Elect. Comm. in Probab. **11** (2006), 347–356

ELECTRONIC COMMUNICATIONS in PROBABILITY

ON THE CHUNG-DIACONIS-GRAHAM RANDOM PROCESS

MARTIN HILDEBRAND
Department of Mathematics and Statistics, University at Albany, State University of New York, Albany, NY 12222 USA
email: martinhi@math.albany.edu

Submitted November 5, 2006, *accepted in final form* December 11, 2006

AMS 2000 Subject classification: 60B15, 60J10
Keywords: Random processes, discrete Fourier analysis

Abstract
Chung, Diaconis, and Graham considered random processes of the form $X_{n+1} = 2X_n + b_n \pmod p$ where $X_0 = 0$, p is odd, and b_n for $n = 0, 1, 2, \ldots$ are i.i.d. random variables on $\{-1, 0, 1\}$. If $\Pr(b_n = -1) = \Pr(b_n = 1) = \beta$ and $\Pr(b_n = 0) = 1 - 2\beta$, they asked which value of β makes X_n get close to uniformly distributed on the integers mod p the slowest. In this paper, we extend the results of Chung, Diaconis, and Graham in the case $p = 2^t - 1$ to show that for $0 < \beta \leq 1/2$, there is no such value of β.

1 Introduction

In [1], Chung, Diaconis, and Graham considered random processes of the form $X_{n+1} = 2X_n + b_n \pmod p$ where p is an odd integer, $X_0 = 0$, and $b_0, b_1, b_2, \ldots$ are i.i.d. random variables. This process is also described in Diaconis [2], and generalizations involving random processes of the form $X_{n+1} = a_n X_n + b_n \pmod p$ where (a_i, b_i) for $i = 0, 1, 2, \ldots$ are i.i.d. were considered by the author in [3] and [4]. A question asked in [1] concerns cases where $\Pr(b_n = 1) = \Pr(b_n = -1) = \beta$ and $\Pr(b_n = 0) = 1 - 2\beta$. If $\beta = 1/4$ or $\beta = 1/2$, then P_n is close to the uniform distribution (in variation distance) on the integers mod p if n is a large enough multiple of $\log p$ where $P_n(s) = \Pr(X_n = s)$. If $\beta = 1/3$, however, for n a small enough multiple of $(\log p)\log(\log p)$, the variation distance $\|P_n - U\|$ is far from 0 for certain values of p such as $p = 2^t - 1$. Chung, Diaconis, and Graham comment "It would be interesting to know which value of β maximizes the value of N required for $\|P_N - U\| \to 0$."
If $\beta = 0$, then $X_n = 0$ with probability 1 for all n. Thus we shall only consider the case $\beta > 0$. We shall show that unless $\beta = 1/4$ or $\beta = 1/2$, then there exists a value $c_\beta > 0$ such that for certain values of p (namely $p = 2^t - 1$), if $n \leq c_\beta (\log p)\log(\log p)$, then $\|P_n - U\| \to 1$ as $t \to \infty$. Furthermore, one can have $c_\beta \to \infty$ as $\beta \to 0^+$. Work of the author [3] shows that for each β, there is a value c'_β such that if $n \geq c'_\beta (\log p)\log(\log p)$, then $\|P_n - U\| \to 0$ as $p \to \infty$. Thus one may conclude that there is no value of β which maximizes the value of N required for $\|P_N - U\| \to 0$.

This paper will consider a broader class of distributions for b_n. In particular, $\Pr(b_n = 1)$ need not equal $\Pr(b_n = -1)$. The main argument here relies on a generalization of an argument in [1].

2 Notation and Main Theorem

Recall that the variation distance of a probability P on a finite group G from the uniform distribution on G is given by

$$\begin{aligned}\|P - U\| &= \frac{1}{2}\sum_{s\in G} |P(s) - 1/|G|| \\ &= \max_{A\subseteq G} |P(A) - U(A)| \\ &= \sum_{s:P(s)>1/|G|} |P(s) - 1/|G||\end{aligned}$$

The following assumptions are used in the main theorem. Suppose $\Pr(b_n = 1) = a$, $\Pr(b_n = 0) = b$, and $\Pr(b_n = -1) = c$. We assume $a + b + c = 1$ and a, b, and c are all less than 1. Suppose $b_0, b_1, b_2, \ldots$ are i.i.d. and $X_0 = 0$. Suppose $X_{n+1} = 2X_n + b_n \pmod p$ and p is odd. Let $P_n(s) = \Pr(X_n = s)$. The theorem itself follows:

Theorem 1 *Case 1: Suppose either $b = 0$ and $a = c = 1/2$ or $b = 1/2$. If $n > c_1 \log_2 p$ where $c_1 > 1$ is constant, then $\|P_n - U\| \to 0$ as $p \to \infty$ where p is an odd integer.*
Case 2: Suppose a, b, and c do not satisfy the conditions in Case 1. Then there exists a value c_2 (depending on a, b, and c) such that if $n < c_2(\log p)\log(\log p)$ and $p = 2^t - 1$, then $\|P_n - U\| \to 1$ as $t \to \infty$.

3 Proof of Case 1

First let's consider the case where $b = 1/2$. Then $b_n = e_n + d_n$ where e_n and d_n are independent random variables with $\Pr(e_n = 0) = \Pr(e_n = 1) = 1/2$, $\Pr(d_n = -1) = 2c$, and $\Pr(d_n = 0) = 2a$. (Note that here $a + c = 1/2 = b$. Thus $2a + 2c = 1$.) Observe that

$$\begin{aligned}X_n &= \sum_{j=0}^{n-1} 2^{n-1-j} b_j \pmod p \\ &= \sum_{j=0}^{n-1} 2^{n-1-j} e_j + \sum_{j=0}^{n-1} 2^{n-1-j} d_j \pmod p\end{aligned}$$

Let

$$Y_n = \sum_{j=0}^{n-1} 2^{n-1-j} e_j \pmod p.$$

If P_n is the probability distribution of X_n (i.e. $P_n(s) = \Pr(X_n = s)$) and Q_n is the probability distribution of Y_n, then the independence of e_n and d_n implies $\|P_n - U\| \le \|Q_n - U\|$. Observe that on the integers, $\sum_{j=0}^{n-1} 2^{n-1-j} e_j$ is uniformly distributed on the set $\{0, 1, \ldots, 2^n - 1\}$. Each element of the integers mod p appears either $\lfloor 2^n/p \rfloor$ times or $\lceil 2^n/p \rceil$ times. Thus

$$\|Q_n - U\| \le p\left(\frac{\lceil 2^n/p \rceil}{2^n} - \frac{1}{p}\right) \le \frac{p}{2^n}.$$

If $n > c_1 \log_2 p$ where $c_1 > 1$, then $2^n > p^{c_1}$ and $\|Q_n - U\| \le 1/p^{c_1 - 1} \to 0$ as $p \to \infty$.
The case where $b = 0$ and $a = c = 1/2$ is alluded to in [1] and left as an exercise. □

4 Proof of Case 2

The proof of this case follows the proof of Theorem 2 in [1] with some modifications.
Define, as in [1], the separating function $f : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}$ by

$$f(k) := \sum_{j=0}^{t-1} q^{k2^j}$$

where $q := q(p) := e^{2\pi i/p}$. We shall suppose $n = rt$ where r is an integer of the form $r = \delta \log t - d$ for a fixed value δ.
If $0 \le j \le t-1$, define

$$\Pi_j := \prod_{\alpha=0}^{t-1} \left(aq^{(2^\alpha(2^j-1))} + b + cq^{-(2^\alpha(2^j-1))} \right).$$

Note that if $a = b = c = 1/3$, then this expression is the same as Π_j defined in the proof of Theorem 2 in [1].
As in the proof of Theorem 2 in [1], $E_U(f) = 0$ and $E_U(f\overline{f}) = t$. Furthermore

$$\begin{aligned}
E_{P_n}(f) &= \sum_k P_n(k) f(k) \\
&= \sum_k \sum_{j=0}^{t-1} P_n(k) q^{k2^j} \\
&= \sum_{j=0}^{t-1} \hat{P}_n(2^j) \\
&= \sum_{j=0}^{t-1} \prod_{\alpha=0}^{t-1} \left(aq^{2^\alpha 2^j/p} + b + cq^{-2^\alpha 2^j/p} \right)^r \\
&= t\Pi_1^r.
\end{aligned}$$

