SOME RANDOM PROCESSES
RELATED TO AFFINE RANDOM WALKS

By

Martin Hildebrand

IMA Preprint Series # 1210
January 1994
SOME RANDOM PROCESSES RELATED TO AFFINE RANDOM WALKS

Martin Hildebrand

Department of Mathematics, The University of Michigan, Ann Arbor, MI 48109-1003

Keywords: affine group; random walks; random number generators; Diaconis-Shahshahani upper bound lemma

ABSTRACT

This paper considers random processes of the form $X_{n+1} = a_n X_n + b_n \pmod{p}$ where $(a_n, b_n)$ are independent random variables, $p$ is an odd integer, and $P(a_n = (p + 1)/2)$ is a positive constant. This paper searches for the time it takes the sequence $X_0, X_1, X_2, \ldots$ to get close to uniformly distributed on $\mathbb{Z}/p\mathbb{Z}$. This paper shows that the order of this time will depend on the probabilities for $a_n$. In particular if $a_n$ may take on values 1, 2, or $(p + 1)/2$ and must take on at least 2 of these values and if $b_n$ is independent of $a_n$, then this time depends on whether $P(a_n = 2) = P(a_n = (p + 1)/2)$. This paper also considers some results when $a_n$ and $b_n$ are dependent.

INTRODUCTION

A pseudo-random number generator sometimes used on computers utilizes a recurrence equation of the form

$$X_{n+1} = a X_n + b \pmod{p}$$

where $a$ and $b$ are constants. Although the sequence $X_0, X_1, X_2, \ldots$ is deterministic, this sequence shares some properties of random sequences. See Knuth (1981) for more details.

Further work has examined random processes of the form

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

where the $a_n$'s and $b_n$'s are independent random variables with the $a_n$'s identically distributed and the $b_n$'s identically distributed. Cases where $a_n$ has a fixed probability on $\mathbb{Z}^+$ and $b_n$ has a fixed probability on $\mathbb{Z}$ have been explored in a number of previous works. See Chung Diaconis, and Graham (1987) and Hildebrand (1990, 1993a, 1993b). Questions where $a_n$ has a distribution which depends on $p$ (e.g. $P(a_n = (p + 1)/2) = P(a_n = 1) = P(a_n = 2) = 1/3$ for odd values of $p$) appear in Diaconis (1988). The question of interest is how long does it take for $X_n$ to get close to uniformly distributed on $\mathbb{Z}/p\mathbb{Z}$. Using random
walks on the affine group, Xu (1990) provides an upper bound to this time for certain values
of \( p \) but wonders if the bound can be improved. This paper finds some lower bounds for
this time and provides an upper bound which uses different techniques and a broader range
of values of \( p \) than Xu.

Using the notation of the next section, this paper shows the following 3 theorems where
\( a_n \) and \( b_n \) are assumed to be independent.

**Theorem 1:** If \( P(a_n = (p + 1)/2) = P(a_n = 2) = 1/2 \) and \( P(b_n = -1) = P(b_n = 1) = 1/2 \)
and \( \epsilon > 0 \) is given, then for some constant \( c > 0 \), if \( n \geq c (\log p)^2 \) then \( \|P_n - U\| < \epsilon \)
for sufficiently large odd values of \( p \).

**Theorem 2:** Suppose \( P(a_n = (p + 1)/2) = a, P(a_n = 1) = b, P(a_n = 2) = c, \) at least 2 of
\( a, b, \) and \( c \) are non-zero, \( a + b + c = 1, P(b_n = 1) = d, P(b_n = 0) = e, P(b_n = -1) = f, \) at
least 2 of \( d, e, \) and \( f \) are non-zero, and \( d + e + f = 1 \). Let

\[
g = \begin{cases} 
2 & \text{if } a = c \\
1 & \text{if } a \neq c
\end{cases}
\]

Let \( \epsilon > 0 \) be given. Then for sufficiently large odd \( p, \|P_n - U\| < \epsilon \) if \( n > c_1 (\log p \log \log p)^g \)
for some value \( c_1 > 0 \) (which may depend on \( a, b, c, d, e, \) and \( f \) but not \( p \)) but \( \|P_n - U\| < \epsilon \)
for almost all odd \( p \) if \( n > c_2 (\log p)^g \) for some value \( c_2 > 0 \) (which also may depend on \( a, b, c, d, e, \) and \( f \) but not \( p \)). By almost all odd \( p \), we mean that the proportion of odd \( p \)
between 1 and \( p_0 \) satisfying this condition approaches 1 as \( p_0 \to \infty \).

**Theorem 3:** With the notation of Theorem 2, there exists a value \( c_3 > 0 \) such that, given
\( \epsilon > 0, \|P_n - U\| > 1 - \epsilon \) if \( n < c_3 (\log p)^g \) and \( p \) is odd.

