A DIRECT METHOD FOR PRODUCING RANDOM DIGITS IN ANY NUMBER SYSTEM

BY H. BURKE HORTON AND R. TYNES SMITH III

Interstate Commerce Commission

1. Summary. A compounding technique first used to produce random binary digits is generalized and extended to other number systems. Formulae for the rate of convergence of probabilities to the desired values are derived. The method is extended to the production of random digits with fixed but unequal probabilities. Numerical results are presented in summary form together with results of tests applied to a set of random digits produced by the method.

2. Introduction. In a note [1] by one of the authors a method of producing random digits was presented. The method was based upon a process, designated "compound randomization," used to produce random binary digits, which can be converted to random digits in other number systems by simple methods. Despite the ease of converting a random binary series to another system, it is of interest to examine the problem of direct production of random digits in any number system. In the course of producing random binary digits with machine tabulating equipment, and while designing an electronic device to produce random binary digits, it was noted that the multiplication process described in the earlier paper was the equivalent of addition modulo 2 of a series of binary digits. This observation laid the basis for generalizing to other number systems.[1]

3. Initial conditions and notation. Let us assume that there is available a source of digits, $0, 1, 2, \cdots (n-1)$, in a number system of base n, where n is a positive integer, $n > 1$. Let p_{rs} represent the probability of obtaining the rth digit in the sth trial. Assume that initial conditions can be controlled so that the trials are independent[2] and

$$p_{rs} \geqq \epsilon \tag{3.1}$$

where $0 < \epsilon \leqq 1/n$ is a fixed positive number. (It may be noted at this point that conventional "single-stage" methods of producing random numbers are based upon the assumption that $p_{rs} = \epsilon = 1/n$.) Let π_{rs} represent the probability of obtaining the rth digit by addition modulo n of the digits obtained in s individual trials. In order to express π_{rs} in terms of p_{rs}, consider two sets of matrices whose elements are defined as follows:

[1] In acting as referee for [1] Dr. George W. Brown suggested generalizing to other number systems by addition modulo n.

[2] J. E. Walsh [2] has considered, in terms of conditional probabilities, the effect of intercorrelation on compound randomization in the binary system.

$$a_s = \left\| \begin{matrix} p_{0,s} & p_{n-1,s} & p_{n-2,s} \cdots\cdots p_{1,s} \\ p_{1,s} & p_{0,s} & p_{n-1,s} \cdots\cdots p_{2,s} \\ p_{2,s} & p_{1,s} & p_{0,s} \quad \cdots\cdots p_{3,s} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ p_{n-1,s} & p_{n-2,s} & p_{n-3,s} \cdots\cdots p_{0,s} \end{matrix} \right\| ; \tag{3.2}$$

$$\alpha_s = \left\| \begin{matrix} \pi_{0,s} & \pi_{n-1,s} & \pi_{n-2,s} \cdots\cdots \pi_{1,s} \\ \pi_{1,s} & \pi_{0,s} & \pi_{n-1,s} \cdots\cdots \pi_{2,s} \\ \pi_{2,s} & \pi_{1,s} & \pi_{0,s} \quad \cdots\cdots \pi_{3,s} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \pi_{n-1,s} & \pi_{n-2,s} & \pi_{n-3,s} \cdots\cdots \pi_{0,s} \end{matrix} \right\| . \tag{3.3}$$

Note that a_s and α_s are Markoff matrices with two additional restrictions: (1) there are no zero elements, and (2) column (as well as row) sums are unity. Each $n \times n$ matrix is made up of only n distinct elements, namely, the n different probabilities associated with the sth trial for a_s, or the n different probabilities associated with the sum of s trials for α_s.

