PROBABILITIC METHOD ON THE UNIFORM DISTRIBUTION OF SEQUENCES OF INTEGERS MOD M

均匀分配之機率處理法

by

Jau-shyong Shiue

薛 昭 雄

The theory of probability is a classical branch of mathematics, and it has many applications of physics and other branch of mathematics (see〔2〕,〔3〕).

There are a few examples of using probability theory method in the theory of asymptotic distribution mod 1, and it seems quite natural to apply the similar procedure to the theory of uniform distribution of sequences of integers mod m, where m is an integer $\geq$ 2, which was first introduced by I. Niven〔7〕in 1961.

In the present paper, we apply the results of probability theory in order to investigate the theory of uniform distribution of sequence of integers mod m. (for the elementary proof see〔4〕).

Let Z^+ be the set of all rational positive integers. Let Z be the set of all rational integers. Let F be the finite algebra of all subsets of Z^+ and let R be the set of all real numbers. Let $A=\{1,2,..,N\}\subset Z^+$ Define the function $P: F \to R$ by

$$P(E)=\lim_{N\to\infty}\frac{|E\cap A|}{N} \qquad \text{(provided the limit exists),}$$

where $|E\cap A|$ denotes the cardinal numbers of $E\cap A$.

Theorem 1. (Z^+,F,P) is a (finite) probability space.

Proof. To show (Z^+,F,P) is a (finite) probability space, we need prove that

(1) If $E\in F$ then $P(E)\geq 0$,

(2) $P(\phi)=0$, $P(Z^+)=1$, and

(3) If $E_i\in F(i=1,2,\cdots,n)$ and $E_i\cap E_j=\phi$, provided $i\neq j$, then $P(\bigcup_{i=1}^{n}E_i)=\sum_{i=1}^{n}P(E_i)$.

(1) and (2) are clear. For the part of (3), we shall use mathematical induction on n. Let n=2, then

$$P(E_1\cup E_2)=\lim_{N\to\infty}\frac{|(E_1\cup E_2)\cap A|}{N}$$

$$=\lim_{N\to\infty}\frac{|(E_1\cap A)\cup(E_2\cap A)|}{N}=\lim_{N\to\infty}\frac{|E_1\cap A|+|E_2\cap A|}{N},$$

because $(E_1\cap A)\cap(E_2\cap A)=E_1\cap E_2=\phi$.

Hence $P(E_1\cup E_2)=P(E_1)+P(E_2)$.

Now we suppose (3) is true for n-1, i.e. $P(\bigcup_{i=1}^{n-1}E_i)=\sum_{i=1}^{n-1}P(E_i)$

Let $F=\bigcup_{i=1}^{n-1}E_i$ then $\bigcup_{i=1}^{n}E_i=F\cup E_n$. By the preceding result, we have $P(F\cup E_n)=P(F)+P(E_n)=\sum_{i=1}^{n-1}P(E_i)+P(E_n)$

$$=\sum_{i=1}^{n}P(E_i).$$

i.e. $P(\bigcup_{i=1}^{n}E_i)=\sum_{i=1}^{n}P(E_i)$.

Therefore (Z^+,F,P) is a (finite) probability space.

A random variable in a probability space (Ω,F,P) is a real valued function defined on Ω such that $\{w\in\Omega : f(w)<r , r\in R\}\in F$.

According to preceding definition, we may consider the sequence of integers $\{f(n)\}$ such that $\{n : f(n) < k, k \in Z\} \in F$ (*) is a random variable in the probability space (Z^+, F, P). From now on, the random variable in the probability space (Z^+, F, P) will mean the sequence of integers with the property (*).

Theorem 2. Let $\{f(n)\}$ be a random variable in the probability space (Z^+, F, P). Then for all $m, k \in Z$,

(1) $\{n \in Z^+ : f(n) = k\} \in F$,

(2) $\{n \in Z^+ : f(n) \leq k\} \in F$,

(3) $\{n \in Z^+ : f(n) > m\} \in F$,

(4) $\{n \in Z^+ : f(n) \geq m\} \in F$, and

(5) $\{n \in Z^+ : k \leq f(n) \leq m\} \in F$.

