Erratum to “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
August 18, 2007

Abstract
This note corrects a flawed statement in the paper “On the Chung-
Diaconis-Graham random process”.

1 The Flaws and Corrections
On p. 352 of [1], the claim that

\[
\lim_{t \to \infty} \frac{G\left(\frac{2^{t-1}-2^i-1}{p}\right) G\left(\frac{2^t-2^i}{p}\right) G\left(\frac{2^{t-2}-2^i}{p}\right)}{G\left(\frac{2^{t-1}}{p}\right) G\left(\frac{2^t-2}{p}\right) G\left(\frac{2^{t-2}}{p}\right)} = \frac{G(1/2)}{G(0)} < 1
\]

can be shown has flaws. If \( j \) is constant, the limit is \( G(0.5 * (1 - 2^{-j})) / G(0) \). If \( b = 0 \), then \( G(1/2) / G(0) = 1 \).

First we shall consider the case where \( b \neq 0 \). Let \( M = \sup_{x \in [1/4, 1/2]} G(x) \). Then, we can show the fact that \( M < 1 \). To see this fact, we will let \( H(x) = |ae^{2\pi ix} + b| \) in the case \( a \neq 0 \). \( H(x) \) is decreasing on \([0, 1/2]\), and \( a + b - H(1/4) > 0 \). For \( x \in [1/4, 1/2] \), we have \( G(x) \leq H(x) + c = 1 - (a + b - H(1/4)) \leq 1 - (a + b - H(1/4)) \). If \( a = 0 \), then \( c > 0 \) and a similar argument using \( |ae^{2\pi ix} + b| \) applies. Since \( G(0) = 1 \), we conclude that

\[
\lim_{t \to \infty} \frac{G\left(\frac{2^{t-1}-2^i-1}{p}\right) G\left(\frac{2^t-2^i}{p}\right) G\left(\frac{2^{t-2}-2^i}{p}\right)}{G\left(\frac{2^{t-1}}{p}\right) G\left(\frac{2^t-2}{p}\right) G\left(\frac{2^{t-2}}{p}\right)} \leq M / G(0) < 1,
\]

and the rest of the argument is unaffected.

If \( b = 0 \), Case 2 of Theorem 1 can be proved by considering the following random processes on the integers mod \( p \).
1. \( X_0 = 0 \) and \( X_{n+1} = 2X_n + b_n \pmod{p} \) where \( P(b_n = 1) = a \) and \( P(b_n = -1) = 1 - a \)

2. \( Y_0 = 0 \) and \( Y_{n+1} = 2Y_n + d_n \pmod{p} \) where \( P(d_n = 2) = a \) and \( P(d_n = 0) = 1 - a \)

3. \( Z_0 = 0 \) and \( Z_{n+1} = 2Z_n + e_n \pmod{p} \) where \( P(e_n = 1) = a \) and \( P(e_n = 0) = 1 - a \)

If \( P_n(s) = Pr(X_n = s) \), \( Q_n(s) = Pr(Y_n = s) \), and \( R_n(s) = Pr(Z_n = s) \), then \( \|P_n - U\| = \|Q_n - U\| = \|R_n - U\| \). To see this, we can let \( d_n = 2e_n \) and \( b_n = d_n - 1 \) so that \( Y_n = 2Z_n \) and \( X_n = Y_n - \sum_{i=0}^{n-1} 2^i \) for \( n \geq 1 \). To conclude the case where \( b = 0 \), use the argument with \( b \neq 0 \) on the third random process (provided that \( a \neq 1/2 \) so that we are in Case 2).

2 Acknowledgment

The author thanks Ravi Montenegro for pointing out a flaw in the original argument.

References