What's the Fuss: The Excitement, Prospects and Software/Hardware Challenges of Distributing Entanglement over a Quantum Network

Neil M. Zimmerman

NIST, 100 Bureau Dr, Gaithersburg, MD 20899, USA;
neilz@mailaps.org; +1 301 975 5887

Abstract: In this paper, I review the notion of a quantum network, which I define as one that can distribute entanglement between stationary qubits, and then discuss challenges relevant for the Optical Fiber Conference (OFC). © 2022 The Author(s)

Outline:

1) A crash course in quantum mechanics, Q 2.0, and Quantum Networks (QN's).
2) Why are people so excited by the prospect of a QN, and ultimately the Quantum Internet?
3) What are some of the most important challenges, especially for the OFC?
   a. Fibers:
      i. Loss and dispersion
      ii. Rayleigh scattering and Q/classical coexistence
   b. Single-photon (SP) switches
   c. SP sources and detectors
   d. Going from table-top experiments to photonic integrated circuits (PICs).
   e. Quantum Repeaters (QR's), to allow extension beyond metropolitan distances (beyond 100 km).

A crash course in quantum mechanics, Q 2.0, and Quantum Networks (QN).

I suspect most of the readers are familiar with pulses of light travelling in air, in space, or in … fibers. Let's consider what magical new things we can do if we cut down the amplitude of the light pulse by about one trillion times, so that we're working with single photons (single quantized packets of light energy).

Many of the readers probably recall the idea of Schrodinger's cat (if you don't, please go to a Modern Physics textbook or the WWW). A modern-day version of this is the statement that a single photon can exist simultaneously with both horizontal and vertical polarization, with both 1530 and 1570 nm wavelengths, …, or even both exist and not exist. One reason this could be exciting is that this notion of superposition suggests an exponential speedup in computation: instead of having one bit (one electron or one photon) be either LOW or HIGH, we can have one quantum bit or "qubit" that is both LOW and HIGH at the same time. This means that (take a simple example of multiplying two numbers ranging from 0 to 15) instead of having to run the calculation $16^2 = 256$ times to fill out the "Times Table", instead we can run the quantum calculation just once! [Unfortunately, the Universe isn't quite that optimum – at the end, we have to read out the answer which will "collapse" the qubits into having just one value each, and we need to do this multiple times for averaging].

The net result of this exponential speedup is that we can imagine solving problems that were considered unsolvable before – see various reports of "quantum advantage", in which teams have reported solving certain problems with a smallish quantum computer (QC) faster than on a classical computer. Some years ago, Shor's algorithm [1] was published; this proposal to use a large QC to factorize very large integers (one basis of modern-day WWW encryption) is what has led to a great deal of the excitement of Q 2.0.

So, what do I mean by "Q 2.0"? About a century ago, smart people invented Quantum Mechanics (QM) to try to predict the weird behavior that experiments were showing (things like the photoelectric effect, stability of the atom, discrete lines in the Sun's spectrum, …). These effects are generally quite slow, or time-independent.

More recently, other smart people realized that, if they threw in fast manipulation of atoms or photons or electrons or

…, they could start to see manifestly QM behavior in the time dynamics of those particles. This means that a human being (size scale 2 m) can reach into an experiment, grab a single atom or photon or electron, and make that particle do manifestly quantum mechanical tricks. For instance, in a "Rabi oscillation", we can put an electron in two places at once, and then hit it with a pulse and watch it coherently oscillate between the two positions [2]. [I must note that using English to describe QM is fraught with peril, and that basically everything in this paper is only somewhat true – if you want to know the accurate underlying mathematical descriptions, please consult the literature].

Now that we've considered superposition (one particle having two values at the same time), we need one more concept: entanglement, where two or more particles share their QM state. For instance, let's consider two of Schrodinger's cats (lions named Dopey and Doc in two different boxes), each of which can be asleep or awake. Then, the most general state of the Pride is (please note that I have used the "ket" notation of |state>; feel free to ignore this if you wish):

|Pride> = |Dopey awake> |Doc awake> + |Dopey awake> |Doc asleep> + |Dopey asleep> |Doc awake> + |Dopey asleep> |Doc asleep>

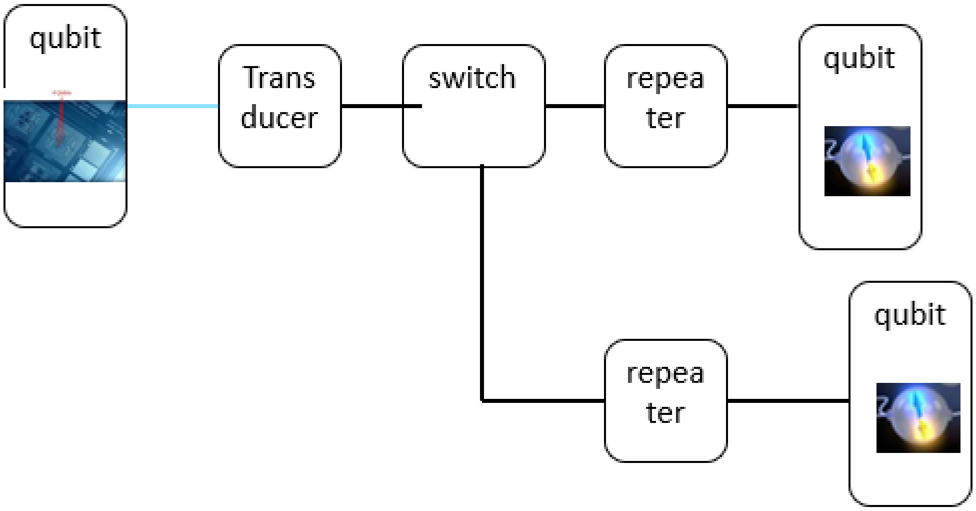
What we see here is that all four possible states are part of |Pride>, so that we'll have to open up both boxes to find out whether the lions are sleeping or not. Instead, if we make this state (using the "fast manipulation" I mentioned above)

|Pride> = |Dopey awake> |Doc awake> + |Dopey asleep> |Doc asleep>,

now we have something very special: If we open the first box and see Dopey is awake, then we know Doc is awake without opening the second box! This goes by the terms "entanglement" or "spooky-action-at-a-distance", and will allow us to imagine doing some very cool things.

