A PROBABILISTIC APPROACH TO PROBLEMS OF DIOPHANTINE APPROXIMATION

BY P. ERDÖS AND A. RÉNYI

Introduction

Let $z_1, z_2, \cdots, z_n$ denote unimodular complex numbers

$$|z_j| = 1, \qquad j = 1, 2, \cdots, n.$$

We put $z_j = e^{i\varphi_j}(0 \leqq \varphi_j < 2\pi)$ and

$$S_k = \sum_{j=1}^{n} z_j^k \qquad (k = 1, 2, \cdots). \tag{1}$$

By a well known theorem of *Dirichlet*, for any integer $\omega \geqq 2$ we can find a positive integer k with $1 \leqq k \leqq \omega^n$ and integers $b_1, b_2, \cdots, b_n$ such that

$$\left| \frac{k\varphi_j}{2\pi} - b_j \right| \leqq \frac{1}{\omega} \qquad (j = 1, 2, \cdots, n). \tag{2}$$

It follows for $\omega \geqq 5$ that among the power sums S_k $(1 \leqq k \leqq \omega^n)$, there is at least one for which

$$|S_k| \geqq n \cos \frac{2\pi}{\omega}.$$

This can be stated also as follows: *For any choice of the unimodular numbers* z_j $(j = 1, 2, \cdots, n)$, *we have*

$$\max_{1 \leqq k \leqq [A(c)]^n} |S_k| \geqq cn \tag{3}$$

for any c *such that* $0 < c < 1$, *where* $A(c) = [2\pi/\arccos c] + 1$. (Here and in what follows $[x]$ denotes the integral part of x.)

It is well known that Dirichlet's theorem can not be improved. For instance, if $\varphi_j = 2\pi/\omega^j$ $(j = 1, 2, \cdots, n)$, where $\omega \geqq 2$ is an integer, then among the integers $1 \leqq k \leqq \omega^n - 1$ there is none for which all the inequalities

$$\left| \frac{k\varphi_j}{2\pi} - b_j \right| < \frac{1}{\omega} \qquad (j = 1, 2, \cdots, n),$$

where $b_1, b_2, \cdots, b_n$ are integers, would be satisfied.

A simple example of *G. Hajós* (see [1], p. 16) shows that Dirichlet's theorem can not be much improved, even when we admit nonintegral values for k. The example of *Hajós* is as follows: if we choose

$$\varphi_j = \frac{2\pi}{6 \cdot 5^{j-1}} \qquad (j = 1, 2, \cdots, n),$$

Received January 21, 1957.

then among the real numbers $1 \leqq t \leqq 6 \cdot 5^{n-1} - 1$ there is none for which the relations

$$\left| \frac{t\varphi_j}{2\pi} - b_j \right| < \frac{1}{6} \qquad (j = 1, 2, \cdots, n)$$

would all hold, where $b_1, b_2, \cdots, b_n$ are integers. Similar examples could be constructed for other values of ω.

In the present paper we approach the same problems by an entirely different—probabilistic—method. Let $C^{(n)} = C^{(1)} * C^{(1)} * \cdots * C^{(1)}$ denote the direct product of n unit circles, and define a probability measure P on $C^{(n)}$ as the direct product of the uniform measures on each of the factors $C^{(1)}$. In other words, we consider the set $z_1, z_2, \cdots, z_n$ of complex random variables, where $z_j = e^{i\varphi_j}$, and the φ_j are independent real random variables uniformly distributed in the interval $(0, 2\pi)$.

We shall show in §1, by using standard methods of the calculus of probability, that for every $n > 1$ and $0 < c < 1$ the set of those n-tuples of unimodular complex numbers $z_1, z_2, \cdots, z_n$ (i.e. those points of $C^{(n)}$) for which

$$\max_{1 \leqq k < \frac{1}{4}\exp(nc^2/2)} |S_k| < cn, \tag{4}$$

has positive measure [Theorem 2]. This proves the existence of an infinity of essentially different sets $z_1, z_2, \cdots, z_n$ with $z_j = e^{i\varphi_j}$ $(0 \leqq \varphi_j < 2\pi)$ for which the inequalities

$$\left| \frac{k\varphi_j}{2\pi} - b_j \right| \leqq \frac{\arccos c}{2\pi} \qquad (j = 1, 2, \cdots, n) \tag{5}$$

can not hold for an integer k in the interval $1 \leqq k < \frac{1}{4}e^{nc^2/2} (0 < c < 1)$ and with integers b_j $(j = 1, 2, \cdots, n)$, because (5) would imply $|S_k| \geqq cn$. (In fact we shall prove still more; see Theorems 1 and 3.)

