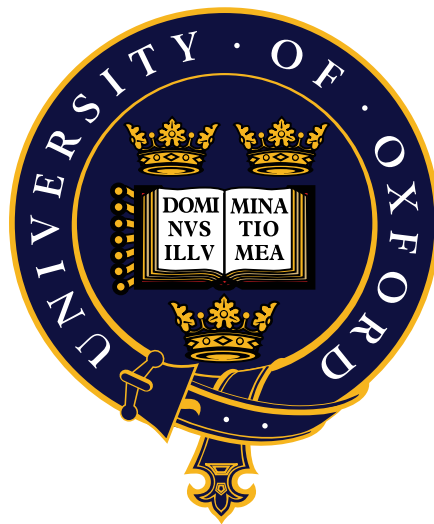


Robust Quantum Phenomena
for
Quantum Information Processing



Tom Close
Oriel College

Thesis submitted for the degree of
Doctor of Philosophy
at the
University of Oxford
Hilary Term 2013

Robust Quantum Phenomena for Quantum Information Processing

Tom Close
Oriol College, University of Oxford
Hilary Term 2013

Abstract of thesis submitted for the degree of Doctor of Philosophy

This thesis is concerned with investigating and proposing robust components for quantum information processing systems. We examine three different areas covering techniques for spin measurement, photon preparation and error correction.

The first research chapter presents a robust spin-measurement procedure, using an amplification approach: the state of the spin is propagated over a two-dimensional array to a point where it can be measured using standard macroscopic state measurement techniques. The work is an example of how simple propagation rules can lead to predictable macroscopic behaviour and the techniques should be applicable in other state propagation schemes.


In the next chapter, we evaluate a quantum dot single photon source system, suggesting strategies to overcome decoherence from phonon interactions. We introduce a master equation technique for quantum jump situations that should have wide application in other situations.

The final chapter focusses on toric error correcting codes. We investigate the power of small scale toric codes and determine the minimum size of code necessary for a first experimental demonstration of toric coding power.

Chapter 1

Introduction

The theory of quantum mechanics is arguably the biggest scientific breakthrough of the 20th Century. The seemingly simple postulates that model behaviour of atomic-scale systems give rise to deep-reaching and counter-intuitive consequences. The philosophical implications of quantum mechanics in terms of the apparent lack of determinism in the universe we inhabit, the various interpretations of the quantum superposition and wavefunction collapse, and the apparent paradoxes afforded by phenomenon of quantum entanglement have, and continue, to occupy physicists and philosophers alike.

It is somewhat remarkable that a theory provoking such controversy has been such a success experimentally and technologically. When the philosophical implications are put aside and the laws accepted, we are left with an incredibly powerful tool for modelling and reasoning about the behaviour of atomic-scale systems. Many of the key technological advances responsible for shaping our world originated in insights afforded by quantum mechanics: the transistor depends on the quantum mechanical treatment of solid state physics that explains the PN junction; the laser depends both on solid state physics and the quantum mechanical description of light. Without quantum mechanics the world we see around us would be cognisable.

Quantum Information Processing has the potential to introduce a new wave of technological advances. The theory of the field is well developed and provides powerful new applications of quantum mechanics. The problem is now one of engineering, in particular how to build robust devices that operate on the nanoscale, with an ability to protect information stored in the quantum wavefunction. In this thesis we examine robust techniques for spin measurement, photon preparation and error correction.

We start with a general introduction to Quantum Information Processing in Chapter 2, surveying different areas of research and detailing important recent developments. The next two chapters introduce the theoretical framework and techniques used later in the thesis. Chapter ?? covers relevant parts of the theory of Open Quantum Systems and Chapter ?? contains topics we will use when modelling interactions between matter and light.

In Chapter ?? we present a robust spin-measurement procedure, using an amplification approach: the state of the spin is propagated over a two-dimensional array to a point where it can be measured using standard macroscopic state measurement techniques. The work is an example of how simple propagation rules can lead to predictable macroscopic behaviour and the techniques should be applicable in other state propagation schemes.

Chapter ?? is concerned with the creation of a reliable single photon source in the face of phonon decoherence. We introduce a master equation technique for quantum jump situations that should have wide application in other situations.

Finally, in Chapter ?? we look at toric error correcting codes. The chapter is self contained, starting with an overview and review of the basic toric code and current decoding approaches. We then go on to investigate the power of small scale toric codes and determine the minimum size of code necessary for a first experimental demonstration of toric coding power.

