

A LOWER BOUND FOR THE CHUNG-DIACONIS-GRAHAM RANDOM PROCESS

MARTIN HILDEBRAND

(Communicated by Richard C. Bradley)

ABSTRACT. Chung, Diaconis, and Graham considered random processes of the form $X_{n+1} = a_n X_n + b_n \pmod{p}$ where p is odd, $X_0 = 0$, $a_n = 2$ always, and b_n are i.i.d. for $n = 0, 1, 2, \dots$. In this paper, we show that if $P(b_n = -1) = P(b_n = 0) = P(b_n = 1) = 1/3$, then there exists a constant $c > 1$ such that $c \log_2 p$ steps are not enough to make X_n get close to being uniformly distributed on the integers mod p .

1. INTRODUCTION

In [2], Chung, Diaconis, and Graham considered random processes of the form

$$X_{n+1} = 2X_n + b_n \pmod{p}$$

where $X_0 = 0$, b_n are i.i.d. for $n = 0, 1, 2, \dots$, and p is odd. They focussed on the case where $P(b_n = 1) = P(b_n = 0) = P(b_n = -1) = 1/3$. These random processes have some similarity to certain pseudorandom sequences used by computers. Subsequently some generalizations of this random process have been considered. See, for example, [1], [4], [5], and [6]. Suppose $P_n(s) = P(X_n = s)$ where $s \in \mathbb{Z}/p\mathbb{Z}$. Define the variation distance of a probability P on $\mathbb{Z}/p\mathbb{Z}$ from the uniform distribution U on $\mathbb{Z}/p\mathbb{Z}$ by

$$\|P - U\| = \frac{1}{2} \sum_{s \in \mathbb{Z}/p\mathbb{Z}} |P(s) - 1/p| = \max_{A \subseteq \mathbb{Z}/p\mathbb{Z}} |P(A) - U(A)|.$$

Chung, Diaconis, and Graham showed that for almost all odd p , if $N \geq \frac{\log p}{\log(9/5)} + c$, then $\|P_N - U\| = O((5/9)^c)$. They also state that more complicated arguments give the following result: For any $\epsilon > 0$ and almost all odd p , if $N \geq (\hat{c} + \epsilon) \log_2 p$, then $\|P_N - U\| < \epsilon$ where

$$\hat{c} = \left(1 - \log_2 \left(\frac{5 + \sqrt{17}}{9} \right) \right)^{-1} = 1.01999186\dots$$

Note that the values of X_N , when viewed as integers, range from $-2^N + 1$ to $2^N - 1$, inclusive. Thus, if $N < (1 - \epsilon) \log_2 p$ where $\epsilon > 0$ is given, the number of values in this range is at most $2p^{1-\epsilon} - 1$, and $\|P_N - U\| > 1 - (2p^{1-\epsilon} - 1)/p \rightarrow 1$ as $p \rightarrow \infty$.

Received by the editors June 2, 2008.

2000 *Mathematics Subject Classification*. Primary 60C05; Secondary 60B15.

©2008 American Mathematical Society
Reverts to public domain 28 years from publication

Chung, Diaconis, and Graham [2] speculate, “It is conceivable that in fact $(1 + o(1)) \log_2 p$ steps are enough for almost all [odd] p to force P_N to converge to uniform.” However, we shall show that this statement, although described as conceivable in [2], is in fact false. In particular, we shall prove the following theorem:

Theorem 1. *If $P(b_n = 1) = P(b_n = 0) = P(b_n = -1) = 1/3$ and X_n and P_n are as above, then there exists a value $c_1 > 1$ such that if $n = n(p) < c_1 \log_2 p$, then $\|P_n - U\| \rightarrow 1$ as $p \rightarrow \infty$.*

To motivate somewhat the proof of this theorem, we shall also prove the following theorem:

Theorem 2. *If $P(b_n = 1) = 0.4$, $P(b_n = 0) = 0.6$, and X_n and P_n are as above, then there exists a value $c_2 > 1$ such that if $n = n(p) < c_2 \log_2 p$, then $\|P_n - U\| \rightarrow 1$ as $p \rightarrow \infty$.*

2. PROOF OF THEOREM 2

First observe that the following proposition holds:

Proposition 1. *If $X_0 = 0$ and $X_{n+1} = 2X_n + b_n$ for $n \geq 0$, then*

$$X_n = \sum_{i=0}^{n-1} 2^{n-1-i} b_i.$$

Now suppose $P(b_n = 1) = 0.4$ and $P(b_n = 0) = 0.6$. Let $A_n = |\{m : 0 \leq m \leq n - 1, b_m = 1\}|$. By elementary arguments, for any $\epsilon > 0$, $P((0.4 - \epsilon)n < A_n < (0.4 + \epsilon)n) \rightarrow 1$ as $n \rightarrow \infty$. Thus, except on a set which has probability approaching 0 as $n \rightarrow \infty$, X_n takes on at most

$$\sum_{j=\lceil(0.4-\epsilon)n\rceil}^{\lfloor(0.4+\epsilon)n\rfloor} \binom{n}{j}$$

different values. We shall assume that $0.4 + \epsilon < 0.5$. Note that Stirling’s formula implies

$$\begin{aligned} & \sum_{j=\lceil(0.4-\epsilon)n\rceil}^{\lfloor(0.4+\epsilon)n\rfloor} \binom{n}{j} \\ & \leq (2\epsilon n + 1) \binom{n}{\lfloor(0.4 + \epsilon)n\rfloor} \\ & \leq \frac{(2\epsilon n + 1)c_3 n^n \sqrt{2\pi n}}{((0.4 + \epsilon)n)^{(0.4+\epsilon)n} ((0.6 - \epsilon)n)^{(0.6-\epsilon)n} 2\pi \sqrt{((0.4 + \epsilon)n)((0.6 - \epsilon)n)}} \\ & \leq \frac{c_3(2\epsilon n + 1)\sqrt{2\pi n}}{2\pi \sqrt{((0.4 + \epsilon)n)((0.6 - \epsilon)n)}} \cdot \frac{1}{(0.4 + \epsilon)^{(0.4+\epsilon)n} (0.6 - \epsilon)^{(0.6-\epsilon)n}} \end{aligned}$$

where c_3 is a positive constant. Note that

$$(0.4 + \epsilon)^{(0.4+\epsilon)n} (0.6 - \epsilon)^{(0.6-\epsilon)n} = 2^{n((0.4+\epsilon) \log_2(0.4+\epsilon) + (0.6-\epsilon) \log_2(0.6-\epsilon))}.$$

It can be shown that if $0 < \epsilon < 0.1$, then

$$-((0.4 + \epsilon) \log_2(0.4 + \epsilon) + (0.6 - \epsilon) \log_2(0.6 - \epsilon)) < 1.$$

If

$$c_2 < \frac{1}{-((0.4 + \epsilon) \log_2(0.4 + \epsilon) + (0.6 - \epsilon) \log_2(0.6 - \epsilon))}$$

and $n = n(p) < c_2 \log_2 p$, then

$$\frac{\sum_{j=\lceil(0.4-\epsilon)n\rceil}^{\lfloor(0.4+\epsilon)n\rfloor} \binom{n}{j}}{p} \rightarrow 0$$

as $p \rightarrow \infty$. Thus $\|P_n - U\| \rightarrow 1$ as $p \rightarrow \infty$ if $n = n(p) < c_2 \log_2 p$. Note that c_2 can be chosen so that $c_2 > 1$, since

$$\frac{1}{-((0.4 + \epsilon) \log_2(0.4 + \epsilon) + (0.6 - \epsilon) \log_2(0.6 - \epsilon))} > 1.$$

□

3. OVERVIEW OF THE PROOF OF THEOREM 1

By Proposition 1, X_n is determined by the n -tuple $(b_0, b_1, \dots, b_{n-1})$. However, if $P(b_n = 1) = P(b_n = 0) = P(b_n = -1)$, then many possible n -tuples $(b_0, b_1, \dots, b_{n-1})$ may give the same value for X_n . For example, if $n = 3$, the 3-tuples $(1, -1, -1)$, $(0, 1, -1)$, and $(0, 0, 1)$ all give $X_3 = 1$. We shall place the n -tuple in a standard form $(\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1})$ so that

$$2^{n-1}\tilde{b}_0 + 2^{n-2}\tilde{b}_1 + \dots + \tilde{b}_{n-1} = 2^{n-1}b_0 + 2^{n-2}b_1 + \dots + b_{n-1}.$$

