Ricky's Afterthought:

Quantum Entanglement and Cryptography

A.C. (Ricky) Metaxas

Life Fellow St John's College Cambridge UK
Email: acm33@cam.ac.uk

Were you aware that of all Einstein's papers the one most read (ever apparently) is the so called EPR paper published in 1935 by Einstein, Podolsky and Rosen in the American Physical Review when they were colleagues at the Institute of Advanced Study near Princeton? Einstein, then director at the Institute, regarded Podolsky and one of the most brilliant young theoretical physicists of his generation who had published papers with Paul Dirac, famous for his elegant equation that predicted the existence of antimatter [$(i\partial\!\!\!/-m)\psi=0$ where $\partial\!\!\!/$ is Feynman's slash notation, ψ is a wave function, m its rest mass and (x,t) the space-time coordinates]. Dirac, by the way, was Lucasian Professor of Mathematics at Cambridge University and a Fellow at St John's College in the 1930's. This incidental fact does make me wonder whether he ever occupied one of the five rooms I have resided in, a notion that instigates quivers of excitement. However, I will not rush to check in case I find that it is but wishful thinking.

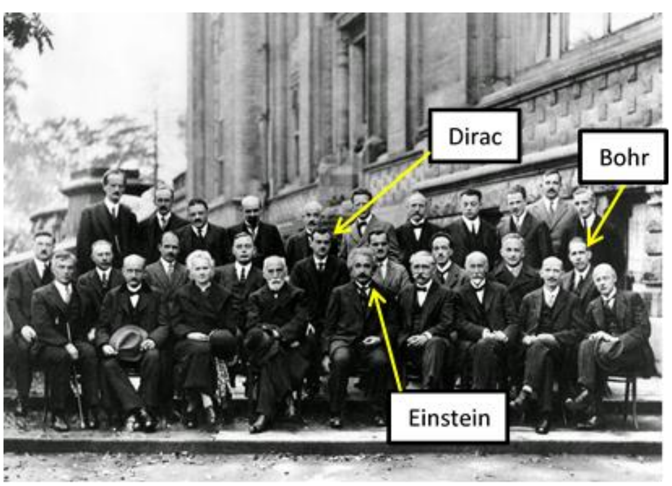

Fig.1: The iconic group photo of the 1927 Solvay meeting

The group photo taken at the 1927 Solvay conference on electrons and photons, where they discussed issues related to quantum mechanics, shows Einstein amongst most of the famous scientists at the time. Einstein mentioned time and time again that quantum mechanics gave excellent agreement with what happens in the subatomic level but more needed to be done to give it physical reality such as one finds with classical physics. Einstein debated this issue with Bohr, who aided by his colleagues, was able to answer all the Einstein's questions so Neils Bohr felt all was well with quantum mechanics.

Where was I? Oh yes, the EPR paper. So when in 1935 the EPR paper was published it essentially shook the whole foundation of quantum mechanics. This is because in that paper Einstein and his colleagues use their arguments to cast doubt on Niels Bohr's interpretation of entangled (or linked) functions. To put the problem in its more simplistic form, say we have two photons, which originate from the same source and find themselves one in Cambridge and one in Valencia (well you could take two photons in different galaxies in the cosmos but let us be more realistic) then measurement of one entangled particle will instantaneously determine what is measured at the other entangled particle, regardless of how far apart they are, that is, they are linked or to use a more scientific term the quanta, or more generally wave functions, are entangled. Einstein referred to this notion as "spooky action at a distance" when he came across quantum entanglement. The EPR paper implied that if the two entangled photons were able to communicate instantly then this had to be done faster than the speed of light which goes against Einstein's special theory of relativity. So the argument rested for a while and in the following couple of decades we see the development of the laser, disc drives, the transistor and the digital revolution commences, all relying heavily on the principles of quantum mechanics which Einstein insisted was incomplete. Of course Bohr and Einstein despite their disagreement had high respect for each other.

