

ON THE QUANTUM COMPUTING DELUSION (2.0.0)

Quantum mechanics is certainly imposing. But an inner voice tells me that it is not yet the real thing. The theory says a lot, but does not really bring us any closer to the secret of the old one. I, at any rate, am convinced that He does not throw dice.

Albert Einstein

The prospect of an up-coming quantum computer revolution is big news these days, with some technologists predicting that a scalable quantum computer is a mere 4 - 5 years away. It has even been claimed -by D-Wave co-founder Eric Ladizinsky- that this prospective revolution will be civilization's next big revolution. The *truth* is that quantum computers that are anything more than toys are, not merely difficult to engineer, but mathematically impossible, and based on a fundamental misunderstanding of the relationship between classical and quantum physics...

Super-Intelligent Aliens

Asked in an interview if he worries, like some theoretical physicists, that our universe is the simulation created by super-intelligent aliens, computer scientist Scott Aaronson responded:

If we can get evidence, then the aliens are basically just the gods of traditional religions, differing only in details like their motivations or how many arms they have. In that case, the reason to be skeptical of them is the same reason to be skeptical of traditional religions: namely, where's the evidence? Why have these gods/aliens, just like the conspirators who set up Lee Harvey Oswald as a patsy, demolished the Twin Towers from the inside, etc. etc., done such a spectacular job of hiding themselves?

The second possibility is that the simulating aliens belong to a higher metaphysical realm, one that's empirically inaccessible to us even in principle. In that case, to be honest, I don't care about them! Given any theory of the world that we might formulate involving the aliens, we can simplify the theory by cutting the aliens out. They're explanatorily irrelevant.

I disagree. To conclude that there is no evidence for something, one must first know what such evidence would look like: the absence of the fingerprints of *X* from the murder weapon is an absence of evidence that *X* is the murderer only because the *presence* of these fingerprints on the murder weapon is the *presence* of evidence that *X* is the murderer. What then are the signs of the *presence* of a super-intelligent alien creator? This question is far harder than both atheists and theists might fondly imagine. By definition, the creator of the universe is at least to some extent outside of the universe, and thus is by definition not 'empirically accessible' in any ordinary sense of the expression, but does "empirically inaccessible" means "explanatorily irrelevant"? Not at all. The truths of mathematics are not empirically accessible, but yet you can't have an explanation without them. The role of such truths is that they are, not the objects, but the *conditions* of sensory experience. A super-intelligent alien creator would function first and foremost as a *condition* of sensory experience.

Is Scalable Quantum Computation Possible?

A not-unrelated disagreement between myself and Aaronson concerns his specialist topic of quantum computing: he thinks that we will very probably have scalable quantum computers one day. Believing that QC can work, he says, doesn't make you a 'starry-eyed visionary', but a 'scientific conservative'. He regards himself as a scientific conservative, and he has offered \$100,000 to any scientific 'radical' who can convince him that there is some reason why QC is impossible.

Hi, I'm Scott Aaronson. I study quantum computing at MIT. Recently, on my blog, I offered a \$100,000 reward for a demonstration, convincing to me, that scalable quantum computing is impossible in the physical world...

Would he ever actually pay out? Not according to Joy Christian, who claims to have disproved QC, and with whom Scott has had a somewhat acrimonious relationship:

There is absolutely nothing that would convince you to part with your 100,000. You know that, and everyone else knows that ... The whole thing is just a smug scam to look smarter than the rest of us without having to do the hard work. Good luck with that.

Scott says that it is necessary and sufficient to convince the majority of the physics community:

Do you hope and expect to do that? If so, then you can expect my \$100,000; if not, then not. If a scientific revolution has taken place only inside the revolutionary's head, then let the monetary rewards be likewise confined to his head.

The reason he made the bet was, he says, "to draw attention to the case that quantum computing skeptics have yet to offer."

If quantum computing really does turn out to be impossible for some fundamental reason, then once I get over the shock to my personal finances, I'll be absolutely thrilled. Indeed, I'll want to participate myself in one of the greatest revolutions in physics of all time, a revolution that finally overturns almost a century of understanding of quantum mechanics. And whoever initiates that revolution will certainly deserve my money. But what I know for sure is that quantum computing isn't impossible for some trivial reason that's simply been overlooked for 20 years by a very large group of physicists, mathematicians, computer scientists, and engineers. And I hope putting my money where my mouth is will help more people realize that.

The Projective Universe

I'm not a fan of the "wisdom of the crowds" theories of truth. Is the earth more likely to be flat, or light to have infinite speed... because the "physics community" have agreed amongst themselves - as they once did- that such things are so? A false notion doesn't become truth regardless of how many people, or what class of people, believe it, and a true notion remains true regardless of how many people, or what class of people, *disbelieve* it. But I *fully* agree with the point about triviality: I think that the reason QC is impossible is far from trivial, and that it arises from a deep misunderstanding of the relationship between the classical and quantum domains. To see this misunderstanding clearly, we start with Newton and his misunderstanding of the nature of the relationship between light and space - he took the mistaken view that space was a dark, inert background or a stage against which luminous objects of one sort or another moved or played. This view goes back at least as far as Democritus and Leucippus, who saw the world as comprised of atoms separated by empty space. Einstein modified this picture in a good direction by allowing that space was active rather than passive, by allowing that space could influence the objects within it. But his proposal that *mass* curves space implies that the fundamental condition of the universe is infinitely massive -all of the mass in the universe is supposedly compressed to a point. This is wrong, a *reductio ad absurdum* of the idea that mass produces curvature: since this fundamental condition involves no space and time, nor can it involve mass, which by definition and by experiment (the Pauli exclusion principle forbids fermions from occupying the same space, and we never see a lone quark) is a spatio-temporal phenomenon. It follows that the curvature of the original universe is not function of mass. Mass is a combination of light and space, and if we reject atomism, and give priority to light rather than space, then the fundamental condition of the universe involves no mass, and curvature can at first be deemed to be a function of concentrated light. In a region in which there is a *balance* of light and space, the law of gravitation that comes out of this re-conception will agree with the old law, but in regions in which this balance is tipped toward light the new law will make different predictions. In a region where this balance is tipped toward *space*, the new law will again make different predictions, but this form of imbalance is to be associated to the end rather than the beginning of the universe. We can say more about this fundamental condition of the universe, and how we come to be where we are now, by considering the *Wolfram Mathworld* definition of a projection:

A projection is the transformation of points and lines in one plane onto another plane by connecting corresponding points on the two planes with parallel lines. This can be visualized as shining a (point) light source (located at infinity) through a translucent sheet of paper and making an image of whatever is drawn on it on a second sheet of paper.