Proof. (1) Since $\{n \in Z^+ : f(n) = k\}$
$= \{n \in Z^+ : f(n) < k+1\} \cdot \{n \in Z^+ : f(n) < k\}$,we have
$\{n \in Z^+ : f(n) = k\} \in F$.

The relation (2) through (5) can be shown in a similar way.

Definition. Let $\{f_1(n)\}$, $\{f_2(n)\}$, ………… , $\{f_k(n)\}$ be k random variables in (Z^+, F, P). $\{f_1(n)\}$, $\{f_2(n)\}$, ………….., $\{f_k(n)\}$ are said to be independent if

$$P(\{n \in Z^+ \mid f_1(n) < m_1, \cdots, f_k(n) < m_k\})$$
$$= \prod_{i=1}^{k} P(\{n \in Z^+ \mid f_i(n) < m_i\}).$$

Definition Let $\{f(n)\}$ be a random variable in (Z^+, F, P) and $h(k) = P(\{n \in Z^+ : f(n) < k\})$, ($k = 0, \pm 1, \pm 2, \cdots$). h(k) is called the distribution function of the random variable $\{f(n)\}$.

By using the result of probability theory on distribution function, we have

Theorem 3. h(k) is a nonnegative and monotonically increasing function. Moreover h(k) (if properly extended) is continuous on the left.

Theorem 4. Let $\{f(n)\}$ be a random variable in (Z^+, F, P) and $-a<f(n)<a$, $\forall n$, Then

$$M(f)=\int_{-a}^{a} x\,dh(x)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N} f(i).$$

Proof. Since $-a<f(n)<a$, $\forall n$, and h(x) is the distribution function of $\{f(n)\}$. $h(a)=1$, $h(-a)=0$ Now

$$\int_{-a}^{a} x\,dh(x)=\sum_{m=-a+1}^{a-1} mP(\{f(n)=m\})$$

$$=\sum_{m=-a+1}^{a-1} m\lim_{N\to\infty}\frac{1}{N}|\{n\in Z^+ : f(n)=m\}\cap A|$$

$$=\lim_{N\to\infty}\frac{1}{N}\sum_{-a+1}^{a-1} m|\{n\in Z^+ : f(n)=m\}\cap A|$$

$$=\lim_{N\to\infty}\frac{1}{N}(f(1)+f(2)+\cdots+f(N)).$$

By the preceding proof, we also have

Theorem 5. Let $\{f(n)\}$ be a random variable, and let $\{f(n)\}$ assumes the values $0,1,2,\ldots,m-1$. Let $k=1,2,\cdots,m-1$. Then

$$\int_0^{m-1} e^{2\pi i\frac{k}{m}x}\,dh(x)=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{n} e^{2\pi i\frac{k}{m}f(n)},$$

where h(x) is the distribution function of the random variable $\{f(n)\}$.

Definition. Let $\{f(n)\}$ be a random variable. $\{f(n)\}$ is uniformly distributed mod m, where m is a positive integer ≥ 2, if the distribution function of $\{f(n)\ (\text{mod } m)\}$ is same as that of $\{n\ (\text{mod } m)\}$.

Theorem 6. Let $\{f(n)\}$ be a random variable. $\{f(n)\}$ is uniformly distributed mod m if and only if

$$M(e^{2\pi i\frac{k}{m}f(n)})=0,\ \forall k=1,2,\cdots\cdots\cdots\cdots,m-1.$$

Proof. Necessity. We have

$$M(e^{2\pi i\frac{k}{m}f(n)})=\lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}e^{2\pi i\frac{k}{m}f(n)}.$$

Now by theorem 5 we have also

$$M(e^{2\pi i\frac{k}{m}f(n)})=\int_0^{m-1}e^{2\pi i k x/m}dh(x),$$

where the h(x) is the distribution function of the random variable {f(n) (mod m)} . As the distribution function of {f(n) (mod m)} in the case of uniform distribution is the same as the distribution function of { n (mod m) } , we have for k=1, 2, ..., m-1.

$$\begin{aligned} M(e^{2\pi i\frac{k}{m}f(n)}) &= M(e^{2\pi i kn/m}) \\ &= \lim_{N\to\infty}\frac{1}{N}e^{2\pi i\frac{k}{m}}\frac{1-e^{2\pi i kN/m}}{1-e^{2\pi i k/m}} \\ &= 0\ ,\ \text{for}\ \left|\frac{1-e^{2\pi i kN/m}}{1-e^{2\pi i k/m}}\right|\leq\frac{2}{|1-e^{2\pi i k/m}|}\ . \end{aligned}$$

For the proof of sufficiency, refer to [8].