In §1 we prove the existence of various sets $z_1, z_2, \cdots, z_n$ of unimodular complex numbers, such that many of their power sums are relatively small (or, expressed in another form, such sets $z_1, z_2, \cdots, z_n$ of unimodular complex numbers that the numbers $z_1^k, z_2^k, \cdots, z_n^k$ are rather uniformly distributed on the unit circle for many values of k [Theorem 4]). Our method is principially unable to yield an explicit construction of such sets, though such a construction by some other method would be rather interesting. The reader, however, who is acquainted with the book [1] of *P. Turán*, will immediately see why the proof of the existence of sets with the mentioned properties is also in itself not without interest. In fact our results show that the inequality (3), which is a consequence of Dirichlet's theorem, can not be essentially improved, i.e. the range of k can not be replaced by a range of definitely smaller order of magnitude for $n \to \infty$. Now in the book of *Turán* mentioned above, a series of important applications are given of lower estimates concerning $\operatorname{Max}_{a \leqq k < b} |S_k|$ with a relatively small range (a, b) of k. Such estimates have been found by *Turán*; of course his results on the "short

range" maximum of $|S_k|$ give only small lower bounds. Our results prove that this is inevitable.

In §2 we also shall prove a result [Theorem 6] giving a lower estimate of $\mathrm{Max}_{1\leqq k\leqq N}|S_k|$ (and another [Theorem 5] of the maximal discrepancy of the set z_j^k $(j = 1, 2, \cdots, n)$ for $1 \leqq k \leqq N$), valid for *every* set $z_1, \cdots, z_n$ of unimodular complex numbers, which shows that the results of §1 are not far from being best possible. Theorem 6 differs from the much deeper results obtained by *P. Turán* [1] in that it deals with the long range maximum of $|S_k|$, while *Turán's* results are on the short range maximum of $|S_k|$; it should be mentioned that Turán's results are valid under more general conditions (the z_k need not be unimodular).

In §3 we call attention to some unsolved problems and to further possible developments of our method.

1. Construction of particular sets of unimodular complex numbers

THEOREM 1. *There exists for every integer* $n \geqq 2$ *a set* $z_1, z_2, \cdots, z_n$ *of unimodular complex numbers such that, putting* $S_k = \sum_{j=1}^n z_j^k$, *we have*[1]

$$|S_k| < \sqrt{6n \log (k+1)} \qquad \text{for } k = 1, 2, \cdots. \tag{6}$$

Theorem 1 clearly implies

$$\max_{1\leqq k<\exp(nc^2/6)} |S_k| < cn \qquad \text{for } 0 < c < 1; \tag{4'}$$

the slightly stronger relation (4) can be proved by considerations similar to those used in the proof of Theorem 1, but it does not follow from Theorem 1. Thus we have besides Theorem 1 the following

THEOREM 2. *There exists for every* $n \geqq 2$, *a set* $z_1, z_2, \cdots, z_n$ *of unimodular complex numbers such that, putting* $S_k = \sum_{j=1}^n z_j^k$ $(k = 1, 2, \cdots)$, *we have*

$$\max_{1\leqq k<\frac{1}{4}\exp(nc^2/2)} |S_k| < cn$$

for every c *in* $0 < c < 1$.

Remark. Of course Theorem 2 does not contradict (3), because

$$e^{c^2/2} < \frac{2\pi}{\arccos c}$$

for $0 < c < 1$ as $e^{c^2/2} \leqq e^{1/2} \leqq 4 \leqq 2\pi/\arccos c$.

To prove Theorems 1 and 3 we shall need the following

LEMMA 1. *Let* $z_1, z_2, \cdots, z_n$ *denote independent complex-valued random variables, each of which is uniformly distributed on the circumference of the unit circle. Then we have, putting* $\zeta_n = z_1 + z_2 + \cdots + z_n$,

$$P(|\zeta_n| \geqq cn) \leqq 4e^{-c^2 n/2} \qquad (n = 1, 2, \cdots), \tag{7}$$

[1] The inequality (6) is of course interesting only for $k + 1 < e^{n/6}$, because for $k + 1 \geqq e^{n/6}$ the inequality becomes trivial as $|S_k| \leqq n$ for any k.

for $0 < c < 1$. *(Here and in what follows* $P(\cdots)$ *denotes the probability of the relation in the bracket.)*

Proof of Lemma 1. Let us evaluate the mean value of $|e^{\lambda\zeta_n}|$ which we denote by $M(|e^{\lambda\zeta_n}|)$ where λ is real. By our suppositions

$$M(|e^{\lambda\zeta_n}|) = M\left(\prod_{j=1}^{n}|e^{\lambda z_j}|\right) = [M(|e^{\lambda z_1}|)]^n,$$

and thus

$$M(|e^{\lambda\zeta_n}|) = \left(\frac{1}{2\pi}\int_0^{2\pi} e^{\lambda\cos\varphi}\,d\varphi\right)^n = (\mathcal{J}_0(i\lambda))^n, \tag{8}$$

where $\mathcal{J}_0(x)$ denotes the Bessel function of order 0,

$$\mathcal{J}_0(x) = \sum_{k=0}^{\infty}\frac{(-1)^k(\frac{1}{2}x)^{2k}}{k!^2}. \tag{9}$$