But a "(point) light source" is the same thing as a zero-dimensional light source, which involves the infinite concentration and the zero diffusion of light, the fundamental condition of the universe according to the reasoning above. The problem with the *Wolfram Mathworld* definition of projection, and with every physical theory that relies on multiple

zero-dimensional point-sources, is that these involve an infinite concentration and zero diffusion of light. Kepler and Newton showed that the motions of heavenly bodies follow orbits resulting from the intersection of a cone by a plane, i.e, they showed that gravitational attraction can be understood in terms of the intersection of a cone by a plane. By implication, if the plane intersects the cone at its root, and at 90 degrees, we have an infinite concentration and a zero diffusion of light, which is a picture of the fundamental condition of the universe and the *Wolfram Mathworld* point (light) source, but it is not a picture of anything else. A *solution* to the aforesaid problem then, is that for every way of positioning the plane that allows for light to be diffused over space, a further point-source is required such that this is greater than zero-dimensional and involves therefore a finite quantity of concentrated light and a non-zero quantity of diffused light:

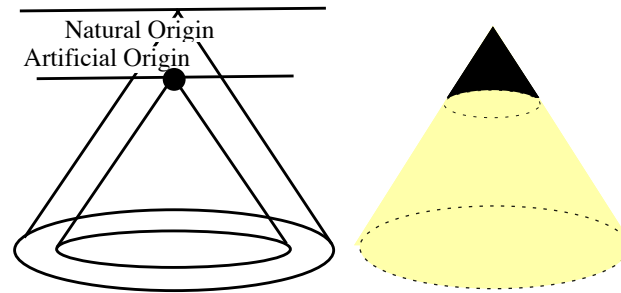


Figure 1: Artificial point-sources

Note that nothing is to be done to the light, and thus that we have the idea of a universe which is created according to the ancient Hebraic tradition by the projection, not of light, but of space. This is a heuristic picture, but we can if we wish extract as much detail as we desire by identifying these differences with atoms: as the gap narrows, the atom concentrates light, jumps to a higher energy level; and as the gap widens, the atom diffuses light, jumps to a lower energy level...

The Extension of Pi

Essential to this notion of a light-centric *-projective-* universe is the distinction between the projection and the projector, and to draw it we require unorthodox mathematics. To get at this mathematics consider firstly the inverse square law behind the $1/r^2$ formula. Classically, the law describes a fixed quantity can be increasingly spread over an increasing area, which means that there is a symmetric relationship between that quantity and the area. If the quantity or the area *died-off* with distance, then that would be an asymmetric relationship. In particular then, a light-centric physical theory must involve a broader concept of circularity, one that includes the traditional circle as a special case, but where the relationship between light and space can be an asymmetrical one. If a circle is supposed to have an area of 1, then an light source S located at the center will posses the same strength from center to circumference for $S/1 = S$. This is the same thing as saying that there is no difference between center and circumference. If there is no such difference, then either the circle has no area and no radius, or infinite area and an infinite radius; S either has either infinite strength or no strength. But in reality the strength of S always lies between these extremes. By the πr^2 formula we know that a circle of area 1 has a radius of $1/\sqrt{\pi}$ or 0.56419, but there is no clear way to extract sufficient variation from π to permit a potentially infinite number of energy levels less than infinity but greater than 0. $1/\sqrt{\pi}$ or $0.56419 \approx e^{-\gamma}$ or $\frac{1}{\sqrt{e^{2\gamma}}}$ or 0.561459:

$$0.56419 - 0.561459 = 0.002731$$

Since gamma is the limit (of the difference between the sum and the integral of the harmonic series)

$$\gamma = \lim_{x \rightarrow \infty} \left(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn \right)$$

a measure that is better able to give us what we want than π is $e^{2\gamma}$ or 3.17222 rather than 3.14159. Gamma is the limit of a potentially infinite number of values, so instead of

$$\pi \sqrt{\frac{1}{\pi}} = 1$$

we may write

$$\lim_{x \rightarrow \infty} e^{2\gamma} \left(\sqrt{\frac{1}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}} \right)^2 = 1$$

Old formula...

$$\pi R^2 = A$$

gives

$$\pi \sqrt{\frac{1}{\pi}} = 1$$

which describes a singularity. New formula

$$e^{2\gamma} \sqrt{\frac{1}{e^{2\gamma}}} = 1$$

followed by $\lim_{x \rightarrow \infty} e^{2\gamma} \left(\sqrt{\frac{1}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}} \right)^2 = 1.$

Newton's and Einstein's equations for gravity are couched in terms of the traditional unit circle (where the radius rather than the area is 1), the old formula for which is $\sqrt{\frac{A}{\pi}} = R$ gives $\sqrt{\frac{\pi}{\pi}} = 1.$

New formula

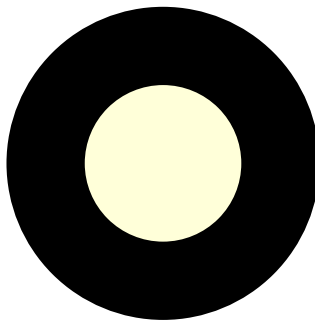
$$\sqrt{\frac{e^{2\gamma}}{e^{2\gamma}}} = 1$$

followed by:

$$\lim_{x \rightarrow \infty} \sqrt{\frac{e^{2\gamma}}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}} = 1$$

The new equations will at first look strange, but they are merely variants of the old π^2 formula which allow π to vary beyond its classical limits, are therefore able to take account of curvature caused extreme imbalances of light (extreme example = singularity of light behind the beginning of time) and space (pseudo-singularities in black holes at the end of time). To make this new improved formula work properly, the following pair of shapes must be regarded dualistically, as having positive and negative elements.