4. Relation of π_{rs} to p_{rs} Assuming independent trials, we have the following relationships:

$$\begin{aligned} \alpha_1 &= a_1 ; \\ \alpha_2 &= a_2 \cdot \alpha_1 = a_2 \cdot a_1 ; \\ \alpha_3 &= a_3 \cdot \alpha_2 = a_3 \cdot a_2 \cdot a_1 ; \\ &\cdots\cdots\cdots \\ &\cdots\cdots\cdots \\ \alpha_k &= a_k \cdot \alpha_{k-1} = \prod_{s=1}^{k} a_s . \end{aligned} \tag{4.1}$$

Thus, since any row (or any column) of α_k is a permutation of the π_{rk}, by (4.1) the π_{rk} are expressed in terms of the individual probabilities, p_{rs}.

5. Convergence of π_{rk} to $1/n$. (5.01) THEOREM.[3] $\text{Lim}_{k\to\infty} \pi_{rk} = 1/n$.

PROOF. Let ρ_s denote the range of the elements of α_s. Each element of α_s is a weighted mean of the n distinct elements of α_{s-1}. The n distinct elements of a_s are used as weights in the averaging process. Now the range of a set of weighted means (weights > 0) of a set of values must be less than the range of the values themselves, unless both ranges are zero. Therefore, since the weights, $p_{rs} > 0$ by condition (3.1),

$$\rho_s < \rho_{s-1}, \text{ for } \rho_{s-1} \neq 0, \text{ or in the special case } \rho_{s-1} = 0, \rho_s = 0. \tag{5.02}$$

Also, since $\sum_{r=0}^{n-1} \pi_{rs} = 1$,

[3] While this article was awaiting publication, J. Wolfowitz independently proved theorem (5.01).

(5.03) $$1/n - \rho_s \leqq \pi_{rs} \leqq 1/n + \rho_s .$$

In order to show that $\lim_{s\to\infty} \rho_s = 0$, and to derive formulae for the rate of convergence of π_{rs} to the limiting value, $1/n$, let w_i represent the ordered p_{rs} for any given s: w_1 = the smallest p_{rs} , $\cdots$ w_n = the largest of the p_{rs} . In a similar manner let x_i represent the ordered $\pi_{r,s-1}$. The following inequalities for the maximum and minimum π_{rs} can be set down immediately:

(5.04) $$\max_r \pi_{rs} \leqq w_n \cdot x_n + w_{n-1} \cdot x_{n-1} + \cdots + w_1 \cdot x_1 ;$$

(5.05) $$\min_r \pi_{rs} \geqq w_n \cdot x_1 + w_{n-1} \cdot x_2 + \cdots + w_1 \cdot x_n .$$

And since $\rho_s = \max_r \pi_{rs} - \min_r \pi_{rs}$,

(5.06) $$\rho_s \leqq w_n(x_n - x_1) + w_{n-1}(x_{n-1} - x_2) + \cdots + w_2(x_2 - x_{n-1}) + w_1(x_1 - x_n).$$

For n even, let $m = n/2 + 1$, then by regrouping terms,

(5.07) $$\begin{aligned} \rho_s \leqq (w_n - w_1)(x_n - x_1) + (w_{n-1} - w_2)(x_{n-1} - x_2) + \cdots \\ + (w_m - w_{m-1})(x_m - x_{m-1}). \end{aligned}$$

Noting that $\rho_{s-1} = (x_n - x_1) \geqq (x_{n-1} - x_2) \geqq \cdots \geqq (x_m - x_{m-1})$, the following substitutions can be made:

(5.08) $$\rho_s \leqq (w_n - w_1)\rho_{s-1} + (w_{n-1} - w_2)\rho_{s-1} + \cdots + (w_m - w_{m-1})\rho_{s-1} .$$

For compactness, this may be written,

(5.09) $$\rho_s \leqq \left[\sum_{i=m}^{n} w_i - \sum_{i=1}^{m-1} w_i \right] \cdot \rho_{s-1} .$$

Similarly for n odd, let $m = (n + 1)/2$; proceeding in the same manner as above, the median term vanishes, yielding as a final result,

(5.10) $$\rho_s \leqq \left[\sum_{i=m+1}^{n} w_i - \sum_{i=1}^{m-1} w_i \right] \cdot \rho_{s-1} .$$

