

Re: FFT test with few kbits

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2004-02/1706.html>

From: Ernst Lippe (*ernstl-at-planet-dot-nl_at_ignore.this*)

Date: 02/23/04

Date: Mon, 23 Feb 2004 19:15:54 +0100

On Mon, 23 Feb 2004 12:58:07 +0000, Cristiano wrote:

> *Cristiano wrote:*

>> *Bill Unruh wrote:*

>>> *Yes, they are independent.*

>>> $\langle c(m)c(n) \rangle = \sum_k \sum_l \langle b(k)b(l) \rangle \cos(2\pi m k) \cos(2\pi n l)$

>>> $= \sum_k \langle b^2(k) \rangle \cos(2\pi m k) \cos(2\pi n k)$

>>> $= \langle b^2 \rangle \sum_k [\cos(2\pi (m+n) k) + \cos(2\pi (m-n) k)] / 2$

>>> $= 0$ unless $m=n$ or $m=-n$

>>> *Similarly for the sine and the cross ones.*

>>> *I used that the bits at different positions are independent, and*

>>> *that all of the positions have the same mean square (1/2 in your*

>>> *system). Thus the correlations between different values are zero.*

>>

>> *As you know, my math skill is poor, so I sent your answer to the*

>> *Italian mathematician to hear his thought.*

>

> *I got his answer; hard translation...*

>

> *To be honest, when I said they are not independent I had a doubt. But*

> *strictly speaking I'm right. The question is a bit subtle.*

Yes, it is. Bill was referring to the fact that they are not linearly correlated, which is, as you correctly noted, a different notion.

> *Showing that the mean value of the product of two random variate is the product of the mean values is just a needed condition for the independence, (The standard english mathematical term is "necessary" condition) but not sufficient.*

OK!

> *You can easily see that they are not independent taking a small n, e.g. n=2.*

> *For big n's the $c[m]$ tend to be normal and for random variate normally*

> *distributed the above condition is also sufficient.*

> *Thus they are not independent, but they are independent as n get bigger;*

> *in other word, increasing n, the independence is stronger.*

I am feeling a bit uncomfortable with this sentence. First of all, the standard statistical definition of independence is a pure black-and-white one, two random variables are either independent or they are not independent. As far as I know there is not really a standard measure for the "degree of independence".

In one of my previous post I more or less suggested an ad-hoc measure of the "degree of independence" based on entropy, and I argued that according to this measure two different Fourier components are actually what you would call highly dependent. Your statement at least suggests that when N becomes very big the dependence between two Fourier components becomes small. In the example that I gave when N is a prime the degree of dependence will be high even when N becomes very large (and I expect that you will find similar results for the case that N is not prime, they are just somewhat harder to analyze).

So, in order to give a mathematical interpretation to your notion of "independence" we should first have some way to quantify it, and even when you select such a measure, I am not all that certain that it is true that the "independence" become really larger when N gets larger.

Ernst Lippe