In the early 1960's the Irish physicist John Bell claimed that the EPR paradox had not been addressed. He continued to reflect on the Einstein/Bohr debates and in 1964 published a remarkable paper in which he proposed a "thought experiment" to resolve the issue of causality and locality that lies at the heart of quantum mechanics versus classical physics as regards the interpretation of quantum entanglement. He is well known for his so called Bell's theorem which basically seeks to find out whether particles (the photons I described above) talk to each other faster than the speed of light. If they do not then that disproves quantum mechanics. He found that they do, so at the time he could only say that quantum mechanics was not wrong. But it violates Einstein's special relativity in that it introduces a violation of locality. Another explanation that Bell put forward was that when the photons were born they had in them an "embedded DNA" with some hidden variables that would govern precisely what happens to each throughout the entirety of their existence. Since Einstein and his colleagues believed explicitly in classical physics, they would have aspired to this second explanation. But Bell's inequality proved that the notion of the embedded DNA was not true hence the only explanation was that particles do communicate faster than the speed of light. In his paper Bell put forward an expression that could be tested experimentally and could therefore ascertain whether Einstein or Bohr was correct.

However, the paper remained hidden and unnoticed from the scientific community for a number of years. Then in 1972 John Clauser of the University of California read Bell's paper and found it fascinating while pondering why nobody had thus far tested Bell's inequality. He, and his colleague, Stuart Freedman carried out the first "Bell Test experiment" by firing a laser onto calcium atoms producing entangled particles which they then passed through polarisers and checked how often the answers correlated. Their experiment was what one would describe as a "Heath Robinson device", meaning a device that was simultaneously absurdly ingenious and impracticable and could have loopholes which cast doubt on the validity of the results obtained. So what was needed was a more rigorous approach.

After numerous attempts on the "Bell's Test experiments" by other scientists, a collaborative experiment was conducted in 2015 under the direction of Anton Zeilinger's group of the Quantum Optics at the University of Vienna and performed in a sub-basement at the Vienna Hofburg Palace using a source which created entangled photons. These were distributed, one in each of two optical glass fibres, to measurement stations called Alice and Bob. After many observations quantum entanglement was confirmed. However, physicists still questioned whether all the possible loopholes were covered and in that respect Prof Zeilinger spent the best part of the following a few years devising an amazing experiment which included light emanating from two distant quasars. This time his colleagues teamed up with researchers at MIT and many other institutions and conducted quantum entanglement experiments on the island of La Palma in the Canaries, using two large telescopes the Telescopio Nazionale Galileo and the William Herschel Telescope. Essentially this created a giant "Bell Test experiment" where a source of entangled particles was equidistant (500m) from the two telescopes.

A laser created a pair of perfectly timed photons which travelled through the air reaching the receivers of the two telescopes. At the same time light from two distant quasars and from opposite sides of the cosmos, arrive at the two telescopes and as they had travelled such vast distances it was highly unlikely to influence the randomness of the test. The quasars were used as random number generators and determined which filters the photons were passing through. Variations of the colour in the quasar light were then used to control which kind of measurement was performed on the two photons from an entangled pair created in a mobile laboratory on Las Palmas. Finally, they examined the polarisation of each entangled photon emanating from the light fluctuations from each distant quasar. After conducting many experiments and recording the results quantum entanglement was confirmed.

Now, you may think that all this is academic and has no bearing to any practical use. In fact superposition and entanglement is at the heart of research into quantum computers. Instead of storing data in bits, as in today's computers, quantum bits or qubits are used to do so. The qubits could be in states 1 or zero or both and groups of qubits could be linked to form a quantum computer. By using entangled qubits real problems can be tackled much faster than using digital computers, for example, in cryptography where one-time pad, that is, a set of random numbers-the key-is used in order to encode and decode messages. Putting it simply both parties would have the same cipher thanks to quantum entanglement. Should a hacker attempt to secretly listen to the conversation, the symmetry would be broken and the parties would instantly realise that something was wrong. Chinese scientists have launched the Micius satellite setting up intercontinental quantum communication amongst multiple locations on earth with a maximum separation of 7.6 km. None other than Anton Zeilinger from Vienna is involved in this project with his Chinese colleagues, led by Jian-Wei Pan at the University of Science and Technology of China in Hefei, China.

So, can one categorically state that Einstein was wrong? Remember, he only stated that quantum mechanics was incomplete. I let our readers draw their own conclusions.

For further reading

https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777

https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/

http://news.mit.edu/2018/light-ancient-quasars-helps-confirm-quantum-entanglement-0820