

# NIST 800-22 Corrections

Nick Galbreath

<http://modp.com/release/nist800-22/>

Version 1 -- 28-Jun-2005

The NIST 800-22 specification (with May 15, 2001 revision) contains a few errors. Here's what I've found.

## ■ G-SHA-1 Data set

A few of the examples use G-SHA-1 dataset (2.9.8, and another). The problem is the data provided is only 1,000,000 bits while the examples require 1,048,576 bits

## ■ 2.7.4, Page 34

In step 3, "Thus **after** block 1..." should be "Thus **in** block 1..."

## ■ 2.11.4, Page 45

Oddly for steps 5-7, the example is not computed.

## ■ 2.12.4, Page 47

Step 2, " $v_{111} = 0$ " should be " $v_{111} = 1$ "

## ■ 2.12.4, Page 48

Step 5, is completely bugged. The formulas and computations are incorrect (however, the general formal presented earlier is correct, and the correct computations appear in the next step).

## ■ 2.12.5 Page 48

The conclusion step need clarification. This test computes two P-values but does the conclusion depend on both values being  $\leq 0.01$ ? Or is this really two tests?

### ■ 2.13.4, Page 51

In step 6, error in computation of  $\chi^2$ . The result given 0.502193 needs multiplying  $2 \times 10$ .

### ■ 2.14.8, Page 54

In processing step, z should be 16 and 19 (not 1.6 and 1.9)

In conclusion step, I assume P-value  $\geq 0.01$ , and not P-value  $> 0.01$

### ■ 3.8, page 77

The formulas for  $P(U=3)$  and  $P(U=4)$  are incorrect.

```
In[4]:=
Pr[0, x_] := Power[E, -x]
Pr[u_Integer, x_] :=
  x * (E^-x) * (2^-u) * Sum[Binomial[u - 1, i - 1] * (x^(i - 1)) / Factorial[i], {i, 1, u}];
```

```
In[7]:= Pr[3, n]
```

$$\text{Out[7]} = \frac{1}{8} e^{-n} n \left( 1 + n + \frac{n^2}{6} \right)$$

```
In[10]:= Pr[4, n]
```

$$\text{Out[10]} = \frac{1}{16} e^{-n} n \left( 1 + \frac{3n}{2} + \frac{n^2}{2} + \frac{n^3}{24} \right)$$

This can also be generated by the equivalent formula of

```
In[11]:= Pr[u_Integer, x_] := x * (E^-(2 x)) * (2^-u) * Hypergeometric1F1[u + 1, 2, x]
```

```
In[12]:= Pr[3, n]
```

$$\text{Out[12]} = \frac{1}{8} e^{-n} n \left( 1 + n + \frac{n^2}{6} \right)$$

```
In[13]:= Pr[4, n]
```

$$\text{Out[13]} = \frac{1}{16} e^{-n} n \left( 1 + \frac{3n}{2} + \frac{n^2}{2} + \frac{n^3}{24} \right)$$

### ■ Appendix E, page 129

While not incorrect, the *Mathematica* program given in Appendix E is outdated. On my version (5.1), the default \$MaxPrecision value is 1,000,000, so this program actually cripples *Mathematica* by setting it to a smaller number 302500. In either case, if it is set too small, *Mathematica* will complain instead of producing invalid output.

Also note that this program does produce output in the same format as the the example data given.

If you are looking for an exact number of digits, note that **First[RealDigits[n,2],x]** will round the last digit, while **Take[First[RealDigits[n,2]],x]** will provide the exact digit at the end.