For simplicity denote the expression in brackets by δ_s ; then

(5.11) $$\rho_s \leqq \delta_s \cdot \rho_{s-1} ,$$

where for n even, δ_s represents the sum of the largest $n/2$ of the p_{rs} minus the sum of the smallest $n/2$ of the p_{rs} , and for n odd δ_s represents the sum of the largest $(n - 1)/2$ of the p_{rs} minus the sum of the smallest $(n - 1)/2$ of the p_{rs} . Continuing the process developed above, we find that

(5.12) $$\rho_s \leqq \delta_s \cdot \delta_{s-1} \cdot \rho_{s-2} ;$$

(5.13) $$\rho_s \leqq \delta_s \cdot \delta_{s-1} \cdot \delta_{s-2} \cdot \cdots \cdot \delta_2 \cdot \rho_1 .$$

Since $\delta_1 \geqq \rho_1$, the following simple inequality holds:

$$\rho_k \leqq \prod_{s=1}^{k} \delta_s, \tag{5.14}$$

Now $\delta_s \leqq 1 - n\epsilon$, by condition (3.1) and the definition of δ_s. Therefore,

$$\lim_{k\to\infty} \rho_k \leq \lim_{k\to\infty} \prod_{s=1}^{k} \delta_s \leq \lim_{k\to\infty} (1 - n\epsilon)^k = 0, \tag{5.15}$$

and (5.01) is proven. In the special case of constant probabilities from trial to trial, $\delta_s = \delta_0$, a constant,and (5.14) becomes

$$\rho_k \leqq (\delta_0)^k. \tag{5.16}$$

Since the mean π_{rs} is $1/n$, we have the following useful inequalities:

$$1/n - \prod_{s=1}^{k} \delta_s \leqq \pi_{rk} \leqq 1/n + \prod_{s=1}^{k} \delta_s, \tag{5.17}$$

in the case of varying probabilities, and

$$1/n - (\delta_0)^k \leqq \pi_{rk} \leqq 1/n + (\delta_0)^k, \tag{5.18}$$

in the case of constant probabilities. If δ_s is not known in each trial, an upper bound, δ_b, may be estimated on the basis of knowledge (including statistical tests) of the digit generating process. Then the following inequality will hold:

$$1/n - (\delta_b)^k \leqq \pi_{rk} \leqq 1/n + (\delta_b)^k, \tag{5.19}$$

where $\delta_b \leqq (1 - n\epsilon)$.

It is worthy of note that inequalities (5.14) and (5.15) become equalities if $n = 2$ (binary system), thus,

$$\rho_k = \prod_{s=1}^{k} \delta_s = \prod_{s=1}^{k} | p_s - q_s | = \prod_{s=1}^{k} | 2p_s - 1 |; \tag{5.14b}$$

$$\rho_k = (\delta_0)^k = | p - q |^k = | 2p - 1 |^k. \tag{5.15b}$$

These results were obtained by different methods in [1].

6. Discussion of results. Certain facts are implicit in the foregoing analysis, but are worthy of mention in passing. The compounding process may consist of addition modulo n of digits taken from a number of digit-producing machines. If any machine, h, is perfect, i.e., $p_{rh} = 1/n$ for all r, each element of the probability matrix a_h will be equal to $1/n$, and $\rho_h = 0$. Consequently, each element of α_s, $s \geqq h$, will be equal to $1/n$ by (5.17) and the special case of (5.02). Thus any combination which contains a perfect machine is perfect. This is equivalent to a restatement of Von Mises' [3] requirement that the sum of a random set and any other set must itself be a random set. Furthermore, by (5.02) the results taken from any machine, no matter how nearly perfect, can be improved by combining with the results of another machine, no matter how biased the latter may be. In the limiting case, $p_{rs} = 1$ (or 0), the probabilities of the various digits are merely interchanged.