Also note

$$\begin{aligned}
E_{P_n}(f\overline{f}) &= \sum_k P_n(k) f(k)\overline{f}(k) \\
&= \sum_k \sum_{j,j'} P_n(k) q^{k(2^j - 2^{j'})} \\
&= \sum_{j,j'} \hat{P}_n(2^j - 2^{j'}) \\
&= \sum_{j,j'} \prod_{\alpha=0}^{t-1} \left(a q^{2^\alpha (2^j - 2^{j'})} + b + c q^{-2^\alpha (2^j - 2^{j'})} \right)^r \\
&= t \sum_{j=0}^{t-1} \Pi_j^r.
\end{aligned}$$

(Note that the expressions for $E_{P_N}(f)$ and $E_{P_N}(f\overline{f})$ in the proof of Theorem 2 of [1] have some minor misprints.)
The (complex) variances of f under U and P_n are $\mathrm{Var}_U(f) = t$ and

$$\begin{aligned}
\mathrm{Var}_{P_n}(f) &= E_{P_n}(|f - E_{P_n}(f)|^2) \\
&= E_{P_N}(f\overline{f}) - E_{P_n}(f) E_{P_n}(\overline{f}) \\
&= t \sum_{j=0}^{t-1} \Pi_j^r - t^2 |\Pi_1|^{2r}.
\end{aligned}$$

Like [1], we use the following complex form of Chebyshev's inequality for any Q:

$$Q\left(\left\{ x : |f(x) - E_Q(f)| \geq \alpha \sqrt{\mathrm{Var}_Q(f)} \right\}\right) \leq 1/\alpha^2$$

where $\alpha > 0$. Thus

$$U\left(\left\{ x : |f(x)| \geq \alpha t^{1/2} \right\}\right) \leq 1/\alpha^2$$

and

$$P_n\left(\left\{ x : |f(x) - t\Pi_1^r| \geq \beta \left(t \sum_{j=0}^{t-1} \Pi_j^r - t^2 |\Pi_1|^{2r} \right)^{1/2} \right\}\right) \leq 1/\beta^2.$$

Let A and B denote the complements of these 2 sets; thus $U(A) \geq 1 - 1/\alpha^2$ and $P_n(B) \geq 1 - 1/\beta^2$. If A and B are disjoint, then $\|P_n - U\| \geq 1 - 1/\alpha^2 - 1/\beta^2$.
Suppose r is an integer with

$$r = \frac{\log t}{2 \log(1/|\Pi_1|)} - \lambda$$

where $\lambda \to \infty$ as $t \to \infty$ but $\lambda \ll \log t$. Then $t|\Pi_1|^r = t^{1/2} |\Pi_1|^{-\lambda} \gg t^{1/2}$. Observe that the fact a, b, and c do not satisfy the conditions in Case 1 implies $|\Pi_1|$ is bounded away from 0 as $t \to \infty$. Furthermore $|\Pi_1|$ is bounded away from 1 for a given a, b, and c.
In contrast, let's consider what happens to $|\Pi_1|$ if a, b, and c do satisfy the condition in Case 1. If $b = 1/2$, then the $\alpha = t - 1$ term in the definition of Π_1 converges to 0 as $t \to \infty$ and thus

Π_1 also converges to 0 as $t \to \infty$ since each other term has length at most 1. If $a = c = 1/2$ and $b = 0$, then the $\alpha = t-2$ term in the definition of Π_1 converges to 0 as $t \to \infty$ and thus Π_1 also converges to 0 as $t \to \infty$.

Claim 1

$$\frac{1}{t}\sum_{j=0}^{t-1}\left(\frac{\Pi_j}{|\Pi_1|^2}\right)^r \to 1$$

as $t \to \infty$.

Note that this claim implies $(\mathrm{Var}_{P_n}(f))^{1/2} = o(E_{P_n}(f))$ and thus Case 2 of Theorem 1 follows. Note that $\Pi_0 = 1$. By Proposition 1 below, $\overline{\Pi_j} = \Pi_{t-j}$. Thus $t\sum_{j=0}^{t-1}\Pi_j^r$ is real. Also note that since $\mathrm{Var}_{P_n}(f) \geq 0$, we have

$$\frac{t\sum_{j=0}^{t-1}\Pi_j^r}{t^2|\Pi_1|^{2r}} \geq 1.$$

Thus to prove the claim, it suffices to show

$$\frac{1}{t}\sum_{j=0}^{t-1}\left(\frac{|\Pi_j|}{|\Pi_1|^2}\right)^r \to 1.$$

Proposition 1 $\overline{\Pi_j} = \Pi_{t-j}$.