$$\text{Area of Exterior Circle} = e^{2\gamma} \sqrt{\frac{1}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}}^2 \quad \text{Area of Interior Circle} = e^{2\gamma} \sqrt{\frac{1}{e^{2\gamma}}} - e^{2\gamma} \sqrt{\frac{1}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}}^2$$

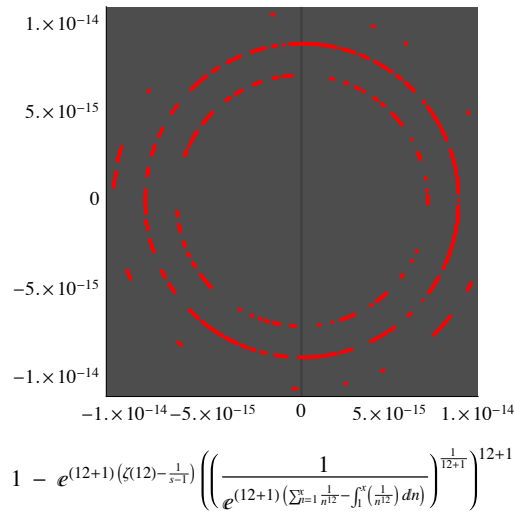


Once it is agreed that γ is a special case of $\zeta(s) - \frac{1}{s-1}$, we can go from $\lim_{x \rightarrow \infty} e^{2\gamma} \sqrt{\frac{1}{e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}}}^2 = 1$ to the more general:

$$\lim_{x \rightarrow \infty} e^{(s+1)(\zeta(s) - \frac{1}{s-1})} \left(\left(\frac{1}{\exp((s+1)(\sum_{n=1}^x \frac{1}{n^s} - \int_1^x \frac{1}{n^s} dn))} \right)^{\frac{1}{s+1}} \right)^{s+1} = 1$$

Now consider that although the limit is 1, regardless of the values of x or s , we get an inter-relationship between the exterior and interior circles that is non-repeating if and only $s = 1$, meaning for instance that the exterior circles in the figures above can be expanded indefinitely and/or that the interior circles contracted indefinitely. These dynamics are

associated with spirals that unfold forever. If s takes on a (positive) real value other than 1 -when the circles take on certain maximum/minimum size- we get an inter-relationship, and a contraction/expansion process that *is* repetitive. *These* dynamics are associated with the *circular* forms of a spiral.



We can use this idea to see the inverse square law as special case of a larger law, and to extend this law and Newton's/Einstein's law of gravity beyond regions in which there is a balance of light and space, indeed to *all* regions amenable to mathematical description. Take the $1/r^2$ formula, and consider a circle of area 1. There is in the limit a perfect balance of light and space ($E = 1$ and $A = 1$). If however if we write π as the partial sum/integral $e^{2(\sum_{n=1}^x \frac{1}{n} - \int_1^x \frac{1}{n} dn)}$ and/or s is a real number other than 1, then we have an imbalance. We can say the following: if $s = 1$, then there is an approximately symmetrical relationship between light and space, and the new formula will yield predictions which are similar to those yielded by $1/r^2$. If however $s \neq 1$, the balance is strongly tipped toward light (extreme example the singularity of concentrated light at the root of the universe), or conversely toward space (extreme example the interior of black holes), and the new formula makes *entirely* different predictions than $1/r^2$. When $s \neq 1$, the region of space described by the new law curves back on itself. In these light or space dense environments, curvature -as a function of density- is far greater:

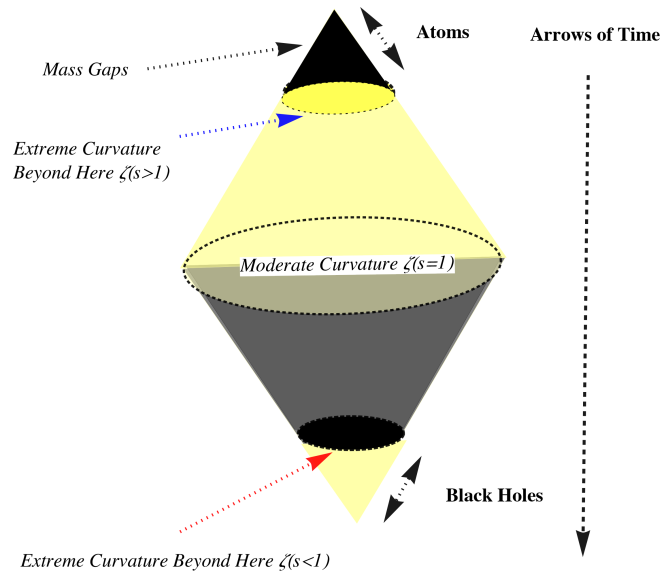


Figure 2: Depicting of the projective universe

The Golden Key

Consider now Euler's argument in *Variae observationes circa series infinitas* (1737) (justifiably called by John Derbyshire "The Golden Key"). Here he notes that the product continued to infinity of this fraction

$$\frac{2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \dots}{2 \times 4 \times 6 \times 10 \times 12 \times 16 \times 18 \dots}$$

in which the numerators are prime numbers and the denominators are one less than the numerators, equals the sum of the infinite series

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} \dots$$

and they are both infinite. To prove his point Euler invites us to imagine the extraction from the second series a prime denominator and all remaining multiples of that prime denominator until everything except the first term 1 has been eliminated. Let

$$x = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} \dots$$

Then

$$\frac{1}{2}x = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \frac{1}{8} \dots$$

This leaves

$$\frac{1}{2}x = 1 + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} \dots$$

To eliminate the denominators that are divisible by 3, we divide both sides to get

$$\frac{1 \times 1}{2 \times 3}x = \frac{1}{3} + \frac{1}{9} + \frac{1}{15} + \frac{1}{21} \dots$$

