_n)|^{p/(p-1)}\right)^{(p-1)/p}\left(\sum_{k=-\infty}^{+\infty}[\Delta F_n(k, A_n)]^p\right)^{1/p}.$$

Passing to the limit as $n\to\infty$ and using (1.103) we deduce that

$$\left|\int_{-\infty}^{+\infty}\phi(x)dF(x)\right| \leqq M\left(\int_{-\infty}^{+\infty}|\phi(x)|^{p/(p-1)}dx\right)^{(p-1)/p}$$

This result is sufficient to guarantee the absolute continuity of $F(x)$ and that $F'(x)$ is in L_p. As a matter of fact we get also that

$$\left(\int_{-\infty}^{+\infty}[F'(x)]^p dx\right)^{1/p} \leqq M. \tag{1.105}$$

The $p=\infty$ case is easily taken care of. For then, (1.103) is to be written in the form

$$\frac{1}{A_n}\operatorname{Max}\Delta F_n(k, A_n) \leqq M < \infty.$$

However, this implies that for every $1<p<\infty$

$$\frac{1}{A_n^{(p-1)/p}}\left(\sum_{k=-\infty}^{+\infty}[\Delta F_n(k, A_n)]^p\right)^{1/p} \leqq M^{(p-1)/p}.$$

But we have seen that this induces the absolute continuity of $F(x)$ and that

$$\left(\int_{-\infty}^{+\infty}[F'(x)]^p dx\right)^{1/p} \leqq M^{(p-1)/p}.$$

Passing to the limit as $p\to\infty$ we get

$$F'(x) \leqq M \text{ (a.e.)}.$$

To prove the remaining part of the assertion we observe that for any x and A we have

$$\Pr\{x < y \leqq x + A, |z_n| \leqq A\} \leqq \Pr\{x - A < y \leqq x + 2A\}. \tag{1.106}$$

The independence of y_n and z_n implies that

$$\Pr\{x < y_n \leqq x + A, |z_n| \leqq A\} = \Pr\{x < y_n \leqq x + A\}\Pr\{|z_n| \leqq A\}. \tag{1.107}$$

Finally, we must also have

$$A_n^2 \Pr\{|z_n| > A_n\} \leqq E(z_n^2). \tag{1.108}$$

Thus, if $E(z_n^2)/A_n^2 < 1/2$, we can combine (1.108), (1.107), and (1.106) to obtain

$$F_n(x + A_n) - F_n(x) \leqq 2[F(x + 2A_n) - F(x - A_n)]. \tag{1.109}$$

We can deduce from this that for a given $p > 1$

$$[\Delta F_n(k, A_n)]^p \leqq 2^p 3^{p-1}([\Delta F(k+1, A_n)]^p + [\Delta F(k, A_n)]^p + [\Delta F(k-1, A_n)]^p).$$

Summing with respect to k we finally obtain

$$\frac{1}{A_n^{(p-1)/p}}\left(\sum_{k=-\infty}^{+\infty} [\Delta F_n(k, A_n)]^p\right)^{1/p} \leqq \frac{2 \cdot 3^{1/p}}{A_n^{(p-1)/p}}\left(\sum_{k=-\infty}^{+\infty} [\Delta F(k, A_n)]^p\right)^{1/p}. \tag{1.1010}$$

The right-hand side of this inequality is readily shown to be uniformly bounded when $F(x)$ is absolutely continuous and $F'(x) \in L_p$. Thus the necessity part of the assertion for $p < \infty$ is established when

$$\liminf_{n \to \infty} A_n / E(z_n^2) > 2.$$

When only (1.102) is known to hold, we can certainly find an integer σ such that

$$\liminf_{n \to \infty} 2^{2\sigma} A_n^2 / E(z_n^2) > 2.$$

Thus the inequality (1.1010) must eventually hold when A_n is replaced by $2^\sigma A_n$. The factor 2^σ is then easily removed by replacing (1.1010) by a weaker inequality obtained by a successive use of the inequality

$$[\Delta F_n(2k+1, A_n)]^p + [\Delta F_n(2k, A_n)]^p \leqq [\Delta F_n(k, 2A_n)]^p$$

which is always valid when $p > 1$.

