The Annals of Mathematical Statistics
1971, Vol. 42, No. 6, 1922–1929

RANDOM VARIABLES WITH INDEPENDENT BINARY DIGITS

BY GEORGE MARSAGLIA

McGill University

Let $X = .b_1b_2b_3\cdots$ be a random variable with independent binary digits b_n taking values 0 or 1 with probability p_n and $q_n = 1-p_n$. When does X have a density? A continuous density? A singular distribution? This note gives necessary and sufficient conditions for the distribution of X to be: discrete: $\Sigma \min(p_n, q_n) < \infty$; singular: $\Sigma_m^\infty [\log(p_n/q_n)]^2 = \infty$ for every m; absolutely continuous: $\Sigma_m^\infty [\log(p_n/q_n)]^2 < \infty$ for some m. Furthermore, X has a density that is bounded away from zero on some interval if and only if $\log(p_n/q_n)$ is a geometric sequence with ratio $\frac{1}{2}$ for $n > k$, and in that case the fractional part of 2^kX has an exponential density (increasing or decreasing with the uniform a special case).

1. Introduction. It is well known that one can construct a uniform random variable by choosing the binary digits with successive flips of a good coin, ($p = \frac{1}{2}$). Such considerations date back to the beginnings of probability theory—indeed, to the development of measure and integration theory.

For bad coins, $0 < p < 1$, $p \neq \frac{1}{2}$, the resulting number has a distribution that is continuous but singular, as it is concentrated on a set of Lebesgue measure zero. This note is concerned with the case where the binary digits are independent, but not identically distributed. Are there any interesting random variables that arise from this situation? It turns out that there are some interesting singular distributions, and that there are distributions which have densities. This note will show that there is essentially one conventional type density that can arise this way—the exponential (increasing or decreasing, with the uniform a special case), if by conventional we mean a density that is positive on some interval. We will also find necessary and sufficient conditions that the distribution be singular. If it is not singular, it will be absolutely continuous. The conclusion is that independent binary digits lead to one of three possibilities:

(i) A singular distribution. This happens if and only if the series $\sum_{n=m}^\infty \log^2(p_n/q_n)$ diverges for every m. Some interesting continuous but singular distributions arise. See Section 3. A special, but uninteresting, case is the discrete distribution arising when $p_nq_n = 0$ for all suitably large n. There are non-trivial discrete distributions, when $\sum \min(p_n, q_n) < \infty$. See Section 4.

(ii) A piecewise-exponential density, with pieces equally spaced and of similar shape. This happens only when the tail of the sequence $\log(p_n/q_n)$ is geometric with ratio $\frac{1}{2}$. It is the only way to get a distribution which has a positive derivative on some interval. See Section 2.

Received February 9, 1970; revised November 16, 1970.

(iii) A distribution with a density, but a strange density that vanishes at least once in every interval. This will happen if the tail of $\sum \log^2 (p_n/q_n)$ converges but is not geometric with ratio $\frac{1}{2}$.

2. Distributions with reasonable densities. The most interesting case seems to be the assignment of probabilities to the bits so that the resulting random variable has a conventional density function. We will show that there is essentially only one way to do this. The general statement is Theorem 2 below, but by shifting the binary decimal point to the right far enough we may assume we are dealing only with the fractional part taking values on the unit interval, and in that case we can formulate the basic requirement as follows:

THEOREM 1. *If X is a random variable on the unit interval with independent binary digits,*

$$X = .b_1 b_2 b_3 \cdots = \sum_{n=1}^{\infty} b_n 2^{-n},$$

b's independently 0 *or* 1, *and if the distribution function of X, say $F(x)$, has a positive derivative at $\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \cdots$ that is, $F'(.1)$, $F'(.01)$, $F'(.001)$, $\cdots$ all exist and are positive, then X has an exponential distribution with density*

$$f(x) = \frac{\beta e^{\beta x}}{e^{\beta} - 1}, \qquad 0 < x < 1, \ -\infty < \beta < \infty$$

and the probabilities for the bits of X are given by the formula

$$P[b_n = 0] = \frac{1}{1 + e^{\beta/2^n}} \qquad P[b_n = 1] = \frac{e^{\beta/2^n}}{1 + e^{\beta/2^n}}.$$

