

- [8] W. LeVeque, *The distribution mod 1 of trigonometric sequences*, Duke Math. J. 20 (1953), pp. 367-374.
 [9] H. Weyl, *Über die Gleichverteilung die Zahlen mod Eins*, Math. Annalen 77 (1916), pp. 313-352.

INSTITUTE OF MATHEMATICS
 HEBREW UNIVERSITY
 Jerusalem, Israel

Received on 27.6.1986

(1659)

Large deviations of sums of independent random variables

by

HUGH L. MONTGOMERY* (Ann Arbor, Mich.) and
 ANDREW M. ODLYZKO (Murray Hill, N.J.)

Dedicated to Pál Erdős on the occasion of his 75-th birthday

1. Statement of results. Our object is to estimate the probability that a sum of independent random variables is large. In this direction we derive a rather precise upper bound, and a corresponding lower bound.

THEOREM 1. Let X_1, X_2, \dots be independent random variables such that $P(X_n = 1) = 1/2$, $P(X_n = -1) = 1/2$. Let $\{r_n\}$ be a non-increasing sequence of non-negative real numbers for which

$$(1) \quad \sigma^2 = \sum_{n=1}^{\infty} r_n^2 < \infty,$$

and put $X = \sum_{n=1}^{\infty} r_n X_n$. If N and V are chosen so that $\sum_{n \leq N} r_n \leq V/2$, then

$$(2) \quad P(X \geq V) \leq \exp\left(-\frac{1}{8} V^2 \left(\sum_{n > N} r_n^2\right)^{-1}\right).$$

If $\sum_{n \leq N} r_n \geq 2V$ then

$$(3) \quad P(X \geq V) \geq 2^{-22} \exp\left(-120 V^2 \left(\sum_{n > N} r_n^2\right)^{-1}\right).$$

Also, if $\sum_{n \leq N} r_n \geq V$ then

$$(4) \quad P(X \geq V) \geq 2^{-N-1}.$$

* Research supported in part by National Science Foundation Grant NSF DMS 85-02804.



The upper bound (2) was proved earlier by Saltzberg [8]. We include the easy proof, since it is short and the inequalities used in this proof are used in the proof of (3) as well.

By Kolmogorov's three series theorem we see that condition (1) ensures that the series defining X converges a.e. It is well known (see Petrov [6], p. 58) that if $V \geq 0$ then

$$(5) \quad P(X \geq V) \leq \exp(-V^2/(2\sigma^2)).$$

This is sharp for $V \approx \sigma$ if σ is large compared to $\max_n r_n$, but otherwise $P(X \geq V)$ is significantly smaller. Since $\sum_{n>N} r_n^2 \rightarrow 0$ as $N \rightarrow \infty$, we see from (2) that $P(X \geq V)$ tends to 0 more quickly as $V \rightarrow \infty$ than it would if X were normally distributed. As the X_n are symmetrically and identically distributed, the requirement that the r_n be positive and nonincreasing does not occasion any loss of generality. From Theorem 1 we see that

$$\exp(-c_1 V^4) \leq P(\sum_n X_n/n^{3/4} \geq V) \leq \exp(-c_2 V^4)$$

for $V \geq 1$. In this situation the lower bounds (3) and (4) are comparable, but if $\sum r_n^2$ converges slowly, e.g. $r_n = n^{-1/2}(\log n)^{-1}$, then (3) is superior to (4). On the other hand, if $\sum r_n$ diverges slowly, then (3) is inferior to (4) and (2) can be refined by taking more care in the choice of parameters. For example, the method we use to derive (2) can be used to show that

$$P(\sum_n X_n/n \geq V) \leq \exp(c_3 e^V)$$

for $V \geq 0$, while (4) gives

$$P(\sum_n X_n/n \geq V) \geq \exp(c_4 e^V)$$

for $V \geq 0$. S.O.Rice [7] has determined these probabilities for small V . In general, when the r_n decrease in a regular way, an asymptotic expansion of $P(X \geq V)$ as $V \rightarrow \infty$ can be determined by the saddle point method.