The necessity part of the assertion for $p = \infty$ follows immediately from (1.109). Thus the proof of the theorem is complete.

1.11. Perhaps a few observations are in order concerning the implications of this theorem.

First of all we note that a simple argument shows that in general for any $p > 1$, whether $F'(x)$ is in L_p or not, we must necessarily have

$$\liminf_{n \to \infty} \frac{1}{A_n^{1-1/p}}\left(\sum_{k=-\infty}^{+\infty} [\Delta F_n(k, A_n)]^p\right)^{1/p} > 0.$$

Thus, the establishment of such an inequality as (1.103) in any particular case may require some rather refined estimates.

For this reason, in the case that $y_n = \sum_{k=1}^{n} \pm\beta^k$, $y = \sum_{k=1}^{\infty} \pm\beta^k$, $\beta = 1/\alpha$, $1 < \alpha < 2$, to the best of our knowledge the only specific α's for which (1.91) is known to hold for some $p > 1$ are the algebraic numbers of Theorem 1.8.

From the results of Erdös quoted in the introduction it is easy to show the existence of a whole interval $(1, \alpha_0)$ for which (1.91) must hold for some $p > 1$ for almost all $\alpha \in (1, \alpha_0)$.

It is probably true that (1.91) holds for $p = 2$ for almost all $\alpha \in (1, 2)$; however, so far, this is only a conjecture.

Finally, we should point out that in the case that

$$r = (1/\alpha, 1/\alpha^2, \cdots, 1/\alpha^n, \cdots)$$

the numbers $M_{k,n}$ defined in 1.9 can be taken, for each k and n, to be equal to the number of sign distributions for which

$$k < \pm\alpha \pm \alpha^2 \pm \cdots \pm \alpha^n \leqq k + 1$$

and the condition (1.91) in this case can be written in the form

$$\sum_{k=-\infty}^{+\infty} M_{k,n}^{p} \leqq M \frac{2^{np}}{\alpha^{n(p-1)}}. \tag{1.111}$$

2. **A criterion for the singularity of $F(x, r)$.** 2.1. We have seen that if the components $r_1, r_2, \cdots, r_n, \cdots$ of r are independent over the numbers $\pm 1, 0$, in some strong sense, then $F(x, r)$ is necessarily absolutely continuous. We shall now take the opposite viewpoint. We shall assume the presence of an evergrowing number of relations and prove that the singularity of $F(x, r)$ necessarily follows.

Clearly these criteria may leave a wide gap in the general case. Nevertheless, in the case $r = (\beta, \beta^2, \cdots, \beta^n, \cdots)$ no examples are known which do not fall within the reach of one of these two criteria.

It is probably the case that the sequence $\beta, \beta^2, \cdots, \beta^n, \cdots$ has such properties of rigidity that the function $F(x, \beta)$ may be either singular in a bad way or absolutely continuous in some tame way.

2.2. Given a sequence $r = (r_1, r_2, \cdots, r_n, \cdots)$ and an integer $p > 1$ we shall decompose the random variable $y(w, r) = \sum_{n=1}^{\infty} \pm r_n$[13] in the sum

$$y(w, r) = z_1 + z_2 + \cdots + z_N + \cdots$$

where

$$z_N = \sum_{n=1}^{p} (\pm 1) r_{(N-1)p+n}.$$

---

[13] By w we denote a sequence $\pm 1, \pm 1, \pm 1, \cdots$.

Let us suppose that the sequence r is such that each random variable z_N takes only $\sigma < 2^p$ values

$$\overset{1}{z}_N, \overset{2}{z}_N, \cdots, \overset{\sigma}{z}_N \qquad (\sigma \text{ independent of } N)(14)$$

with probabilities

$$p^1, p^2, \cdots, p^\sigma \qquad (\text{independent of } N)(14)$$

It will be convenient, for any integer τ, to let D_τ denote the finite probability space consisting of the equally probable elements $1, 2, \cdots, \tau$. We shall also set

$$D_\tau^n = D_\tau \times D_\tau \times \cdots \times D_\tau \qquad (n \text{ times})$$

and again consider all elements equally probable. The space of all sequences $(\pm, \pm 1, \cdots, \pm 1)$ (n times) shall be identified with D_2^n.