PROOF. Represent the probabilities for the bits of X as follows:

$$P[b_n = 0] = \frac{1}{1 + e^{c_n}} \qquad P[b_n = 1] = \frac{e^{c_n}}{1 + e^{c_n}}.$$

We will get a relation between the c's by representing $F'(.1)$ as the limit of two sequences of difference quotients:

$$(1) \qquad \frac{F(.101) - F(.1)}{2^{-3}}, \qquad \frac{F(.1001) - F(.1)}{2^{-4}}, \qquad \frac{F(.10001) - F(.1)}{2^{-5}}, \cdots$$

and

$$(2) \qquad \frac{F(.1) - F(.01)}{2^{-2}}, \qquad \frac{F(.1) - F(.011)}{2^{-3}}, \qquad \frac{F(.1) - F(.0111)}{2^{-4}}, \cdots$$

The general term of sequence (1) has the form

$$\frac{e^{c_1}}{\prod_{i=1}^{n} \left(\frac{1 + e^{c_i}}{2} \right)}$$

and the general term of sequence (2) has the form

$$\frac{\exp[c_2+c_3+\cdots+c_n]}{\prod_{i=1}^{n}\left(\frac{1+e^{c_i}}{2}\right)}.$$

Since $F'(.1)$ exists and is positive, we conclude that the infinite product converges, that

$$F'(.1)=\frac{e^{c_1}}{\prod_{1}^{\infty}\left(\frac{1+e^{c_i}}{2}\right)}=\frac{e^{c_2+c_3+\cdots}}{\prod_{1}^{\infty}\left(\frac{1+e^{c_i}}{2}\right)}$$

and hence $c_1 = c_2+c_3+\cdots$.

A similar argument on $F'(.01)$ shows that $c_2 = c_3+c_4+\cdots$; on $F'(.001)$ shows $c_3 = c_4+c_5+\cdots$ and thus we conclude that there is a β such that $c_1 = \beta/2, c_2 = \beta/4$, $c_3 = \beta/8, \cdots$. This provides the formulas for the probabilities of bits of X as given in the theorem. We still must show that if the bits of X have those probabilities, then X has an exponential density with parameter β. (Note that β can be either positive or negative, with $\beta = 0$ giving the uniform density.)

Writing

$$X=\frac{b_1}{2^1}+\frac{b_2}{2^2}+\frac{b_3}{2^3}+\cdots$$

we express the characteristic function of X as an infinite product

$$\prod_{k=1}^{\infty}\left[\frac{1+e^{(\beta+it)/2^k}}{1+e^{\beta/2^k}}\right].$$

Using the relation

$$1-e^z=(1+e^{z/2})(1-e^{z/2})=(1+e^{z/2})(1+e^{z/4})(1-e^{z/4})=\cdots$$

we have

$$\prod_{k=1}^{n-1}(1+e^{z/2^k})=\frac{1-e^z}{1-e^{z/2^n}}$$

and hence

$$\prod_{k=1}^{n-1}\left[\frac{1+e^{z/2^k}}{1+e^{\beta/2^k}}\right]=\left[\frac{1-e^z}{1-e^{\beta}}\right]\left[\frac{1-e^{\beta/2^n}}{1-e^{z/2^n}}\right].$$

The right side converges to

$$\left[\frac{1-e^z}{1-e^{\beta}}\right]\left[\frac{\beta}{z}\right]$$

which, with $z = \beta+it$, is the characteristic function of X with density $\gamma e^{\beta x}$ on $0 < x < 1$.

To get a more general theorem, we note that if the distribution of Y, say $F(y)$, has a derivative that exists and is positive on some interval, $F'(y) > 0$, $a < y < b$ then there are integers r and k such that

$$a \leqq \frac{r}{2^k} < y < \frac{r+1}{2^k} \leqq b$$

and hence the distribution of the fractional part of $2^k Y$ has a derivative that exists and is positive on the unit interval; the above theorem applies, and we have:

THEOREM 2. *If Y is a random variable with independent binary digits, and if Y has a distribution whose derivative exists and is positive on some interval, $F'(y) > 0$, $a < y < b$, then Y may be scaled by a power of 2, that is, its binary decimal may be relocated, so that its fractional part is exponentially distributed with density*

$$\frac{\beta e^{\beta x}}{e^{\beta} - 1} \qquad 0 < x < 1.$$

(For some β, $-\infty < \beta < \infty$, with the uniform density corresponding to $\beta = 0$.)