In this standard form, either none of $\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1}$ are -1 or none of $\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1}$ are 1 . In the first case (excluding the event where b_0, b_1, \dots, b_{n-1} are all 0), we shall show that for every $\epsilon > 0$, the number of values a in $\{1, \dots, n - 1\}$ such that both \tilde{b}_{a-1} and \tilde{b}_a are 1 lies between $(4/18 - \epsilon)n$ and $(4/18 + \epsilon)n$, except for events which have probability approaching 0 as $n \rightarrow \infty$. Likewise, in the second case (excluding the event where b_0, b_1, \dots, b_{n-1} are all 0), the number of values a in $\{1, 2, \dots, n - 1\}$ such that both \tilde{b}_{a-1} and \tilde{b}_a are -1 lies between $((4/18) - \epsilon)n$ and $((4/18) + \epsilon)n$, except for events which have probability approaching 0 as $n \rightarrow \infty$. A Stirling's formula argument will give the theorem.

We shall divide the n -tuples $(b_0, b_1, \dots, b_{n-1})$ into three cases. In the first case, there exists a value j in $\{0, 1, \dots, n - 1\}$ such that $b_j = 1$ and $b_k = 0$ if $0 \leq k < j$. We call this case "first 1 ". In the second case, there exists a value j in $\{0, 1, \dots, n - 1\}$ such that $b_j = -1$ and $b_k = 0$ if $0 \leq k < j$. We call this case "first -1 ". In the third case, $b_0 = b_1 = \dots = b_{n-1} = 0$. As $n \rightarrow \infty$, the probability of "first 1 " approaches $1/2$, and the probability of "first -1 " approaches $1/2$. (Both probabilities are $(1/2)(1 - (1/3)^n)$.) In "first 1 ", none of $\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1}$ are -1 . In "first -1 ", none of $\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1}$ are 1 . We shall give detailed arguments for "first 1 "; the arguments for "first -1 " are similar.

If we are in "first 1 ", consider the infinite sequence (b_0, b_1, b_2, \dots) . After some leading zeroes, with probability 1 this sequence consists of strings of "blocks" B_1, B_2, \dots where each B_i is a finite string starting with 1 and having no other 1 's in it. For example, if $(b_0, b_1, \dots, b_{10}) = (0, 0, 1, -1, 0, 1, 0, 1, -1, 1, 1)$, then there are two leading zeroes, followed by $B_1 = (1, -1, 0)$, $B_2 = (1, 0)$, $B_3 = (1, -1)$, and $B_4 = (1)$. Also we say that the first coordinate of B_1 is b_2 and that B_1 has b_2, b_3 , and b_4 as its coordinates. Note that the blocks B_1, B_2, \dots are i.i.d. given that we are in "first 1 ".

Given an infinite series (b_0, b_1, b_2, \dots) , technically the values $\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1}$ may depend on n . For example, if $(b_0, b_1, b_2) = (0, 0, 1)$, then $(\tilde{b}_0, \tilde{b}_1, \tilde{b}_2) = (0, 0, 1)$ and $\tilde{b}_2 = 1$ if $n = 3$. If $(b_0, b_1, \dots, b_{10}) = (0, 0, 1, -1, 0, 1, 0, 1, -1, 1, 1)$, then $(\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{10}) = (0, 0, 0, 1, 0, 1, 0, 0, 1, 1, 1)$ and $\tilde{b}_2 = 0$ if $n = 11$ even though b_0, b_1 , and b_2 are unchanged. Suppose a is such that B_i has b_a as one of its coordinates. Then for all $n > a$ such that B_i does not also have b_n as one of its coordinates, $(\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_a)$ will no longer vary with n .

4. NUMBER OF a SUCH THAT $\tilde{b}_{a-1} = \tilde{b}_a = 1$

We shall consider several distinct ways to get values a such that $\tilde{b}_{a-1} = \tilde{b}_a = 1$. These ways are detailed in the following lemmas.

Lemma 1. *Let n_1 be the number of a in $\{1, \dots, n-1\}$ such that $\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} = 1$, and $b_a = 1$. Let $\epsilon > 0$ be given. Given that we are in “first 1”, the probability that $((1/18) - \epsilon)n < n_1 < ((1/18) + \epsilon)n$ approaches 1 as $n \rightarrow \infty$.*

Lemma 2. *Let n_2 be the number of a in $\{1, \dots, n-1\}$ such that $\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} = 1$, and $b_a \neq 1$. Then $n_2 = 0$.*