As

$$\mathcal{J}_0(i\lambda) = \sum_{k=0}^{\infty}\frac{(\frac{1}{2}\lambda)^{2k}}{k!^2} \leqq \sum_{k=0}^{\infty}\frac{(\frac{1}{2}\lambda)^{2k}}{k!} = e^{\lambda^2/4}, \tag{10}$$

it follows that

$$M(|e^{\lambda\zeta_n}|) \leqq e^{n\lambda^2/4}. \tag{11}$$

Let us denote by $\Re(w)$ the real part of the complex number w. As the variables z_j, $-z_j$, iz_j and $(-iz_j)$ are identically distributed, $\Re(z_j)$, $\Re(-z_j)$, $\Re(iz_j)$, and $\Re(-iz_j)$ are also identically distributed. Taking into account that for $w = u + iv$ we have

$$|w| = \sqrt{u^2+v^2} \leqq \sqrt{2}\,\mathrm{Max}(|u|, |v|)$$
$$= \sqrt{2}\,\mathrm{Max}\,(\Re(w), \Re(-w), \Re(iw), \Re(-iw)),$$

we obtain

$$|\zeta_n| \leqq \sqrt{2}\,\mathrm{Max}\,(\Re(\zeta_n), \Re(-\zeta_n), \Re(i\zeta_n), \Re(-i\zeta_n)). \tag{12}$$

It follows from (12) that for $\lambda > 0$

$$P(|\zeta_n| \geqq cn) \leqq 4\,P(\Re(\zeta_n) \geqq cn/\sqrt{2}), \tag{13}$$

and thus

$$P(|\zeta_n| \geqq cn) \leqq 4\,P\left(|\exp\lambda\zeta_n| \geqq \exp\frac{\lambda cn}{\sqrt{2}}\right). \tag{14}$$

Now we need the well known inequality of *Markov* according to which for any nonnegative random variable ξ we have

$$P(\xi \geqq A) \leqq M(\xi)/A$$

for any $A > 0$. Applying this inequality to the probability on the right of (14), we obtain, taking (11) into account, that

$$P\left(|\exp \lambda\zeta_n| \geqq \exp \frac{\lambda cn}{\sqrt{2}}\right) \leqq \exp n\left(\frac{\lambda^2}{4} - \frac{c\lambda}{\sqrt{2}}\right). \tag{15}$$

From (14) and (15) it follows that

$$P(|\zeta_n| \geqq cn) \leqq 4 \exp n\left(\frac{\lambda^2}{4} - \frac{c\lambda}{\sqrt{2}}\right), \tag{16}$$

for $0 < c < 1$ and $\lambda > 0$. Choosing for λ the value $\lambda = c\sqrt{2}$, we obtain the assertion of Lemma 1, which is therewith proved.

To prove Theorems 1 and 2, we start from the remark that if z_j is uniformly distributed on the unit circle, the same is true regarding z_j^k for $k = 1, 2, \cdots$. It follows that if the random variables $z_1, z_2, \cdots, z_n$ are independent, and each is uniformly distributed on the unit circle, the random variables $S_k = \sum_{j=1}^{n} z_j^k$ are all identically distributed, and we have by Lemma 1

$$P(|S_k| \geqq cn) \leqq 4e^{-c^2 n/2} \qquad (0 < c < 1). \tag{17}$$

It follows from (17) that

$$P\left(\operatorname*{Max}_{1 \leqq k \leqq N} |S_k| \geqq cn\right) \leqq 4Ne^{-c^2 n/} \tag{18}$$

Choosing $N < \frac{1}{4}e^{nc^2/2}$, we obtain

$$P\left(\operatorname*{Max}_{1 \leqq k < \exp(nc^2/2)} |S_k| \geqq cn\right) < 1, \tag{19}$$

which implies the existence of a set $z_1, z_2, \cdots, z_n$, with $|z_j| = 1$ $(j = 1, 2, \cdots, n)$, for which $|S_k| < cn$ for $k < \frac{1}{4}e^{nc^2/2}$.

This proves Theorem 2.

To prove Theorem 1, we deduce from (17) that

$$P(|S_k| \geqq \sqrt{6n \log (k+1)}) \leqq \frac{4}{(k+1)^3} \qquad (k = 1, 2, \cdots). \tag{20}$$

Thus we obtain

$$P\left(\operatorname*{Max}_{k \geqq 1} \frac{|S_k|}{\sqrt{\log (k+1)}} \geqq \sqrt{6n}\right) \leqq 4 \sum_{k=1}^{\infty} \frac{1}{(k+1)^3} < 1 \tag{21}$$

as

$$\sum_{k=1}^{\infty} \frac{1}{(k+1)^3} < \frac{1}{2^3} + \int_2^{\infty} \frac{dx}{x^3} = \frac{1}{4}.$$

This implies the existence of sets $z_1, z_2, \cdots, z_n$ for which

$$|S_k| < \sqrt{6n \log (k+1)} \qquad \text{for} \quad k = 1, 2, \cdots,$$

Theorem 1 is thus also proved.[2]

For values of c near to 1, the range $1 \leqq k \leqq N$ for which $\mathrm{Max}_{1\leqq k\leqq N} \mid S_k \mid < cn$, for a suitably chosen set $z_1, z_2, \cdots, z_n$, can be considerably enlarged. This is expressed by