In other words, Y may be represented in the form $2^k(M + X)$ where M is a random integer, independent of the fractional part X having density $\gamma e^{\beta x}$, $0 < x < 1$.

3. Singular distributions. Let $p_n = P[b_n = 0]$. If some subsequence of the p's converges to a value other than $\frac{1}{2}$, then the distribution of $X = .b_1 b_2 b_3 \cdots$ will be singular, for it will be concentrated on a set of Lebesgue measure 0. It is easy to get many representations of singular variates in this way. In particular, one can get two singular distributions whose convolution has an exponential or a uniform distribution, by writing

$$X_1 = .0b_2 0b_4 0b_6 0 \cdots$$

$$X_2 = .b_1 0b_3 0b_5 0b_7 \cdots$$

where the b's take values with probabilities given by Theorem 1. Then $X_1 + X_2$ has an exponential density $\gamma e^{\beta x}$ on $0 < x < 1$.

To get two singular distributions whose convolution is the ordinary exponential density $\alpha e^{-\alpha x}$, $0 < x < \infty$, write

$$X = \cdots d_3 d_2 d_1 d_0 . d_{-1} d_{-2} d_{-3} \cdots$$

where

$$P[d_k = 0] = \frac{1}{1 + e^{\alpha 2^k}}$$

and

$$X_1 = \cdots d_3 0 d_1 0 . d_{-1} 0 d_{-3} 0 d_{-5} \cdots$$

$$X_2 = \cdots d_4 0 d_2 0 d_0 . 0 d_{-2} 0 d_{-4} 0 \cdots.$$

We now turn to the general question of when the distribution of $X = .b_1b_2b_3\cdots$ is singular, where b_n takes values 0 or 1 with probabilities p_n and q_n. If p_n does not converge to $\frac{1}{2}$ then the distribution of X will be singular, but what happens when $p_n \to \frac{1}{2}$ but not according to the formulas of Theorem 1? We know that X cannot have a continuous density but if $p_n \to \frac{1}{2}$ very very quickly we might expect that X will have some kind of a density, though a weird one. The answer is yes, there is always a density if $p_n \to \frac{1}{2}$ quickly enough.

We first point out that there is no in-between; the distribution of X is either singular or absolutely continuous. This follows from a theorem of Jessen and Wintner (1935) that any convergent series of independent discrete random variables has a pure law, either singular (including discrete) or absolutely continuous. The theorem uses the zero-one law; for an excellent elementary account see Breiman (1968), page 49.

We will show that the distribution of X is singular (including discrete) if and only if $\sum_{n=m}^{\infty} \log^2 (p_n/q_n) = \infty$ for every m. To prove this result we need a preliminary lemma which gives a formula for $F'(x)$ when it exists:

LEMMA 1. *Let* $X = .b_1b_2b_3\cdots$ *have independent binary digits with*

$$P[b_n = 0] = p_n, \qquad P[b_n = 1] = q_n.$$

Let F *be the distribution function of* X. *If* F' *exists at* $v = .v_1v_2v_3\cdots$ *then*

$$F'(v) = [2g_1(v_1)][2g_2(v_2)][2g_3(v_3)]\cdots \tag{3}$$

where $g_n(0) = p_n$ *and* $g_n(1) = q_n$.

PROOF. Since $F'(v)$ exists it can be represented

$$F'(v) = \lim_{s,t\to v;\, s<v<t} \frac{F(t)-F(s)}{t-s}$$

and we may write

$$F'(.v_1v_2v_3\cdots) = \lim_{n\to\infty} 2^n[F(.v_1v_2\cdots v_n + 2^{-n}) - F(.v_1v_2\cdots v_n)].$$

Then (3) follows from the fact that the expression in brackets is $g_1(v_1)g_2(v_2)\cdots g_n(v_n)$.

