THEMIS SIGNAL ANALYSIS STATISTICS RESEARCH PROGRAM

DEVELOPMENT OF BINARY DIGITS THAT ARE SUFFICIENTLY ACCURATE FOR SIMULATIONS AND OTHER USES

by

John E. Walsh and Grace J. Kelleher

Technical Report No. 60
Department of Statistics THEMIS Contract

March 31, 1970

Research sponsored by the Office of Naval Research
Contract N00014-68-A-0515
Project NR 042-260

DEPARTMENT OF STATISTICS
Southern Methodist University

DEVELOPMENT OF BINARY DIGITS THAT ARE SUFFICIENTLY ACCURATE FOR SIMULATIONS AND OTHER USES

*John E. Walsh and Grace J. Kelleher
Southern Methodist University

ABSTRACT

Desired is a set of very nearly random binary digits (very closely represent independent flips of an ideal coin with sides 0 and 1). Available is m X n array of approximately random binary digits obtained experimentally. No one of these digits is necessarily independent of any of the others but the level of dependence among rows is very small. A method is given for compounding these digits to obtain a smaller set that is much more nearly random. The randomness of a set of digits is measured by its "maximum bias." A set is very nearly random if its maximum bias is very small. A maximum bias for compounded digits is determined from: The compounding method, the largest contribution to the maximum bias from within rows, and the largest contribution from the dependence among rows (very small). The maximum bias for a compounded set can be very small (even when the maximum bias for the initial set is quite large) but has a lower bound depending on the bias contribution from dependence among rows. One approach is oriented toward minimizing m for a given maximum bias for the compounded set, so that obtaining the initial set is simplified. Another approach is oriented toward having the number of compounded digits a reasonably large fraction of the number in the initial set.

---

*Research partially supported by Mobil Research and Development Corporation. Also associated with ONR Contract N00014-68-A-0515 and NASA Grant NGR 44-007-028.

INTRODUCTION AND DISCUSSION

The obtaining of more nearly random binary digits by compounding of approximately random binary digits has been considered several times. H. Burke Horton [1] developed the original method for the case where the initial digits are statistically independent. A more complicated but more efficient method, where the initial digits can be placed in an $m \times n$ array, with independence among rows (but not necessarily within rows), is considered in [2]. This method, with independence also assumed within rows, is used to obtain random permutations and sets of random binary digits in [3].

Independence is assumed among most of the digits of the initial set in all three cases. However, examples show that even mild dependences of some kinds can strongly affect the maximum bias of a compounded set. The principle of extreme geographical separation outlined in [2] can be used to obtain an acceptable level of independence among rows of an $m \times n$ array of initial digits but could require substantial effort. A seemingly better way is to obtain the array of $m \times n$ initial digits less carefully but careful enough to assure that the contribution to the maximum bias of the set from the dependence among rows is at most some very small value (say, 10^{-6} or 10^{-7}). The effect of dependence among rows is then explicitly considered in determining a bound on the closeness of the compounded set to being "independent flips of an ideal coin with sides 0 and 1." Ways of doing this are the subject of this paper.

Each of the random variables making up a set of binary digits is called a binary digit (not to be confused with the value obtained for the random variable). Consider the absolute value of the deviation from 1/2 of the conditional probability that a specified binary digit has the value 0 (or 1), given conditions on a stated zero or more remaining digits of the set. This absolute deviation is called the bias of that digit for the given conditions. The maximum bias of a binary digit is the maximum of the biases of that digit over all the possible conditions. The maximum bias of the set is the largest of the maximum biases for the digits of the set. A set of binary digits is random if and only if its maximum bias is zero.

The method of proof is of the nature of starting with axioms (assumptions) and drawing conclusions. The conclusions necessarily hold if the axioms are satisfied.