THEOREM 3. *There exists, for every $n \geqq 10$ and every ε with $0 < \varepsilon < \frac{1}{16}$, a set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers such that, putting*

$$S_k = \sum_{j=1}^{n} z_j^k \qquad (k = 1, 2, \cdots),$$

we have

$$\max_{1\leqq k\leqq (16ne^{n-1})^{-1/2}} \mid S_k \mid < n(1 - \varepsilon).$$

Proof of Theorem 3. We have clearly

$$\int_0^{\pi} e^{\lambda\cos\varphi}\, d\varphi < \int_0^{\pi/2} e^{\lambda\cos\varphi}\, d\varphi + \frac{\pi}{2}.$$

Introducing the new variable $x = \sqrt{2\lambda(1 - \cos\varphi)}$, we obtain

$$\int_0^{\pi} e^{\lambda\cos\varphi}\, d\varphi < \frac{e^{\lambda}}{\sqrt{\lambda}} \int_0^{\sqrt{2\lambda}} \frac{e^{-x^2/2}\, dx}{\sqrt{1 - x^2/4\lambda}} + \frac{\pi}{2}.$$

As $1/\sqrt{1-t} < 1 + t$ for $0 < t < \frac{1}{2}$, it follows that

$$\int_0^{\pi} e^{\lambda\cos\varphi}\, d\varphi < \frac{e^{\lambda}}{\sqrt{\lambda}} \left(\int_0^{\infty} e^{-x^2/2}\, dx + \frac{1}{4\lambda} \int_0^{\infty} x^2 e^{-x^2/2}\, dx \right) + \frac{\pi}{2}.$$

Thus we obtain

$$\frac{1}{2\pi} \int_{-\pi}^{+\pi} e^{\lambda\cos\varphi}\, d\varphi < \frac{e^{\lambda}}{\sqrt{2\pi\lambda}} \left(1 + \frac{1}{4\lambda}\right) + \frac{1}{2}. \tag{22}$$

We follow an argument essentially the same as that used in the proof of Theorem 2. Taking into account that for any complex number w and any positive integer $h \geqq 4$, we have

$$\mid w \mid \leqq \frac{1}{\cos\frac{\pi}{h}} \cdot \max_{0\leqq r\leqq h-1} \Re\left(w \exp -\frac{2\pi i r}{h}\right), \tag{23}$$

further that

$$S_k \exp -\frac{2\pi i r}{h} = \sum_{j=1}^{n} \left(z_j \exp -\frac{2\pi i r}{hk}\right)^k$$

has the same distribution as S_1, we obtain for any $k \geqq 1$

[2] It can be seen from the argument that the assertion

$$\mid S_k \mid < \sqrt{6n \log (k+1)} \qquad (k = 1, 2, \cdots)$$

could be replaced by $\mid S_k \mid < \sqrt{4n \log (k+4)}$ or more generally by

$$\mid S_k \mid < \sqrt{2(1+\delta)n \log (k + (4\delta^{-1})^{1/\delta})} \qquad \text{for any } \delta > 0.$$

$$P(|S_k| \geqq n(1-\epsilon)) \leqq P\left(\operatorname*{Max}_{0\leqq r\leqq h-1} \Re\left(S_k \exp -\frac{2\pi i r}{h}\right) \geqq n(1-\varepsilon)\cos\frac{\pi}{h}\right),$$

which implies

$$P(|S_k| \geqq n(1-\varepsilon)) \leqq hP\left(\Re(S_1) \geqq n(1-\varepsilon)\cos\frac{\pi}{h}\right). \tag{24}$$

Thus we obtain

$$\begin{aligned} P(|S_k| \geqq n(1-\varepsilon)) &\leqq hP\left(|e^{\lambda S_1}| \geqq \exp\left\{n\lambda(1-\varepsilon)\cos\frac{\pi}{h}\right\}\right) \\ &\leqq h\cdot\left(\frac{\frac{e^\lambda}{\sqrt{2\pi\lambda}}\left(1+\frac{1}{4\lambda}\right)+\frac{1}{2}}{\exp\left\{\lambda(1-\varepsilon)\cos\frac{\pi}{h}\right\}}\right)^n \end{aligned} \tag{25}$$

As for $\lambda > 4$, $\frac{1}{2} < e^\lambda/4\lambda\sqrt{2\pi\lambda}$, it follows from (25) that

$$\begin{aligned} &P\left(\operatorname*{Max}_{1\leqq k\leqq N}|S_k| \geqq n(1-\varepsilon)\right) \\ &\leqq Nh\left(\frac{\left(1+\frac{1}{2\lambda}\right)\exp\left\{\lambda\left(1-(1-\varepsilon)\cos\frac{\pi}{h}\right)\right\}}{\sqrt{2\pi\lambda}}\right)^n. \end{aligned} \tag{26}$$