Lemma 3. *Let n_3 be the number of a in $\{1, \dots, n-1\}$ such that $\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} \neq 1$, and $b_a = 1$. Let $\epsilon > 0$ be given. Given that we are in “first 1”, the probability that $((1/18) - \epsilon)n < n_3 < ((1/18) + \epsilon)n$ approaches 1 as $n \rightarrow \infty$.*

Lemma 4. *Let n_4 be the number of a in $\{1, \dots, n-1\}$ such that $\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} \neq 1$, and $b_a \neq 1$. Let $\epsilon > 0$ be given. Given that we are in “first 1”, the probability that $((1/9) - \epsilon)n < n_4 < ((1/9) + \epsilon)n$ approaches 1 as $n \rightarrow \infty$.*

Proof of Lemma 2. If we are not in “first 1”, then \tilde{b}_a is never 1. If we are in “first 1”, then one obtains $(\tilde{b}_0, \tilde{b}_1, \dots, \tilde{b}_{n-1})$ from $(b_0, b_1, \dots, b_{n-1})$ as follows. If j is such that $b_j = 1$ and $b_k = 0$ whenever $0 \leq k < j$, then $\tilde{b}_k = 0$ whenever $0 \leq k < j$. Otherwise, for each j_0 such that $b_{j_0} = 1$, let $j_1 = \min(n, \min\{\ell : \ell > j_0, b_\ell = 1\})$. (By convention, assume that the minimum of an empty set is ∞ .) If $b_k = 0$ for all k with $j_0 < k < j_1$, then $\tilde{b}_{j_0} = 1$ and $\tilde{b}_k = 0$ for all k with $j_0 < k < j_1$. Otherwise $\tilde{b}_{j_0} = 0$, and one can figure out the unique values for \tilde{b}_k in $\{0, 1\}$ when $j_0 < k < j_1$. Lemma 2 follows. \square

Proof of Lemma 4. To prove Lemma 4, let j be such that $b_j = 1$ and $b_k = 0$ whenever $0 \leq k < j$. Suppose that $a-1 > j$ and $a < n$. Then $P(b_{a-1} \neq 1, b_a \neq 1) = 4/9$. Suppose $j_0 < a < j_1$ with $b_{j_0} = 1$ and $j_1 = \min(n, \min\{\ell : \ell > j_0, b_\ell = 1\})$. Given j_0 and j_1 , there are $2^{j_1-j_0-1}$ possibilities for $(b_{j_0+1}, \dots, b_{j_1-1})$ and $2^{j_1-j_0-1}$ possibilities for $(\tilde{b}_{j_0+1}, \dots, \tilde{b}_{j_1-1})$. The possibilities for $(b_{j_0+1}, \dots, b_{j_1-1})$, which range from $(0, \dots, 0)$ to $(-1, \dots, -1)$, are in one-to-one correspondence with the possibilities for $(\tilde{b}_{j_0+1}, \dots, \tilde{b}_{j_1-1})$, which range from $(0, \dots, 0)$ to $(1, \dots, 1)$. Thus $P(\tilde{b}_{a-1} = 1, \tilde{b}_a = 1 | b_{a-1} \neq 1, b_a \neq 1) = 1/4$, and $P(\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} \neq 1, b_a \neq 1) = 1/9$. Let $C_a = \{\tilde{b}_{a-1} = 1, \tilde{b}_a = 1, b_{a-1} \neq 1, b_a \neq 1\}$. Conditioned on j such that $b_j = 1$ and $b_k = 0$ for $0 \leq k < j$, the events C_a for $a-1 > j, a < n$, and a even are independent, and the events C_a for $a-1 > j, a < n$, and a odd are independent. Since $P(j > \epsilon_1 n) \rightarrow 0$ as $n \rightarrow \infty$ (given that we are in “first 1”) for each $\epsilon_1 > 0$, Lemma 4 follows by elementary arguments. \square