The first step consists of obtaining m sets (rows) of n approximately random binary digits by some experimental process (such as flipping coins that are not badly malformed). The experimental process is assumed to be such that the maximum bias within rows, where each row constitutes a separate set, is at most β. Also, the overall contribution to the maximum bias from the dependence among the m sets is at most ϵ. Thus, the maximum bias for the $m \times n$ array of initial binary digits is at most $\beta + \epsilon$. Here, β could be moderately large (say, 1/4 or 1/5) but ϵ is very small (say, 10^{-7} or 10^{-6}), with the implication that terms of order ϵ^2 can be neglected in derivations.

The assumption (axiom) of $\beta \leq 1/4$ should be satisfied beyond any reasonable doubt if the n digits for a row are obtained at all carefully. For example, the separate and careful flipping of standard coins should produce sets of n digits that satisfy this assumption. In fact, the assumption of $\beta \le 1/10$ should hold if the coins are carefully selected and are separately and carefully flipped, to land on a flat and even surface that is hard. The assumption $\epsilon \le 10^{-7}$ should be satisfied beyond reasonable doubt if the sets of n digits are obtained at separate locations and/or at separate times.

A basic type of compounding method is given. Suitable repetitive use of this method yields a final set of compounded binary digits. One use is oriented toward obtaining a specified maximum bias from an initial set of digits with minimum value for m. Then, the number of separate locations or times that need to be used for obtaining the initial set is minimum. Another use is oriented toward obtaining a final set whose size, for a specified maximum bias, is a reasonably large fraction of the number of digits in the initial set.

The question of when the maximum bias of a set is small enough for satisfactory use of these binary digits is considered in [2]. If N is the number of digits, the set should be acceptably satisfactory for virtually any use when

$$N \le \left[50 \text{ (maximum bias)}\right]^{-1}.$$

In particular, this criterion can be used to decide on the suitability of a table of (approximately) random binary digits.

The next section contains the basic compounding method, discussion of repetitive uses, and some theorems. Verification for the theorems is given in the final section.

COMPOUNDING METHOD AND THEOREMS

Let us consider the array of mn binary digits

$$\begin{array}{l} x_{11},\ x_{12}, \dots, x_{1n} \\ x_{21},\ x_{22}, \dots, x_{2n} \\ \vdots \quad\ \vdots \qquad \vdots \\ x_{m1},\ x_{m2}, \dots, x_{mn}, \end{array}$$

which satisfies the following conditions

(i) The maximum bias for a row, considered by itself, is at most β.

(ii) Statistical dependence among rows is such that if β^* is the maximum bias for a digit, over the row in which it occurs, then $\beta^* + \epsilon^*$ is the maximum bias for this digit over all the other digits, where $\epsilon^* \le \epsilon$.

A new set of $(m-1)n$ binary digits y_{ij} is formed by the compounding **process**

$$y_{ij} = x_{mj} + x_{ij} \pmod 2, \quad (i = 1, \dots, m-1;\ j = 1, \dots, n).$$

The biases of the y_{ij} have the properties

<u>THEOREM 1</u> <u>If exactly</u> $t-1$ <u>of</u> $y_{ij}, \dots, y_{(i-1)j}, y_{(i+1)j}, \dots, y_{(m-1)j}$ <u>have known values (nothing known about the values of the others), and any set of zero or more of the</u> y_{pq} <u>with</u> $q \neq j$ <u>have known values, the maximum bias of</u> y_{ij} <u>does not exceed</u> $B(\beta, \epsilon_x, t)$, <u>which equals</u>

$$\beta\left[(1/2 + \beta)^t - (1/2 - \beta)^t\right]\left[(1/2 + \beta)^t + (1/2 - \beta)^t\right]^{-1}$$

$$+ \epsilon_x \left(1 + (t-1)\left\{ 2 - \beta\left[(1/2 + \beta)^t + (1/2 - \beta)^t\right]^{-1}\left[(1/2 + \beta)^{t-1} - (1/2 - \beta)^{t-1} - \left\{(1/2 + \beta)^{t-1} + (1/2 - \beta)^{t-1}\right\}\left\{(1/2 + \beta)^t - (1/2 - \beta)^t\right\}\right]\right\}\right)$$

<u>plus terms that are</u> $O(\epsilon_x^2)$. <u>Here,</u> ϵ_x <u>is the bias contribution from dependence among rows for this compounding and</u> $\epsilon_x \le \epsilon$.