Let us suppose $n \geqq 10$ and $0 < \varepsilon < \frac{1}{16}$ and choose

$$\lambda = \frac{1}{2\varepsilon} \tag{27}$$

and

$$h = \left[\pi\sqrt{\frac{n}{\varepsilon}}\right] + 1. \tag{28}$$

It follows from (26), (27), and (28) that

$$P\left(\operatorname*{Max}_{1\leqq k\leqq N}|s_k| \geqq n(1-\varepsilon)\right) \leqq 4N\sqrt{n}\varepsilon^{(n-1)/2}.$$

Thus

$$P\left(\operatorname*{Max}_{1\leqq k\leqq N}|S_k| \geqq n(1-\varepsilon)\right) < 1 \quad \text{if} \quad N < (16n\varepsilon^{n-1})^{-1/2}$$

Thus there exist sequences $z_1, z_2, \cdots, z_n$ of unimodular complex numbers such that

$$\operatorname*{Max}_{1\leqq k\leqq (16n\varepsilon^{n-1})^{-1/2}}|S_k| < n(1-\varepsilon).$$

Theorem 3 is therewith proved.

It is easy to see that by a slight modification of our argument we could prove the existence of a set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers for which assertions of the type of Theorem 1 and Theorem 3 hold simultaneously; of course the constants figuring in these theorems are to be modified for this purpose. We obtain this way that, for $n \geqq 10$ and

$0 < \varepsilon < \frac{1}{16}$, there exists a set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers such that, putting $S_k = \sum_{j=1}^{n} z_j^k$, we have

$$|S_k| \leqq \sqrt{6n \log (k+2)} \quad \text{for} \quad k \leqq e^{n/6},$$

and at the same time

$$|S_k| \leqq n(1-\varepsilon) \quad \text{for} \quad k \leqq (64n\varepsilon^{n-1})^{-1/2}.$$

In our Theorems 1, 2, and 3, instead of considering successive power sums, i.e. $S_1, S_2, \cdots, S_N$, we may consider $S_{k_1}, S_{k_2}, \cdots, S_{k_N}$, where $k_1, k_2, \cdots, k_N$ is any set of different integers. We formulate only Theorem 2 in this generalized form.

THEOREM 2a. *Let $n \geqq 2$ be an arbitrary integer, $0 < c < 1$ and $k_1, k_2, \cdots, k_N$ an arbitrary set of different integers, $N < \frac{1}{4}e^{nc^2/2}$. Then there can be found unimodular complex numbers $z_1, z_2, \cdots, z_n$ such that, putting $S_k = \sum_{j=1}^{n} z_j^k$, we have*

$$\operatorname*{Max}_{1 \leqq r \leqq N} |S_{k_r}| < cn.$$

The results proved up to now give no information whatever about the numbers $z_1, z_2, \cdots, z_n$ for which all the values $|S_k|$ $(1 \leqq k \leqq N)$ are relatively small, except the existence of an abundant set of such n-tuples. Nevertheless we can say something about the numbers z_j figuring in our theorems, by a slight modification of our argument.

In fact we can prove that the numbers z_j $(j = 1, 2, \cdots, n)$ in Theorem 2 can all be chosen to be roots of unity of order p, where p is a prime greater than $e^{n/2}$. The modification of the proof consists in that we suppose concerning the random variables z_j, not that they are equidistributed on the unit circle, but that they take on each of the values ρ^h $(h = 0, 1, \cdots, p-1)$ where $\rho = e^{2\pi i/p}$ with the probability $1/p$; here as mentioned above, p is a prime, $p > e^{n/2}$. In place of the fundamental formula (8) we obtain, provided that k is not divisible by p, putting again $\zeta_n = \sum_{j=1}^{n} z_j^k$,

$$M(|e^{\lambda \zeta_n}|) = \left[1 + \sum_{r=1}^{[p/2]} \frac{(\frac{1}{2}\lambda)^{2r}}{r!^2} + \sum_{r \geqq p} \frac{b_r \lambda^r}{r!}\right] \tag{29}$$

where $|b_r| \leqq 1$ for $r \geqq p$. Thus we obtain

$$M(|e^{\lambda \zeta_n}|) \leqq e^{\lambda^2 n/4} \quad \text{if} \quad \lambda \leqq \sqrt{2}, \tag{8'}$$

and therefore Theorems 1 and 2 remain valid with the additional requirement that $z_1, z_2, \cdots, z_n$ should all be roots of the equation $z^p = 1$, where $p > e^{n/2}$ is a prime. Theorem 3 can also be proved with this additional requirement, but in this case we have to suppose of course

$$p > (16n\varepsilon^{n-1})^{-1/2}$$

We can develop our results somewhat further by considering not only the power sums $S_k = \sum_{j=1}^{n} z_j^k$ for positive integer values of k, but also the sums $S_\alpha = \sum_{j=1}^{n} z_j^\alpha$ for real values of α.

In this direction we can prove the following result:

THEOREM 1b. *There can be found for every* $n \geqq 2$, *a set* $z_1, z_2, \cdots, z_n$ *of unimodular complex numbers*

$$z_j = e^{i\varphi_j} \qquad (0 \leqq \varphi_j < 2\pi; j = 1, 2, \cdots n),$$

such that, putting $S_\alpha = \sum_{j=1}^{n} e^{i\varphi_j \alpha}$ *where* α *is real, we have*

$$|S_\alpha| \leqq \sqrt{6n \log(\alpha\sqrt{n} + 1)} + 2\pi(\sqrt{n} + 2)$$

for any $\alpha \geqq 1/[\sqrt{n}]$.

