Ann. Inst. Statist. Math.
Vol. 44, No. 2, 379–385 (1992)

SOME CHARACTERIZATIONS OF THE UNIFORM DISTRIBUTION WITH APPLICATIONS TO RANDOM NUMBER GENERATION

LIH-YUAN DENG AND E. OLUSEGUN GEORGE

Department of Mathematical Sciences, Memphis State University, Memphis, TN 38152, U.S.A.

(Received September 5, 1989; revised October 22, 1990)

Abstract. Let U and V be independent random variables with continuous density function on the interval $(0,1)$. We describe families of functions g for which uniformity of U and V is equivalent to uniformity of $g(U,V)$ on $(0,1)$. These results are used to prescribe methods for improving the quality of pseudo-random number generators by making them closer in distribution to the $U(0,1)$ distribution.

Key words and phrases: Characterization of uniform distribution, independence, pseudo-random number generator, fractional sum.

1. Introduction

Characterization of the uniform distribution often provides useful tools for constructing goodness-of-fit statistics, simulation of highly complex statistical procedures and testing the quality of pseudo-random number generators. Although the uniform distribution is extensively characterized, Kotz (1974) has noted that there is a need for a complete survey of the characterization results, particularly those results that have meaningful practical applications. This observation underscores a need for "global" characterizations of the uniform distribution.

In this paper, we address and provide some answers to the following question: If U and V are independent random variables having continuous density function with support $(0,1)$, for what family of functions g does the uniformity of U and V imply (and is implied by) uniformity of $g(U,V)$? In providing partial answers to this question, we introduce three classes of such functions in Section 2. In Section 3 we show how some members of these families characterize the uniform distribution. In Section 4, we consider the case when U and V are not exactly uniformly distributed. We use results of Section 3 to transform these variates into random variables that are closer in distribution to the uniform distribution. The use of these results to improve the quality of pseudo-random number generators are discussed.

2. Characterization results

Let U and V be independent random variables with the continuous density functions $f_U(u)$ and $f_V(v)$ having support $(0,1)$. Also let g be a measurable function from $[0,1] \times [0,1]$ to $[0,1]$.

2.1 *The class of functions* $\mathcal{G}$

DEFINITION 1. We define $\mathcal{G}$ to be the class of all functions g such that

$$W = g(U,V) \sim U(0,1), \tag{2.1}$$

and W independent of V if and only if $U \sim U(0,1)$.

Examples of function which belong to $\mathcal{G}$ (proved later) are

$$g_1(u,v) = \min\left(\frac{u}{v}, \frac{1-u}{1-v}\right), \tag{2.2}$$

$$g_2(u,v) = |u-v|\left(\frac{\delta}{v} + \frac{1-\delta}{1-v}\right), \tag{2.3}$$

where $\delta = I_{(v>u)}$, the indicator function of $v > u$, and

$$g_3(u,v) = u + v \bmod 1. \tag{2.4}$$

2.2 *The class of functions* $\mathcal{H}$

Let m be the Lebesgue measure on the unit interval. For a measurable set $A \subset [0,1]$, let $H^g(A) = \{(u,v) \mid g(u,v) \in A\}$. The "cross-section" of $H^g(A)$ at a fixed $v \in (0,1)$ is defined by $H_v^g(A) = \{u \mid g(u,v) \in A\}$.

DEFINITION 2. $\mathcal{H}$ is the class of all functions g that satisfy (i)

$$m(H_v^g(A)) = m(A) \quad \text{for all} \quad v \in (0,1), \quad A \subset (0,1), \tag{2.5}$$

and (ii) for any interval $(a,b) \subset [0,1]$, there exist $v \in (0,1)$ and $A \subset (0,1)$ such that

$$(a,b) = H_v^g(A). \tag{2.6}$$

Clearly, if $A_1, A_2, \ldots$ is a sequence of disjoint subsets of $(0,1)$, and $v \in (0,1)$, then $H_v^g(A_1), H_v^g(A_2), \ldots$ is a sequence of disjoint subsets of $(0,1)$, and

$$H_v^g\left(\bigcup_i A_i\right) = \bigcup_i H_v^g(A_i).$$

Consequently,

$$m\left[H_v^g\left(\bigcup_i A_i\right)\right] = \sum_i m[H_v^g(A_i)].$$

Hence if $g \in \mathcal{H}$,

$$m\left[H_v^g\left(\bigcup_i A_i\right)\right] = \sum_i m(A_i). \tag{2.7}$$

Using (2.7), it is clear that (2.5) can be verified by choosing intervals $A = (0, w)$, $0 < w < 1$. We may thus relax (2.5) to