Proof: Note that

$$\overline{\Pi_j} = \prod_{\alpha=0}^{t-1}\left(aq^{-(2^\alpha(2^j-1))} + b + cq^{(2^\alpha(2^j-1))}\right)$$

and

$$\Pi_{t-j} = \prod_{\beta=0}^{t-1}\left(aq^{(2^\beta(2^{t-j}-1))} + b + cq^{-(2^\beta(2^{t-j}-1))}\right).$$

If $j \leq \beta \leq t-1$, then note

$$\begin{aligned} 2^\beta(2^{t-j}-1) &= 2^{\beta-j}(2^t - 2^j) \\ &= 2^{\beta-j}(1-2^j) \pmod p \\ &= -2^{\beta-j}(2^j-1). \end{aligned}$$

Thus the terms in Π_{t-j} with $j \leq \beta \leq t-1$ are equal to the terms in $\overline{\Pi_j}$ with $0 \leq \alpha \leq t-j-1$. If $0 \leq \beta \leq j-1$, then note

$$\begin{aligned} 2^\beta(2^{t-j}-1) &= 2^{t+\beta}(2^{t-j}-1) \pmod p \\ &= 2^{t+\beta-j}(2^t - 2^j) \\ &= 2^{t+\beta-j}(1-2^j) \pmod p \\ &= -2^{t+\beta-j}(2^j-1). \end{aligned}$$

Thus the terms in Π_{t-j} with $0 \leq \beta \leq j-1$ are equal to the terms in $\overline{\Pi_j}$ with $t-j \leq \alpha \leq t-1$.
□

Now let's prove the claim. Let $G(x) = |ae^{2\pi ix} + b + ce^{-2\pi ix}|$. Thus

$$|\Pi_j| = \prod_{\alpha=0}^{t-1} G(2^\alpha(2^j-1)/p).$$

Note that if $0 \le x < y \le 1/4$, then $G(x) > G(y)$. On the interval $[1/4, 1/2]$, where G increases and where G decreases depends on a, b, and c.
We shall prove a couple of facts analogous to facts in [1].
Fact 1: There exists a value t_0 (possibly depending on a, b, and c) such that if $t > t_0$, then $|\Pi_j| \le |\Pi_1|$ for all $j \ge 1$.
Since $G(x) = G(1-x)$, in proving this fact we may assume without loss of generality that $2 \le j \le t/2$. Note that

$$|\Pi_j| = \prod_{i=0}^{t-j-1} G\left(\frac{2^{i+j}-2^i}{p}\right) \prod_{i=0}^{j-1} G\left(\frac{2^{i+t-j}-2^i}{p}\right).$$

We associate factors x from $|\Pi_j|$ with corresponding factors $\pi(x)$ of $|\Pi_1|$ in a manner similar to that in [1]. For $0 \le i \le t-j-2$, associate $G((2^{i+j}-2^i)/p)$ with $G(2^{i+j-1}/p)$. Note that for $0 \le i \le t-j-2$, we have $G((2^{i+j}-2^i)/p) \le G(2^{i+j-1}/p)$. For $0 \le i \le j-3$, associate $G((2^{i+t-j}-2^i)/p)$ in $|\Pi_j|$ with $G(2^i/p)$ in $|\Pi_1|$. Note that for $0 \le i \le j-3$, we have $G((2^{i+t-j}-2^i)/p) \le G(2^i/p)$.
The remaining terms in $|\Pi_j|$ are

$$G\left(\frac{2^{t-1}-2^{t-j-1}}{p}\right) G\left(\frac{2^{t-1}-2^{j-1}}{p}\right) G\left(\frac{2^{t-2}-2^{j-2}}{p}\right)$$

and the remaining terms in $|\Pi_1|$ are

$$G\left(\frac{2^{t-1}}{p}\right) G\left(\frac{2^{t-2}}{p}\right) G\left(\frac{2^{j-2}}{p}\right).$$

It can be shown that

$$\lim_{t\to\infty} \frac{G\left(\frac{2^{t-1}-2^{t-j-1}}{p}\right) G\left(\frac{2^{t-1}-2^{j-1}}{p}\right) G\left(\frac{2^{t-2}-2^{j-2}}{p}\right)}{G\left(\frac{2^{t-1}}{p}\right) G\left(\frac{2^{t-2}}{p}\right) G\left(\frac{2^{j-2}}{p}\right)} = \frac{G(1/2)}{G(0)} < 1.$$