Proof of Lemma 1. To prove this lemma, suppose that we are in “first 1” and $b_{a-1} = 1$ with a in $\{1, \dots, n-1\}$. Then $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ if and only if $b_a = 1$ and $b_k = 0$ for all k with $a < k < j_1$ where $j_1 = \min(n, \min\{\ell > a : b_\ell = 1\})$. Let us consider the infinite sequence (b_0, b_1, \dots) . For positive integers i , let D_i be the event that $B_i = (1)$ and B_{i+1} has no -1 's in it. Note that $P(D_i) = (1/3)(\sum_{i=1}^\infty (1/3)^i) = 1/6$. Observe that D_1, D_3, D_5, \dots are independent and that D_2, D_4, D_6, \dots are independent. Furthermore, given $\epsilon_1 > 0$, with probability approaching 1 as $n \rightarrow \infty$, the number of a in $\{1, \dots, n-1\}$ such that $b_{a-1} = 1$ lies between $((1/3) - \epsilon_1)n$ and $((1/3) + \epsilon_1)n$ given that we are in “first 1”. Suppose we are given $\epsilon' > 0$. Choose $\epsilon_1 > 0$ so that $\epsilon_1 < 6\epsilon'$. Then with probability approaching 1 as $n \rightarrow \infty$, at least $((1/18) - \epsilon')n$ events D_i occur with $i < ((1/3) - \epsilon_1)n$, while at most $((1/18) + \epsilon')n$ events D_i occur with $i \leq ((1/3) + \epsilon_1)n$. Thus, given $\epsilon' > 0$, the number of i such that D_i occurs and the first coordinate of B_{i+1} is b_ℓ for some $\ell < n$ is, with probability approaching 1 as $n \rightarrow \infty$, between $((1/18) - \epsilon')n$ and $((1/18) + \epsilon')n$. This number of i is within 1 of the number of a in Lemma 1; the only possible difference occurs when the block B_{i+1} has b_n as one of its coordinates. \square

Proof of Lemma 3. To prove this lemma, suppose we are in “first 1”, $b_{a-1} \neq 1$, and $b_a = 1$ with a in $\{1, \dots, n-1\}$. Then $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ if and only if $b_{a-1} = -1$ and $b_k = 0$ for all k with $a < k < j_1$ where $j_1 = \min(n, \min\{\ell > a : b_\ell = 1\})$. Let us consider the infinite sequence (b_0, b_1, \dots) . For positive integers i , let E_i be the event that B_{i+1} has no -1 's in it and that B_i ends with -1 . Note that $P(E_i) = 1/6$, that E_1, E_3, E_5, \dots are independent, and that E_2, E_4, E_6, \dots are independent. Furthermore, given $\epsilon_1 > 0$, with probability approaching 1 as $n \rightarrow \infty$, the number of a in $\{1, \dots, n-1\}$ with $b_a = 1$ lies between $((1/3) - \epsilon_1)n$ and $((1/3) + \epsilon_1)n$ given that we are in “first 1”. Thus, given $\epsilon' > 0$, the number of i such that E_i occurs and the first coordinate of B_{i+1} is b_ℓ for some $\ell < n$ is, with probability approaching 1 as $n \rightarrow \infty$, between $((1/18) - \epsilon')n$ and $((1/18) + \epsilon')n$. This number of i is within 1 of the number of a in Lemma 3; the only possible difference occurs when B_{i+1} has b_n as one of its coordinates. \square

In conclusion, the number of a in $\{1, \dots, n-1\}$ such that $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ (given that we are in “first 1”) lies, with probability approaching 1 as $n \rightarrow \infty$, between $((4/18) - \epsilon)n$ and $((4/18) + \epsilon)n$ for each $\epsilon > 0$.

5. STIRLING'S FORMULA ARGUMENT

If the number of a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ is no more than $((4/18) + \epsilon)n$, then either the number of odd a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ is no more than $((2/18) + \epsilon/2)n$ or the number of even a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ is no more than $((2/18) + \epsilon/2)n$.

Let us suppose that n is even and the number of odd a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ is no more than $((2/18) + \epsilon/2)n$, where $\epsilon > 0$ is such that $(2/18) + \epsilon/2 < 1/8$. Then, the number of possible values of $\sum_{i=0}^{n-1} 2^{n-1-i} b_i$ if we have “first 1” is at most

$$\sum_{(\ell_1, \ell_2, \ell_3, \ell_4) \in R_n} \frac{((1/2)n)!}{\ell_1! \ell_2! \ell_3! \ell_4!}$$

where $R_n = \{(\ell_1, \ell_2, \ell_3, \ell_4) : \ell_1 + \ell_2 + \ell_3 + \ell_4 = (1/2)n, \ell_1 \leq ((2/18) + \epsilon/2)n\}$. The values ℓ_1, ℓ_2, ℓ_3 , and ℓ_4 represent the number of odd a in $\{1, \dots, n-1\}$ such that

$\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$, $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 0$, $\tilde{b}_{a-1} = 0$ and $\tilde{b}_a = 1$, and $\tilde{b}_{a-1} = 0$ and $\tilde{b}_a = 0$, respectively.