7. Production of random numbers with fixed but unequal probabilities. The principles presented above can be adapted to the production of random numbers with unequal probabilities as follows: Assume that a set of random digits, 0, 1, 2, $\cdots$ $(n - 1)$, is required in a number system of base n, with probabilities q_0, q_1, q_2, $\cdots$ q_{n-1}, $\sum_{i=0}^{n-1} q_i = 1$, where each q_i is a proper rational fraction which may be written as the quotient of two positive integers, $q_i = \frac{u_i}{v_i}$. Choose m as the basis of a new number system, where m is the least common multiple of the v_i,

$$q_i = \frac{u_i}{v_i} = \frac{mu_i/v_i}{m}. \tag{7.1}$$

A set of random digits, 0, 1, 2, $\cdots$ $(m - 1)$, in a number system of base m may be generated by the process described above, or a set of such digits may be constructed by entering an existing table of random digits, base n, and interpreting appropriate numerical quantities, base n, as digit symbols, base m. Since $\frac{mu_i}{v_i}$ is an integer, groups of digits, mu_0, mu_1, $\cdots$ mu_{n-1}, in the m system may be coded as digits, 0, 1, 2, $\cdots$ $(n - 1)$, in the n system. An upper bound for the maximum bias of q_i will be $\frac{mu_i}{v_i} \rho_k$, where ρ_k is the range of π_{rk} in the m system. Thus, by increasing k, the bias of q_i can be made smaller than any preassigned quantity.

8. Convergence under more general conditions. Convergence of π_{rs} to $1/n$ occurs under a variety of conditions less restrictive than (3.1).

(8.1) THEOREM. *In the case of independent trials, a necessary and sufficient condition that* $\lim_{s\to\infty} \pi_{rs} = 1/n$ *is that* $\begin{Bmatrix} \pi_{0t} \\ \pi_{1t} \end{Bmatrix} \geqq \epsilon$, *where* ϵ *is a fixed positive number, arbitrarily small, and* t *is a fixed positive integer, arbitrarily large.* It is obvious that (8.1) is a necessary condition for convergence. To prove that it is a sufficient condition, consider the following:

(8.2) LEMMA. *If* $\begin{Bmatrix} p_{0s} \\ p_{1s} \end{Bmatrix} \geqq \eta$, *where* η *is a fixed positive number, arbitrarily small, then* $\lim_{s\to\infty} \pi_{rs} = 1/n$.

PROOF: Take a fixed integer, h, $h \geqq n - 1$. Now any digit, r, can be obtained in at least one way; i.e., as the sum of r *ones* and $(h - r)$ *zeros*. Therefore,

$$\pi_{rh} \geqq \tau, \qquad \text{where } \tau = \eta^h. \tag{8.3}$$

We now regard h trials as a single trial of a complex machine. Let u represent the number of such complex trials. Let π'_{ru} represent the probability of obtaining the rth digit as the result of addition modulo n of u complex trials. Then,

$$\lim_{u\to\infty} \pi'_{ru} = \lim_{u\to\infty} \pi_{r,(uh)} = 1/n, \tag{8.4}$$

by (5.01). Now $s = uh + j$, $0 \leqq j < h$, (j an integer), or $uh \leqq uh + j < (u + 1)h$. The j simple trials cannot increase the maximum bias, by (5.02): consequently,

$$\lim_{u\to\infty} \pi_{r,(uh+j)} = \lim_{(uh+j)\to\infty} \pi_{r,(uh+j)} = 1/n. \tag{8.5}$$

Since there is a one-to-one correspondence between the elements of $\{s\}$ and $\{uh + j\}$,

$$\lim_{s\to\infty} \pi_{rs} = 1/n. \tag{8.6}$$

By a natural extension of the lemma, we may regard t trials as a single complex trial. Theorem (8.1) thus assumes the form of (8.2).

9. Numerical results in various number systems. More efficient convergence formulae can be devised to meet special conditions. Those presented in (5) have the advantages of simplicity and generality. To test the efficiency of (5.15) several numerical examples, based upon unusual hypothetical probabilities, were worked by matrix multiplication as in (4.1). In these problems $p_{rs} = p_r$, a constant, from trial to trial. A tabular comparison of the ranges, computed by (4.1), and the upper bounds, determined by (5.15), is presented in Table 1 for $k = 10$.