$$m(H_v^g(0, w)) = w, \quad \text{for all} \quad v \in (0, 1). \tag{2.8}$$

2.3 *The class of functions* $\mathcal{K}$

DEFINITION 3. $\mathcal{K}$ is the class of functions g such that

$$g(U, V) \sim U(0, 1) \tag{2.9}$$

whenever V and U are i.i.d. $U(0, 1)$.

It is easily shown that

$$g_4(u, v) = \frac{\min(u, v)}{\max(u, v)} \tag{2.10}$$

and

$$g_5(u, v) = \frac{\log u}{\log u + \log v} \tag{2.11}$$

belong to $\mathcal{K}$ but not to $\mathcal{G}$.

3. The main results

We will now show how a simple relationship among $\mathcal{H}$, $\mathcal{G}$ and $\mathcal{K}$ leads to some simple characterizations of the uniform distribution.

THEOREM 3.1. $\mathcal{H} \subset \mathcal{G} \subset \mathcal{K}$.

PROOF. Clearly $\mathcal{G} \subset \mathcal{K}$. To show that $\mathcal{H} \subset \mathcal{G}$, let $g \in \mathcal{H}$ and let $U \sim U(0, 1)$. Then the conditional distribution of $W = g(U, V)$, given $V = v$, is

$$\begin{aligned} P[W \in A \mid V = v] &= P[g(U, v) \in A] = P[U \in H_v^g(A)] \\ &= m(H_v^g(A)) = m(A). \end{aligned}$$

That is, the conditional distribution of W given $V = v$ is $U(0, 1)$. Since this distribution does not depend on v, W is independent of V and $W \sim U(0, 1)$. On the other hand, if $W \sim U(0, 1)$ and independent of V, then for any $(a, b) \subset (0, 1)$, there exist $v \in (0, 1)$ and $A \subset (0, 1)$ such that $(a, b) = H_v^g(A)$.

$$\begin{aligned} (b - a) &= P[W \in (a, b)] = P[W \in (a, b) \mid V = v] = P[g(U, v) \in A] \\ &= P[U \in H_v^g(A)] = \int_{H_v^g(A)} f_U(u) du. \end{aligned}$$

This would imply that $f_U(u) = 1$, for all $0 < u < 1$. □

THEOREM 3.2. *Let U and V be independent random variables distributed over $(0,1)$ with the continuous p.d.f. $f_U(u)$ and $f_V(v)$, respectively. Then the following statements are equivalent:*

(i) $U \sim U(0,1)$.

(ii) $W_1 = \min(U/V, (1-U)/(1-V)) \sim U(0,1)$, *and independent of* V.

(iii) $W_2 = |U-V|(\Delta/V + (1-\Delta)/(1-V)) \sim U(0,1)$, *and independent of* V, *where* $\Delta = I_{(V>U)}$, *the indicator function of* $V > U$.

(iv) $W_3 = U + V \bmod 1 \sim U(0,1)$, *and independent of* V.

PROOF. From the definition of $\mathcal{G}$ and equations (2.2), (2.3) and (2.4), Theorem 3.2 follows immediately if we can show g_1, g_2 and $g_3 \in \mathcal{G}$. From Theorem 3.1, it is sufficient to show that g_1, g_2 and $g_3 \in \mathcal{H}$. Note that

$$\begin{aligned} g_2(u,v) &= \max\left(1 - \frac{u}{v}, 1 - \frac{1-u}{1-v}\right) \\ &= 1 - \min\left(\frac{u}{v}, \frac{1-u}{1-v}\right) \\ &= 1 - g_1(u,v). \end{aligned}$$

Since $g \in \mathcal{H}$ if and only if $1 - g \in \mathcal{H}$, it suffices to prove that g_1 and g_3 belong to $\mathcal{H}$. For $0 < w < 1$, let $A = (0,w)$. Then

$$H_v^{g_1}(A) = (0, vw) \cup (1 - w + vw, 1),$$

and

$$H_v^{g_3}(A) = \begin{cases} (0, w-v) \cup (1-v, 1), & \text{if } v < w \\ (1-v, 1+w-v), & \text{if } v > w. \end{cases}$$

Clearly

$$m(H_v^{g_1}(A)) = w = m(H_v^{g_3}(A)),$$

thus equation (2.5) is satisfied.