For some polynomial $p_1(n)$ of n ,

$$\begin{aligned} & \sum_{(\ell_1, \ell_2, \ell_3, \ell_4) \in R_n} \frac{((1/2)n)!}{\ell_1! \ell_2! \ell_3! \ell_4!} \\ & \leq \left(\left(\frac{2}{18} + \frac{\epsilon}{2} \right) n + 1 \right) n^2 \frac{(\frac{1}{2}n)!}{\lfloor (\frac{2}{18} + \frac{\epsilon}{2}) n \rfloor! (\lfloor (\frac{7}{54} - \frac{\epsilon}{6}) n \rfloor!)^3} \\ & \leq p_1(n) \frac{(\frac{1}{2}n)^{(1/2)n}}{\left((\frac{2}{18} + \frac{\epsilon}{2}) n \right)^{((2/18)+\epsilon/2)n} \left((\frac{7}{54} - \frac{\epsilon}{6}) n \right)^{((7/54)-\epsilon/6)3n}} \\ & = p_1(n) 2^{(0.5 \log_2(0.5) - ((2/18)+\epsilon/2) \log_2((2/18)+\epsilon/2) - ((7/18)-\epsilon/2) \log_2((7/54)-\epsilon/6))n}. \end{aligned}$$

But if

$$c_1 < \frac{1}{0.5 \log_2(0.5) - \frac{2}{18} \log_2\left(\frac{2}{18}\right) - \frac{7}{18} \log_2\left(\frac{7}{54}\right)},$$

where c_1 is constant and $n = n(p) < c_1 \log_2 p$, then we can choose $\epsilon > 0$ so that

$$\frac{p_1(n) 2^{(0.5 \log_2(0.5) - ((2/18)+\epsilon/2) \log_2((2/18)+\epsilon/2) - ((7/18)-\epsilon/2) \log_2((7/54)-\epsilon/6))n}}{p} \rightarrow 0$$

as $p \rightarrow \infty$.

Thus for such values n , at most $o(p)$ values of $\sum_{i=0}^{n-1} 2^{n-1-i} b_i$ occur in “first 1” if n is even and the number of odd a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ is no more than $((2/18) + \epsilon/2)n$. Minor adaptations of this argument apply if n is odd, if we consider the number of even a instead of the number of odd a , or if we consider “first -1” instead of “first 1”. (For example, if n is odd but we still consider odd a in “first 1”, note that there are at most $o(p)$ different values of X_{n-1} and 3 different values of b_n to get that there are at most $o(p)$ different values of X_n in this case.) There is only one value which is neither in “first 1” nor in “first -1”.

Observe that

$$\frac{1}{0.5 \log_2(0.5) - \frac{2}{18} \log_2\left(\frac{2}{18}\right) - \frac{7}{18} \log_2\left(\frac{7}{54}\right)} \approx 1.001525.$$

Thus we may choose a value $c_1 > 1$ such that if $n = n(p) < c_1 \log_2 p$, then X_n has, except for events with probability approaching 0 as $p \rightarrow \infty$, at most $o(p)$ values. Thus $\|P_n - U\| \rightarrow 1$ as $p \rightarrow \infty$. □

6. A LARGER VALUE FOR c_1

A more careful analysis of the proofs of Lemmas 1, 3, and 4 shows that for each $\epsilon > 0$, the number of odd a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ and the number of even a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 1$ both lie between $((2/18) - \epsilon)n$ and $((2/18) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$ given that we are in “first 1”. Given j , the events C_a are independent when a is odd, $a - 1 > j$, and $a < n$, and also the events C_a are independent when a is even, $a - 1 > j$, and $a < n$; therefore the extension of Lemma 4 is straightforward. To see how to extend Lemma 1, consider the following argument. Let i_k be the k -th odd value of i such that D_i occurs, and let m_k be the value of a such that b_a is the first coordinate of the block B_{1+i_k} . Note that $m_2 - m_1, m_3 - m_2, m_4 - m_3, \dots$ are i.i.d. Let p be the probability that $m_2 - m_1$ is odd.