R.Monach [5] has calculated similar probabilities in connection with the distribution of the error term in the prime number theorem and with the distribution of $\arg L(1, \chi)$ for Dirichlet characters $\chi \pmod q$. Chowla and Erdős [1] proved that if $s > 3/4$ is fixed then the numbers

$$L_d(s) = \sum_{n=1}^{\infty} \left(\frac{d}{n}\right) n^{-s}$$

have a limiting distribution in the sense that there is a function $F(s, V)$ such that

$$\lim_{X \rightarrow \infty} \frac{2}{X} \text{card} \{d: 0 < d \leq X, d \equiv 0 \text{ or } 1 \pmod 4, d \neq s^2, L_d(s) \leq V\} = F(s, V).$$

Elliott [2] extended the range of validity to $s > 1/2$, and established corresponding results for complex s for which $\text{Re } s > 1/2$. From his analysis and Theorem 1 it can be shown that there are constants $a_i = a_i(s)$ such that if $1/2 < s < 1$ then

$$(6) \quad \exp(-a_1 (\log V)^{1/(1-s)} (\log \log V)^{s/(1-s)}) < 1 - F(s, V) < \exp(-a_2 ((\log V)^{1/(1-s)} (\log \log V)^{s/(1-s)}))$$

for $V \geq 4$. Moreover, these inequalities remain valid with $1 - F(s, V)$ replaced by $F(s, 1/V)$.

Concerning other independent random variables, we note that (5) depends only on the fact that $E(e^{\lambda X_n}) \leq \exp(\lambda^2/2)$. The sharper bound (2) requires additionally that $|X_n| \leq 1$. Our method yields the following more general result, which we state without proof.

THEOREM 2. For $n = 1, 2, \dots$ let Y_n be independent real valued random variables such that $E(Y_n) = 0$ and $|Y_n| \leq 1$. Suppose there is a constant $c > 0$ such that $E(Y_n^2) \geq c$ for all n . Put $Y = \sum r_n Y_n$ where $\sum r_n^2 < \infty$. If $\sum_{|r_n| \geq \alpha} |r_n| \leq V/2$, then

$$P(Y \geq V) \leq \exp(-\frac{1}{16} V^2 (\sum_{|r_n| < \alpha} r_n^2)^{-1}).$$

If $\sum_{|r_n| \geq \alpha} |r_n| \geq 2V$, then

$$P(Y \geq V) \geq a_1 \exp(-a_2 V^2 (\sum_{|r_n| < \alpha} r_n^2)^{-1}).$$

Here $a_1 > 0$ and $a_2 > 0$ depend only on c .

D. Joyner [3] has used Theorem 2 to estimate the asymptotic distribution of $|\zeta(\sigma + it)|$ for given σ , $1/2 < \sigma < 1$. His result is similar to the estimate (6).

We derive our main results from simple inequalities for the characteristic functions of the random variables involved. In §4 we indicate how these results can instead be derived from inequalities for moments. This latter approach is convenient when investigating complex valued random variables, or random variables which are only approximately independent.

2. Basic lemmas. We employ the following elementary inequalities (see Kahane [4], p. 6).

LEMMA 1: If $Z \in L^1(\Omega)$ and $Z \geq 0$, then

$$P(Z \geq aE(Z)) \leq 1/a$$

for all $a > 0$. If $Z \in L^2(\Omega)$ and $0 < a < 1$, then

$$P(Z \geq aE(Z)) \geq (1-a)^2 E(Z)^2/E(Z^2).$$

Clearly $E(e^{\lambda X_n}) = \cosh \lambda$. Bounds for this quantity are provided by
 LEMMA 2. For any $u \geq 0$,

$$(7) \quad \cosh u \leq e^u$$

and

$$(8) \quad \cosh u \leq e^{u^2/2}.$$

Moreover,

$$(9) \quad \cosh u > e^{u^2/6}$$

for $0 < u \leq 3$, and

$$(10) \quad \cosh u > 2e^{u/2}$$

for $u \geq 3$.

Proof. Clearly $\cosh u = \frac{1}{2}e^u + \frac{1}{2}e^{-u} \leq e^u$ for $u \geq 0$, and

$$\cosh u = \sum_{n=0}^{\infty} \frac{u^{2n}}{(2n)!} \leq \sum_{n=0}^{\infty} \frac{(u^2/2)^n}{n!} = e^{u^2/2},$$

since $n! 2^n \leq (2n)!$. If $0 < v \leq 9$ then $1 + v/2 > e^{v/6}$, and hence

$$\cosh u = \sum_{n=0}^{\infty} \frac{u^{2n}}{(2n)!} > 1 + u^2/2 > e^{u^2/6}$$

for $0 < u \leq 3$. Finally, $\cosh u = \frac{1}{2}e^u + \frac{1}{2}e^{-u} > \frac{1}{2}e^u$, so that

$$\cosh u > \frac{1}{2}e^u > 2e^{u/2}$$

for $u \geq 3$.