2.3. Under our assumptions the sum

$$\zeta_N = z_1 + z_2 + \cdots + z_N$$

originates and obvious map Φ of $D_2^{N_p}$ onto D_σ^N. If $w = (a_1, a_2, \cdots, a_n) \in D_2^{N_p}$ we shall set $z_k(w) = \sum_{n=1}^{p} a_{(k-1)p+n}\, r_{(k-1)p+n}$ and $\Phi w = (i_1, i_2, \cdots, i_N)$ if and only if

$$z_k(w) = \overset{i_k}{z}_k \qquad k = 1, 2, \cdots, N.$$

Let $A \cup B = D_\sigma$, $A \cap B = \varnothing$ be a partition of D_σ and $p_A = \sum_{k \in A} P^k$. For given integers N, q with $1 \leqq q \leqq N$ we define a subset of $D_\sigma^N E_{N,q}$ (depending upon the partition A, B) as follows:

A point $\xi = (i_1, i_2, \cdots, i_N)$ of D_σ^N will be put in $E_{N,q}$ if and only if exactly q of the i_k fall in A. If S is a set containing a finite number of elements, by $\nu(S)$ we shall denote the number of elements of S. We then have that

$$\nu(E_{N,q}) = C_{N,q}[\nu(A)]^q[\sigma - \nu(A)]^{N-q}. \tag{2.31}$$

We shall define a subset $E_{N,q}^{-1}$ of $D_2^{N_p}$ by setting

$$E_{N,q}^{-1} = \{w: \Phi w \in E_{N,q}\}.$$

The probability that $\Phi w \in E_{N,q}$ is given by

$$\Pr[E_{N,q}^{-1}] = C_{N,q} P_A^q (1 - P_A)^{N-q}. \tag{2.32}$$

For a given function $1 < \gamma(N) < N$ we shall set

$$E_N = \bigcup_{q \geq \gamma(N)} E_{N,q}$$

(14) These assumptions may seem rather restrictive, but they are adopted to simplify the exposition that follows. Similar results can be obtained by replacing these equalities with suitable inequalities.

and

$$E_N^{-1} = \bigcup_{q \geq \gamma(N)} E_{N,q}^{-1}.$$

Since the sets $E_{N,q}$, $E_{N,q}^{-1}$ of D_σ^n and $D_2^{N_p}$ are clearly disjoint, in view of (2.31) and (2.32) we have that

$$\nu(E_N) = \sum_{q \geq \gamma(N)} C_{N,q}[\nu(A)]^q[\sigma - \nu(A)]^{N-q}, \tag{2.33}$$

$$\Pr(E_N^{-1}) = \sum_{q \geq \gamma(N)} C_{N,q} P_A^q (1 - P_A)^{N-q}. \tag{2.34}$$

2.4. The equalities (2.33) and (2.34) yield immediately a criterion for the singularity of $F(x, r)$ which applies in the case that $\sum_{n=1}^{\infty} r_n < \infty$. In fact we have the following

THEOREM 2.4. *If the partition A and the sequence $\gamma(N)$ can be chosen in such a way that*

$$\lim_{N \to \infty} \left(\sum_{k=N_{p+1}}^{\infty} r_k \right) \sum_{q \geq \gamma(N)} C_{N,q}[\nu(A)]^q[\sigma - \nu(A)]^{N-q} = 0, \tag{2.41}$$

$$\limsup_{N \to \infty} \sum_{q \geq \gamma(N)} C_{N,q} P_A^q (1 - P_A)^{N-q} > 0 \tag{2.42}$$

then $F(x, r)$ is necessarily singular.