	$\tilde{b}_{a-1} = 0,$ $\tilde{b}_a = 0$	$\tilde{b}_{a-1} = 0,$ $\tilde{b}_a = 1$	$\tilde{b}_{a-1} = 1,$ $\tilde{b}_a = 1$	$\tilde{b}_{a-1} = 1,$ $\tilde{b}_a = 0$
$b_{a-1} = 1, b_a = 1$	0	0	1/18	1/18
$b_{a-1} \neq 1, b_a \neq 1$	1/9	1/9	1/9	1/9
$b_{a-1} = 0, b_a = 1$	1/18	1/18	0	0
$b_{a-1} = -1, b_a = 1$	0	0	1/18	1/18
$b_{a-1} = 1, b_a = 0$	0	1/18	0	1/18
$b_{a-1} = 1, b_a = -1$	1/18	1/18	0	0

TABLE 1. Cases for $\tilde{b}_{a-1}, \tilde{b}_a, b_{a-1},$ and b_a

If m_1 is even, then the sequence m_1, m_2, m_3, \dots consists of r_1 consecutive even values, then r_2 consecutive odd values, then r_3 consecutive even values, etc., where r_1, r_2, r_3, \dots are i.i.d. geometric random variables with parameter p . If m_1 is odd, then the sequence m_1, m_2, m_3, \dots consists of r_1 consecutive odd values, then r_2 consecutive even values, then r_3 consecutive odd values, etc., where r_1, r_2, r_3, \dots are i.i.d. geometric random variables with parameter p . Note that for each $\epsilon > 0$, by Kolmogorov’s maximal inequality (see p. 61 of Durrett [3], for example), $\max(|r_1 - r_2|, |(r_1 - r_2) + (r_3 - r_4)|, \dots, |(r_1 - r_2) + (r_3 - r_4) + \dots + (r_{n-1} - r_n)|) < \epsilon n$ for even n with probability approaching 1 as $n \rightarrow \infty$. Since for some positive constant c , $\max(r_1, r_2, \dots, r_n) < c \ln(n)$ with probability approaching 1 as $n \rightarrow \infty$, this result and a similar result involving D_i when i is even imply that, for each $\epsilon > 0$, the number of odd a in $\{1, \dots, n - 1\}$ such that $b_{a-1} = 1, b_a = 1, \tilde{b}_{a-1} = 1,$ and $\tilde{b}_a = 1$ minus the number of even a in $\{1, \dots, n - 1\}$ with $b_{a-1} = 1, b_a = 1, \tilde{b}_{a-1} = 1,$ and $\tilde{b}_a = 1$ has absolute value less than ϵn with probability approaching 1 as $n \rightarrow \infty$ given that we are in “first 1”. Thus, given $\epsilon > 0$, the number of such odd a lies between $((1/36) - \epsilon)n$ and $((1/36) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$ given that we are in “first 1”. A similar argument applies for Lemma 3.

With arguments resembling the proofs of Lemmas 1, 2, 3, and 4, one can show the following:

Lemma 5. *Given that we are in “first 1”, the number of a in $\{1, \dots, n - 1\}$ such that $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 0$ lies, for each $\epsilon > 0$, between $((5/18) - \epsilon)n$ and $((5/18) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$.*

Lemma 6. *Given that we are in “first 1”, the number of a in $\{1, \dots, n - 1\}$ such that $\tilde{b}_{a-1} = 0$ and $\tilde{b}_a = 0$ lies, for each $\epsilon > 0$, between $((4/18) - \epsilon)n$ and $((4/18) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$.*

Lemma 7. *Given that we are in “first 1”, the number of a in $\{1, \dots, n - 1\}$ such that $\tilde{b}_{a-1} = 0$ and $\tilde{b}_a = 1$ lies, for each $\epsilon > 0$, between $((5/18) - \epsilon)n$ and $((5/18) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$.*

While the details are not shown here, Table 1 outlines the arguments to be shown. For example, the entry 1/18 for $b_{a-1} = 1, b_a = -1, \tilde{b}_{a-1} = 0,$ and $\tilde{b}_a = 0$ means that the number of a in $\{1, \dots, n - 1\}$ with $b_{a-1} = 1, b_a = -1, \tilde{b}_{a-1} = 0,$ and $\tilde{b}_a = 0$ lies, for a given $\epsilon > 0$, between $((1/18) - \epsilon)n$ and $((1/18) + \epsilon)n$ with probability approaching 1 as $n \rightarrow \infty$ given that we are in “first 1”.