Now let $0 < a < b < 1$. Let

$$v_1 = \frac{a}{(1-b)+a}, \qquad w_1 = (1-b) + a \qquad \text{and} \qquad A_1 = (w_1, 1).$$

Also let

$$v_3 = 1 - a, \qquad w_3 = b - a \qquad \text{and} \qquad A_3 = (0, w_3).$$

Clearly $H_{v_1}^{g_1}(A_1) = (a,b) = H_{v_3}^{g_3}(A_3)$. Hence g_1 and $g_3 \in \mathcal{H}$. □

This theorem generalizes the well-known property that if U and V are independent and $U \sim U(0,1)$, then $W = U + V \bmod 1 \sim U(0,1)$, and W and V are also independent (see Theorem 2.1 of Stapleton (1963)).

4. Improving pseudo-random number generators

It is well known that no algorithm exists for generating truly uniform random variables. The above results can be used to improve the quality of generated pseudo-random numbers.

THEOREM 4.1. *Let U and V be two generated random variables with respective densities f_U and f_V, and let*

$$\epsilon_1 = \sup_{0\le t\le 1} |f_U(t) - 1|, \qquad \epsilon_2 = \sup_{0\le t\le 1} |f_V(t) - 1|.$$

Let $W = g(U,V)$, $W' = g'(U,V) = g(V,U)$ and let f_W, $f_{W'}$ denote the p.d.f. of W and W'.

(1) *If $g \in \mathcal{K}$, then $(1-\epsilon_1)(1-\epsilon_2) \le f_W(w) \le (1+\epsilon_1)(1+\epsilon_2)$.*
(2) *If $g \in \mathcal{H}$, then $1-\epsilon_1 \le f_W(w) \le 1+\epsilon_1$.*
(3) *If $g, g' \in \mathcal{H}$, then $1-\epsilon_1\epsilon_2 \le f_W(w), f_{W'}(w) \le 1+\epsilon_1\epsilon_2$.*

PROOF. For $w \in (0,1)$, choose $h > 0$ such that $w + h < 1$. Then

$$P(w \le W \le w+h) = \int_0^1 \int_{H_v^g(w,w+h)} f_U(u)du f_V(v)dv. \tag{4.1}$$

Since $g \in \mathcal{K}$,

$$\int_0^1 \int_{H_v^g(w,w+h)} dudv = h.$$

Using the fact that $1-\epsilon_1 \le f_U(u) \le 1+\epsilon_1$ and $1-\epsilon_2 \le f_V(v) \le 1+\epsilon_2$ in (4.1), we have

$$\int_0^1 \int_{H_v^g(w,w+h)} (1-\epsilon_1)(1-\epsilon_2)dudv \le P(w \le W \le w+h) \le \int_0^1 \int_{H_v^g(w,w+h)} (1+\epsilon_1)(1+\epsilon_2)dudv.$$

Therefore,

$$(1-\epsilon_1)(1-\epsilon_2) \le \frac{P(w \le W \le w+h)}{h} \le (1+\epsilon_1)(1+\epsilon_2).$$

Part (1) follows by letting $h \to 0$. To prove (2), we use the fact that $1-\epsilon_1 \le f_U(u) \le 1+\epsilon_1$. From (2.5), $\int_{H_v^g(w,w+h)} du = h$. Hence

$$\int_0^1 \int_{H_v^g(w,w+h)} (1-\epsilon_1)du f_V(v)dv \le P(w \le W \le w+h) \le \int_0^1 \int_{H_v^g(w,w+h)} (1+\epsilon_1)du f_V(v)dv.$$

Consequently,

$$(1-\epsilon_1) \leq \frac{P(w \leq W \leq w+h)}{h} \leq (1+\epsilon_1).$$

Part (2) follows by letting $h \to 0$. To prove (3), let $\delta_1(u) = f_U(u) - 1$ and $\delta_2(v) = f_V(v) - 1$ in (4.1). Then

$$P(w \leq W \leq w+h) = \int_{H^g(w,w+h)} (1 + \delta_1(u) + \delta_2(v) + \delta_1(u)\delta_2(v))dudv.$$