Theorems 2 and 3 answer, up to a factor of \((\log \log p)^2\), a question posed on p. 35 of
Diaconis (1988). This question has \( a = b = c = 1/3 \) and \( d = e = f = 1/3 \) and asks how
long it takes for \( X_n \) to get close to uniformly distributed on \( \mathbb{Z}/p\mathbb{Z} \).

This paper also shows the following results where \( a_n \) and \( b_n \) may be dependent.

**Theorem 4:** Let \( p \) be odd. Suppose \( (a_n, b_n) \) is defined so that \( P(a_n = 2) = P(a_n = \)
\( (p + 1)/2 \) = \( 1/2(1 - P(a_n = 1)) \) \( \neq 0 \) and that \( b_n \) has a fixed distribution on \( \mathbb{Z} \) and has
finitely many possible values. Suppose the \( (a_n, b_n) \)'s are i.i.d. Let \( \epsilon > 0 \) be given. There
exists a value \( c > 0 \) (not depending on \( p \) but depending on the values for the probabilities
on \( (a_n, b_n) \)) such that if \( n < c (\log p)^2 \), then \( \|P_n - U\| > 1 - \epsilon \) for sufficiently large \( p \).

**Theorem 5:** Suppose that \( p \) is odd and that \( (a_n, b_n) \) is chosen uniformly from \((2, 1), (2, -1), \)
\((p + 1)/2, ((p + 1)/2), \) and \((p + 1)/2, -(p + 1)/2) \). Then there exists a value \( c > 0 \)
such that if \( n > c (\log p)^3, \|P_n - U\| \to 0 \) as \( p \to \infty \).
NOTATION AND BACKGROUND

Let $P$ be a probability on $\mathbb{Z}/p\mathbb{Z}$. Define the variation distance of $P$ from the uniform distribution $U$ by

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

One can readily show that

$$\|P - U\| = \max_{A \subseteq \mathbb{Z}/p\mathbb{Z}} |P(A) - U(A)|.$$ 

This variation distance is the one defined in Diaconis (1988).

Suppose $X_0 = 0$ and

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

where the $(a_n, b_n)$'s are i.i.d. We shall define $P_n$ to be the probability distribution of $X_n$ (where $X_n$ is viewed as a random variable on $\mathbb{Z}/p\mathbb{Z}$). By abuse of notation, we shall also call $\|P_n - U\|$ the distance of $X_n$ from uniform.

Let $X$ and $Y$ be independent random variables on $\mathbb{Z}/p\mathbb{Z}$ with probability distributions $P$ and $Q$. Let $P \ast Q$ be the probability distribution of $X + Y$. The following proposition will be useful:

**Proposition 1:**

$$\|P \ast Q - U\| \leq \|P - U\|$$

The proof is left as an exercise.

PROOF OF THEOREM 1

In this section, we shall prove Theorem 1. Throughout this section, we shall assume $p$ is odd. The proof builds on the following lemmas.

**Lemma 1:** Suppose $Y_0 = 0$ and

$$Y_{n+1} = 2Y_n + b_n \pmod{p}$$

where $b_n$ is as in Theorem 1. If $n > c_1 \log_2 p$ where $c_1 > 1$, then $\|Q_n - U\| \to 0$ as $p \to \infty$ if $Q_n$ is the probability distribution of $Y_n$.

**Proof:** If $n \geq 1$, then $Y_n$ (viewed in $\mathbb{Z}$) is uniform on the odd integers from $-2^n + 1$ to $2^n - 1$. Since $2^n > p^{c_1}$ and $c_1 > 1$, the result follows by a straightforward consideration of these odd integers mod $p$. 


3
The next lemma is a property of random walks.

**Lemma 2:** Suppose $P(W_n = 1) = P(W_n = -1) = 1/2$. Let $V_n = \sum_{i=1}^{n} W_i$ (with $V_0 = 0$), let $M_n = \max_{i=0,\ldots,n} V_i$, and let $m_n = \min_{i=0,\ldots,n} V_i$. Given $c_1 > 0$, there exists a value $c$ such that if $n > c(\log p)^2$ then $P(M_n - m_n \leq c_1 \log p) < \epsilon/2$.

The proof of this lemma may be derived quickly from the Central Limit Theorem. ■

Next observe that

\[
X_1 = b_1 \\
X_2 = a_2 b_1 + b_2 \\
X_3 = a_3 a_2 b_1 + a_3 b_2 + b_3 \\
\ldots
\]

Consider the sequence $a_{n+1}, a_{n+1}a_n, \ldots, a_{n+1}a_n \ldots a_2$. Observe that this sequence can also be written as $2^V_1, 2^V_2, \ldots, 2^V_n$ where $V_1, \ldots, V_n$ are as in Lemma 2. If $j > 0$, $2^{-j}$ denotes $((p + 1)/2)^j$ in the integers mod $p$ since 2 is a unit in $\mathbb{Z}/p\mathbb{Z}$ and has multiplicative inverse $(p + 1)/2$.