THEOREM 3. *Let* $X = .b_1b_2b_3\cdots$ *have independent binary digits with* b_n *taking values* 0 *or* 1 *with probabilities* p_n *and* q_n. *In order that* X *have a singular distribution function (derivative equals zero almost everywhere) it is necessary and sufficient that for every positive integer* m,

$$\sum_{n=m}^{\infty} [\log (p_n/q_n)]^2 = \infty.$$

If, on the other hand, $\sum_{n=m}^{\infty} \log^2 (p_n/q_n)$ *is finite for some* m, *then the distribution of* X *is absolutely continuous, but with a density that vanishes at least once in every interval, except when the sequence* $\log(p_n/q_n)$ *has the form* $\beta, \beta/2, \beta/4, \beta/8, \cdots$ *for* $n \geqq k$, *and in that case the fractional part of* 2^kX *has density* $\gamma e^{\beta x}$ *(uniform density when* $\beta = 0$).

PROOF. Let F be the distribution function. It has a finite derivative almost everywhere. Thus from Lemma 1, for almost all $x = .x_1x_2x_3 \cdots$ we have F' expressed as an infinite product:

$$F'(.x_1x_2x_3\cdots) = [2g_1(x_1)][2g_2(x_2)][2g_3(x_3)]\cdots, \tag{4}$$

where $g_n(0) = p_n$ and $g_n(1) = q_n$.

Another interpretation of the fact that F has a derivative almost everywhere is to say that if $.v_1v_2v_3 \cdots$ is chosen at random with the v's independently 0 or 1 with probability $\frac{1}{2}$, then with probability 1 the product in (3) converges to a (possibly zero) constant. According to a standard theorem on infinite products, (see, e.g., Knopp (1948), page 223), the tail of the product in (4) converges to a nonzero constant e^L if and only if for some m,

$$\sum_{n=m}^{\infty} \log [2g_n(x_n)] = L.$$

Thus the question of whether F' is positive almost everywhere or zero almost everywhere hinges on the convergence of the random series

$$\sum_{n=m}^{\infty} \log [2g_n(v_n)],$$

where the v's take values 0 or 1 with probability $\frac{1}{2}$. We apply the three series theorem (see, e.g., Fisz (1963), page 248) after computing

$$E\{\log [2g_n(v_n)]\} = \tfrac{1}{2}\log (4p_nq_n), \qquad \text{Variance} = \tfrac{1}{4}[\log (p_n/q_n)]^2.$$

If the tail of $\sum \log^2 (p_n/q_n)$ converges, so does the tail of $-\sum \log (4p_nq_n)$, for the terms of the former dominate the terms of the latter. (Write $2p_n = 1+t$, $2q_n = 1-t$ then note that $\log^2 [(1+t)/(1-t)]+\log (1-t^2) \geqq 0$ for $-1 < t < 1$.)

Applying the three series theorem to the random series $\sum \log (2g_n(v_n))$ and interpreting the result in terms of the infinite product (4) we conclude: If $\sum_{n=m}^{\infty} \log^2 (p_n/q_n)$ converges for some m, then $F'(x) > 0$ for almost all x and F, being of pure type, is absolutely continuous; if it diverges for all m, then $F'(x) = 0$ for almost all x and hence F is singular.

4. Discrete distributions. The above results do not distinguish between singular distributions that are discrete, continuous, or a mixture of both. The following theorem shows that the distribution of X is either continuous everywhere or purely discrete, and gives conditions:

THEOREM 4. *If $X = .b_1b_2b_3 \cdots$ has independent binary digits, $b_n = 0$ or 1 with probability p_n and q_n, then its distribution function F has a point of increase if and only if*

$$\prod_{n=1}^{\infty} \max (p_n, q_n) > 0, \qquad \textit{or what is the same,} \qquad \sum_{n=1}^{\infty} \min (p_n, q_n) < \infty$$

and in that case F is purely discrete, with jumps at those points $v = .v_1v_2v_3 \cdots$ which differ from $s = .s_1s_2s_3 \cdots$ only in a finite number of binary locations, where $s_n = 0$ or 1 according to whether $p_n \geqq q_n$ or $p_n < q_n$.