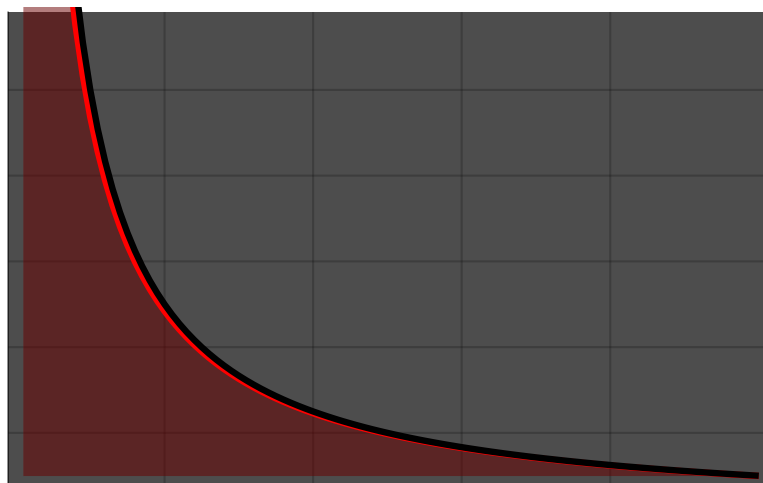
Subtracting again eliminates all remaining denominators that are multiples of 3 leaving

$$\frac{1 \times 2}{2 \times 3}x = 1 + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} \dots$$

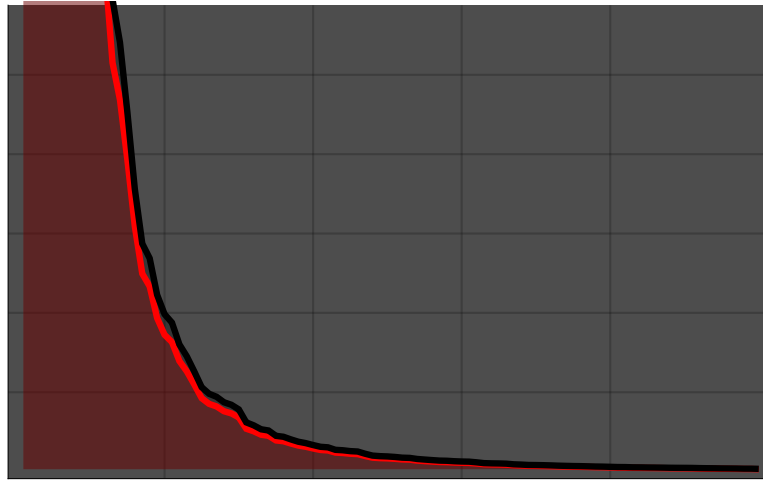
Applying this eliminatory process to *all* of the prime numbers leaves

$$\left(\frac{1 \times 2 \times 4 \times 5 \times 10 \times 12 \times 16 \times 18 \dots}{2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17 \times 19 \dots} \right) x = 1$$

This is a thought-experiment -mere imagination- but if these eliminations could be performed in the physical world, they would result in the disappearance of any distinction between the form and the content of a coordinate system, and therefore the shrinking of space and the slowing of time to a zero-dimensional point. An idea we can take from Euler's thought-experiment is that, since both prime-density *and* energy-density must at this point be infinite, this is the state of infinitely concentrated light required by, but conspicuously missing from the General Theory of Relativity. From here we can begin to relate the equations above to the theory according to which the projective universe arises from a process involving the distribution of the prime numbers in the number line....



$$\text{---} -e^{2\gamma} \sqrt{\frac{1}{e^{2(\frac{1}{n-1} - \frac{1}{n})^2 d n}}} + e^{2\gamma} \sqrt{\frac{1}{e^{2\gamma}}} + 1 \text{ ---} \frac{1}{x} + 1$$



$$\text{---} -e^{2\gamma} \left(\left(\frac{1}{\exp((s+1) \left(\sum_{n=1}^{p_x} \frac{1}{n^s} - \int_1^{p_x} \frac{1}{n^s} dn \right))} \right)^{\frac{1}{s+1}} \right)^2 + e^{2\gamma} \left(\left(\frac{1}{e^{(s+1) \left(\zeta(s) - \frac{1}{s-1} \right)}} \right)^{\frac{1}{s+1}} \right)^2 + \frac{1}{s} \quad \text{---} \frac{1}{p_{s-1}} + \left(\frac{1}{p_x} \right)^s$$

$$U = e^{2\gamma} \sqrt{\frac{1}{e^{2\gamma}} + \epsilon}$$

$$0 = -e^{2\gamma} \left(\sqrt{\frac{1}{\exp(2 \left(\sum_{n=1}^{p_x} \frac{1}{n} - \int_1^{p_x} \frac{1}{n} dn \right))}} \right)^2 + e^{2\gamma} \sqrt{\frac{1}{e^{2\gamma}} + 1}$$

$$\begin{pmatrix} 0 & -U & -U & -U & -U & \dots \\ U & 0 & -U & -U & -U & \dots \\ U & U & 0 & -U & -U & \dots \\ U & U & U & 0 & -U & \dots \\ U & U & U & U & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

$$u = e^{2\gamma} \left(\left(\frac{1}{e^{(s+1) \left(\zeta(s) - \frac{1}{s-1} \right)}} \right)^{\frac{1}{s+1}} \right)^2 + \epsilon$$

$$0 = -e^{2\gamma} \left(\left(\frac{1}{\exp((s+1) \left(\sum_{n=1}^{p_x} \frac{1}{n^s} - \int_1^{p_x} \frac{1}{n^s} dn \right))} \right)^{\frac{1}{s+1}} \right)^2 + e^{2\gamma} \left(\left(\frac{1}{e^{(s+1) \left(\zeta(s) - \frac{1}{s-1} \right)}} \right)^{\frac{1}{s+1}} \right)^2 + \frac{1}{s}$$

\hbar = the point at which the gap between $e^{2\gamma} \left(\left(\frac{1}{e^{(s+1) \left(\zeta(s) - \frac{1}{s-1} \right)}} \right)^{\frac{1}{s+1}} \right)^2$

and $e^{2\gamma} \left(\left(\frac{1}{\exp((s+1) \left(\sum_{n=1}^{p_x} \frac{1}{n^s} - \int_1^{p_x} \frac{1}{n^s} dn \right))} \right)^{\frac{1}{s+1}} \right)^2 + \frac{1}{s}$ ceases to decrease.