Suppose $a_1, \ldots, a_{n+1}$ are given such that $M_n - m_n > c_1 \log p$ where the values $M_n$ and $m_n$ refer to the values $V_1, \ldots, V_n$ in the previous paragraph. Let $Z_{n+1} = a_{n+1} \cdot a_2 b_1 + a_{n+1}a_3 b_2 + \ldots + b_{n+1}$ be a random variable for these particular choices of $a_1, \ldots, a_{n+1}$ but with $b_1, \ldots, b_{n+1}$ still being i.i.d. random variables with the same distribution as in Theorem 1. Let $R_n$ be the distance of $Z_n$ from uniform. Note that since $p$ is odd, $R_{n+1}$ is also the distance of $2^{-m} Z_{n+1}$ from the uniform. Note that

\[
2^{-m} Z_{n+1} = \sum_{i=0}^{M_n - m_n} 2^i \tilde{b}_i + \sum_{i=M_n - m_n + 1}^{n} 2^{r(i)} \tilde{b}_i
\]

where the values $r(i)$ are determined by $a_1, \ldots, a_{n+1}$ and $\tilde{b}_i$ are i.i.d. random variables with the same distribution of $b_n$. (The $\tilde{b}_i$'s are obtained from the $b_i$'s by relabeling the subscripts.) Since $r(i)$ is determined and the $\tilde{b}_i$'s are i.i.d., Proposition 1 says that the distance of $2^{-m} Z_{n+1}$ from uniform is less than the distance of

\[
\sum_{i=0}^{M_n - m_n} 2^i \tilde{b}_i
\]

from uniform; the latter distance goes to 0 as $p \to \infty$. Since $P(M_n - m_n \leq c_1 \log p) < \epsilon/2$, we may thus conclude that $\|P_n - U\| < \epsilon$ for large enough odd values of $p$. ■
PROOF OF THEOREM 2

The technique illustrated by the proof of Theorem 1 is readily generalizable to other distributions for $a_n$ and $b_n$. Theorem 2 proves a generalization, but the replacement for Lemma 1 is more complicated. Throughout this section, we assume $p$ is odd.

**Lemma 3:** Suppose $Y_0 = 0$ and $Y_{n+1} = 2Y_n + b_n \pmod{p}$. Let $Q_n$ be the probability distribution of $Y_n$. For some value $\tilde{c}_1 > 0$ if $n > \tilde{c}_1 \log p \log \log p$, then $\|Q_n - U\| \to 0$ as $p \to \infty$. For some value $\tilde{c}_2 > 0$ if $n > \tilde{c}_2(\log p)$ then $\|Q_n - U\| \to 0$ for almost all odd $p$. (Note $\tilde{c}_1$ and $\tilde{c}_2$ may depend on $d$, $e$, and $f$.)

This lemma is a straightforward generalization of Theorems 1 and 3 of Chung, Diaconis, and Graham (1987) and is left to the reader. ■

Lemma 2 is replaced by the following lemma.

**Lemma 4:** Suppose $P(W_n = -1) = a$, $P(W_n = 0) = b$, and $P(W_n = 1) = c$ with $a$, $b$, and $c$ as in Theorem 2. Let $V_n$, $M_n$, and $m_n$ be obtained from $W_1, \ldots, W_n$ as in Lemma 2. Then given $\tilde{c}_1 > 0$ and $\tilde{c}_2 > 0$, there exist values $c_1 > 0$ and $c_2 > 0$ (which may depend on $a$, $b$, and $c$) such that $P(M_n - m_n \leq \tilde{c}_1 \log p \log \log p) < \epsilon/2$ if $n > c_1(\log p \log \log p)^g$ while $P(M_n - m_n \leq \tilde{c}_2 \log p) < \epsilon/2$ if $n > c_2(\log p)^g$ where $g$ is as defined in Theorem 2.

This lemma can be shown from the Central Limit Theorem. ■

The remainder of the proof of Theorem 2 is virtually identical to the last portion of the proof of Theorem 1 provided that one takes into account the two cases in Lemma 3. ■

PROOF OF LOWER BOUNDS

The proof of Theorem 3 is straightforward in the case $g = 1$. Since there are no more than $9^{c_3 \log p} \leq p^{c_3 \log^9}$ possible values that $X_n$ can have if $n = [c_3 \log p]$, then the set of also possible values of $X_n$ will have probability under $p^{c_3 \log^9 - 1}$ under $U$. If $c_3 < 1/\log 9$, this implies that $\|P_n - U\| \to 1$ as $p \to \infty$.

