**University of Rochester – Ian Walmsley**

**Summary:** Our work in CQI has centered on two themes: how to manage the entanglement of photons, and how to properly account for the resources needed to construct a quantum information processor. We have had some significant achievements in both of these areas, and expect to continue them for the remainder of the program.

**Managing Photonic Entanglement:** Our first goal in this project has been the development of novel high-brightness sources of down-converted radiation that will provide thorough control over the spatio-temporal wave functions of the produced photons. We have accomplished this goal by combining the technology of nonlinear waveguides with quasi-phase-matching to allow engineering of the two-photon wave function in the spatio-spectral domain.

The use of waveguides has two important advantages. First, the nonlinear interaction can be more efficient, so that lower pump powers can be used. Second, the spatial mode confinement means that the generated photons can be easily matched to the detectors. Spontaneous parametric down-conversion in nonlinear waveguides has been recently reported by several groups, including ours. We believe that this technology has several very promising features, especially in experiments involving multiple sources.

Specific achievements aside from this include several theoretical papers outlining how to engineer the spectral entanglement of photons, and how to characterize it, as well as how to disentangle photons, a technique that is necessary to multi-photon interference and Bell-state detection. Since the latter is the cornerstone of teleportation protocols, such engineering of the bi-photon state is important for reliable quantum communications.

In the continuation of our project, we plan to gain a much more precise control over the generated states by performing conditional detection on one of the photons in the pairs. Such a procedure removes completely the uncertainty about the number of photons, as firing of the trigger detectors implies unambiguously that the conjugate photons have been generated. Using this method, we can generate two or more photons simultaneously, and then perform collective operations that will generate entanglement. One problem related to this scheme is that the probability of generating $N$ photon pairs simultaneously decreases in a geometrical order with the number of pairs. So far, only experiments with the simultaneous generation of two photon pairs have been realized. Our goal is to push this limit to the simultaneous generation of three photon pairs with sufficiently high count rates. This should enable us to prepare deterministic three-photon entangled states in a conditional manner. Of course, it would be rather difficult to view this direction as a straightforward route towards scalable generation of multiparticle entanglement. However, it is well recognized that three-particle entanglement exhibits a variety of novel features that are not present in bipartite quantum systems, and therefore it constitutes an important research goal by itself. Furthermore, the experimental techniques we plan to study in this project can be used as a test bed for entangling operations using linear optics and conditional detection, which in longer term have the potential of developing into fully scalable all-optical quantum computing.

**Resources and Scaling Issues for Quantum Information Processing:** The viability of any quantum information processor is predicated on whether it scales efficiently. That is, whether it requires fewer resources to perform a specific task than a classical computer. The notion of exactly what constitutes a resource in critical in answering the question. We have developed a procedure for quantifying resources that is based on the physical properties of the system. As quantum information processing has shown, information is physical, and physical theories therefore provide a means to answer questions of this sort.

One of the consequences of the model is that we have shown that all information processing that makes use only of quantum interference (i.e. within a single particle system) is no more efficient than a classical wave-based processor. We also performed an experiment that demonstrated this explicitly for the case of searching a database using a modified Grover algorithm. This was the all-optical analog of the quantum storage and retrieval idea of Ahn et al. An important conclusion to be drawn from this demonstration is that there appear to be things that can be done within the realm of classical physics that provide different information processing capabilities than is possible with conventional classical particle-based computers.

The next stage of the project is to determine whether it is possible to use this classical apparatus to implement some of the “quantum” algorithms that do not require entanglement. Such protocols build on the prototype proposed by Deutsch and Josza, though are geared toward more sophisticated problems that are standards for computer science. These have been analyzed by Meyer, based on ideas of Bernstein and Vazirani. If we are successful, then we shall have demonstrated a way to improve information processing without using quantum mechanics. The technological implications of this would be great. It would be possible to use much of the optical telecommunications technology to build computers that outperform standard models for computation, and to avoid the need for manipulating sensitive quantum systems at the level of individual particles.

Another path that we plan to follow is to use this starting point to better understand the role that entanglement plays in providing quantum enhancement. It is clear from our present studies that binary coding allows classical wave-based processing to achieve the same readout efficiency as an entangled-particle computer. But it is almost certainly the case that the unitary operations of the processor cannot be efficiently implemented by classical interference. But to what extent is it possible to use classically correlated subsystems with interference to achieve some of the power of quantum computers? If we can answer this, then we will have shown exactly the realm in which a full-blown quantum computer is necessary, and thereby delineated the bounds for improvements in computational power within classical physics.