Proof. Considering each $D_2^{N_p}$ and its subsets naturally imbedded in $D_2^{\infty} = D_2 \times D_2 \times \cdots$ we can define without abuse of language

$$y(E_N) = \{y : y = y(w, r),\ w \in E_N\}.$$

Since $y \in y(E_N)$ only if $|y(w) - \zeta_N(w)| \leqq \sum_{k=N_{p+1}}^{\infty} r_k$ and $w \in E_N$ in view of (2.33) the Lebesgue measure of $y(E_N)$ will satisfy the inequality

$$m[y(E_N)] \leqq 2 \left(\sum_{k=N_{p+1}}^{\infty} r_k \right) \sum_{q \geq \gamma(N)} C_{N,q}(\nu(A))^q(\sigma - \nu(A))^{N-q}.$$

On the other hand the probability that $y(w, r) \in y(E_N)$ is certainly not less than the probability that $\Phi w \in E_N$ so that in view of (2.34) we have

$$\Pr(y(E_N)) = \int_{y(E_N)} dF(x, r) \geqq \sum_{q \geq \gamma(N)} C_{N,q} P_A^q (1 - P_A)^{N-q}.$$

Thus the singularity of $F(x, r)$ follows readily from the assumptions.

2.5. The theorem of last section can be strengthened to include the case in which $\sum_{n=1}^{\infty} r_n$ diverges. To this end we shall need a useful lemma. Let y_n, y, $z_n = y - y_n$, $F(x)$ and $F_n(x)$ be defined as in the beginning of §1.10. Then the following holds:

LEMMA 2.5. *If A_n is any sequence decreasing to zero, then $F(x)$ has a singular part only if the following condition is satisfied:*

Condition S. *There exists a $\gamma>0$ such that for any integer n_0 and $\epsilon>0$ it is possible to find a set of integers S such that for some $n>n_0$*

$$\text{(2.51)} \qquad \text{(a)} \quad \sum_{k\in S} \Delta F_n(k, A_n) > \gamma$$

$$\text{(2.52)} \qquad \text{(b)} \quad \nu(S) = \sum_{k\in S} 1 \leqq \epsilon/A_n.$$

On the other hand if

$$\text{(2.53)} \qquad \liminf_{n\to\infty} A_n^2/E(z_n^2) > 0$$

then condition S *is also sufficient to guarantee the singularity of $F(x)$.*

Proof. If $F(x)$ has a singular part, there exists a $\gamma>0$ such that for any ϵ there is a disjoint finite union of open intervals $0=\bigcup_i I_i$ ($I_i=(a_i, b_i)$) such that $\int_0 dF(x)>\gamma$, $\sum_i (b_i-a_i)<\epsilon$. Since $F(x)$ is a uniform limit of $F_n(x)$ if we define $k_{i,n}^a=(\sup k$ such that $kA_n\leqq a_i)$, and $k_{i,n}^b=(\inf k$ such that $kA_n\geqq b_i)$ we get that

$$k_{i,n}^b \to b_i, \qquad k_{i,n}^a \to a_i$$

and therefore, after n is large enough, not only the intervals $(k_{i,n}^a A_n, k_{i,n}^b A_n)$ are disjoint, but if we let $S=\bigcup_i \{k: k_{i,n}^a\leqq k\leqq k_{i,n}^b-1\}$ we have also (2.51) and (2.52).

Suppose now that condition S is satisfied and that (2.53) holds. It is no loss of generality to assume that there is an integer π such that

$$\pi^2 A_n^2 \geqq 2E(z_n^2).$$

By the independence of y_n and $z_n=y-y_n$ we get (as in §1.10) that for any x whatever

$$\text{(2.54)} \qquad F_n(x+\pi A_n) - F_n(x) \leqq 2[F(x+2\pi A_n) - F(x-\pi A_n)].$$

Given a set S let us define $S^{-\pi}$, $S^{-\pi+1}$, $\cdots$, $S^{2\pi}$ by setting

$$S^\mu = \{h: k+\mu = h, k\in S\} \qquad (\mu = -\pi, -\pi+1, \cdots, 2\pi).$$

In view of (2.51) and (2.54) we have that

$$\gamma < \sum_{k\in S} \Delta F_n(k/\pi, \pi A_n) \leqq 2 \sum_{\mu=-\pi}^{2\pi} \sum_{k\in S^\mu} \Delta F(k, A_n).$$

This implies that for at least one μ we must have

$$\sum_{k\in S^\mu} \Delta F(k, A_n) > \gamma/6\pi.$$

Because of (2.52) we get

$$\sum_{k\in S^{\mu}} A_n < \epsilon.$$

This result implies that $F(x)$ is not absolutely continuous. Thus the proof of the lemma is complete.