Next consider the case where $g = 2$. Define $M_n$ and $m_n$ as in the proof of Theorem 1. Let $\epsilon > 0$ be given. By elementary considerations from the Central Limit Theorem and a reflection principle, we can show that there exists a value $c_3 > 0$ such that if $n = [c_3(\log p)^2]$, then $P(M_n - m_n > [(1/4) \log_2 p]) < \epsilon/2$. If $M_n - m_n \leq [(1/4) \log_2 p]$, consider

$$2^{[(1/4) \log_2 p]} X_{n+1} = 2^{[(1/4) \log_2 p]} a_n a_2 b_1 + 2^{[(1/4) \log_2 p]} a_n a_3 b_2 + \ldots + 2^{[(1/4) \log_2 p]} b_n.$$ 

Observe that since $((p + 1)/2) \equiv 1 \pmod{p}$, then

$$2^{[(1/4) \log_2 p]} a_n a_2, 2^{[(1/4) \log_2 p]} a_n a_3, \ldots, 2^{[(1/4) \log_2 p]} b_n \subseteq [1, 2^{2(1/4) \log_2 p}] \pmod{p}.$$
There are \( \lfloor c_3 (\log p)^2 \rfloor \) terms on the right. Mod \( p \), each term is in the range

\[
\left[ -2^{2^{\lfloor (1/4) \log_2 p \rfloor}}, 2^{2^{\lfloor (1/4) \log_2 p \rfloor}} \right] \subseteq [-\sqrt{p}, \sqrt{p}].
\]

Thus

\[
2^{\lfloor (1/4) \log_2 p \rfloor} X_{n+1} \subseteq \left[ -\sqrt{pc_3 (\log p)^2}, \sqrt{pc_3 (\log p)^2} \right] \pmod{p}.
\]

Thus, for this choice of \( n \),

\[
\|P_n - U\| > (1 - (\epsilon/2)) - \frac{1 + 2\sqrt{pc_3 (\log p)^2}}{p}
\]

\[
> 1 - \epsilon
\]

for sufficiently large \( p \).

Theorem 4 is a straightforward generalization of the previous theorem.

In some cases where \( b_n \) does not have a fixed distribution on \( \mathbb{Z} \), similar claims may still be made:

**Corollary:** Let \( p \) be odd. If \( P((a_n, b_n) = (2, 1)) = P((a_n, b_n) = ((p + 1)/2, -(p + 1)/2)) = 1/2 \), then, given \( \epsilon > 0 \), there exists a values \( c > 0 \) such that if \( n < c(\log p)^2 \), then \( \|P_n - U\| > 1 - \epsilon \) for sufficiently large \( p \).

**Proof:** \( X_n \) and \( 2X_n \) are the same distance from uniform. Since \( 2(-(p + 1)/2) \equiv -1 \pmod{p} \), we have

\[
2X_n = a_{n-1}a_2b_1 + a_{n-1}a_3b_2 + \ldots + b_{n-1} \pmod{p}
\]

with \( P((a_n, b_n) = (2, 2)) = P((a_n, b_n) = ((p + 1)/2, -1)) = 0.5 \). The previous theorem provides the lower bound for how long it takes for \( X_n \) to get close to uniform on \( \mathbb{Z}/p\mathbb{Z} \).

**PROOF OF THEOREM 5**

The proof utilizes the upper bound lemma of Diaconis and Shahshahani. Let \( P \) be a probability on \( \mathbb{Z}/p\mathbb{Z} \) and let

\[
\hat{P}(k) = \sum_{j=0}^{p-1} P(j)q^{jk}
\]

where \( q := q(p) := e^{2\pi i/p} \). The expression \( \hat{P}(k) \) is called the Fourier transform of \( P \) in \( \mathbb{Z}/p\mathbb{Z} \). The upper bound lemma uses techniques from Fourier analysis to conclude

**Lemma 5:**

\[
\|P - U\|^2 \leq \frac{1}{d} \sum_{k=1}^{p-1} |\hat{P}(k)|^2.
\]
A generalization of this lemma is described and proved in Diaconis (1988).

The proof of the theorem shall use a recurrence relation among the Fourier transforms; a similar relation is used in Hildebrand (1990, 1993a, 1993b). The recurrence relation among the Fourier transforms will follow from the following lemma.

**Lemma 6:**

\[ P(X_{n+1} = k) = \frac{1}{4} P(X_n = ((p + 1)/2)k - ((p + 1)/2)) \]

\[ + \frac{1}{4} P(X_n = ((p + 1)/2)k + ((p + 1)/2)) \]

\[ + \frac{1}{4} P(X_n = 2k - 1) + \frac{1}{4} P(X_n = 2k + 1) \]

The proof is straightforward and follows from the recurrence relation relating \(X_{n+1}\) to \(X_n\).