<u>COROLLARY 1.</u> <u>The maximum bias of the entire set of</u> y_{ij} <u>does not exceed</u> $B(\beta, \epsilon, m-1)$.

When the first term in the expression for $B(\beta, \epsilon_x, t)$ is predominant, the more conservative $[1 + 2(t-1)]\ \epsilon_x$ can be used for the second term, and the computations are simplified. However, the computations for evaluations of the first term can provide values that are usable for the second term, so evaluation of the second term need not require a large amount of additional computation.

Now, consider repetitive use of these basic results and the special case where m is the form $(1+t_1)\ldots(1+t_K)$ for given values of K and $t_1,\ldots,t_K$. First, the rows are (unbiasedly) divided into $(1+t_2)\ldots(1+t_K)$ sets, each consisting of $(1+t_1)$ rows, in some specified way. Each of these sets is an array of $(1+t_1) \times n$ binary digits and is a special case of Theorem 1 with $(1+t_1)$ used in place of m. Apply the method to obtain y_{ij} from x_{uv} separately to each of these arrays. Each array yields $t_1 n$ binary digits. In each of these $(1+t_2)\ldots(1+t_K)$ sets, arrange the $t_1 n$ digits into a single row in some stated way. This provides a $(1+t_2)\ldots(1+t_K) \times t_1 n$ array which is the type considered with $(1+t_2\ldots(1+t_K)$ in place of m and $t_1 n$ in place of n. Repeat this procedure with respect to t_2, obtaining an array of $(1+t_3)\ldots(1+t_K) \times t_1 t_2 n$ digits that is of the type considered. Continue until a $(1+t_K) \times t_1\ldots t_{K-1} n$ array is obtained. Finally, using this array in the manner used to obtain the y_{ij}, form a set of binary digits Y_{gh}, $(g=1,\ldots,t_K;\ h=1,\ldots,t_1\ldots t_{K-1} n)$.

of the initial set of mn digits. The same upper bound on β_K can be accomplished with the number of final digits a reasonably large fraction of mn. In some cases, however, having the smallest possible value for m can be the predominant consideration.

Next, consider situations where the number of digits in the final compounded set is required to be at least a specified fraction 1/C, ($C > 1$), of the original number of digits. Then, K and $t_1, \ldots, t_K$ are to be chosen so that

$$t_1 \ldots t_K \big/ (1+t_1) \ldots (1+t_K) \geq 1/C.$$

Also, for given K and C, it seems desirable to choose $t_1, \ldots, t_K$ so that β_K is approximately minimized. Examination of Theorem 2 indicates that a reasonable way of selecting $t_1, \ldots, t_K$ is to choose t_1 as small as possible; then, using this t_1, choose t_2 as small as possible, etc. It has been found (see [2]) that t_1 is the smallest integer satisfying

$$t_1 > 1/(C-1).$$

Also, for $2 \leq w \leq K-1$, and already having determined $t_1, \ldots, t_{w-1}$ as their minimum values, t_w is the smallest integer such that

$$t_w > \left[-1 + Ct_1 \ldots t_{w-1} \big/ (1+t_1) \ldots (1+t_{w-1})\right]^{-1}.$$

Finally, given $t_1, \ldots, t_{K-1}$ as their minimum values, t_K is the smallest integer satisfying

$$t_K \geq \left[-1 + Ct_1 \ldots t_{K-1}, \big/ (1+t_1) \ldots (1+t_{K-1})\right]^{-1}.$$

VERIFICATIONS

First, consider verification of Theorem 1. For convenience, suppose that y_{11} is the binary digit considered and that $y_{21}, y_{31}, \ldots, y_{t1}$, $(1 \le t \le m-1)$, are the t-1 of $y_{21}, \ldots, y_{(m-1)1}$ have known values. Also, a set S of zero or more of the y_{ij} with $j \ne 1$ have known values. Nothing is known about the values of any of the other y_{ij}. Use of t=1 implies that none of $y_{21}, \ldots, y_{(m-1)1}$ have known values.