2.6. With the notation of §2.3 we can state the following strengthened version of Theorem 2.4.

THEOREM 2.6. *If the partition A and the sequence $\gamma(N)$ can be chosen in such a way that*

$$\lim_{N\to\infty}\left(\sum_{k=N_{p+1}}^{\infty} r_k^2\right)^{1/2} \sum_{q\geq\gamma(N)} C_{N,q}(\nu(A))^q(\sigma-\nu(A))^{N-q} = 0, \tag{2.61}$$

$$\limsup_{N\to\infty} \sum_{q\geq\gamma(N)} C_{N,q}P_A^q(1-P_A)^{N-q} > 0 \tag{2.62}$$

then $F(x, r)$ is necessarily singular.

Proof. We shall set $A_n=(\sum_{k=N_{p+1}}^{\infty} r_k^2)^{1/2}$, $n=N_p$. For each N we let $S_N=\{k\colon [kA_n,\ kA_n+A_n)\ni\zeta_N(w)$ for some $w\in E_N\}$. At worst each interval $(kA_n,\ kA_n+A_n]$ may contain only one value of $\zeta_N(w)$; thus in any case

$$\sum_{k\in S_N} 1 \leqq \sum_{q\geq\gamma(N)} C_{N,q}(\nu(A))^q(\sigma-\nu(A))^{N-q}.$$

On the other hand the probability of $\zeta_N(w)$ falling in an interval $(kA_n, kA_n+A_n]$ with $k\in S_N$ is certainly not less than that of $\zeta_N(w)$ falling in the same interval and in addition $w\in E_N$. This implies that

$$\sum_{k\in S_N} \Delta F_n(k, A_n) \geqq \sum_{q\geq\gamma(N)} C_{N,q}(P_A)^q(1-P_A)^{N-q}.$$

Thus the conclusion of the theorem can be deduced from Lemma 2.5.

2.7. We can give the conditions (2.61) and (2.62) a slightly weaker but more explicit form.

In fact, it is easy to see that for a given $0<\beta<1$ the condition

$$\lim_{N\to\infty} \sum_{q\geq\gamma(N)} C_{N,q}\beta^q(1-\beta)^{N-q} > 0$$

pretty much determines the growth of $\gamma(N)$. For our purposes, given a partition A, there is no need to let $\gamma(N)$ grow any faster than

$$\gamma(N) = P_AN + QN^{1/2} \tag{2.71}$$

for some $Q>0$. This will assure the validity of (2.62).

On the other hand, from familiar estimates on the binomial distribution we obtain that, if $\gamma(N)$ is given by (2.71) and $\alpha<P_A<1$

$$\sum_{q \geq \gamma(N)} C_{N,q}\alpha^q(1-\alpha)^{N-q} = O\left(\left([\alpha/P_A]^{P_A}\left[\frac{1-\alpha}{1-P_A}\right]^{1-P_A}\right)^N\left[\frac{\alpha}{P_A}\,\frac{1-P_A}{1-\alpha}\right]^{QN^{1/2}}\right). \tag{2.72}$$

Now, given a set of probabilities $p^1, p^2, \cdots, p^\sigma$ and supposing that they are not all equal, we can always pick a set of indices in such a way that

$$P_A = \sum_{i \in A} p^i > \frac{\nu(A)}{\sigma}. \tag{2.73}$$

For such a choice of A, setting $\alpha = \nu(A)/\sigma$ in (2.72), from Theorem 2.6 we deduce

THEOREM 2.7. *If the partition A and the number $Q>0$ can be chosen in such a way that*

$$\lim_{N\to\infty} \sigma^N\left(\sum_{k=N_{p+1}}^{\infty} r_k^2\right)^{1/2}\left[\left(\frac{\nu(A)}{\sigma P_A}\right)^{P_A}\left(\frac{\sigma-\nu(A)}{\sigma-\sigma P_A}\right)^{1-P_A}\right]^N \cdot\left[\frac{\nu(A)(1-P_A)}{P_A(\sigma-\nu(A))}\right]^{QN^{1/2}} = 0, \tag{2.74}$$

then the function $F(x, r)$ is necessarily singular.