$$\begin{pmatrix} 0 & -u & -u & -u & \dots & -u \\ u & 0 & -u & -u & \dots & -u \\ u & u & 0 & -u & \dots & -u \\ u & u & u & 0 & \dots & -u \\ \vdots & \vdots & \vdots & \vdots & \ddots & -u \\ u & u & u & u & u & \hbar \end{pmatrix}$$

In this arrangement, various members of the harmonic series are associated to the values on the center diagonal -with the zeros- of these matrices, but while the infinite matrix is associated to *all* the members of this series, the finite matrices are associated only to the reciprocals of the primes and their squares. This the basis of Euler's thought experiment. What happens if *per impossible* we eliminate all the finite matrices from the infinite matrix? Same thing that happens if we eliminate all of the reciprocals of the primes and their powers from the harmonic series - we reduce the infinite matrix to a state we can associate to 1/0 and to an infinite concentration of light. Thus we have clear distinction between the projection (potentially infinite matrices and $s = 1$) and the projectors (strictly finite matrices and $s \neq 1$ remembering that s is a positive real value in this context) such that a projection involves a balance of concentrated and diffused light, and a projector involves an *imbalance* in favour of concentrated light.

Quantum Computing and the P versus NP Problem

Quantum systems lose coherence upon interaction with the environment and become classical. Quantum coherence is known to decay exponentially in time, so that macroscopic quantum superpositions are generally unsustainable. But strongly perturbed quantum systems such as the kicked rotator (a particle constrained to move on a rotating stick and subject to phase noise) exhibit decay times that are initially *polynomial*. These systems are able to mimic classical systems for a limited time, before reaching a state of localization sometimes known as "break-time":

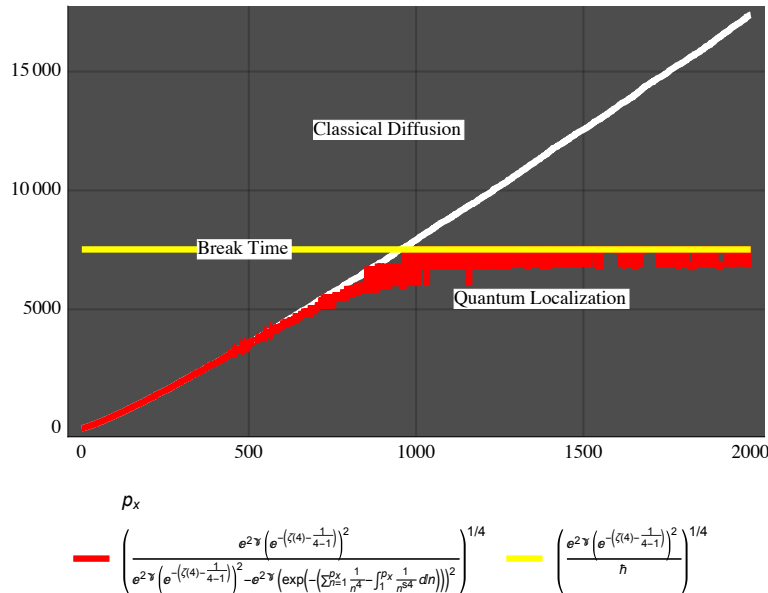


Figure 3: Quantum break time

This phenomenon -the phenomenon of quantum chaos- led Julian Brown to proclaim in the *New Scientist* (1996) that

If we could study a classical system for longer than its quantum break time, we would see that the behavior was not chaotic but quasi-periodic instead.

He was quite wrong: if classical systems are merely highly perturbed quantum systems, and every classical system will eventually reach break-time, then the primes are finite. Michael Berry rightly rejects Brown’s view:

...this explanation (as the classical limit is approached – as objects get bigger and heavier – the time taken for chaos to be suppressed by quantum mechanics gets ever longer, and would be infinite in the strict limit) fails because the ‘chaos suppression time’ is often surprisingly short... The true reason for the prevalence of chaos is that large quantum systems are hard to isolate from their surroundings. Even the ‘patter of photons’ from the Sun (whose re-emission gives the light by which we see Hyperion) destroys the delicate interference underlying the quantum regularity. This effect, of large quantum systems being dramatically sensitive to uncontrolled external influences, is called decoherence. In the classical limit, the quantum suppression of chaos is itself suppressed by decoherence, allowing chaos to re-emerge as a familiar feature of the large scale world.

But from a superficial perspective, this problem of the suppression of decoherence, as a quantum system is scaled up, may be only an *engineering* problem, and of course this is the assumption on which the quantum computing industry is based. But the quantum computing industry is based on the misunderstanding that blights the sciences generally and quantum mechanics in particular - atomism. Consider the ‘P versus NP’ question, which concerns the question of whether the class of decision problems whose solutions are quickly verifiable (NP) by a computer is the same as the class of problems that are *quickly solvable* by computer (P). Historically the problem arose because certain problems seem to be hard to solve. More particularly, they seem to require a lot of *time* -an exponentially growing amount of time- to solve. An example of a NP problem that seeming takes exponential time is Factoring. While it doesn't take long to factor 15 or 21, imagine trying to factor the 200 digit integer

27 997 833 911 221 327 870 829 467 638 722 601 621 070 446 786 955 428 537 560 009 929 326 128 400 107 609 345 671 052 -
 955 360 856 061 822 351 910 951 365 788 637 105 954 482 006 576 775 098 580 557 613 579 098 734 950 144 178 863 178 -
 946 295 187 237 869 221 823 983

You can easily check that it divides evenly into the primes

3 532 461 934 402 770 121 272 604 978 198 464 368 671 197 400 197 625 023 649 303 468 776 121 253 679 423 200 058 547 -
956 528 088 349

and

7 925 869 954 478 333 033 347 085 841 480 059 687 737 975 857 364 219 960 734 330 341 455 767 872 818 152 135 381 409 -
304 740 185 467

Although it takes a pocket calculator a spit second to do the multiplication, it would take a single 2.2 GHz computer roughly *75 years* to do the division. Factoring is one of numerous (NP) problems that are easy in the one direction, and seem to be hard in the other. Here we have a further -computational- arrow of time. We can argue for the conclusion that this arrow really is asymmetric by considering the Travelling Salesman Problem, which is the problem of whether a salesman can visit a number of cities exactly once and return to a home-city for a certain cost.