Indeed, for some t_0, if $t > t_0$ and $2 \le j \le t/2$,

$$\begin{aligned} & G\left(\frac{2^{t-1}-2^{t-j-1}}{p}\right) G\left(\frac{2^{t-1}-2^{j-1}}{p}\right) G\left(\frac{2^{t-2}-2^{j-2}}{p}\right) \\ \le \; & G\left(\frac{2^{t-1}}{p}\right) G\left(\frac{2^{t-2}}{p}\right) G\left(\frac{2^{j-2}}{p}\right). \end{aligned}$$

$\square$

Fact 2: There exists a value t_1 (possibly depending on a, b, and c) such that if $t > t_1$, then the following holds. There is a constant c_0 such that for $t^{1/3} \le j \le t/2$, we have

$$\frac{|\Pi_j|}{|\Pi_1|^2} \le 1 + \frac{c_0}{2^j}$$

To prove this fact, we associate, for $i = 0, 1, \ldots, j-1$, the terms

$$G\left(\frac{2^{t-i-1} - 2^{j-i-1}}{p}\right) G\left(\frac{2^{t-i-1} - 2^{t-j-i-1}}{p}\right)$$

in $|\Pi_j|$ with the terms

$$\left(G\left(\frac{2^{t-i-1}}{p}\right)\right)^2$$

in $|\Pi_1|^2$. Suppose $A = \max |G'(x)|$. Note that $A < \infty$. Then

$$\left|G\left(\frac{2^{t-i-1} - 2^{j-i-1}}{p}\right)\right| \le \left|G\left(\frac{2^{t-i-1}}{p}\right)\right| + A\frac{2^{j-i-1}}{p}.$$

Thus

$$\frac{\left|G\left(\frac{2^{t-i-1}-2^{j-i-1}}{p}\right)\right|}{\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|} \le 1 + A\frac{2^{j-i-1}}{p\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|}.$$

Likewise

$$\frac{\left|G\left(\frac{2^{t-i-1}-2^{t-j-i-1}}{p}\right)\right|}{\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|} \le 1 + A\frac{2^{t-j-i-1}}{p\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|}.$$

Since we do not have the conditions for Case 1, there is a positive value B and value t_2 such that if $t > t_2$, then $|G(2^{t-i-1}/p)| > B$ for all i with $0 \le i \le j-1$. By an exercise, one can verify

$$\prod_{i=0}^{j-1} \frac{\left|G\left(\frac{2^{t-i-1}-2^{j-i-1}}{p}\right) G\left(\frac{2^{t-i-1}-2^{t-j-i-1}}{p}\right)\right|}{\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|^2} \le 1 + \frac{c_3}{2^j}$$

for some value c_3 not depending on j.
Note that the remaining terms in $|\Pi_j|$ all have length less than 1. The remaining terms in $|\Pi_1|^2$ are

$$\prod_{i=j}^{t-1}\left|G\left(\frac{2^{t-i-1}}{p}\right)\right|^2.$$

Since $G'(0) = 0$, there are positive constants c_4 and c_5 such that

$$\left|G\left(\frac{2^{t-i-1}}{p}\right)\right| \ge 1 - c_4\left(\frac{2^{t-i-1}}{p}\right)^2 \ge \exp\left(-c_5\frac{2^{t-i-1}}{p}\right)$$

for $i \geq j \geq t^{1/3}$. Observe

$$\begin{aligned}
\prod_{i=j}^{t-1} \exp\left(-c_5 \frac{2^{t-i-1}}{p}\right) &= \exp\left(-c_5 \sum_{i=j}^{t-1} 2^{t-i-1}/p\right) \\
&= \exp\left(-c_5 \sum_{k=0}^{t-j-1} 2^k/p\right) \\
&= \exp\left(-c_5 \frac{2^{t-j}-1}{2^t-1}\right) \\
&> \exp\left(-c_5 \frac{2^{t-j}}{2^t}\right) \\
&= \exp(-c_5/2^j) > 1 - c_5/2^j.
\end{aligned}$$