One of those cool things is to distribute entanglement as a resource over long distances, so that we can entangle two qubits that are quite far away – *this is the basic idea of a Quantum Network*. We can now define "flying qubits" (the particles that carry the entanglement to remote locations) and "stationary qubits" (the particles that hold the information at nodes and can be used for logic, sensing, timekeeping, …). These definitions means that, in this paper, I won't be discussing QKD (quantum key distribution), which does not require stationary qubits.

Fig. 1: A simple diagram of a 3-node QN. One important notion: Every one of these components must preserve the very fragile quantum information – **much harder than for classical light pulses**. There must also be a great deal of classical communication in parallel, for synchronization, routing, etc.



Why are people so excited by the prospect of a QN, and ultimately the Quantum Internet?

Rather than try to give a comprehensive list, instead I'm going to give a flavor of a few different possible applications. [BTW, now seems like a good time to explain why I'm giving so few references in this paper: Since I'm trying to describe very high-level ideas, I think it's better to let each reader find a favorite source to understand these concepts (lots of great stuff is out there) than to prescribe particular sources].

First of all, what particle [3] are we going to use to distribute entanglement? It's got to be easy to move around, not require special channels, be easy to switch and measure, maintain its quantum coherence (HIGH or LOW or superposition of both) over very long distances, …; while I hope to someday see a neutrino network, for right now it seems clear that photons (light) are the only sensible choice. Also, it looks likely that for most moderate distances, we will use fiber as the channel, with the possibility of satellites for inter-continental distances.

Cloud QC: In part because the QM data in qubits is much more fragile than the data in bits, it is quite likely that it will be a long time before anyone builds the "one-big-QC" with 100 million qubits. Instead, it's likely that a big QC will be made of a bunch of smaller QC's, perhaps all in the same building or city or …; in order to maintain the exponential speedup inherent in QC's, we will need to entangle all of the remote smaller QC's, thus meaning we need a QN.

Blind cloud QC: Perhaps you want to run a program on a cloud QC from your garage terminal – easy if you have the money, just send information to/from the cloud QC over the existing classical Internet. Now, let's say that you want to ensure that no one can find out i) what question you asked or ii) what answer you got; a possible way to do this is to have a quantum terminal in your garage and entangle your terminal with the cloud QC – this requires a QN.

Better time synchronization: I included this one because it's close to my heart since I work at NIST. Nowadays, people can make clocks with a stability (accuracy) better than one part in 10^{18}! However, it's not possible (at least, not now) to synchronize two of these clocks to better than about one part in 10^{15}. There is a proposal [4] that suggests that, if we synchronize a large number of the existing atomic clocks around the World by entangling them, we could reduce that synchronization error down by at least a factor of 100.

What are some of the most important challenges, especially for the OFC?

1) Fibers: Single photons are quite fragile, and very importantly, we can not use amplification to transport them long distances (in a sense, photons are like snowflakes – every one is unique). For this reason, loss and dispersion in fibers are crucial – for even the best present-day fibers, we'll be limited to about 100 km distance without Quantum Repeaters (QR's), which are really tough to achieve.

   We would also like to have classical light pulses and single photons on the same fiber; this means that we need to have really excellent filters and fibers with very low Rayleigh scattering.
2) Single-photon (SP) switches: The switches in the classical Internet will not preserve the flying qubits (converting from optical to electronic and back is like melting and then re-freezing the snowflake). While SP-compatible switches do exist now, making them much faster and less expensive would be very helpful.
3) SP sources and detectors: An ultimate Quantum Internet is going to require millions (billions?) of these around the World. While they exist now, they are too expensive, bulky, …, to be practicable. Also, it would be nice to avoid a need for cryogenics, and to have detectors with the ability to count many photons.
4) Going from table-top experiments to PICs: It seems very likely that beating the SWAP (Size, Weight, Power, Cost) limits will require lots of the components being on a chip. This is a burgeoning research field, and we will need lots more R and even more D.
5) Quantum Repeaters (QR's), to allow extension beyond metropolitan distances (beyond 100 km). QR's are perhaps the (potentially) hardest part of a QN beyond metropolitan (100 km) scale, because they require us to receive, hold for a specified time and then transmit the fragile quantum information. There's a great deal of room in this "space" for great new ideas and new apparatus.

References:

[1] Shor, P.W. (1994). "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press: 124–134. doi:10.1109/sfcs.1994.365700. ISBN 0818665807. S2CID 15291489.
[2] Y. Nakamura, Yu. A. Pashkin and J.- S. Tsai, "Coherent control of macroscopic quantum states in a single-Cooper-pair box", Nature 398, 786-788 (1999), doi:10.1038/19718, arXiv:9904003
[3] I should note that one can also run a QN with "continuous variable" encoding; this allows one to use coherent light (lasers) instead of the "discrete variable" (DV) encoding of single photons. A nice tutorial is located at http://infiniquant.com/tutorial-continuous-variable-quantum-communication/. CV and DV encoding both have advantages and disadvantages, with the ultimate winner unknown.
[4] P. Komar, E. M. Kessler, L. Bishof, M.; Jiang,A. S. Sorensen, J. Ye, and M. D. Lukin, Nature Physics 10, 582 (2014).