

Re: [Diehard] Overlap sum test

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-09/2170.html>

From: Cristiano (cristiano.pi_at_NSquipo.it)

Date: 09/27/03

Date: Sat, 27 Sep 2003 09:17:14 GMT

Ernst Lippe wrote:

> *On Wed, 24 Sep 2003 08:59:43 +0000, Cristiano wrote:*

>

>> *Ernst Lippe wrote:*

>

>>> *So far so good. Each individual y is the sum of a set of
>>> i.i.d. variables, so from the central limit theorem its distribution
>>> must approach the normal distribution when n_{sum} is sufficiently
>>> large.*

>>>

>>> *[interesting]*

>>>

>>> *I have not done the actual calculations to determine if this
>>> non-normality would have a real influence on the outcomes of the
>>> test, but I still find it somewhat strange. I would expect that a
>>> non-linear transformation would give better results.*

>>

>> *Why don't you have done the actual calculations? I done many tests*

>> *to write what I wrote and they have taken much time.*

>> *I'd like to hear some comment based on real facts. The theory is*

>> *beautiful, but the practice is wonderful! :-)*

>

> *But I gave you a fact, if I understand Marsaglia's post correctly*

> *I pointed you to the source of the problem.*

Yes. In my philosophy the statement "I have not done the actual calculations..." is not very beautiful. :-)

Anyway, I pasted your explanation in the source code of my implementation of the overlapping sum test.

>>> *On the other hand, I don't expect that this is the source of your
>>> problems. Marsaglia is an expert so it seems reasonable to assume
>>> that his approximation is OK.*

>>

>> *Well, in this case don't touch a thing.*

>> *I totally disagree when I hear this kind of argument. Nobody is*

>> *infallible.*

>

sci.crypt: Re: [Diehard] Overlap sum test

> *OK, you were certainly right in this case.*

With the phrase "Nobody is infallible" *always* clear in mind I solved many issues. :-)

> *BTW, thanks for your efforts, the Diehard battery of tests are highly useful, and it is important to have a good implementation.*

I agree. And for that reason I am very surprised when someone post a possibly bug and nobody seems interested in that post. I seen this strange behavior for all the post related to a bug of DH.

I'd like to see the effort of everybody to fix the problem; the effort of the author should be the first! :-)

Cristiano