

Re: FFT test with few kbits

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-03/0036.html>

From: Paul Pires (*diodude_at_got.net*)

Date: 02/29/04

Date: Sun, 29 Feb 2004 22:12:09 GMT

Ernst Lippe <ernstl-at-planet-dot-nl@ignore.this> wrote in message
news:4042457a\$0\$1154\$ba620dc5@nova.planet.nl...

> *On Fri, 27 Feb 2004 21:00:14 +0000, Paul Pires wrote:*

>

>

> > *Take a moment to look at the common sense. Say this test*

> > *is deployed, say it routinely passes good random streams.*

>

> *But what evidence do you require before you would say that good random
> streams routinely pass this test?*

>

> *This would be easy, if we had a proof that Christiano's statistic*

> *(asymptotically) follows the KS-distribution, but I hope that you can*

> *agree, that we currently don't have such a proof.*

I can agree with that.

>

> *Basically, that leaves just one other option: Monte Carlo*

> *simulations.*

Not to me. To me, the options available depend on the goal.

There are other empirical solutions for the problem if the goal is to refine a discovered phenomenon. Cristiano has dubbed it the FFT test, you are rejecting it since it does not follow the rules for statistics according to FFT.

I personally don't care. I wouldn't even go there at this point.

First I would confirm that the claimed phenomenon actually exists and if it does anything worthwhile.

> *Essentially, what you are doing then is approximating the*

> *empirical distribution of a statistic. Of course this is a valid*

> *approach for any statistic. The only slightly tricky point is to*

> *determine the number of simulations that you need. When someone has*

> *done these simulations for a given value of N, you can of course use*

> *these results in other cases where the sample size is also equal to*

> *N. But what should you do when want to use this test with a different*

- > value for N ? The most prudent approach (which AFAIK is also followed
- > by statistical packages such as Diehard and NIST's) is to assume that
- > the test should only be used for the values of N for which simulations
- > have been performed. When you believe that we can be more lenient,
- > i.e. that we can also use the test even for values of N for which
- > there are no simulation results, could you explain why and under which
- > conditions?

As I said, I don't care. My supposition (now improved) was that you run this test (with any N) on the data sets from different sources. If some sources consistently "pass" but one or more source consistently fails, then the test is a discriminator. It can identify a source from an output.

At THIS point I care about how the test is doing it and I don't limit my scrutiny to it's theoretical foundation. Most discoveries have far more to do with serendipity than a rational plan.

If it fails all data from all sources including physical stuff that should really be random then we know that it is a broke test OR that there is no such thing as random and we have a definitive test for that thing we have now proved doesn't exist. I'd save the headache and just call it a broke test.

If it cannot be shown to do anything usefull (like discriminate), Then I would insist as you would that it has a sound foundation if it would be seen as an affirmative test that output should generally pass. But I still wouldn't care one way or another whether that effort succeeded. That's all we need, one more test that doesn't tell us anything new about a "suspected random" set of data in the range of "goodness" that is interesting:—)

- > (One of the reasons why I would be cautious about
- > extrapolations is that the Fourier components show some curious
- > patterns that depend on the prime factors in N , and I would not be
- > surprised if the prime factorization also influenced the distribution)

Sounds like something to test.

- >
- > From a cryptographic point of view, of course, we are only interested
- > to see if the test can be used as a discriminator. But one of the
- > problems at the current stage is that it cannot be used in
- > isolation. For any other statistical test it would be reasonable to
- > reject a RNG based on the sole fact that it consistently fails that
- > test. At the current stage, we can't do that with Christiano's test,
- > because we must also show that a good RNG would not have failed as
- > well, something that is not necessary for statistical tests with a
- > known distribution (it does not matter if that distribution was
- > computed from its analytical solution or by simulations).

I think you have it quite wrong here. Statistical tests with a known distribution share this problem in a practical sense even if they don't from the science viewpoint. I have seen brain farts in both

concept and execution of such tests that would have been caught if such tests were held to the same standard of doubt. It is an unreachable standard for sure but that just means that all tests must be viewed as suspect since there is no actual qualification for any of them.

Having this viewpoint I see little practical difference between a test with good lineage and a heuristically derived one if they are both equally qualified in practical terms and both are doubted as a working assumption.

>

> > *I think it would be more usefull at this point to characterize the test rather than "prove" it. Make a matrix of tested outputs of many generators tested with many popular tests and also your proposed test. Post the results.*

>

> *That's a good idea of course.*

Here's another one. What this feild needs is a real, working, rational program of quality assurance for tests. Cristiano has shown a gift in this area although from time to time he gets a little "over animated". Agree to disagree and then co-operate. We all know how much snake oil is produced when rational thought is replaced by enthusiasm. Have you ever wondered how much innovation is lost to dogma? I've seen it time and time again.

I dismount my soap box. Have a nice day!

Paul

>

> *Ernst Lippe*

>