

Re: issues with statistical test suite from <http://csrc.nist.gov/rng/>

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-01/1768.html>

From: Cristiano (cristiano.pi_at_NSquipo.it)

Date: 01/26/04

Date: Mon, 26 Jan 2004 19:58:56 GMT

Mack wrote:

> On Sun, 25 Jan 2004 13:23:29 GMT, "Cristiano"

> <cristiano.pi@NSquipo.it> wrote:

>

>> Mack wrote:

>>> On Sat, 24 Jan 2004 16:28:27 GMT, "Cristiano"

>>> <cristiano.pi@NSquipo.it> wrote:

>>>

>>>> Mack wrote:

>>>>> On Thu, 22 Jan 2004 19:30:50 GMT, "Cristiano"

>>>>> <cristiano.pi@NSquipo.it> wrote:

>>>

>>> Skewness measures symmetry about a point. Kurtosis could be
>>> used but the expected value would not be zero as for the normal
>>> curve when applied to a uniform distribution, although this can be
>>> easily calculated.

>>>

>> Sure, it is $6/5 * (n^2+1) / (n^2-1)$ for a discrete uniform
>> distribution. And when you got, for example, 7/6 what do you say? It
>> is good? It is bad? And how much?

>>

>> Here I have two doubts:

>> 1) Surely we get some information from those parameters, but can the
>> information gotten be used in testing a rng (in an efficient way)?

>> 2) You say: "Skewness measures symmetry about a point". I don't know
>> how you calculate "your" skewness. Do you calculate it using the
>> absolute moments or the central moments in some "strange" way?

>

> skewness= $1/n * (\text{sum from } 1 \text{ to } n((Y_i - \text{expected mean})^3)) / \text{expected}$
> deviation³

>

> specifically:

>

> Skewness is a measure of symmetry, or more precisely, the lack of
> symmetry. A distribution, or data set, is symmetric if it looks the
> same to the left and right of the center point

>

> from: <http://www.itl.nist.gov/div898/handbook/eda/section3/eda35b.htm>

They wrote that Y is the mean, not the expected mean and that you should use the standard deviation, not the expected deviation.

As I already said, you use a useless method in a bad way.

>>>> *Diehard doesn't give KS results except where it is appropriate.*

>>>>

>>>> *So does NIST test. But exactly, what do you mean?*

>>>>

>>> *The finalAnalysisReport returns KS test values*

>>> *where these values are not appropriate.*

>>

>> *Who say that? Have you done a new discovery?*

>> *If you calculate the KS test for *only* one sequence, then the KS is*

>> *good enough.*

>

> *Why would you ever use a KS test on one p -value?*

Uh!? I know that my English is bad, but not so bad! Do you understand what I say?

You said that the KS test used for the final report is not appropriate.

I said that if you run once the FFT test, the related KS test is far good.

One can use whatever he wants, but the KS test used for the finalAnalysisReport is appropriate.

>> *But if you calculate the KS of the KS's gotten from 100 or 1000 sequences, then the overall p -value is useless because the 100 or 1000 p -values are too binned.*

>>

>>

>>>> *Unfortunately the output is pretty hard to read.*

>>>> *I usually open it with a text editor and search for results of*

>>>> *.000, .00, and .0.*

>>>>

>>>> *And when you find them what do you do?*

>>>>

>>> *Repeat that specific test with more data to determine if it is*

>>> *isolated or consistent.*

>>

>> *With more data? Each test needs a fixed number of 32-bit numbers*

>> *(some test requires slight variations on the number of input*

>> *numbers).*

>>

>> *Anyway, when a generator is definitely good or bad?*

>>

>

> *A generator is bad when it fails a test that has a good mathematical*

> *foundation in a spectacular manner*

Could you list some test that has a good mathematical foundation?

> *Or alternatively you can say that*
> *a generator is bad when fails some test (mathematical or empirical)*
> *that other "good" generators pass. Of course a single number that is*
> *.0000 or .9999 is not an indication of failure it must do so*
> *consistently, since a value like that happens randomly 1 time in*
> *10000.*

You still haven't said when a generator is good or bad.

> *A generator is good when it meets the criteria for which it will be*
> *used.*

If the criteria are showed by a test, then this is an incredibly big error!
What do you mean, exactly?

> *A bad generator such as a simple congruential generator may*
> *be a "good" generator if we are using it in a non-demanding*
> *application.*

It seems to me that you don't have an objective method to say: "this is good" or "this is bad".

I think it is because of the way you use skewness mixed with KS, chi-square and ayes.

>>>> *I am also having to create my own test suite because nothing*
>>>> *else meets my current needs. sts seems like a good package but*
>>>> *it has its limitations.*
>>>>
>>>> *Yes, all the tests have limitations. I think if one uses a test in*
>>>> *a proper*
>>>> *way the test can be useful anyway. The "proper way" could be also*
>>>> *to discard*
>>>> *a test! I done that with some test in dh.*
>>>>
>>> *I have never found it necessary to discard a DH test. They may not*
>>> *detect a problem where there isn't one but they have never given*
>>> *a strong result of a problem where one didn't exist.*
>>>
>> *I don't know the status of the newer version of dh, but that test*
>> *has had many problems (for example you could see my post on*
>> *september 2003 about the bad distribution of the overlap sum test).*
>>
>
> *The newer version is still being listed as 0.2 beta. However that*
> *error has been corrected. The big three tests Gorilla, GCD, and*
> *Birthday Spacings test all seem to be functioning adequately.*

sci.crypt: Re: issues with statistical test suite from <http://csrc.nist.gov/rng/>

Have you double checked that?

Cristiano