Errata for
A Statistical Test Suite for Random and Pseudorandom Number Generators
for Cryptographic Applications
NIST Special Publication 800-22
May 15, 2001

Modification to Section 2.5.4, step 5 (page 26) - (the parameters for the **igamc** function):

(5) Compute $P-value = e^{-c^2(obs)/2}$. Since there are 3 classes in the example, the *P-value* for the example is equal to $igamc\left(1, \frac{c^2(obs)}{2}\right)$.

Modification to Section 2.9.4, step 1, paragraph 3 (page 37) - the text prior to the table; the definition of the string for the initialization segment):

For example, if $\varepsilon = 0101101001110101011 1$, then $n = 20$. If $L = 2$ and $Q = 4$, then $K = \ddot{e}n/L\hat{u} - Q = \ddot{e}20/2\hat{u} - 4 = 6$. The initialization segment is 01011010; the test segment is 011101010111. The L-bit blocks are shown in the following table:

Modification to Section 12.2.4, step 5 (page 48) - (the parameters and final result of the **igamc** function for the example):

(5) Compute: *P-value1* = **igamc** $\left(2^{m-2}, \nabla y_m^2\right)$ and

P-value2 = **igamc** $\left(2^{m-3}, \nabla^2 y_m^2\right)$.

For the example in this section,

$$\textit{P-value1} = \textbf{igamc}\left(2, \frac{1.6}{2}\right) = 0.9057$$

$$\textit{P-value2} = \textbf{igamc}\left(1, \frac{0.8}{2}\right) = 0.8805.$$

Modification to Section 2.14.4, steps 3 and 4 (page 53) - (the equation for z and its example in step 3; the *P-value* equation and its example in step 4):

(3) Compute the test statistic $z = max_{1 \le k \le n}|S_k|$, where $max_{1 \le k \le n}|S_k|$ is the largest of the absolute values of the partial sums S_k.

For the example in this section, the largest value of S_k is 4, so $z = 4$.

(4) Compute *P-value* = $1 - \sum_{k=\left(\frac{-n}{z}+1\right)/4}^{\left(\frac{n}{z}-1\right)/4} \left[\Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right) - \Phi\left(\frac{(4k-1)z}{\sqrt{n}}\right)\right] +$

$$\sum_{k=\left(\frac{-n}{z}-3\right)/4}^{\left(\frac{n}{z}-1\right)/4}\left[\Phi\left(\frac{(4k+3)z}{\sqrt{n}}\right)-\Phi\left(\frac{(4k+1)z}{\sqrt{n}}\right)\right]$$

where F is the Standard Normal Cumulative Probability Distribution Function as defined in Section 5.5.3.3.

For the example in this section, *P-value* = 0.4116588.

Modification to Section 2.14.6 (page 54) - (the *P-value*):

Since the *P-value* obtained in step 4 of Section 2.14.4 is ≥ 0.01 (*P-value* = 0.411658), the conclusion is that the sequence is random.

Note that when mode = 0, large values of this statistic indicate that there are either "too many ones" or "too many zeros" at the early stages of the sequence; when mode = 1, large values of this statistic indicate that there are either "too many ones" or "too many zeros" at the late stages. Small values of the statistic would indicate that ones and zeros are intermixed too evenly.

Modification to Section 2.14.8 (page 54) - (the ouput *P-values*):

(input) *e* = 11001001000011111101101010100010001000010110100011
00001000110100110001001100011001100010100010111000
(input) *n* = 100
(input) *mode* = 0 (forward) || *mode* = 1 (reverse)
(processing) *z* = 1.6 (forward) || *z* = 1.9 (reverse)
(output) *P-value* = 0.219194 (forward) || *P-value* = 0.114866 (reverse)
(conclusion) Since *P-value* > *0.01*, accept the sequence as random.

Modification to Section 2.15.4, step 6 (page 58) - (entry in the table for *x* = 2):

	Number of Cycles					
State *x*	**0**	**1**	**2**	**3**	**4**	**5**
-4	3	0	0	0	0	0
-3	3	0	0	0	0	0
-2	3	0	0	0	0	0
-1	2	1	0	0	0	0
1	1	1	0	1	0	0
2	2	0	0	1	0	0
3	3	0	0	0	0	0
4	3	0	0	0	0	0

Modification to Section 2.16.3 (page 60) - (reference in the definition of *x*):

x: For a given state *x*, the total number of times that the given state is visited during the entire random walk as determined in step 4 of Section 2.15.4.

Modification to 2.16.4, step 5 (page 62) - (correction of the parameter for the **erfc** function for the example):

For the example in this section, when $x = 1$, *P-value* = $\boldsymbol{erfc}\left(\frac{|4-3|}{\sqrt{2 \bullet 3(4|1|-2)}}\right)$ = 0.683091.Modification to Section 2.16.6 (page 62) - (correction of the *P-value* result for the example):

Since the *P-value* obtained in step 7 of Section 2.16.4 is ≥ 0.01 for the state $x = 1$ (*P-value* = 0.683091), the conclusion is that the sequence is random.

Modification to Section 3.12 (page 88) - (the input parameters for *P-value1* and *P-value 2*):

*P-value*1 = **igamc**(2^{m-2}, $\nabla\psi^2_m/2$)
*P-value*2 = **igamc**(2^{m-3}, $\nabla^2\psi^2_m/2$)

Modification to Section 3.15 (page 95) - (definition of $p_5(x)$):

$$p_5(x) = P(x(x) \geq 5) = \frac{1}{2|x|}\left(1 - \frac{1}{2|x|}\right)^4$$

Modification of Appendix A, paragraph 1 (page 117) - (the matrix will be in triangular form rather than diagonal form):

Apply elementary row operations where the addition operator is taken to be the exclusive-OR operation. The matrices are reduced to upper triangular form using forward row operations, and the operation is repeated in reverse in order using backward row operations in order to arrive at a matrix in triangular form. The rank is then taken to be the number of nonzero rows in the resulting Gaussian reduced matrix.