Figure 4. The Travelling Salesman Problem

First we transform it into a problem of whether a computer (salesman) can execute some number of instructions (visit some number of cities) which executes every instruction exactly once (visits every city exactly once) before returning to a halt state (home-city) for some maximum cost:

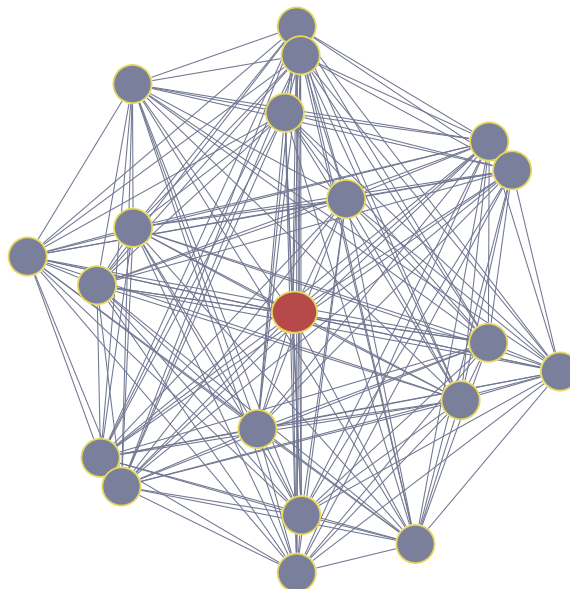


Figure 5. The Travelling Salesman Problem in graphical form

An arbitrary computer is therefore working on the problem of whether an arbitrary computer will halt when run with an arbitrary set of instructions, and thus the point will be reached when the evaluation is a *self-evaluation*, i.e. the point will be reached such that the computer is attempting to determine of itself if it will halt. If we associate to every city an instruction, this self-evaluative point will be reached when the number cities on the tour is not less than the number of instructions in the program. This leads to a contradiction in the case that the number cities is *greater* than the number

of instructions, and by appeal to this contradiction, it follows that TSP involves a limit on the number of cities. This proves that TSP differs from polynomial-time problems, which aren't sensitive to the size of the input, and that P and NP are not equal. More particularly... associate each atomic instruction in some finite set of instructions with some n -SAT formula (such as $(\neg A \vee \neg B \vee C) \wedge (\neg A \vee \neg B \vee D)$), associate each of these formulas to the vertices of a complete graph other than the start/stop vertex. Associate the halt state with this start/stop vertex. Let v be the number of variables per clause, and if the instruction doesn't result in the machine going into an infinite loop, weight the vertex as $\frac{1}{v} + \frac{v-1}{v}$. If the instruction *does* result in the machine going into an infinite loop, weight the offending vertex as $0 + 1$. Weight the halt vertex as 1. $\frac{n-1}{v}$ gives the minimum truth-density, $\frac{(n-1)(v-1)}{v}$ gives the maximum falsity-density of a satisfiable n -SAT instance, $\frac{n-1}{v} + \frac{(n-1)(v-1)}{v} + 1 = n$ gives the maximum imbalance between the truth and falsity-density corresponding to a Travelling Salesman's circuit that is within budget. Let n be the number of instructions/vertices, and we can conclude that

- If and only if it is possible to visit every vertex exactly once before returning to a halt vertex for a cost n without upsetting the balance of minimum truth-density/maximum falsity density $\frac{n-1}{v} + \frac{(n-1)(v-1)}{v} + 1 = n$, there is some Turing machine that will not infinite loop when run with some input.

We can associate the prime numbers to TSP circuits by reference to this equation:

$$\frac{p_n - 1}{v} + \frac{(v - 1)(p_n - 1)}{v} + 1 = p_n$$

Next associate the creation operators b_n^\dagger and f_n^\dagger to prime numbers p_n ... Now we have identified the unique 'factorization' of a state into creation operators acting on the 'vacuum' with the unique factorization of an integer into prime numbers (and we have a hierarchy of states: $|1\rangle$ is the 'vacuum'; $|2\rangle$ and $|3\rangle$ and $|5\rangle$ are one-particle states; $|6\rangle$ is a two-particle state... and so on). By reference to the Witten index -the number of bosonic minus the number of fermionic zero-energy states- we see that the Mobius inversion function

$$\mu n = \{1 = n \text{ has an even number of distinct factors,} \\ -1 = n \text{ has an odd number of distinct factors, } 0 = n \text{ has a repeated factor}\}$$

is equivalent to the operator $(-1)^F$ that distinguishes bosonic from fermionic states, with $\mu(n) = 0$ when n has a repeated factor being equivalent to the Pauli exclusion principle. Given that all of the differences between bosons and fermions arise from the difference between the computation of the Permanent

$$A \text{ Per} = \sum_{\sigma \in P_n} \prod_{i=1}^n a_{i,\sigma(i)}$$

and the related but fundamentally different Determinant

$$A \text{ Det} = \sum_{\sigma \in P_n} (-1)^{\text{sgn}(\sigma)} \prod_{i=1}^n a_{i,\sigma(i)}$$

of a square matrix, it follows in the end that a fast algorithm for Factoring would collapse the polynomial hierarchy. In the light of Shor's algorithm then, a *scalable quantum computer* would collapse this hierarchy.

Aaronson:

Suppose you believe that nothing done by "realistic" quantum systems (the ones found in Nature) can possibly be used to outperform today's classical computers. Then by using today's classical computers, why can't we easily simulate the quantum systems found in Nature? What is the fast classical algorithm for simulating those quantum systems? How does it work? Like a wily defense attorney, the skeptics don't even try to address such questions; their only interest is in casting doubt on the prosecution's case.

