1.2 Models of Quantum Computing

1.2.1 Circuit Model

The circuit model treats quantum computing as a sequence of operations, or gates, applied to qubits - which can be visualised as qubits travelling through a quantum circuit. It was the language in which most of the early work on quantum computing was presented and is still, in many ways, the most natural way to think about and describe most quantum algorithms.

Just as in classical computing, it is sufficient to be able to implement all two-qubit gates in order to be able to build any quantum circuit - we say that two-qubit gates are universal for quantum computing [50]. In 2000 DiVinenzo produced five requirements [51] that any candidate quantum computing system must meet. These can be thought of as defining other features of the circuit: in addition to a universal set of gates, we must be able to initialise our system into some given state, and perform individual qubit measurements. It must also be possible to scale our circuits up, and qubit decoherence lifetimes must be longer than the time it takes for the qubit to travel through the circuit.

1.2.2 Adiabatic Quantum Computing

Adiabatic quantum computing involves manipulating qubits into some state that encodes the solution to the problem you wish to solve. Typically it involves using a time dependent Hamiltonian that interpolates between an initial Hamiltonian, whose ground state is easy to prepare, and a final Hamiltonian, whose ground state represents the solution.

The first adiabatic quantum computing algorithm was given by Farhi *et al.* in 2000 [52] to solve instances of the satisfiability problem. The algorithm's speed is

limited by the requirement that the Hamiltonian must change slowly enough that the system remains in its ground state throughout, a process known as adiabatic evolution. The timescale necessary to maintain adiabatic evolution depends on the gap between the ground state and the next highest state - the smaller the gap, the slower the motion must be. In 2007 it was shown that the adiabatic computing model is equivalent in power and resources to the circuit model [53]. A universal set of Hamiltonians requiring only local terms was found in 2008 [54].

1.2.3 Measurement Based Quantum Computing

Measurement based quantum computation (MBQC) [55], or one-way quantum computation, is a computing paradigm proposed by Raussendorf and Briegel in 2001 [56]. The computation is performed by making irreversible measurements on a highly entangled quantum state - an approach with no classical analogues that offers new perspective on the role of entanglement. The approach hinges on the fact that the quantum teleportation-type protocols can be used to construct a universal set of operations for quantum computing [57]. By measuring a specially entangled state in a particular basis and possibly performing a single qubit rotation depending on the outcome we can implement arbitrary operations. In real algorithms it is not necessary to physically perform the rotations - we can instead adapt the measurement basis for future operations. The fact that information from each measurement outcome needs to be fed back into the process introduces a time ordering on the process.

The beauty of this approach is that it separates the computation into two separate stages: the creation of a suitable entangled state and then the implementation of the algorithm by making local measurements on this state. This is both practically and conceptually useful. Practically it separates the creation of entanglement, and

thus the need for multiple qubit interaction, from the running of the algorithm and allows computations to be implemented using spatially separated entangled qubits by removing the requirement to implement two qubit gates. Conceptually it allows us to view entanglement as a resource to be consumed throughout the computation, to ask questions about how to quantify entanglement and to relate this to the computations we can perform.

The procedure relies on a special class of initial entangled state. Building on the initial proposal, Raussendorf, Browne and Briegel detailed how the computation could be performed using a class of states known as *cluster states* [58]. The fundamental issue of which states could serve as universal resources for quantum computing was tackled by Van den Nest *et al.* in 2007 [59]. We will look at how such states can be created in Section 1.3.1.

1.2.4 Topological Quantum Computing

Topological quantum computing began as a new class of quantum codes, but the area has since developed to the stage where it can now be considered a quantum computing paradigm in its own right. The first codes were introduced by Kitaev [60, 61] arising from an attempt to give simple models of topological order using quantum mechanics. The codes used a large array of physical qubits to encode a pair of logical qubits making use of different toric homology classes. Further examples in the class of topological codes soon followed [62, 63].

Focus then turned to how to implement logical operations on encoded qubits. In 2003 Wang, Harrington and Preskill made a suggestion for performing a CNOT gate by extending the code into a third dimension [64], which was followed in 2007 with an approach from Raussendorf and Harrington which used braiding operations on the code lattices [65, 66]. Both approaches showed error tolerances an order

of magnitude higher than standard concatenated codes when only local operations were allowed. Recently the efficient decoding of topological codes has been an active area of research [67, 68, 69, 70].

1.3 Entanglement and Distributed Architectures

The phenomenon of quantum entanglement has played a central role in the development of quantum theory. One of Einstein's objections to the theory of quantum mechanics was the apparent paradox that quantum entanglement effects appeared to require 'spooky', long-range interactions [71]. Bell's work in 1964 [19] clarified much of the early confusion and showed that entanglement led to essentially quantum correlations that could not be reproduced in classical mechanics. Ekert's communication protocol [18] and the MBQC paradigm [56] show that entanglement can be viewed as a necessary (and essentially sufficient) resource for both quantum communication and quantum computing. Entanglement purification schemes [72] serve to strengthen this view showing that small amounts of entanglement can be combined into a more concentrated, useable form.

The characterisation of entanglement as an essential quantum resource has opened up possibilities in the form of distributed quantum systems. By invisaging an entangled network of spacially separated computational nodes, we overcome many of the common barriers to scalability [73]. The problem of scaling the computation is reduced in part to that of entangling remote quantum systems.

1.3.1 Remote Entanglement Generation

Remote entanglement generation involves entangling two spacially separated quantum systems. The standard technique is that of *path erasure* - which, in informal terms, involves detecting a photon from the two systems and 'forgetting' which

system it came from, to leave them in an entangled state. Formally, the photon detection performs a projective measurement onto an entangled subspace.

The first path erasure method was proposed by Cabrillo *et al.* [74] in 1999 and involved the detection of a single photon. Photon loss is a problem for this system: if two photons are emitted but only one detected the system is left in a mixed state. More sophisticated path erasure schemes [75, 76, 77, 78] overcome this weakness by requiring that a photon be emitted and detected from both systems. The probability of successful entanglement in any run decreases but in return we can be sure that when both photons are detected the systems are genuinely in an entangled state.

Entanglement creation using such schemes was first demonstrated by Moehring *et al.* in 2007 [79]. There has been much recent success using such schemes with entanglement generated between systems up to 100km apart [27, 28]. There have also been theoretical proposals about how to go about using this type of operation to build the entangled network states as required by MBQC proposals [80].

1.4 Candidate Quantum Systems

Many systems exhibit quantum mechanical behaviour of a kind that has the potential to be used for QIP. There are a plethora of different approaches currently under investigation. Here we briefly survey the most well known approaches, noting interesting recent advances.

1.4.1 Nuclear Magnetic Resonance

The first physical realisation of simple quantum computational procedures were performed using nuclear magnetic resonance (NMR) techniques. Thanks to the high existing level of expertise available in the area, initial progress in the late 1990s was quick, following the seminal proposal by Gershenfield and Chuang [81]. By 1998