Using the fact that $\int_0^1 \delta_2(v)dv = 0$, and g satisfies (2.5), we see that

$$\int_{H^g(w,w+h)} \delta_2(v)dudv = \int_0^1 \delta_2(v) \int_{H_v^g(w,w+h)} dudv = h\int_0^1 \delta_2(v)dv = 0.$$

Similarly, since g' satisfies (2.5), we have

$$\int_{H^g(w,w+h)} \delta_1(v)dvdu = 0.$$

Therefore,

$$P(w \leq W \leq w+h) = \int_{H^g(w,w+h)} (1 + \delta_1(u)\delta_2(v))dudv.$$

Since $|\delta_1(u)| \leq \epsilon_1$ and $|\delta_2(v)| \leq \epsilon_2$, we have

$$(1-\epsilon_1\epsilon_2)h \leq P(w \leq W \leq w+h) \leq (1+\epsilon_1\epsilon_2)h.$$

Part (3) follows easily. □

Theorem 4.1 provides a theoretical justification for the practice of generating $U(0,1)$ random numbers by taking the fractional parts of sums of pseudo-random numbers. Several authors have suggested combining several random number generators to get a "more uniform" generator. Wichmann and Hill (1982) suggested adding three simple multiplicative congruential generators and taking the fractional part. They claimed that this procedure "ironed out" the imperfections in the component variates. L'Ecuyer (1988) provided an empirical support for Wichmann and Hill's procedure. Part (3) of Theorem 4.1 shows that the true distribution of the fractional part of a sum of independent pseudo-random number is closer to $U(0,1)$ than each of the component pseudo-random variate.

Marsaglia (1985) empirically compared several popular generators and concluded that the combination generator is superior to others. Other authors such as Collings (1987) and Anderson (1990) also recommended the combination generator. Brown and Solomon (1979), Marsaglia (1985) and Deng and George (1990) provided some theoretical justifications for combining pseudo generators to obtain a more uniform generator. Unfortunately, these authors assume that the individual generators are stochastically independent. This assumption cannot be justified theoretically. Deng *et al.* (1989, 1991) consider combining generators that are not necessarily independent. They showed that such combined generators are asymptotically uniform and independent.

Acknowledgements

The authors would like to thank the two referees for their many constructive and useful comments on an earlier draft of this article.

References

Anderson, S. L. (1990). Random number generators on vector supercomputers and other advanced architectures, *SIAM Rev.*, **32**, 221–251.

Brown, M. and Solomon, H. (1979). On combining pseudorandom number generators, *Ann. Statist.*, **7**, 691–695.

Collings, B. J. (1987). Compound random number generators, *J. Amer. Statist. Assoc.*, **82**, 525–527.

Deng, L. Y. (1988). Robustness study of some random variate generators, *Proceedings of the 20th Symposium on the Interface* (eds. E. J. Wegman, D. T. Gantz and J. J. Miller), 624–626, American Statistical Association, Alexandria, Virginia.

Deng, L. Y. and George, E. O. (1990). Generation of uniform variates from several nearly uniformly distributed variables, *Comm. Statist. Simulation Comput.*, **B 19**, 145–154.

Deng, L. Y., George, E. O. and Chu, Y. C. (1989). On improving "bad" pseudo-random number generators, *Proceedings of the 21st Symposium on the Interface* (eds. K. Berk and L. Malone), 284–286, American Statistical Association, Alexandria, Virginia.

Deng, L. Y., George, E. O. and Chu, Y. C. (1991). On improving pseudo-random number generators, *Winter Simulation Conference* (eds. B. L. Nelson, W. D. Kelton and G. M. Clark), 1035–1042.

Kotz, S. (1974). Characterizations of statistical distributions: a supplement to recent surveys, *Internat. Statist. Rev.*, **42**, 39–65.

L'Ecuyer, P. (1988). Efficient and portable combined random number generators, *Comm. ACM*, **31**, 742–748, 774.

Marsaglia, G. (1985). A current view of random number generators, *Proceedings of the Sixteenth Symposium on the Interface* (ed. L. Billard), 3–10, North-Holland, Amsterdam.

Stapleton, J. H. (1963). A characterization of the uniform distribution on a compact topological group, *Ann. Math. Statist.*, **34**, 319–326.

Wichmann, B. A. and Hill, I. D. (1982). An efficient and portable pseudo-random number generator, *Applied Statistics*, **31**, 188–190.