10. Preparation and tests of a set of random digits. Since an unlimited number of valid tests for randomness may be devised, it is obvious that any finite set of digits cannot meet all such tests. As a matter of fact a truly random process should yield sets which *fail* to meet some proportion of the tests, the fraction being determined by the level of significance adopted in testing. No finite set of digits can be considered random; the tests for randomness are really applied to determine the character of the generating process. However, the concept of "locally random" sets as developed by Kendall and Smith [4] is useful, and some of their tests are used below as evidence that a set of numbers produced by compound randomization is likely to be locally random.

A non-random set of 10,000 decimal digits having the relative frequencies indicated in the starred line of Table 1 was punched in cards and tabulated. Totals were taken for each ten cards and the amount in the unit's position of the counter was cut in a summary card, thereby producing a set of 1,000 digits. The frequencies of digits in the derived set are compared with those of the generating set in Table 2. The frequencies of the derived set are in accord with the hypothesis of equal probabilities.

TABLE 1

Comparison of computed range and formula for maximum bias, $k = 10$
Hypothetical numerical examples, constant probabilities from trial to trial

Number base	Probability in an individual trial												ρ_{10}	$(\delta_0)^{10}$	δ_0
	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_t	p_e			
2	.800	.200	—	—	—	—	—	—	—	—	—	—	.0060466176	.0060466176	.600
3	.500	.300	.200	—	—	—	—	—	—	—	—	—	.0000018357	.0000059049	.300
3	.970	.020	.010	—	—	—	—	—	—	—	—	—	.6616765365	.6648326360	.960
3	.400	.300	.300	—	—	—	—	—	—	—	—	—	.0000000001	.0000000001	.100
4	.200	.100	.400	.300	—	—	—	—	—	—	—	—	.0000032768	.0001048576	.400
5	.050	.200	.400	.020	.330	—	—	—	—	—	—	—	.0007878177	.0156833688	.660
6	.080	.240	.360	.020	.200	.100	—	—	—	—	—	—	.0000168472	.0060466176	.600
7	.300	.020	.240	.050	.130	.170	.090	—	—	—	—	—	.0001778804	.0025329516	.550
8	.200	.050	.060	.180	.160	.090	.150	.110	—	—	—	—	.0000000965	.0000627821	.380
9	.030	.080	.150	.060	.140	.090	.190	.050	.210	—	—	—	.0000052328	.0005259913	.470
10	.050	.150	.200	.050	.050	.120	.080	.020	.180	.100	—	—	.0000132662	.0009765625	.500
10	.010	.020	.030	.040	.050	.060	.070	.080	.090	.550	—	—	.0012522218	.0282475249	.700
10	.110	.110	.110	.110	.110	.110	.110	.110	.110	.010	—	—	.0000000001	.0000000001	.100
10	.150	.150	.150	.150	.150	.050	.050	.050	.050	.050	—	—	.0000009244	.0009765625	.500
10*	.014	.171	.164	.184	.023	.095	.047	.205	.089	.008	—	—	.0000501840	.0111739516	.638
12	.010	.070	.120	.160	.050	.020	.090	.040	.080	.110	.060	.190	.0000002256	.0009765625	.500

* This badly biased set of probabilities was used to produce the set of random decimal digits tested in the next section.

TABLE 2

Digit	0	1	2	3	4	5	6	7	8	9
Generating set.	.014	.171	.164	.184	.023	.095	.047	.205	.089	.008
Derived set.	.088	.112	.086	.105	.113	.102	.101	.098	.097	.098