3. Proof of Theorem 1. By the first part of Lemma 1 with $Z = e^{\lambda X}$, $a = e^{2V}/E(e^{2\lambda X})$ we see that

$$(11) \quad P(X \geq \lambda) \leq e^{-\lambda V} E(e^{\lambda X}).$$

Since the X_n are independent,

$$(12) \quad E(e^{\lambda X}) = \prod_{n=1}^{\infty} E(e^{\lambda r_n X_n}) = \prod_{n=1}^{\infty} \cosh(\lambda r_n).$$

Let N be arbitrary. We use (7) for $1 \leq n \leq N$, and (8) for $n > N$, to see that

$$(13) \quad E(e^{\lambda X}) \leq \exp\left(\lambda \sum_{n \leq N} r_n + \frac{1}{2}\lambda^2 \sum_{n > N} r_n^2\right).$$

Hence if $\sum_{n \leq N} r_n \leq V/2$ then

$$P(X \geq V) \leq \exp\left(-\frac{1}{2}\lambda V + \frac{1}{2}\lambda^2 \sum_{n > N} r_n^2\right),$$

and (2) follows on taking $\lambda = \frac{1}{2}V\left(\sum_{n > N} r_n^2\right)^{-1}$.

Alternatively, we can derive (2) from (5) by writing

$$X = \sum_{n \leq N} r_n X_n + \sum_{n > N} r_n X_n = X' + X'',$$

say. Then $|X'| \leq V/2$, and we obtain (2) by using (5) to estimate $P(X'' \geq V/2)$.

To derive (3) we use the second part of Lemma 1 with $Z = e^{\lambda X}$ and $a = 1/2$; we choose λ so that

$$(14) \quad \frac{1}{2}E(e^{\lambda X}) = e^{\lambda V}.$$

Such a λ must exist, since both sides above are continuous functions of λ , the left-hand side is smaller than the right when $\lambda = 0$, and the reverse is true when $\lambda \geq 3/r_N$, since by (12) and (10),

$$\begin{aligned} \frac{1}{2}E(e^{\lambda X}) &= \frac{1}{2} \prod_{n=1}^{\infty} \cosh(\lambda r_n) > \frac{1}{2} \prod_{n \leq N} \cosh(\lambda r_n) \\ &> \exp\left(\frac{1}{2}\lambda \sum_{n \leq N} r_n\right) \geq \exp(\lambda V). \end{aligned}$$

By Lemma 1 and (14) we see that

$$P(X \geq V) = P(e^{\lambda X} \geq e^{\lambda V}) \geq \frac{1}{4}E(e^{\lambda X})^2/E(e^{2\lambda X}),$$

and by (14) again this is

$$= e^{2\lambda V}/E(e^{2\lambda X}).$$

By applying (13) to estimate $E(e^{2\lambda X})$, we obtain

$$(15) \quad P(X \geq V) e^{-2\lambda V} \geq \exp\left(-2\lambda \sum_{n \leq M} r_n - 2\lambda^2 \sum_{n > M} r_n^2\right)$$

for any M . We take M so that $\lambda r_n \geq 3$ for $n \leq M$, and $\lambda r_n < 3$ for $n > M$. By (9), (10), (12), and (14) we see that

$$(16) \quad 2e^{\lambda V} = E(e^{\lambda X}) > \prod_{n \leq M} (2e^{\lambda r_n/2}) \prod_{n > M} e^{\lambda^2 r_n^2/6} > \exp\left(\frac{1}{2}\lambda \sum_{n \leq M} r_n + \frac{1}{6}\lambda^2 \sum_{n > M} r_n^2\right).$$

We raise both sides of this inequality to the 12-th power, and multiply the two sides of (15) by these quantities to see that

$$P(X \geq V) 2^{12} e^{10\lambda V} \geq 1.$$

If $\lambda V \leq \log 2$ then we have $P(X \geq V) \geq 2^{-22}$, and we are done. Thus we may suppose that

$$(17) \quad \log 2 \leq \lambda V.$$

To complete our proof of (3) it suffices to show that

$$(18) \quad \lambda \leq 12V \left(\sum_{n>N} r_n^2 \right)^{-1}.$$

To this end we first show that $M \leq N$. If it were the case that $M > N$ then by (16) we would have

$$2e^{\lambda V} > \prod_{n \leq M} (2e^{\lambda r_n/2}) \geq 2 \exp\left(\frac{1}{2} \lambda \sum_{n \leq N} r_n\right),$$

which contradicts our hypothesis that $\sum_{n \leq N} r_n \geq 2V$. Hence $M \leq N$, so that by (16),

$$2e^{\lambda V} > \prod_{n>M} e^{\lambda^2 r_n^2/6} \geq \exp\left(\frac{1}{6} \lambda^2 \sum_{n>N} r_n^2\right),$$

which gives

$$\frac{1}{6} \lambda^2 \sum_{n>N} r_n^2 \leq \lambda V + \log 2.$$

By (17) this is $\leq 2\lambda V$, so we have (18), and the proof of (3) is complete.