The following lemma is similar to a recurrence in Hildebrand (1990,1993a):

**Lemma 7:**

\[ \hat{P}_{n+1}(k) = \frac{1}{4} \hat{P}_n(2k)q^k + \frac{1}{4} \hat{P}_n(2k)q^{-k} \]

\[ + \frac{1}{4} \hat{P}_n(((p + 1)/2)k)q^{((p+1)/2)k} + \frac{1}{4} \hat{P}_n(((p + 1)/2)k)q^{-(p+1)/2)k} \]

**Proof:** First observe that

\[ \hat{P}_{n+1}(k) = \sum_{j=0}^{p-1} P(X_{n+1} = j)q^{jk} \]

\[ = \sum_{j=0}^{p-1} \frac{1}{4} P(X_n = ((p + 1)/2)j - ((p + 1)/2))q^{jk} \]

\[ + \sum_{j=0}^{p-1} \frac{1}{4} P(X_n = ((p + 1)/2)j + ((p + 1)/2))q^{jk} \]

\[ + \sum_{j=0}^{p-1} \frac{1}{4} P(X_n = 2j - 1)q^{jk} + \sum_{j=0}^{p-1} \frac{1}{4} P(X_n = 2j + 1)q^{jk} \]

Observe that the mapping from \(j\) to \(((p + 1)/2)j - ((p + 1)/2)\) is a bijection on \(\mathbb{Z}/p\mathbb{Z}\) since \(p\) is odd and since this mapping is the inverse of the bijection on \(\mathbb{Z}/p\mathbb{Z}\) which sends \(j\) to
Thus

\[
\sum_{j=0}^{p-1} P(X_n = 2j + 1)q^j = \sum_{j=0}^{p-1} P(X_n = j)q^{j((p+1)/2)j - ((p+1)/2)^2} \\
= \sum_{j=0}^{p-1} P(X_n = j)q^{j((p+1)/2)k}q^{-(p+1)/2} \\
= \hat{P}_n(((p + 1)/2)k)q^{-(p+1)/2}.
\]

The other terms in the lemma follow similarly.

The recurrence in Lemma 7 provides the key to the proof of Theorem 5. By Lemma 7, we conclude that

\[
|\hat{P}_{n+1}(k)| \leq \frac{1}{2}|\cos 2\pi k/p| |\hat{P}_n(2k)| + \frac{1}{2}|\hat{P}_n(((p + 1)/2)k)|.
\]

Let \(M_n = \max_{k \neq 0} |\hat{P}_n(k)|\). Observe that \(M_0 = 1\) and that \(M_{n+1} < M_n\) if \(n \geq 0\). Also observe that if \(k \in S := ((1/8)p, (3/8)p) \cup ((5/8)p, (7/8)p) \pmod{p}\) then \(|\hat{P}_{n+a}(k)| \leq 0.8M_n\) for \(a = 1, 2, 3, \ldots\). Thus we may claim that

\[
|\hat{P}_{n+1}(k)| \leq \frac{1}{2}f(k)|\hat{P}_n(2k)| + \frac{1}{2}|\hat{P}_n(((p + 1)/2)k)|
\]

where \(f(k) = 0.8\) if \(k \in S\) and \(f(k) = 1\) of \(k \notin S\).

Note that if \(k \neq 0\) and \(k \notin S\), then \(2^k k \in S \pmod{p}\) for some value \(b \leq (\log_2 p)\). Since \(p\) is odd, we may view \((p+1)/2\) as \(2^{-1}\) in the multiplicative group of the units of \(\mathbb{Z}/p\mathbb{Z}\). Let \(d = [c_1(\log p)^2]\). By \(|\hat{P}_{n+d}(k)|\) by expanding \((*)\) recursively \(d\) levels. Define \(W_i\) and \(V_i\) as in Lemma 2. By the Central Limit Theorem, \(V_n > \log_2 p\) with probability at least \(c_2 > 0\). Thus at least the fraction \(c_2\) of the terms will have a multiple of 0.8 coming from the \(f(k)\) term in \((*)\). Thus for all \(n\) and \(k \neq 0\),

\[
|\hat{P}_{n+d}(k)| \leq (0.8c_2 + 1(1 - c_2))M_n.
\]

Observe that that \(c_3 := .8c_2 + (1 - c_2) < 1\) and that \(M_{n+d} \leq c_3 M_n\). Thus for some value \(c_4 > 0\), \(M_{d[c_4 \log p]} \leq c_3^{c_4 \log p} \leq 1/p^2\) for large enough \(p\). By the upper bound lemma, if \(n = d[c_4 \log p]\), then \(\|P_n - U\|^2 < (1/4)((p - 1)/p^2) \rightarrow 0\) as \(p \rightarrow 0\).

PROBLEMS FOR FURTHER STUDY

Theorems 2 and 3 do not provide sharp bounds on the time it takes for \(X_n\) to get close to uniform; the bounds differ by a factor of a constant times \((\log \log p)^g\). This time may vary
by such a factor; such variation appears in results proved in Chung, Diaconis, and Graham (1987) and Hildebrand (1993b). If \( g = 2 \), it is unclear whether such variation will hold, and this uncertainty provides a subject for further study.