I'm a skeptic -I'm a *denier*- but I'm *not* saying that "nothing done by "realistic" quantum systems (the ones found in nature) can possibly be used to outperform today's classical computers." On the contrary, I see the self-conscious human mind as the paradigmatically natural quantum system, able to solve hard computational problems where a classical computer would by the considerations above, not merely fail to solve the problem in polynomial time, but fail to solve it *any* amount of time. I *am* saying that we can't easily simulate the quantum systems found in nature on classical computers.

My answer to the "why" question is that, while classical systems and scalable physical objects are projections as defined above, quantum systems are *projectors*, and capable of only limited scalability: as the projection diffuses more light and the gaps between the primes and atomic matrices of the form

$$\begin{pmatrix} 0 & -U & -U & -U & -U & \dots \\ U & 0 & -U & -U & -U & \dots \\ U & U & 0 & -U & -U & \dots \\ U & U & U & 0 & -U & \dots \\ U & U & U & U & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

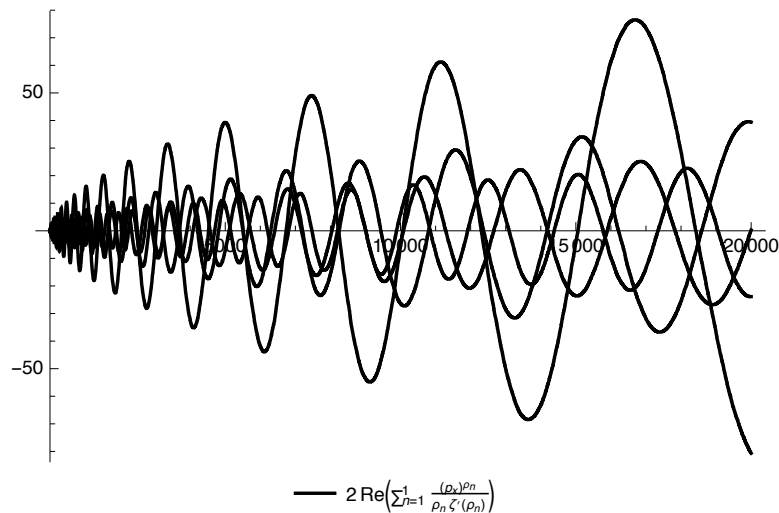
grow larger, it is inevitable that the projector concentrates *less* light and that the gaps between the values of \hbar and atomic matrices of the form

$$\begin{pmatrix} 0 & -u & -u & -u & \dots & -u \\ u & 0 & -u & -u & \dots & -u \\ u & u & 0 & -u & \dots & -u \\ u & u & u & 0 & \dots & -u \\ \vdots & \vdots & \vdots & \vdots & \ddots & -u \\ u & u & u & u & u & \hbar \end{pmatrix}$$

grow smaller. Otherwise put, natural quantum systems are *not* scaled down versions of classical computational systems -to suppose that they are is a category mistake- and in the same way that the physical universe can't *pace* the physics community- be scaled down to quantum size, quantum computers can't be scaled up to classical size. Richard Dawkins talks of the "God-Delusion" based on his assumption that the classical universe is a scaled up form of an extremely simple -non-classical- universe, but in reality the delusion here is that it is possible to get from the singularity of light at root of everything there is to the extremely complex initial condition of our universe (a condition associated to the smallest possible atomic classical matrix, the largest possible atomic quantum matrix, to the maximum amount light concentrated in the projection, and to minimum amount of light diffused by the projector). It is absolutely not possible to get there in the step-wise manner required by any evolutionary account of origins. To bridge this great gap a *stupendous* act of creation is required. Similarly, a stupendous act of creation is required to turn back the various arrows of time, all of which are pointing irreversibly toward black holes and to eternal darkness.

Empiricism, Evolution, and Scalable Quantum Computation

Like many scientists and philosophers of his era, Aaronson is very concerned with 'empirical evidence', and he disbelieves in a super-intelligent alien creator because there is -he says- no empirical evidence such a thing exists. But he forgets that before it is possible to have any sensory experience whatsoever, and divide the world into units and measure it and so on, there must be a *very particular* relationship between the world (that is measured) and the mind (that measures it). This relationship is deeper than the senses, and deeper than the integers, but it is very real. Whilst this proposal might sound vague expressed in terms of 'world' and 'mind', this vagueness can be considerably lessened by talking in terms of the relationship between arithmetic progressions, things which we all agree must be common both to the world and the mind in order for measurement to be possible. Further particularity can be added by declaring in computer-speak that either an input-progression + program-progression involves an error or dis-uniformity that grows no faster than $e^{2\gamma} \sqrt{\frac{p_n}{e^{2\gamma}}}$ or the progressions are not symmetric. P versus NP, this is to say, is the computational form of the Riemann Hypothesis:



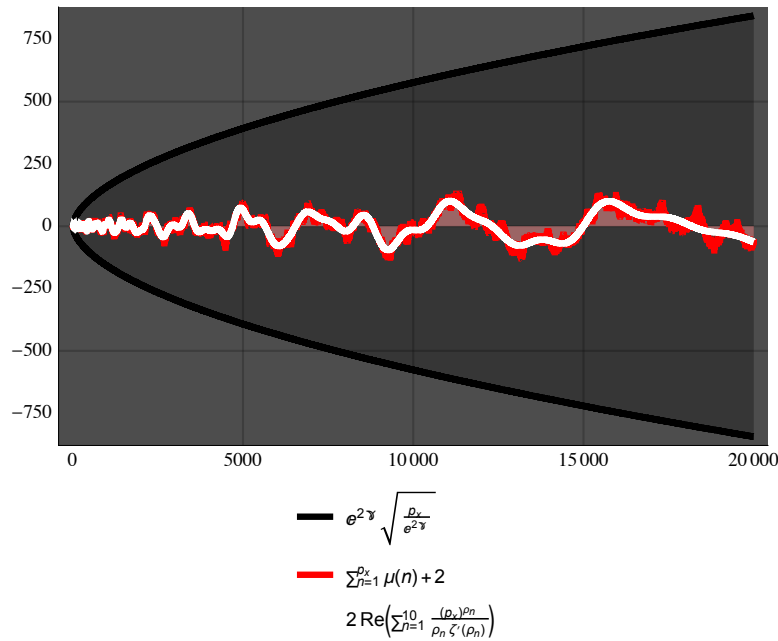


Figure 6: Depicting the Riemann Hypothesis for the physical world

The run times of programs running inputs that don't stand in the appropriate relationship to their programs are certain to be exponential. In a story co-authored with Adolfo Caesars called *Del Rigor en la Ciencia*, or *On Exactitude in Science*, Jorge Luis Borges tells of a map of an empire that is identical with that empire:

... In that Empire, the Art of Cartography attained such Perfection that the map of a single Province occupied the entirety of a City, and the map of the Empire, the entirety of a Province. In time, those Unconscionable Maps no longer satisfied, and the Cartographers Guilds struck a Map of the Empire whose size was that of the Empire, and which coincided point for point with it. The following Generations, who were not so fond of the Study of Cartography as their Forebears had been, saw that that vast map was Useless, and not without some Pitilessness was it, that they delivered it up to the Inclemencies of Sun and Winters. In the Deserts of the West, still today, there are Tattered Ruins of that Map, inhabited by Animals and Beggars; in all the Land there is no other Relic of the Disciplines of Geography. purportedly from Suárez Miranda, *Travels of Prudent Men*, Book Four, Ch. XLV, Lérida, 1658

A map is a way of finding a location in an unknown territory without performing an exhaustive search of that territory, and if we have no map, or if -equivalently- the smallest map we have of a territory is the same size as that territory itself, then as the size of the territory grows arithmetically, the number of places we have to search in order to find our location grows exponentially (a complete graph of n vertices has for example $\frac{1}{2} (n - 1)!$ Hamiltonian cycles). Non-metaphorically, when the smallest program we have to operate on an input is as complex as that input itself, then as the complexity of the input grows arithmetically, it is inevitable that the number of operations grows exponentially. More generally, a scientific theory can be regarded as a computer program for predicting observations, and if the smallest program we have is as complex as the data-set itself, then as the complexity of the data-set grows arithmetically, the number of operations needed to analyze the data and make a prediction grows exponentially. In a fantasy-world where computation is free, it is possible that $P = NP$; but in the *real* world, where there are exponentially steep time-costs to be paid by computational devices running self-inputs, $P \neq NP$.

There is an ideal distance between a representational painting and a viewer. If the viewer stands *too close* or too far from the painting, they will be unable to make out what it is a painting of. If the viewer stands too close to the painting, then all they will see what only appear to be haphazard brush strokes, yet a coherent image emerges from the combination of these brush strokes surveyed from the appropriate distance. Unmeasured particles are like haphazard brush strokes. A scalable quantum object is like a painting that can be seen to convey a coherent image from a vantage point that is too close to permit the conveyance of a coherent image. No amount of technical ingenuity can get around what is a logical problem. Evolutionary cosmology and scalable quantum computing are two sides of the same coin, and Aaronson's failure to see the truth of a super-intelligent alien creator is born of the same thing as his failure to see the falsity of scalable QC: he fails to see that beneath the world of the senses -and beneath the everyday world of mathematics and physics in which so many live so comfortably and unthinkingly- there lies a world that is *not* empirically accessible but without which nothing would work as it does. And not until one acquaints oneself by thought alone with

the strictures of this invisible world is it possible to have anything more than a shallow understanding of the visible one.

REFERENCES

- Aaronson, Scott, *Quantum Computing since Democritus*, Cambridge University Press, 2013.
- Aaronson, Scott, “The Limits of Quantum Computing”, *Scientific American* 298 (3): 62, 2008.
<http://www.scottaaronson.com/blog/>
<http://blogs.scientificamerican.com/cross-check/scott-aaronson-answers-every-ridiculously-big-question-i-throw-at-him/>
- Berry, M (2003), *Quantum chaology*
- Borges, J (1975), *A Universal History of Infamy*
- Brown, J (1996), *When Two Worlds Meet*
- Casiti, G, et al (1979), *Stochastic Behaviour in classical and Quantum Hamiltonian Systems*
- Church, A (1936), *An unsolvable problem of elementary number theory*
- Cook, S (1971), *The complexity of theorem proving procedures*
- Collins, K (2014), *Why quantum computing will be civilisation’s next big revolution*
- Dawkins, R (1986) *The Blind Watchmaker*
- Dawkins, R (2006). *The God Delusion*
- Derbyshire, J. (2004), *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*
- Einstein, A (1916), *Relativity: The Special and General Theory*
- Einstein, A (1926), *Letter to Max Born*
- Euler, L (1737), *Variae observationes circa series infinitas (Various observations concerning infinite series)*
- Gutzwiller, M (1990), *Chaos in Classical and Quantum Mechanics*
- Hawking, S (2003) ed. *On the Shoulders of Giants: The Great Works of Physics and Astronomy (works by Copernicus, Kepler, Galileo, Newton, and Einstein)*
- Juskalian, R (2017), *Practical Quantum Computers: Advances at Google, Intel, and several research groups indicate that computers with previously unimaginable power are finally within reach*
- Martin-Lopez, E, et al (2012), *Experimental realization of Shor’s quantum factoring algorithm using qubit recycling*
- Newton, Isaac (1687), *The Principia: Mathematical Principles of Natural Philosophy*
- Riemann, G (1859), *Über die Anzahl red Primzahlen unter einer gegebenen Grösse (On the Number of Primes Less Than a Given Magnitude)*
- Shor, P (1995), *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*
- Spector, D (1990), *Supersymmetry and the Möbius inversion function*
- Taylor, C (1999), *The atomists, Leucippus and Democritus: fragments, a text and translation with a commentary by C.C.W. Taylor*
- Turing, A (1936-37), *On Computable Numbers, with an Application to the Entscheidungsproblem*
- Turing, A (1939), *Systems of Logic Based on Ordinals*
- Witten, E (1982), *Constraints on supersymmetry breaking*
- Xu, N, et al (2012), *Quantum Factorization of 143 on a Dipolar-Coupling Nuclear Magnetic Resonance System*