Proof of Theorem 1b. Let us choose numbers $z_j = e^{i\varphi_j}$ for which

$$|\sum_{j=1}^{n} z_j^k| \leqq \sqrt{6n \log(k+1)} \qquad (k = 1, 2, \cdots),$$

which is possible according to Theorem 1. Let us put $m = [\sqrt{n}]$ and $w_j = z_j^m$. Then we have

$$\left|\sum_{j=1}^{n} w_j^\alpha\right| \leqq \sqrt{6n \log(\alpha\sqrt{n} + 1)} \quad \text{for} \quad \alpha = \frac{k}{m},\ k = 1, 2, \cdots. \tag{30}$$

As for $z = e^{i\varphi}(0 \leqq \varphi < 2\pi)$, we have

$$|z^\beta - z^\alpha| \leqq (\beta - \alpha)\cdot 2\pi \tag{31}$$

if $0 < \alpha < \beta$, it follows that

$$\left|\sum_{j=1}^{n} w_j^\beta\right| \leqq \left|\sum_{j=1}^{n} w_j^{k/m}\right| + \frac{2\pi n}{m} \tag{32}$$

for $k/m \leqq \beta < (k+1)/m$. Thus by (30) and (32), for $n \geqq 2$ and any $\alpha \geqq 1/m$,

$$|S_\alpha| \leqq \sqrt{6n \log(\alpha\sqrt{n} + 1)} + 2\pi(\sqrt{n} + 2),$$

which implies the assertion of Theorem 1b.

It follows simply from our results that there can be found a set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers such that for no $k < \frac{1}{4}e^{nc^2/2}$ do all the numbers z_j^k $(j = 1, 2, \cdots, n)$ lie on an arc of the unit circle of length 2 arccos c: because if this were so, then, for the set $z_1, z_2, \cdots, z_n$ figuring in Theorem 2, for some $k < \frac{1}{4}e^{nc^2/2}$ we would have $|S_k| > nc$, in contradiction with Theorem 2. But in this way it is impossible to deduce the existence of sets $z_1, z_2, \cdots, z_n$ of unimodular complex numbers for which $z_1^k, z_2^k, \cdots, z_n^k$ do not all lie on an arc of length l with $\pi < l < 2\pi$ for some $k < (1+\delta)^n$. Nevertheless this is a consequence of Theorem 1, but to deduce it we need the finite form of *Weyl*'s theorem due to *P. Erdös* and *P. Turán*.

Let us denote by $N_n^{(k)}(\alpha, \beta)$ the number of those among the numbers z_j $(z_j = e^{i\varphi_j}; 0 \leqq \varphi_j < 2\pi; j = 1, 2, \cdots, n)$ for which

$$0 \leqq \alpha \leqq k\varphi_j < \beta < 2\pi \pmod{2\pi}.$$

According to the theorem of Erdös and Turán [2] we have

$$\left|N_n^{(k)}(\alpha,\beta) - \frac{(\beta-\alpha)n}{2\pi}\right| < A\left(\frac{n}{m+1} + \sum_{l=1}^{m}\frac{|S_{kl}|}{l}\right), \tag{33}$$

where $A > 0$ is an absolute constant and $m \geqq 1$ is an arbitrary integer. If we choose the unimodular complex numbers $z_1, z_2, \cdots, z_n$ so as to satisfy Theorem 1, it follows from (33) that we have for $k = 1, 2, \cdots$

$$\left|N_n^{(k)}(\alpha,\beta) - \frac{(\beta-\alpha)n}{2\pi}\right| < A\left(\frac{n}{m+1} + \sum_{l=1}^{m}\frac{\sqrt{6n\log(kl+1)}}{l}\right). \tag{34}$$

Choosing

$$m = \left[\sqrt{\frac{n}{\log(k+2)}}\right],$$

we obtain

$$\left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| < A\left(\sqrt{\frac{\log(k+2)}{n}} + \log\frac{en}{\log(k+2)}\sqrt{\frac{6}{n}\log(k+1)}\sqrt{\frac{n}{\log(k+2)}}\right). \tag{35}$$

Thus we have

$$\left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| \leqq \frac{c_1(\log n)^{3/2}}{\sqrt{n}} \qquad \text{for } k \leqq n, \tag{36}$$

and further putting $\delta = (\log(k+2))/n$,

$$\left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| \leqq c_2\sqrt{\delta}\log\frac{e}{\delta} \qquad \text{for } \frac{\log(n+2)}{n} \leqq \delta \leqq 1, \tag{37}$$

where c_1 and c_2 are positive constants. As $\sqrt{\delta}\log(e/\delta) \to 0$ for $\delta \to 0$, it follows that the points $z_1^k, z_2^k, \cdots, z_n^k$ are asymptotically equidistributed on the unit circle for $n \to \infty$ and $(\log k)/n \to 0$.