To derive (4) we write

$$X = \sum_{n \leq N} r_n X_n + X'.$$

The variable X' is independent of the X_n for $n \leq N$. Also, $X \geq V$ if $X_n = 1$ for $n \leq N$ and $X' \geq 0$. Hence

$$P(X \geq V) \geq P(X' \geq 0) \prod_{n \leq N} P(X_n = 1) = 2^{-N-1}.$$

4. Moment inequalities. To illustrate the use of moments in the present context we now establish the following further result. It is convenient here to suppose that our basic independent random variables are uniformly distributed on the unit circle $|z| = 1$.

LEMMA 3. *Let Z_1, \dots, Z_N be independent random variables, each one uniformly distributed on the unit circle $|z| = 1$ in the complex plane, suppose that $r_1 \geq r_2 \geq \dots \geq r_N \geq 0$, and put $Z = \sum_{n=1}^N r_n Z_n$. Then*

$$(19) \quad E(|Z|^{2k}) \leq k! \sigma^{2k}$$

for every non-negative integer k , where $\sigma^2 = E(|Z|^2) = \sum_{n=1}^N r_n^2$. Moreover, if

$$(20) \quad \sum_{n < k} r_n^2 \leq \frac{1}{2} \sigma^2$$

then

$$(21) \quad E(|Z|^{2k}) \geq 2^{-k} k! \sigma^{2k}.$$

Proof. Since $E(Z^m) = 0$ for all integers $m \neq 0$ we see that

$$E(|Z|^{2k}) = \sum \binom{k}{a_1 a_2 \dots a_N} r_1^{2a_1} r_2^{2a_2} \dots r_N^{2a_N}$$

where the sum is over all N -tuples of non-negative integers a_n for which $a_1 + a_2 + \dots + a_N = k$. Since the multinomial coefficient never exceeds $k!$, the above is

$$\leq k! \sum \binom{k}{a_1 a_2 \dots a_N} r_1^{2a_1} r_2^{2a_2} \dots r_N^{2a_N} = k! \sigma^{2k}.$$

To obtain the lower bound (21) we restrict our attention to those N -tuples for which $a_n = 0$ or 1 for all n . In this case the multinomial coefficient is exactly $k!$, so that

$$(22) \quad \begin{aligned} E(|Z|^{2k}) &\geq k!^2 \sum_{n_1 < n_2 < \dots < n_k} r_{n_1}^2 r_{n_2}^2 \dots r_{n_k}^2 \\ &= k! \sum_{n_i \text{ distinct}} r_{n_1}^2 r_{n_2}^2 \dots r_{n_k}^2 \\ &= k! \sum_{n_1=1}^N r_{n_1}^2 \sum_{n_2=1, n_2 \neq n_1}^N r_{n_2}^2 \dots \sum_{n_k=1, n_k \neq n_j (j < k)}^N r_{n_k}^2. \end{aligned}$$

Since the r_n are nonincreasing we see that

$$\sum_{\substack{n_i=1 \\ n_i \neq n_j (j < i)}}^N r_{n_i}^2 \geq \sum_{n=i}^N r_n^2.$$

By hypothesis (20) this last sum is $\geq \frac{1}{2} \sigma^2$, and consequently the expression (22) is $\geq k! (\frac{1}{2} \sigma^2)^k$.

An upper bound for $P(|Z| \geq V)$ can be derived from (19) by using the inequality $P(|Z| \geq V) V^{2k} \leq E(|Z|^{2k})$ which is a special case of the first inequality in Lemma 1. A lower bound can be derived by appealing to the fact that if $c > 1$ then

$$P(|Z| \geq V) (c-1)^2 V^{4k} / 4 \leq E(|Z|^{2k} - V^{2k}) (cV^{2k} - |Z|^{2k}).$$