Upper bounds for cases where \( a_n \) and \( b_n \) are dependent need improvement. Both generalizations of the method used in proving Theorem 5 and improvements of the upper bound in Theorem 5 form natural further problems worth studying.

The techniques in this paper can be extended to cases where \( a_n \) is either \( a \), \( 1 \), or the multiplicative inverse of \( a \) if \( p \) and \( a \) are relatively prime. What happens if \( a_n \) takes on a broader range of values? For instance, what happens if \( a_n \) takes on the values \( 1, 2, 3 \), and the multiplicative inverses of \( 2 \) and \( 3 \) with certain probabilities?

ACKNOWLEDGEMENTS

The author thanks Persi Diaconis for suggesting some of the problems and acknowledges that some of this work is based on ideas in chapter 5 of Hildebrand (1990). The author also thanks Mark Conger for a couple of comments on an earlier version of the paper.

BIBLIOGRAPHY


Hildebrand, M. (1993a) “Random Processes of the Form \( X_{n+1} = a_nX_n + b_n \pmod{p} \).” Ann. Prob. 21.

Hildebrand, M. (1993b) “Random Processes of the Form \( X_{n+1} = a_nX_n + b_n \pmod{p} \) Where \( b_n \) Takes on a Single Value,” preprint.


<table>
<thead>
<tr>
<th>#</th>
<th>Author/s</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1121</td>
<td>Nahum Shimkin &amp; Adam Shwartz</td>
<td>Asymptotically efficient adaptive strategies in repeated games, part II: Asymptotic optimality</td>
</tr>
<tr>
<td>1122</td>
<td>M.E. Bradley</td>
<td>Well-posedness and regularity results for a dynamic Von Kármán plate</td>
</tr>
<tr>
<td>1123</td>
<td>Zhangxin Chen</td>
<td>Finite element analysis of the 1D full drift diffusion semiconductor model</td>
</tr>
<tr>
<td>1124</td>
<td>Gang Bao &amp; David C. Dobson</td>
<td>Diffractive optics in nonlinear media with periodic structure</td>
</tr>
<tr>
<td>1125</td>
<td>Steven Cox &amp; Enrique Zuazua</td>
<td>The rate at which energy decays in a damped string</td>
</tr>
<tr>
<td>1126</td>
<td>Anthony W. Leung</td>
<td>Optimal control for nonlinear systems of partial differential equations related to ecology</td>
</tr>
<tr>
<td>1127</td>
<td>H.J. Sussmann</td>
<td>A continuation method for nonholonomic path-finding problems</td>
</tr>
<tr>
<td>1128</td>
<td>Yung-Jen Guo &amp; Walter Littman</td>
<td>The null boundary controllability for semilinear heat equations</td>
</tr>
<tr>
<td>1129</td>
<td>Q. Zhang &amp; G. Yin</td>
<td>Turnpike sets in stochastic manufacturing systems with finite time horizon</td>
</tr>
<tr>
<td>1130</td>
<td>I. Györi, F. Hartung &amp; J. Turi</td>
<td>Approximation of functional differential equations with time- and state-dependent delays by equations with piecewise constant arguments</td>
</tr>
<tr>
<td>1131</td>
<td>I. Györi, F. Hartung &amp; J. Turi</td>
<td>Stability in delay equations with perturbed time lags</td>
</tr>
<tr>
<td>1132</td>
<td>F. Hartung &amp; J. Turi</td>
<td>On the asymptotic behavior of the solutions of a state-dependent delay equation</td>
</tr>
<tr>
<td>1133</td>
<td>Pierre-Alain Gremaud</td>
<td>Numerical optimization and quasiconvexity</td>
</tr>
<tr>
<td>1134</td>
<td>Jie Tai Yu</td>
<td>Resultants and inversion formula for $N$ polynomials in $N$ variables</td>
</tr>
<tr>
<td>1135</td>
<td>Avner Friedman &amp; J.L. Velázquez</td>
<td>The analysis of coating flows in a strip</td>
</tr>
<tr>
<td>1136</td>
<td>Eduardo D. Sontag</td>
<td>Control of systems without drift via generic loops</td>
</tr>
<tr>
<td>1137</td>
<td>Yuan Wang &amp; Eduardo D. Sontag</td>
<td>Orders of input/output differential equations and state space dimensions</td>
</tr>
<tr>
<td>1138</td>
<td>Scott W. Hansen</td>
<td>Boundary control of a one-dimensional, linear, thermoelastic rod</td>
</tr>
<tr>
<td>1139</td>
<td>Robert Lipton &amp; Bogdan Vernescu</td>
<td>Homogenization of two phase emulsions with surface tension effects</td>
</tr>
<tr>
<td>1140</td>
<td>Scott Hansen &amp; Enrique Zuazua</td>
<td>Exact controllability and stabilization of a vibrating string with an interior point mass</td>
</tr>
<tr>