There exists a constant c_0 such that

$$\frac{1 + c_3/2^j}{(1 - c_5/2^j)^2} \leq 1 + c_0/2^j$$

for $j \geq 1$.
Thus, as in [1],

$$\sum_{t^{1/3} \leq j \leq t/2} \left| \left(\frac{|\Pi_j|}{|\Pi_1|^2}\right)^r - 1 \right| \leq \frac{c_6 tr}{2^{t^{1/3}}} < \frac{c_7}{2^{t^{1/4}}}$$

for values c_6 and c_7. Since $|\Pi_j| = |\Pi_{t-j}|$,

$$\begin{aligned}
\frac{1}{t}\sum_{j=0}^{t-1}\left(\frac{|\Pi_j|}{|\Pi_1|^2}\right)^r &\leq \frac{1}{t}\frac{1}{|\Pi_1|^{2r}} + \frac{2}{t}\left(\sum_{1 \leq j < t^{1/3}}\left(\frac{|\Pi_j|}{|\Pi_1|^2}\right)^r + \sum_{t^{1/3} \leq j \leq t/2}\left(\frac{|\Pi_j|}{|\Pi_1|^2}\right)^r\right) \\
&= 1 + o(1)
\end{aligned}$$

as $t \to \infty$. Thus Fact 2, the claim, and Theorem 1 are proved. □
The next proposition considers what happens as we vary the values a, b, and c.

Proposition 2 *If* $a = c = \beta$ *and* $b = 1 - 2\beta$ *and* $m_\beta = \liminf_{t\to\infty} |\Pi_1|$, *then* $\lim_{\beta\to 0^+} m_\beta = 1$.

Proof: Suppose $\beta < 1/4$. Then

$$\Pi_1 = \prod_{\alpha=0}^{t-1} \left((1-2\beta) + 2\beta\cos(2\pi 2^\alpha/p)\right).$$

Let $h(\alpha) = (1-2\beta) + 2\beta\cos(2\pi 2^\alpha/p)$. Note that

$$\begin{aligned}
\lim_{\beta\to 0^+} h(t-1) &= 1 \\
\lim_{\beta\to 0^+} h(t-2) &= 1 \\
\lim_{\beta\to 0^+} h(t-3) &= 1
\end{aligned}$$

Furthermore, for some constant $\gamma > 0$, one can show

$$h(\alpha) > \exp(-\beta\gamma(2^\alpha/p)^2)$$

if $2^\alpha/p \leq 1/8$ and $0 < \beta < 1/10$. So

$$\begin{aligned} \prod_{\alpha=0}^{t-4} h(\alpha) &> \prod_{\alpha=0}^{t-4} \exp(-\beta\gamma(2^\alpha/p)^2) \\ &= \exp\left(-\beta\gamma \sum_{\alpha=0}^{t-4} (2^\alpha/p)^2\right) \\ &> \exp(-\beta\gamma 2^{2(t-4)}(4/3)/p^2) \to 1 \end{aligned}$$

as $\beta \to 0^+$. □

Recalling that

$$r = \frac{\log t}{2\log(1/|\Pi_1|)} - \lambda,$$

we see that $1/(2\log(1/|\Pi_1|))$ can be made arbitrarily large by choosing β small enough. Thus there exist values $c_\beta \to \infty$ as $\beta \to 0^+$ such that if $n \leq c_\beta(\log p)\log(\log p)$, then $\|P_n - U\| \to 1$ as $t \to \infty$.

5 Problems for further study

One possible problem is to see if in some sense, there is a value of β on $[1/4, 1/2]$ which maximizes the value of N required for $\|P_N - U\| \to 0$; to consider such a question, one might restrict p to values such that $p = 2^t - 1$.

Another possible question considers the behavior of these random processes for almost all odd p. For $\beta = 1/3$, Chung, Diaconis, and Graham [1] showed that a multiple of $\log p$ steps suffice for almost all odd p. While their arguments should be adaptable with the change of appropriate constants to a broad range of choices of a, b, and c in Case 2, a more challenging question is to determine for which a, b, and c in Case 2 (if any), $(1 + o(1))\log_2 p$ steps suffice for almost all odd p.

6 Acknowledgments

The author thanks Ron Graham for mentioning the problem at a January, 2005, conference on the Mathematics of Persi Diaconis. The author also thanks Robin Pemantle for a conversation on the topic and the participants in the Probability and Related Fields Seminar at the University at Albany for listening to some ideas on the problem.

References

[1] Chung, F., Diaconis, P., and Graham, R. A random walk problem arising in random number generation. *Ann. Probab.* **15** (1987), 1148-1165. MR0893921

[2] Diaconis, P. *Group Representations in Probability and Statistics.* Institute of Mathematical Statistics, 1988. MR0964069

[3] 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

[4] 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, 1996. MR1395613