In any case, if

$$\sigma^N\left(\sum_{k=N_{p+1}}^{\infty} r_k^2\right)^{1/2} = o(1) \tag{2.75}$$

from Theorem 2.6 it is easy to deduce that $F(x, r)$ is singular. However, this result is quite trivial, for if (2.75) is known to hold, it can be readily inferred that the range of the random variable $\sum_{\nu=1}^{\infty} \pm r_\nu$ is a set of measure zero.

Stronger results can be deduced from Theorem 2.7 when the probabilities $p^1, p^2, \cdots, p^\sigma$ are not all equal. In fact, in this case, in view of (2.73), the product

$$\sigma^N\left(\sum_{k=N_{p+1}}^{\infty} r_k^2\right)^{1/2}$$

may even grow exponentially without affecting the singularity of $F(x, r)$.

2.8. As a first example we shall study the function $F(x, 1/\alpha)$ when $1<\alpha<2$ is a Pisot-Vijayaraghavan number. We can show that in this case the singularity of $F(x, 1/\alpha)$ can be attributed to the fact that the numbers

$$\alpha, \alpha^2, \cdots, \alpha^n$$

satisfy (as $n\to\infty$) a rapidly growing number of linear relations with coefficients ± 1 or 0.

In fact, when $1<\alpha<2$ is a Pisot-Vijayaraghavan number, Lemma 1.6 yields the known result (see [11]) that α satisfies polynomial equations with integer coefficients and height 1.

On the other hand, from Lemma 1.51 it is easy to deduce that the number of distinct values of $\pm\alpha\pm\alpha^2\pm\cdots\pm\alpha^p$ cannot grow any faster than $\gamma\alpha^p$, where γ depends only on α. Thus for a given integer p we get $\sigma\leqq\gamma\alpha^p$. We also obtain

$$\left(\sum_{k=N_{p+1}}^{\infty} r_k^2\right)^{1/2} \leqq L\alpha^{-N_p}$$

where L is a suitable constant.

Finally, it turns out that for any Pisot-Vijayaraghavan number $1<\alpha<2$, by a suitable choice of the integer p and the partition A, we can make the quantity

$$\left(\frac{\nu(A)}{\sigma P_A}\right)^{P_A}\left(\frac{1-\nu(A)/\sigma}{1-P_A}\right)^{1-P_A}$$

arbitrarily small([15]); in particular less than γ. Thus Theorem 2.7 applies.

2.9. Another interesting example is obtained in the case that r is a sequence of the type

$$r = (\rho_1, \rho_1, \cdots, \rho_1; \rho_2, \rho_2, \cdots, \rho_2; \cdots; \rho_N, \rho_N, \cdots, \rho_N; \cdots)$$

where each term appears repeated the same number of times, say p times for some $p\geqq 2$. Setting $\rho=(\rho_1, \rho_2, \cdots, \rho_N, \cdots)$ we see that in this case our random variable $y(w, r)$ decomposes in the sum

$$y(w, r) = y_1(w, \rho) + y_2(w, \rho) + \cdots + y_p(w, \rho)$$

where $y_i(w, \rho)=\sum_{n=1}^{\infty}\pm\rho_n$ $(i=1, 2, \cdots, p)$ are independent and equally distributed random variables. Therefore

$$F(x, r) = F(x, \rho)\times F(x, \rho)\times\cdots\times F(x, \rho) \qquad (p \text{ times}).$$

As an application of our considerations we obtain estimates on the number of times we can convolute a given singular distribution $F(x, \rho)$ with itself and still be sure that the resulting convolution will be singular. In fact, using the notation of §2.2, we set

$$z_N = \pm\rho_N \pm \rho_N \pm \cdots \pm \rho_N \qquad (p \text{ times})$$

and observe that each z_N takes only the $p+1$ values

$$z_N^k = (-p+2k)\rho_N \qquad (k = 0, 1, \cdots, p)$$

with respective probabilities

([15]) This result can be easily deduced from Lemma 2.5.

$$p^k = \frac{1}{2^p} C_{N,k}.$$

Thus Theorem 2.7 applies.