The result obtained is expressed by the following

THEOREM 4. *There exists for every n a set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers such that, denoting by $N_n^{(k)}(\alpha,\beta)$ the number of those among $z_1^k, z_2^k, \cdots, z_n^k$ which are lying in the arc (α,β) of the unit circle, we have*

$$\left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| < c_3\sqrt{\delta}\left(\log\frac{e}{\delta}\right)^{3/2}$$

for $k \leqq e^{\delta n} - 2$, where c_3 is an absolute constant and $0 < \delta < 1$.

Theorem 4 follows by combining the inequalities (36) and (37).

It follows from Theorem 4 that there exist unimodular complex numbers $z_1, z_2, \cdots, z_n$ such that, for any $\varepsilon > 0$ with $0 < \varepsilon < B_1$, for no

$k \leqq \exp\{B_2 n\varepsilon^2(\log 1/\varepsilon)^{-3}\}$ does there exist on the unit circle an arc of length $\geqq 2\pi\varepsilon$ which does not contain any of the numbers $z_1^k, z_2^k, \cdots, z_n^k$; here $B_1 > 0$ and $B_2 > 0$ are absolute constants.

2. Results valid for all sets of unimodular complex numbers

To show that Theorem 4 can not be essentially improved, let us consider arbitrary unimodular complex numbers $z_j = e^{i\varphi_j}(j = 1, 2, \cdots, n)$. Let us choose an integer ω $(1 < \omega < n/2)$; according to Dirichlet's theorem, we can find a positive integer $k < \omega^{[n/\omega]}$ such that

$$\left|\frac{k\varphi_j}{2\pi} - b_j\right| < \frac{1}{\omega}$$

for $j = 1, 2, \cdots, [n/\omega]$, where the b_j are integers. It follows that

$$\left|\frac{N_n^{(k)}\left(-\frac{1}{\omega}, \frac{1}{\omega}\right)}{n} - \frac{1}{\omega\pi}\right| > \frac{1}{6\omega}$$

with some $k < \omega^{[n/\omega]} < (\omega^{1/\omega})^n$. Thus we proved

THEOREM 5. *Let $z_1, z_2, \cdots, z_n$ denote arbitrary unimodular complex numbers, and $\omega > 1$ an integer $(\omega < \frac{1}{2}n)$. Then we have*

$$\operatorname*{Max}_{1\leqq k\leqq \omega^{[n/\omega]}} \operatorname*{Max}_{0\leqq\alpha<\beta<2\pi} \left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| \geqq \frac{1}{6\omega}.$$

To compare Theorem 5 with Theorem 4, let us mention that Theorem 4 can be brought to the following form:

Theorem 4 asserts that for any ε with $0 < \varepsilon < c_1$ and $n \geqq 2$

$$\operatorname*{Min}_{z_1,z_2,\cdots z_n} \operatorname*{Max}_{1\leqq k\leqq (1+\varepsilon)^n} \operatorname*{Max}_{0\leqq\alpha<\beta<2\pi} \left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| < \Delta_1(\varepsilon),$$

where $0 < \Delta_1(\varepsilon) < c_2\sqrt{\varepsilon}\,(\log 1/\varepsilon)^{3/2}$; and Theorem 5 asserts that

$$\operatorname*{Min}_{z_1,z_2,\cdots z_n} \operatorname*{Max}_{1\leqq k\leqq (1+\varepsilon)^n} \operatorname*{Max}_{0\leqq\alpha<\beta<2\pi} \left|\frac{N_n^{(k)}(\alpha,\beta)}{n} - \frac{\beta-\alpha}{2\pi}\right| > \Delta_2(\varepsilon),$$

where

$$\Delta_2(\varepsilon) > \frac{c_3\varepsilon}{\log(1/\varepsilon)},$$

c_1, c_2, and c_3 being absolute constants. Thus Theorem 4 and Theorem 5 each shows that the other is not far from being best possible.

Similarly we can prove a theorem which shows that Theorem 2 can not be essentially improved. Let $z_1, z_2, \cdots, z_n$ denote an arbitrary set of unimodular complex numbers.

Let us suppose $2 \leqq c \leqq n - 1$ and let us denote by r the least integer

$\geqq c$. According to Dirichlet's theorem, if $z_j = e^{i\varphi_j}$, we can find an integer $l < (4\pi n\sqrt{r+1})^{r+1}$ such that

$$\left| \frac{l\varphi_j}{2\pi} - b_j \right| \leqq \frac{1}{[4\pi n\sqrt{r+1}]}$$

for $j = 1, 2, \cdots, r+1$, where $b_1, \cdots, b_{r+1}$ are integers. Now let us put $w_1 = z_{r+2}^l, \cdots, w_{n-r-1} = z_n^l$; according to a theorem of *Cassels* [3], there can be found an integer $h < 2(n-r)$ such that $\Re(\sum_{i=1}^{n-r-1} w_i^h) \geqq 0$; it follows that

$$|S_{lh}| \geqq \Re(S_{lh}) \geqq (r+1)\cos\frac{1}{\sqrt{r+1}} \geqq r \geqq c.$$