Let $b_1, \ldots, b_t$ have arbitrary but specified values that are 0 or 1. Also, note that $y_{11}, \ldots, y_{(m-1)1}$ are obtained from the digits $x_{11}, \ldots, x_{m1}$. Notationally,

$$P(x_{m1} = 0 | x_{11} = b_1, \ldots, x_{t1} = b_t; S) = 1/2 + \alpha_{t+1} + \epsilon'_{t+1},$$

$$P(x_{m1} = 1 | x_{11} = 1-b_1, \ldots, x_{t1} = 1-b_t; S) = 1/2 - \alpha_{t+1} + \epsilon''_{t+1},$$

$$P(x_{m1} = 0 | x_{21} = b_2, \ldots, x_{t1} = b_t; S) = 1/2 + \alpha_{t+1} + \epsilon'''_{t+1}$$

$$P(x_{m1} = 1 | x_{21} = 1-b_2, \ldots, x_{t1} = 1-b_t; S) = 1/2 - \alpha_{t+1} + \epsilon''''_{t+1},$$

where α_{t+1} can have any value from $-\beta$ to β while, separately, each of ϵ'_{t+1}, ϵ''_{t+1}, ϵ'''_{t+1}, ϵ''''_{t+1} can have any value from $-\epsilon_x$ to ϵ_x. Also

$$P(x_{k1} = b_k | x_{11} = b_1, \ldots, x_{(k-1)1} = b_{k-1}; S) = 1/2 + \alpha_k + \epsilon'_k,$$

$$P(x_{k1} = 1-b_k | x_{11} = 1-b_1, \ldots, x_{(k-1)1} = 1-b_{k-1}; S) = 1/2 - \alpha_k + \epsilon''_k,$$

for k=1,...,t, where no conditions other than S occur for k=1. Also, for $t \ge 2$,

$$P(x_{k1} = b_k | x_{21} = 1-b_2, \ldots, x_{(k-1)1} = b_{k-1}; S) = 1/2 + \alpha_k + \epsilon'''_k,$$

$$P(x_{k1} = 1-b_k | x_{21} = 1-b_2, \ldots, x_{(k-1)1} = 1-b_{k-1}; S) = 1/2 - \alpha_k + \epsilon''''_k,$$

with $k=2,\ldots,t$, where no conditions other than S occur for $k=2$. Each α_k can have any value from $-\beta$ to β. All of ϵ'_1, ϵ''_1, ϵ'''_2, ϵ''''_2 are zero. Otherwise, separately, each ϵ'_k, ϵ''_k, ϵ'''_k, ϵ''''_k can have any value from $-\epsilon_x$ to ϵ_x. When $t=1$, the digit x_{21} becomes x_{m1} and $b_2=0$.

In terms of this notation $P(y_{11} = b_1 | y_{21} = b_2, \ldots, y_{t1} = b_t; S)$ can be expressed as

$$\left[(1/2 + \alpha_1) \prod_{k=2}^{t+1} (1/2 + \alpha_k + \epsilon'_k) + (1/2 - \alpha_1) \prod_{k=2}^{t+1} (1/2 - \alpha_k + \epsilon''_k)\right] \tag{1}$$

$$\times \left[(1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 + \alpha_k + \epsilon'''_k) + (1/2 - \alpha_2) \prod_{k=3}^{t+1} (1/2 - \alpha_k + \epsilon''''_k)\right]^{-1},$$

where a product from $k=3$ to $k=t+1$ does not occur when $t=1$. The maximum possible bias, with terms that are $O(\epsilon_x^{\,2})$ neglected, can be determined by maximizing this probability by choice of possible values for the α_k, the ϵ'_k, the ϵ''_k, the ϵ'''_k, and the ϵ''''_k. Alternately, with the same expression being obtained for the maximum possible bias, the value of (1) could be minimized. The verification given is based on maximizing (1).