References

- [1] S. Chowla and P. Erdős, *A theorem on the distribution of the values of L-functions*, J. Indian Math. Soc. (N.S.) 15 (1951), pp. 11–18.
- [2] P. D. T. A. Elliott, *On the distribution of the values of quadratic L-series in the half-plane $\sigma > 1/2$* , Invent. math. 21 (1973), pp. 319–338.
- [3] David Joyner, *Distribution theorems of L-functions*, Longman Scientific, Harlow 1986.
- [4] J.-P. Kahane, *Some random series of functions*, Heath, Lexington 1968.
- [5] William Reynolds Monach, *Numerical investigation of several problems in number theory*, Univ. of Michigan Ph.D. Dissertation, Ann Arbor 1980.
- [6] V. V. Petrov, *Sums of independent random variables*, Springer-Verlag, Berlin 1975.
- [7] S. O. Rice, *Distribution of $\sum a_n/n$, a_n randomly equal to ± 1* , Bell System Technical J. 52 (1973), pp. 1097–1103.
- [8] B. S. Saltzberg, *Intersymbol interference error bounds with applications to ideal bandlimited signaling*, IEEE Trans. Information Theory IT-14 (1968), pp. 563–568.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF MICHIGAN
Ann Arbor, MI 48109
AT&T BELL LABORATORIES
Murray Hill, NJ 07974

Received on 23.7.1986
and in revised form on 25.10.1986

(1663)

Les volumes IV
et suivants sont
à obtenir chez

Volumes from IV
on are available
at

Die Bände IV und
folgende sind zu
beziehen durch

Томы IV и следу-
ющие можно по-
лучить через

Ars Polona, Krakowskie Przedmieście 7, 00-068 Warszawa

Les volumes I-III
sont à obtenir chez

Volumes I-III
are available at

Die Bände I-III sind
zu beziehen durch

Томы I-III можно
получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

BOOKS PUBLISHED BY THE POLISH ACADEMY OF SCIENCES
INSTITUTE OF MATHEMATICS

- S. Banach, *Oeuvres*, vol. II, 1979, 470 pp.
- S. Mazurkiewicz, *Travaux de topologie et ses applications*, 1969, 380 pp.
- W. Sierpiński, *Oeuvres choisies*, vol. I, 1974, 300 pp.; vol. II, 1975, 780 pp.; vol. III, 1976, 688 pp.
- J. P. Schauder, *Oeuvres*, 1978, 487 pp.
- K. Borsuk, *Collected papers*, Parts I, II, 1983, xxiv+1357 pp.
- H. Steinhaus, *Selected papers*, 1985, 899 pp.
- K. Kuratowski, *Selected papers*, in the press.
- W. Orlicz, *Collected papers*, in the press.

MONOGRAFIE MATEMATYCZNE

43. J. Szarski, *Differential inequalities*, 2nd ed., 1967, 256 pp.
50. K. Borsuk, *Multidimensional analytic geometry*, 1969, 443 pp.
51. R. Sikorski, *Advanced calculus*, Functions of several variables, 1969, 460 pp.
58. C. Bessaga and A. Pełczyński, *Selected topics in infinite-dimensional topology*, 1975, 353 pp.
59. K. Borsuk, *Theory of shape*, 1975, 379 pp.
62. W. Narkiewicz, *Classical problems in number theory*, 1986, 363 pp.

BANACH CENTER PUBLICATIONS

- Vol. 1. *Mathematical control theory*, 1976, 166 pp.
- Vol. 5. *Probability theory*, 1979, 289 pp.
- Vol. 6. *Mathematical statistics*, 1980, 376 pp.
- Vol. 7. *Discrete mathematics*, 1982, 224 pp.
- Vol. 8. *Spectral theory*, 1982, 603 pp.
- Vol. 9. *Universal algebra and applications*, 1982, 454 pp.
- Vol. 10. *Partial differential equations*, 1983, 422 pp.
- Vol. 11. *Complex analysis*, 1983, 362 pp.
- Vol. 12. *Differential geometry*, 1984, 288 pp.
- Vol. 13. *Computational mathematics*, 1984, 792 pp.
- Vol. 14. *Mathematical control theory*, 1985, 643 pp.
- Vol. 15. *Mathematical models and methods in mechanics*, 1985, 725 pp.
- Vol. 16. *Sequential methods in statistics*, 1985, 554 pp.
- Vol. 17. *Elementary and analytic theory of numbers*, 1985, 498 pp.
- Vol. 18. *Geometric and algebraic topology*, 1986, 417 pp.
- Vol. 19. *Partial differential equations*, in the press.
- Vol. 20. *Singularities*, in the press.
- Vol. 21. *Mathematical problems in computation theory*, in the press.