PROOF. Once again, using $g_n(0) = p_n$ and $g_n(1) = q_n$ we find that the jump at $F(.v_1v_2v_3\cdots)$ is $\lim_{n\to\infty} F(.v_1v_2\cdots v_n+2^{-n})-F(.v_1v_2\cdots v_n) = g_1(v_1)g_2(v_2)\cdots$ and if $\prod \max(p_n, q_n) = 0$ then F will have no jumps. On the other hand, if $\prod \max(p_n, q_n) > 0$ then F has a jump at s and a jump at every v whose binary expansion has the same tail as s.

If we add the jumps at all v's that agree with s beyond the mth binary place, i.e., $v_{m+1} = s_{m+1}$, $v_{m+2} = s_{m+2}$, $\cdots$ we get $\prod_{n=m+1}^{\infty}\max(p_n, q_n)$ which is as close to 1 as we please. From that we conclude that the sum of the jumps of F is 1.

5. Expansions for bases other than 2. Using the ideas above for the binary expansion we can establish the following general theorem:

THEOREM 5. *Let*

$$X = .d_1d_2d_3\cdots = d_1/k+d_2/k^2+d_3/k^3+\cdots$$

have independent digits in its expansion to the base k. Let d_n take values 0, 1, 2, $\cdots$, $k-1$ *with probability $p_{n1}, p_{n2}, \cdots, p_{nk}$. Then the distribution of X is either purely discrete, purely absolutely continuous or purely continuous singular, and conditions are*:

discrete if and only if $\sum [1-\max(p_{n1}, p_{n2}, \cdots, p_{nk})] < \infty$

absolutely continuous if and only if

$$\sum[(1-kp_{n1})^2+(1-kp_{n2})^2+\cdots+(1-kp_{nk})^2] < \infty.$$

PROOF. Application of the zero-one law assures us that X has a pure law, referring once again to the Jessen-Wintner theorem as given in Breiman (1968), page 49. The condition that X be discrete follows as in Theorem 4 above. To establish absolute continuity we argue as in Theorem 3, that the two series $\sum a_n$ and $\sum s_n^2$ must converge, where a_n and s_n^2 are the average and variance of the k numbers $\log kp_{n1}, \log kp_{n2}, \cdots, \log kp_{nk}$. Let $kp_{nj} = 1+\tau_{nj}$, so that $\sum_{j=1}^{k}\tau_{nj} = 0$. Each ka_n has the form $\sum \log(1+\tau_i)$, and using the Taylor expansion with remainder we have

$$\textstyle\sum_1^k \log(1+\tau_i) = \sum_1^k \tau_i - \frac{1}{2}\sum_1^k \tau_i^2 + o[(\sum_1^k \tau_i^2)^{\frac{3}{2}}].$$

Thus there is a δ such that if $\sum \tau_i = 0$ and $\sum \tau_i^2 < \delta$,

$$.49\textstyle\sum_1^k \tau_i^2 < -\sum_1^k \log(1+\tau_i) < .51\sum_1^k \tau_i^2.$$

It follows that $\sum a_n$ converges if and only if $\sum(\tau_{n1}^2+\cdots+\tau_{nk}^2)$ converges, and the latter is the series in the statement of the theorem. It is easy to show that its convergence implies that of $\sum s_n^2$.

Note that the condition for the binary case, $\sum \log^2(p_n/q_n) < \infty$, may be replaced by $\sum(1-2p_n)^2 < \infty$, as the two series converge or diverge together.

Acknowledgment. I would like to thank Albert W. Marshall and Gordon B. Crawford for stimulating discussions on the problem of independent binary digits.

REFERENCES

BREIMAN, LEO (1968). *Probability*. Addison Wesley, Reading.

FISZ, MAREK (1963). *Probability Theory and Mathematical Statistics*, 3rd ed. Wiley, New York.

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

KNOPP, KONRAD (1948). *Theory and Application of Infinite Series*. Blackie & Son, London.