Evidently (1) is largest when $\epsilon'_k = \epsilon''_k = \epsilon_x$ for $k=2,\ldots,t$ and $\epsilon'''_k = \epsilon''''_k = -\epsilon_x$ for $k=3,\ldots,t$, so that (1) becomes

$$\left[(1/2 + \alpha_1) \prod_{k=2}^{t+1} (1/2 + \alpha_k + \epsilon_x) + (1/2 - \alpha_1) \prod_{k=2}^{t+1} (1/2 - \alpha_k + \epsilon_x)\right]$$

$$\times \left[(1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 + \alpha_k - \epsilon_x) + (1/2 - \alpha_2) \prod_{k=3}^{t+1} (1/2 - \alpha_k - \epsilon_x)\right]^{-1}$$

$$= \Big[(1/2 + \alpha_1)(1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 + \alpha_k - \epsilon_x) +$$

$$(1/2 - \alpha_1)(1/2 - \alpha_2)\prod_{k=3}^{t+1}(1/2 - \alpha_k - \epsilon_x)\Big]$$

$$\times \Big[(1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 + \alpha_k - \epsilon_x) + (1/2 - \alpha_2) \prod_{k=3}^{t+1} (1/2 - \alpha_k - \epsilon_x)\Big]^{-1}$$

$$+ \epsilon_x \Big[(1/2 + \alpha_1)\prod_{k=3}^{t+1} (1/2 + \alpha_k) + (1/2 - \alpha_1)\prod_{k=3}^{t+1} (1/2 - \alpha_k)\Big] \qquad (2)$$

$$+ 2\epsilon_x \Big[(1/2 + \alpha_1)(1/2 + \alpha_2) \sum_{j=3}^{t+1} \prod_{\substack{k=3 \\ k\neq j}}^{t+1}(1/2 + \alpha_k)$$

$$+ (1/2 - \alpha_1)(1/2 - \alpha_2) \sum_{j=3}^{t+1} \prod_{\substack{k=3 \\ k\neq j}}^{t+1} (1/2 - \alpha_k)\Big] + O(\epsilon_x^2).$$

The first of the terms in expression (2) can be stated as

$$1/2 + \alpha_1\Big[(1/2 + \alpha_2)\prod_{k=3}^{t+1} (1/2 + \alpha_k - \epsilon_x) - (1/2 - \alpha_2)\prod_{k=3}^{t+1} (1/2 - \alpha_k - \epsilon_x)\Big]$$

$$\times \Big[(1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 + \alpha_k - \epsilon_x) + (1/2 + \alpha_2) \prod_{k=3}^{t+1} (1/2 - \alpha_k - \epsilon_x)\Big]^{-1}$$

and, by an argument similar to that in [2], this term is easily seen to be maximum when all the α_k equal β. Hence, except for terms that are $O(\epsilon_x)$, expression (2) is maximized by setting all the α_k equal to β. Thus, the maximizing values for the α_k are all of the form $\beta + O(\epsilon_x) \leq \beta$ and the first term is maximum when all the α_k equal β. Also, replacing α_k by β in the second and third terms of (2) has the same effect as replacement by $\beta + O(\epsilon_x)$, if terms that are $O(\epsilon_x^2)$ receive no consideration. Hence, (2) is maximized, except for terms that are $O(\epsilon_x^2)$, when all the α_k are set equal to β. This substitution yields the expression