It is easy to see that, to get the best results, for a given p the following extremum problem has to be solved. Namely, an integer a has to be found which minimizes the quantity

$$\left(\frac{P_a}{p+1-a}\right)^{P_a}\left(\frac{1-P_a}{2a}\right)^{1-P_a}$$

where

$$P_a = \sum_{k=a}^{p-a} \frac{1}{2^p} C_{p,k}.$$

Without solving this extremum problem we see that Theorem 2.7 improves upon the condition

$$\frac{1}{(p+1)^N}\left(\sum_{k=N+1}^{\infty} \rho_N^2\right)^{1/2} = o(1)$$

which assures that the range of $y(w, r)$ is a set of measure zero.

The implications of Theorem 2.7 for this particular example can be reassumed in the following statement (which is readily established by use of standard estimates on the binomial distribution).

There exists a sequence of numbers $\beta_1, \beta_2, \cdots, \beta_p$ *which can be taken so that*

$$\frac{1}{\beta_p} = o((p+1)^\sigma) \qquad \text{for any } \sigma > 1/2$$

and such that if the sequence $\rho = (\rho_1, \rho_2, \cdots, \rho_N, \cdots)$ *satisfies the condition*

$$\left(\sum_{k=N+1}^{\infty} \rho_k^2\right)^{1/2} \beta_p^N = O(\gamma^{N^{1/2}}) \quad \text{as} \quad N \to \infty$$

for some $p \geqq 2$ *and* $\gamma > 1$, *then the distribution function*

$$F^p(x, \rho) = F(x, \rho) \times F(x, \rho) \times \cdots \times F(x, \rho) \qquad (p \text{ times})$$

is singular.

The reader may refer to [3] for a further application of Theorem 2.7.

References

1. P. Erdös, *On a family of symmetric Bernoulli convolutions*, Amer. J. Math. **61** (1939), 974–976.

2. ———, *On the smoothness properties of a family of Bernoulli convolutions*, Amer. J. Math. **62** (1940), 180–186.

3. A. Garsia, *On the distribution function of a geometric series whose terms have random changes of sign*, Bell Telephone Laboratories Technical Memorandum File, 1959.

4. B. Jessen and A. Wintner, *Distribution functions and the Riemann zeta function*, Trans. Amer. Math. Soc. **38** (1935), 48–88.

5. J. P. Kahane and R. Salem, *Sur la convolution d'une infinité de distributions de Bernoulli*, Colloq. Math. **6** (1958), 193–202.

6. S. Karlin, *Some random walks arising in learning models*. I, Pacific J. Math. **3** (1953), 725–756.

7. J. G. Kemeny and J. L. Snell, *Markov processes in learning theory*, Psychometrika **22** (1957), 221–230.

8. R. Kershner and A. Wintner, *On symmetric Bernoulli convolutions*, Amer. J. Math. **57** (1935), 541–548.

9. C. Pisot, *La répartition modulo un et les nombres algébriques*, Ann. Scuola Norm. Sup. Pisa **2** (1938), 205–248.

10. C. Pisot and J. Dufresnoy, *Sur un ensemble fermé de nombres algébriques*, Ann. Sci. Ecole Norm. Sup. **98** (1953), 105–133.

11. C. Pisot and J. Hugot, *Sur certains entiers algébriques*, C. R. Acad. Sci. Paris **246** (1958), 2831–2832.

12. S. O. Rice, *Statistical properties of the response of a resonant circuit to a train of random pulses*, Bell Telephone Laboratories Technical Memorandum File 36676-6.

13. R. Salem, *A remarkable class of algebraic integers, proof of a conjecture of Vijayaraghavan*, Duke Math. J. **11** (1944), 103–108. (See also: R. Salem, *Sets of uniqueness and sets of multiplicity*, Trans. Amer. Math. Soc. **54** (1941), 218–228.)

14. C. L. Siegel, *Algebraic integers whose conjugates lie in the unit circle*, Duke Math. J. **11** (1944), 597–602.

UNIVERSITY OF MINNESOTA,
MINNEAPOLIS, MINNESOTA