More careful arguments (similar to the extensions of Lemmas 1, 3, and 4) show that the number of odd a in $\{1, \dots, n-1\}$ with $\tilde{b}_{a-1} = 1$ and $\tilde{b}_a = 0$ lies between $((5/36) - \epsilon)n$ and $((5/36) + \epsilon)n$ (for a given $\epsilon > 0$) with probability approaching 1 as $n \rightarrow \infty$ given that we are in “first 1”. Similar statements hold for even a here; similar statements (where $2/18$ replaces $4/18$ and $5/36$ replaces $5/18$) also hold for odd a and even a in Lemmas 6 and 7.

The total number of possible values of $\sum_{i=0}^{n-1} 2^{n-1-i} b_i$ (except for events with probability approaching 0 as $n \rightarrow \infty$) in “first 1” is at most (for even n)

$$\sum_{(\ell_1, \ell_2, \ell_3, \ell_4) \in S_n} \binom{\frac{1}{2}n}{\ell_1, \ell_2, \ell_3, \ell_4}$$

with $S_n = \{(\ell_1, \ell_2, \ell_3, \ell_4) : \ell_1 + \ell_2 + \ell_3 + \ell_4 = (1/2)n, ((4/36) - \epsilon)n < \ell_1 < ((4/36) + \epsilon)n, ((5/36) - \epsilon)n < \ell_2 < ((5/36) + \epsilon)n, ((5/36) - \epsilon)n < \ell_3 < ((5/36) + \epsilon)n, ((4/36) - \epsilon)n < \ell_4 < ((4/36) + \epsilon)n\}$.

A Stirling’s formula argument shows that if

$$c_1 < \frac{1}{0.5 \log_2(0.5) - \frac{4}{18} \log_2\left(\frac{4}{36}\right) - \frac{5}{18} \log_2\left(\frac{5}{36}\right)}$$

and $n = n(p) < c_1 \log_2 p$ where c_1 is a constant, then

$$\sum_{(\ell_1, \ell_2, \ell_3, \ell_4) \in S_n} \binom{\frac{1}{2}n}{\ell_1, \ell_2, \ell_3, \ell_4}$$

is $o(p)$. For odd n or “first -1 ”, similar arguments can be used. Thus if $n = n(p) < c_1 \log_2 p$, X_n has $o(p)$ possible different values except for events with probability approaching 0 as $p \rightarrow \infty$. Thus $\|P_n - U\| \rightarrow 1$ as $p \rightarrow \infty$.

Note that

$$\frac{1}{0.5 \log_2(0.5) - \frac{4}{18} \log_2\left(\frac{4}{36}\right) - \frac{5}{18} \log_2\left(\frac{5}{36}\right)} \approx 1.00448.$$

Thus there is a gap between this lower bound and the best upper bound claimed in Chung, Diaconis, and Graham [2]. Exploring this gap is a potential problem for further study.

ACKNOWLEDGMENTS

The author thanks Ron Graham for mentioning this problem in a talk at a conference on the mathematics of Persi Diaconis in 2005. The author also thanks Persi Diaconis for encouragement.

REFERENCES

- [1] Ascì, C. “Generating uniform random vectors”. *J. Theoret. Probab.* **14** (2001), 333-356. MR1838732 (2002c:60115)
- [2] Chung, F., Diaconis, P., and Graham, R. “Random walks arising in random number generation”. *Ann. Probab.* **15** (1987), 1148-1165. MR893921 (88d:60033)
- [3] Durrett, R. *Probability: Theory and Examples*, third edition. Wadsworth & Brooks/Cole, Pacific Grove, CA, 2005. MR1068527 (91m:60002)
- [4] Hildebrand, M. “Random processes of the form $X_{n+1} = a_n X_n + b_n \pmod{p}$ ”. *Ann. Probab.* **21** (1993), 710-720. MR1217562 (94d:60012)

- [5] Hildebrand, M. "Random processes of the form $X_{n+1} = a_n X_n + b_n \pmod{p}$ where b_n takes on a single value". pp. 153-174, *Random Discrete Structures*, ed. Aldous and Pemantle. Springer-Verlag, New York, 1996. MR1395613 (97g:60085)
- [6] Hildebrand, M. "On the Chung-Diaconis-Graham random process". *Electron. Commun. Probab.* **11** (2006), 347-356. MR2274529 (2008g:60017)

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY AT ALBANY, STATE UNIVERSITY
OF NEW YORK, ALBANY, NEW YORK 12222