$$1/2 + \beta\left[(1/2 + \beta)(1/2 + \beta - \epsilon_x)^{t-1} - (1/2 - \beta)(1/2 - \beta - \epsilon_x)^{t-1}\right]$$

$$\times \left[(1/2 + \beta)(1/2 + \beta - \epsilon_x)^{t-1} + (1/2 - \beta)(1/2 - \beta - \epsilon_x)^{t-1}\right]^{-1}$$

$$+ \left[1 + 2(t-1)\right]\epsilon_x \left[(1/2 + \beta)^t + (1/2 - \beta)^t\right] + O(\epsilon_x^2)$$

$$= 1/2 + \beta \left[(1/2 + \beta)^t - (1/2 - \beta)^t\right] \left[(1/2 + \beta)^t + (1/2 - \beta)^t\right]^{-1}$$

$$+ \epsilon_x \Bigg(1 + (t-1) \Big\{2 - \beta \left[(1/2 + \beta)^t + (1/2 - \beta)^t\right]^{-1} \Big[(1/2 + \beta)^{t-1} - (1/2 - \beta)^{t-1}$$

$$- \left\{(1/2 + \beta)^{t-1} + (1/2 - \beta)^{t-1}\right\} \left\{(1/2 + \beta)^t - (1/2 - \beta)\right\}^t\Big]\Big\}\Bigg)$$

plus terms that are $O(\epsilon_x^2)$.

Now consider verification of Theorem 2. This follows in a direct fashion from the successive steps and the fact that the overall contribution to a bias from the dependency among rows never exceeds ϵ. Acrually, for most applications, the value for β_K would change only slightly if all of the ϵ_w are taken equal to ϵ.

REFERENCES

[1] Horton, H. Burke (1948). A method for obtaining random numbers. *Ann. Math. Statist.* **19** 81-85

[2] Walsh, John E. (1949). Concerning Compound randomization in the binary system. *Ann. Math. Statist.* **20** 580-589.

[3] Walsh, John E. (1957). An experimental method for obtaining random digits and permutations. *Sankhyā* **17** 355-360.

UNCLASSIFIED
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) SOUTHERN METHODIST UNIVERSITY	2a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED 2b. GROUP UNCLASSIFIED

3. REPORT TITLE

Development of binary digits that are sufficiently accurate for simulations and other uses.

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

Technical Report

5. AUTHOR(S) (First name, middle initial, last name)

John E. Walsh
Grace J. Kelleher

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
March 31, 1970	13	3

8a. CONTRACT OR GRANT NO. N00014-68-A-0515	9a. ORIGINATOR'S REPORT NUMBER(S) 60
b. PROJECT NO. NR 042-260	
c.	9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)
d.	

10. DISTRIBUTION STATEMENT

This document has been approved for public release and sale; its distribution is unlimited. Reproduction in whole or in part is permitted for any purpose of the United States Government.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY
	Office of Naval Research

13. ABSTRACT

Desired is a set of very nearly random binary digits (very closely represent independent flips of an ideal coin with sides 0 and 1). Available is m X n array of approximately random binary digits obtained experimentally. No one of these digits is necessarily independent of any of the others but the level of dependence among rows is very small. A method is given for compounding these digits to obtain a smaller set that is much more nearly random. The randomness of a set of digits is measured by its "maximum bias". A set is very nearly random if its maximum bias is very small. A maximum bias for compounded digits is determined from: The compounding method, the largest contribution to the maximum bias from within rows, and the largest contribution from the dependence among rows (very small). The maximum bias for a compounded set can be very small (even when the maximum bias for the initial set is quite large) but has a lower bound depending on the bias contribution from dependence among rows. One approach is oriented toward minimizing m for a given maximum bias for the compounded set, so that obtaining the initial set is simplified. Another approach is oriented toward having the number of compounded digits a reasonably large fraction of the number in the initial set.

DD FORM 1 NOV 65 1473 (PAGE 1)
S/N 0101-807-6811

UNCLASSIFIED
Security Classification

A-31408