Thus we have proved

THEOREM 6. *For any set $z_1, z_2, \cdots, z_n$ of unimodular*[3] *complex numbers, putting $S_k = \sum_{j=1}^n z_j^k$, we have for $2 \leqq c \leqq n-1$*

$$\max_{1 \leqq k \leqq (4\pi\sqrt{c+2}\cdot n)^{c+2}\cdot 2n} |S_k| \geqq c.$$

3. Some unsolved problems

(a) In §§1 and 2 we have shown that there exist positive functions $f_1(\varepsilon)$, $f_2(\varepsilon)$, $\Delta_1(\varepsilon)$, $\Delta_2(\varepsilon)$ $(\varepsilon > 0)$, all tending to 0 for $\varepsilon \to 0$, such that, putting

$$A(n, \varepsilon) = \frac{1}{n} \min_{\substack{z_1,\cdots,z_n \\ |z_j|=1}} \max_{1 \leqq k \leqq (1+\varepsilon)^n} |S_k|,$$

and

$$B(n, \varepsilon) = \min_{\substack{z_1,\cdots,z_n \\ |z_j|=1}} \max_{1 \leqq k \leqq (1+\varepsilon)^n} \max_{0 \leqq \alpha < \beta < 2\pi} \left| \frac{N_n^{(k)}(\alpha, \beta)}{n} - \frac{\beta - \alpha}{2\pi} \right|,$$

we have

$$f_1(\varepsilon) \leqq A(n, \varepsilon) \leqq f_2(\varepsilon)$$

and

$$\Delta_1(\varepsilon) \leqq B(n, \varepsilon) \leqq \Delta_2(\varepsilon).$$

The exact orders of magnitude of $A(n, \varepsilon)$ and $B(n, \varepsilon)$ for $\varepsilon \to 0$ remain however unknown.

(b) Dirichlet's theorem asserts that for any set $z_1, z_2, \cdots, z_n$ $(n \geqq 2)$ of unimodular complex numbers, and for any integer $\omega > 2$, there can be found an integer k in the interval $1 \leqq k \leqq \omega^n$ such that the numbers $z_1^k, z_2^k, \cdots, z_n^k$ are all lying in an interval of length $4\pi/\omega$ on the unit circle, and thus an interval of length $2\pi - 4\pi/\omega$ remains free from the numbers z_j^k. Probably this is not a best possible result, and $2\pi - 4\pi/\omega$ can be replaced by a greater number, but nothing is known in this direction. Moreover

[3] It is clear from the proof of Theorem 6 that, instead of $|z_j| = 1$, it suffices to suppose $|z_j| \geqq 1$.

it remains completely unsolved whether there exists a function $\delta(\varepsilon) > 0$ $(0 < \varepsilon < 1)$ such that for any set $z_1, z_2, \cdots, z_n$ of unimodular complex numbers, there can be found an integer k, with $1 \leqq k \leqq (1 + \varepsilon)^n$, such that the numbers $z_1^k, z_2^k, \cdots, z_n^k$ leave free on the unit circle an arc of length $\geqq \delta(\varepsilon)$.

(c) Finally we should like to call attention to the following facts which have not been used explicitly in this paper.

It can be shown by standard methods of the calculus of probability that if $z_1, z_2, \cdots, z_n$ are independent random variables, each of which is uniformly distributed on the unit circle, then, putting

$$S_k = \sum_{j=1}^{n} z_j^k, \qquad \xi_n^{(k)} = \sqrt{\frac{2}{n}}\, \Re(S_k), \quad \text{and} \quad \eta_n^{(k)} = \sqrt{\frac{2}{n}}\, \Im(S_k),$$

the joint distribution of the random variables

$$\xi_n^{(k_1)}, \eta_n^{(k_1)}, \cdots, \xi_n^{(k_r)}, \eta_n^{(k_r)},$$

where r is fixed and $k_i \neq k_j$ for $i \neq j$ $(i, j = 1, 2, \cdots, r)$, tends for $n \to \infty$ to the $2r$-dimensional symmetrical normal distribution with the density function

$$\frac{1}{(2\pi)^r} \exp\left(-\frac{1}{2}\sum_{j=1}^{2r} x_j^2\right).$$

Thus the variables $\xi_n^{(k_1)}, \eta_n^{(k_1)}$ are *in the limit independent* for $n \to \infty$. It seems that this fact has interesting consequences concerning diophantine approximations. We hope to return to this question in a forthcoming paper.

Bibliography

1. P. Turán, *Eine neue Methode in der Analysis und deren Anwendungen*, Budapest, 1953.
2. P. Erdös and P. Turán, *On a problem in the theory of uniform distribution* I, Nederl. Akad. Wetensch. Indagationes Math., vol. 10 (1948), pp. 370–378.
3. J. W. S. Cassels, *On the sums of powers of complex numbers*, Acta Math. Acad. Sci. Hungar., vol. 7 (1956), pp. 283–289.

Budapest, Hungary