<td>1141</td>
<td>Bei Hu &amp; Jiongmin Yong</td>
<td>Pontryagin Maximum principle for semilinear and quasilinear parabolic equations with pointwise state constraints</td>
</tr>
<tr>
<td>1142</td>
<td>Mark H.A. Davis</td>
<td>A deterministic approach to optimal stopping with application to a prophet inequality</td>
</tr>
<tr>
<td>1143</td>
<td>M.H.A. Davis &amp; M. Zervos</td>
<td>A problem of singular stochastic control with discretionary stopping</td>
</tr>
<tr>
<td>1144</td>
<td>Bernardo Cockburn &amp; Pierre-Alain Gremaud</td>
<td>An error estimate for finite element methods for scalar conservation laws</td>
</tr>
<tr>
<td>1145</td>
<td>David C. Dobson &amp; Fadil Santosa</td>
<td>An image enhancement technique for electrical impedance tomography</td>
</tr>
<tr>
<td>1146</td>
<td>Jin Ma, Philip Protter, &amp; Jiongmin Yong</td>
<td>Solving forward-backward stochastic differential equations explicitly — a four step scheme</td>
</tr>
<tr>
<td>1147</td>
<td>Yong Liu</td>
<td>The equilibrium plasma subject to skin effect</td>
</tr>
<tr>
<td>1148</td>
<td>Ulrich Hornung</td>
<td>Models for flow and transport through porous media derived by homogenization</td>
</tr>
<tr>
<td>1149</td>
<td>Avner Friedman, Chaocheng Huang, &amp; Jiongmin Yong</td>
<td>Effective permeability of the boundary of a domain</td>
</tr>
<tr>
<td>1150</td>
<td>Gang Bao</td>
<td>A uniqueness theorem for an inverse problem in periodic diffractive optics</td>
</tr>
<tr>
<td>1151</td>
<td>Angelo Favini, Mary Ann Horn, &amp; Irena Lasiecka</td>
<td>Global existence and uniqueness of regular solutions to the dynamic von Kármán system with nonlinear boundary dissipation</td>
</tr>
<tr>
<td>1152</td>
<td>E.G. Kalnins &amp; Willard Miller, Jr.</td>
<td>Models of $q$-algebra representations: $q$-integral transforms and &quot;addition theorems&quot;</td>
</tr>
<tr>
<td>1153</td>
<td>E.G. Kalnins, V.B. Kuznetsov &amp; Willard Miller, Jr.</td>
<td>Quadrics on complex Riemannian spaces of constant curvature, separation of variables and the Gaudin magnet</td>
</tr>
<tr>
<td>1154</td>
<td>A. Kersch, W. Morokoff &amp; Chr. Werner</td>
<td>Selfconsistent simulation of sputtering with the DSMC method</td>
</tr>
<tr>
<td>1155</td>
<td>Bing-Yu Zhang</td>
<td>A remark on the Cauchy problem for the Korteweg-de Vries equation on a periodic domain</td>
</tr>
<tr>
<td>1156</td>
<td>Gang Bao</td>
<td>Finite element approximation of time harmonic waves in periodic structures</td>
</tr>
<tr>
<td>1157</td>
<td>Tao Lin &amp; Hong Wang</td>
<td>Recovering the gradients of the solutions of second-order hyperbolic equations by interpolating the finite element solutions</td>
</tr>
<tr>
<td>1158</td>
<td>Zhangxin Chen</td>
<td>$L^p$-posteriori error analysis of mixed methods for linear and quasilinear elliptic problems</td>
</tr>
<tr>
<td>1159</td>
<td>Todd Arbogast &amp; Zhangxin Chen</td>
<td>Homogenization of compositional flow in fractured porous media</td>
</tr>
<tr>
<td>1160</td>
<td>L. Qiu, B. Bernhardsson, A. Rantzzer, E.J. Davison, P.M. Young &amp; J.C. Doyle</td>
<td>A formula for computation of the real stability radius</td>
</tr>
<tr>
<td>1161</td>
<td>Maria Inés Troparevsky</td>
<td>Adaptive control of linear discrete time systems with external disturbances under inaccurate modelling: A case study</td>
</tr>
<tr>
<td>1162</td>
<td>Petr Klouček &amp; Frauz S. Rys</td>
<td>Stability of the fractional step $\Theta$-scheme for the nonstationary Navier-Stokes equations</td>
</tr>
<tr>
<td>1163</td>
<td>Eduardo Casas, Luis A. Fernández &amp; Jiongmin Yong</td>
<td>Optimal control of quasilinear parabolic equations</td>
</tr>
<tr>
<td>1164</td>
<td>Darrell Duffie, Jin Ma &amp; Jiongmin Yong</td>
<td>Black's consol rate conjecture</td>
</tr>
<tr>
<td>1165</td>
<td>D.G. Aronson &amp; J.L. Vazquez</td>
<td>Anomalous exponents in nonlinear diffusion</td>
</tr>
</tbody>
</table>
Ruben D. Spies, Local existence and regularity of solutions for a mathematical model of thermomechanical phase transitions in shape memory materials with Landau-Ginzburg free energy