Theorem 7. Let $\{f_1(n)\}$, $\{f_2(n)\}$, ..., $\{f_k(n)\}$ be bounded random variables and independent, then

$$M(\prod_{i=1}^{k}f_i(n))=\prod_{i=1}^{k}M(f_i(n)),\quad \text{and}$$

$$M(\prod_{i=1}^{k}f_i^{l_i}(n))=\prod_{i=1}^{k}M(f_i^{l_i}(n)),$$ where ℓ_i are integers (positive).

Proof. This clearly follows from theorem 1 of [1] (p. 389) and the fact that $\{f_i^{l_i}(n)\}$ is a random variable if $\{f_i(n)\}$ does.

Corollary. 8. Given $\{f_1(n)\}$, $\{f_2(n)\}$, ..., $\{f_k(n)\}$ are random variables. Let $\{f_1(n)$ (mod m)$\}$, $\{f_2(n)$ (mod m)$\}$, ..., $\{f_k(n)$ (mod m)$\}$ are independent.

Then $M(e^{2\pi i(h_1f_1(n)+h_2f_2(n)+\cdots+h_kf_k(n))/m})$

$$= \prod_{i=1}^{k} M(e^{2\pi i\, h_i f_i(n)/m})$$

for all $h_1, h_2, \ldots, h_k = 0, 1, 2, \ldots, m-1$.

Theorem 9. Given $\{f_1(n)\}$, $\{f_2(n)\}$, $\cdots\cdots\cdots$, $\{f_k(n)\}$ are random variables. Let $\{f_1(n) \pmod m\}$, $\{f_2(n) \pmod m\}$, ..., $\{f_k(n) \pmod m\}$ are independent. Suppose the random variable $\{f_1(n)\}$ is uniformly distributed mod m. Then the sum (pointwise) of random variables $\{f_1(n)+f_2(n)+\cdots\cdots+f_k(n)\}$ is uniformly distributed mod m.

Proof. Since $\{f_1(n)\}$ is uniformly distributed mod m, we have, by theorem 6,

$$M(e^{2\pi i \frac{k}{m} f(n)}) = 0, \quad \forall k = 1, 2, \cdots\cdots\cdots, m-1.$$

Moreover by the fact that $\{f_1(n) \pmod m\}$, $\{f_2(n) \pmod m\}$, ..., $\{f_k(n) \pmod m\}$ are independent. We also have

$$M(e^{2\pi i(h_1 f_1(n)+h_2 f_2(n)+\cdots+h_k f_k(n))/m})$$

$$= \prod_{i=1}^{k} M(e^{2\pi i h_i/m f_i(n)}) = 0.$$

Hence $\{f_1(n)+f_2(n)+\cdots\cdots\cdots\cdots+f_k(n)\}$ is uniformly distributed mod m.

REFERENCES

1. M. Eisen, Introduction to Mathematical Probability Theory, Prentice-Hall Inc., 1969.

2. M. Kac, Statistical Independence in Probability, Analysis and Number Theory, Carus Monogramy No. 12, 1959.

3. M. Kac, Probability and Related Topics in Physical Sciences, Boalder Lectures in Applied Mathematics, Vol. 1.

4. L. Kuipers and Jau-shyong Shiue, Asymptotic Distribution mod m of Sequences of Integers and the Notion of Independence I. to appear.

5. L. Kuipers and A. J. Stam, On a General Form of the Weyl Criterion in the Theory of Asymptotic Distribution, Proc. Japan Acad., 45(1969), 530-540.

6. L. Kuipers, Some Aspects of the Theory of Asymptotic Distribution Modulo 1, Bulletin de la Société Mathématique de Belgique, XV(1963), 380-388.

7. I. Niven, Uniform Distribution of Integers, Trans. Amer. Mathe. Soc., 98(1961), 52-61.

8. S. Uchiyama, On the Uniform Distribution of Sequences of Integers, Proc. Japan Acad., 37(1961), 605-609.

Department of Mathematics
National Taiwan Normal University