Re: true random number generator

Source: http://www.derkeiler.com/Newsgroups/sci.crypt/2004−04/0851.html

---

From: Bill Unruh (*unruh_at_string.physics.ubc.ca*)
Date: 04/12/04

Date: Mon, 12 Apr 2004 16:24:45 +0000 (UTC)

"Gary Shannon" <gary@fiziwig.com> writes:

]>
]> Again, the conclusion is that only quantum mechanical events are
]> "truly" random and that all classical events are ultimately,
]> theoretically predictable if quantum effects are (theoretically)
]> excluded.

]Granted, the most popular _interpretation_ of QM supposes that true
]randomness exists, but in spite of it's pervasive popularity this is only an
]unproven, and indeed, usupported hypothesis. In fact, Bohm's formulation of
]QM makes all the same predictions, is a perfect fit the experiemtnal data,
]and does NOT claim that any such thing as "true" randomness exists.

Bohm's theory is one that is loved by philosophers and hated by
physicists−− because it is awkward and does not generalise.Bohm's theory
has immense problems with both spin, fermions, and field theories, which
quantum mechanics handles with no problems whatsoever. And all of these
are tested with wonderful precision.

]"Bohm's theory is the only serious proposal around just now that is fully
]deterministic." ... "Moreover, and this point is important, it is free of
]any of the metaphysical perplexities associated with QM superposition."

]−− David Z. Albert in _Bohm's Alternative to Quantum Mechanics_ Scientific
]American, May, 1994

Albert is one of those philosophers.

]So the assumption that QM events are random is pure conjecture and is
]without any experimental support inasmuch as every experiment that is used

It has immense experimental support.

]to bolster that interpretation also supports Bohm's deterministic
]interpretation. In other words, to believe that QM events are random

False. There are no Bohmian prediction for the vast majority of physics experiments.

]requires that you take it on faith that they are random. Taking something]as fundamental as that on faith seems pretty risky to me.

No. Since Bohmian mechanics ALSO postulates a fundamental inherent randomness to the world. It is a thoery about the time development of a statistical ensemble. And that ensemble is not refineable (ie you cannot reduce it down to a single member by any set of measurements) since otherwise it would disagree with QM. Ie, Bohmian mechanics is also inherently non−deterministic. It may be locally realistic, but still indeterministic.