Frequency test (derived set) $\chi^2 = 7.0 \qquad P = .63$

TABLE 3

*i*th digit	$(i + 1)$th digit									
	0	1	2	3	4	5	6	7	8	9
0	11	8	7	7	5	7	12	12	11	8
1	10	13	15	9	11	14	11	8	10	11
2	11	10	7	10	10	7	6	9	7	9
3	9	10	3	14	12	17	9	8	11	12
4	6	12	10	10	19	6	16	14	13	7
5	9	17	11	14	10	6	5	15	6	9
6	6	14	9	9	14	10	15	8	6	10
7	13	10	9	9	8	11	7	12	7	12
8	7	8	8	12	9	11	14	8	10	10
9	6	10	7	11	15	13	6	4	16	10

$\chi^2 = 96.8 \qquad P = .90$

In the serial test adjacent pairs of digits are tabulated. The distribution of these pairs in the derived set appears in Table 3. This test indicates that adjacent digits are independent.

TABLE 4

Gap test

Digit		Length of gap 0–1	2–4	5–7	8 and over	χ^2	P
		Frequencies					
0	Observed........	16	18	11	42	1.25	.75
	Expected........	16.53	19.10	13.92	37.45		
1	Observed........	27	27	21	36	5.44	.15
	Expected........	21.09	24.37	17.76	47.78		
2	Observed........	16	17	10	42	1.90	.60
	Expected........	16.15	18.66	13.60	36.59		
3	Observed........	19	26	18	41	.90	.92
	Expected........	19.76	22.83	16.64	44.77		
4	Observed........	31	17	20	44	7.39	.06
	Expected........	21.28	24.59	17.92	48.21		
5	Observed........	15	21	15	50	2.04	.57
	Expected........	19.19	22.17	16.16	43.48		
6	Observed........	27	25	12	36	5.95	.12
	Expected........	19.00	21.95	16.00	43.05		
7	Observed........	20	19	16	42	.40	.93
	Expected........	18.43	21.29	15.52	41.76		
8	Observed........	14	19	21	42	3.27	.35
	Expected........	18.24	21.07	15.36	41.32		
9	Observed........	18	18	21	40	2.53	.48
	Expected........	18.43	21.29	15.52	41.76		

The gap test is based upon the distribution of lengths of intervals between given digits. A comparison of the number of gaps of specified lengths and the expected number in each case is presented in Table 4. The results of this test are also in accord with the assumption of local randomness. Noting the badly biased probabilities of the initial set of digits, the results of these tests demonstrate the effectiveness of the compound randomization process.

The use of tabulating equipment for producing random decimal digits by addition modulo 10 is relatively fast and simple. The authors have just completed production of a set of 105,000 digits in less than two days' tabulating time. 75,000 cards, representing approximately 3 months' receipts of a current carload waybill study, were used to generate the digits, 14 non-correlated columns being added simultaneously. A chain of length 10 was used, although the nature of the initial data was such that a shorter length would probably have given satisfactory results. The derived set is now recorded on 1500 cards, 70 digits per card. Preliminary tests for local randomness confirm the random nature of the generating process. Upon completion of the tests this set will be reproduced in tabular form.

REFERENCES

[1] H. B. Horton, "A method for obtaining random numbers," *Annals of Math. Stat.*, Vol. 19 (1948), pp. 81–85.

[2] J. E. Walsh, "Concerning compound randomization in the binary system," unpublished manuscript, *Project RAND, Douglas Aircraft Co.*, Santa Monica, California.

[3] R. von Mises, *Probability, Statistics and Truth*, The Macmillan Co., New York, 1939.

[4] M. G. Kendall and B. B. Smith, "Randomness and random sampling numbers," *Roy. Stat. Soc. Jour.*, Vol. 101 (1938), pp. 147–166.

[5] M. G. Kendall and B. B. Smith, "Second paper on random sampling numbers," *Supp. to Roy. Stat. Soc. Jour.*, Vol. 6 (1939), pp. 51–61.

[6] G. U. Yule, "A test of Tippett's random sampling numbers," *Roy. Stat. Soc. Jour.*, Vol. 101 (1938), pp. 167–172.

[7] C. W. Vickery, "On drawing a random sample from a set of punched cards," *Supp. to Roy. Stat. Soc. Jour.*, Vol. 6 (1939), pp. 62–66.