Pu Sun, On circular pipe Poiseuille flow instabilities

Angelo Favini, Mary Ann Horn, Irena Lasiecka & Daniel Tataru, Global existence, uniqueness and regularity of solutions to a Von Kármán system with nonlinear boundary dissipation

A. Dontchev, Tz. Donchev & I. Slavov, On the upper semicontinuity of the set of solutions of differential inclusions with a small parameter in the derivative

Jin Ma & Jiongmin Yong, Regular-singular stochastic controls for higher dimensional diffusions — dynamic programming approach

Alex Solomonoff, Bayes finite difference schemes

Todd Arbogast & Zhangxin Chen, On the implementation of mixed methods as nonconforming methods for second order elliptic problems

Zhangxin Chen & Bernardo Cockburn, Convergence of a finite element method for the drift-diffusion semiconductor device equations: The multidimensional case

Boris Mordukhovich, Optimization and finite difference approximations of nonconvex differential inclusions with free time

Avner Friedman, David S. Ross, and Jianhua Zhang, A Stefan problem for reaction-diffusion system

Alex Solomonoff, Fast algorithms for micromagnetic computations

Nikan B. Firouzye, Homogenization on lattices: Small parameter limits, H-measures, and discrete Wigner measures

G. Yin, Adaptive filtering with averaging

Wlodzimierz Byrc and Amir Dembo, Large deviations for quadratic functionals of Gaussian processes

Ilija Schmelzer, 3D anisotropic grid generation with intersection-based geometry interface

Alex Solomonoff, Application of multipole methods to two matrix eigenproblems

A.M. Latypov, Numerical solution of steady euler equations in streamline-aligned orthogonal coordinates

Bei Hu & Hong-Ming Yin, Semilinear parabolic equations with prescribed energy

Bei Hu & Jianhua Zhang, Global existence for a class of Non-Fickian polymer-penetrant systems

Rongze Zhao & Thomas A. Posbergh, Robust stabilization of a uniformly rotating rigid body

Mary Ann Horn & Irena Lasiecka, Uniform decay of weak solutions to a von Kármán plate with nonlinear boundary dissipation

Mary Ann Horn, Irena Lasiecka & Daniel Tataru, Well-posedness and uniform decay rates for weak solutions to a von Kármán system with nonlinear dissipative boundary conditions

Mary Ann Horn, Nonlinear boundary stabilization of a von Kármán plate via bending moments only

Frank H. Shaw & Charles J. Geyer, Constrained covariance component models

Tomasz Luczak, A greedy algorithm estimating the height of random trees

Timo Seppäläinen, Maximum entropy principles for disordered spins

Yuandan Lin, Eduardo D. Sontag & Yuan Wang, Recent results on Lyapunov-theoretic techniques for nonlinear stability

Svante Janson, Random regular graphs: Asymptotic distributions and contiguity

Rachid Ababou, Random porous media flow on large 3-D grids: Numerics, performance, & application to homogenization

Moshe Fridman, Hidden Markov model regression

Petr Klouček, Bo Li & Mitchell Luskin, Analysis of a class of nonconforming finite elements for Crystalline microstructures

Steven P. Lalley, Random series in inverse Pisot powers

Rudy Yaksick, Expected optimal exercise time of a perpetual American option: A closed-form solution

Rudy Yaksick, Valuation of an American put catastrophe insurance futures option: A Martingale approach

János Pach, Farhad Shahrokhi & Mario Szegedy, Application of the crossing number

Avner Friedman & Chaoheng Huang, Averaged motion of charged particles under their self-induced electric field

Joel Spencer, The Erdős-Hanani conjecture via Talagrand's inequality

Zhangxin Chen, Superconvergence results for Galerkin methods for wave propagation in various porous media

Russell Lyons, Robin Pemantle & Yuval Peres, When does a branching process grow like its mean? Conceptual proofs of $L \log L$ criteria

Robin Pemantle, Maximum variation of total risk

Robin Pemantle & Yuval Peres, Galton-Watson trees with the same mean have the same polar sets

Robin Pemantle, A shuffle that mixes sets of any fixed size much faster than it mixes the whole deck

Itai Benjamini, Robin Pemantle & Yuval Peres, Martin capacity for Markov chains and random walks in varying dimensions

Wlodzimierz Bryc & Amir Dembo, On large deviations of empirical measures for stationary Gaussian processes

Martin Hildebrand, Some random processes related to affine random walks

Alexander E. Mazel & Yuriii M. Suhov, Ground states of a Boson quantum lattice model