As the research chapters address a rather broad range of different questions in different physical systems, they will each have their own conclusion section in which we summarise key results of the study and discuss interesting remaining questions and avenues for further work.

Chapter 2

Introduction to Quantum Information Processing

2.1 Quantum Information Processing

Quantum Information Processing (QIP) is the study of how quantum mechanical systems can be used to perform information processing tasks. In this section we will look at three key fields of QIP: Quantum Computing, Quantum Communication, and Quantum Simulation.

2.1.1 Quantum Computing

The original suggestion that quantum mechanics could be used to improve computing capabilities can be traced back to Feynman [1] in 1981. Feynman made the observation that the exponentially growing number of paths in quantum processes, which make their simulation hard classically, could potentially be exploited for increased computational power. In 1985 Deutsch built upon this work to define the concept, and postulate the existence, of a *universal quantum computer* [2] - a quantum generalisation of the universal Turing machine.

The first quantum algorithm was proposed by Deutsch and Josza [3] in 1992 and was soon followed by several others, including Grover's search algorithm [4, 5]. These early algorithms demonstrated that, in some cases, quantum computers could be used to obtain increased computational power. The most significant contribution to the field of quantum algorithms was made by Shor in 1997 [6]. Shor showed how a quantum computer could be used to factorise a number in polynomial time - a feat thought to be impossible with classical resources. The result attracted widespread attention, not least due to the implications efficient factorisation would have for the RSA algorithm [7], which is widely used to secure communication.

Despite the early interest generated by quantum algorithms, prominent critics, such as Landauer, questioned whether quantum computation could ever be made robust enough to run algorithms at scale [8]. It is important when running a quantum algorithm that the quantum superposition is preserved throughout the calculation [9]. Interactions with external systems can lead to a deterioration in the superposition - a phenomenon known as *decoherence*. The concern was that these effects would make it impossible to practically realise quantum computing power.

An important step towards answering these concerns was made by Shor in 1995, who proposed encoding a single logical qubit using nine physical qubits to allow correction of common errors [10]. Further suggestions for error correcting codes followed from Steane and Laflamme [11, 12, 13] using seven and five qubits respectively. In 1997 Aharonov and Ben-Or proved the *quantum threshold theorem* [14] - that fault tolerant quantum computing is possible if the error per gate can be reduced below a certain (code dependent) threshold. Work by Knill in 2005 [15] demonstrated codes for which this threshold is as high as 3%.

A fully scalable quantum computer has yet to be created but, with robust computing theoretically possible, the challenge is now considered to be one of engineering quantum systems. Since its inception, the field of quantum computing has developed

rapidly, with the addition of several new computing paradigms and many competing experimental approaches. We will return to cover these points later in the chapter.

2.1.2 Quantum Communication

The field of cryptography has a long and colourful history [16] in enabling secret communication between two or more parties. The only classical encryption method to be proven to be secure is the ‘one-time pad’, which uses a shared sequence of random numbers to encrypt and decrypt the messages sent between the two parties. All other classical cryptographic algorithms are only computationally secure - the probability of cracking them in a reasonable amount of time using current computational means is very small. The security of such systems therefore depends as much on the computational means as on the algorithm itself; in the face of full-scale quantum computing power, algorithms - such as the RSA algorithm - which were hitherto considered secure can no longer be relied upon.

The main challenge in using a one-time pad as a cryptographic system lies in establishing the shared sequence of random numbers. This sequence, often referred to as a key, is consumed throughout communication and must therefore be continually replenished. *Quantum Key Distribution (QKD)* protocols provide a solution to the key distribution problem. At the heart of these proposals lies one of the core principles of quantum mechanics: the observation of a quantum mechanical system by an observer alters its state. QKD schemes use this principle to establish a shared key in such a way that it is impossible, even in principle, to eavesdrop without disturbing the transmission in a way that can be detected. If we accept that quantum mechanics is valid, QKD is secure.

The first QKD scheme was proposed by Bennett and Brassard in 1984 [17]. The scheme uses the polarisation states of a stream of photons to establish a shared key

between the two parties, who we call Alice and Bob. Alice prepares each photon in random state chosen from one of four polarisation states. Bob randomly chooses one of two possible directions to measure for each photon. On average, half of the time Bob will choose the direction that corresponds to Alice's preparation. In this case he will be able to determine the exact state that Alice prepared. The other half of the time Bob chooses the 'wrong' direction and his measurement outcome will be random. After a measurement has been performed Bob reveals his measurement choice to Alice and she tells him whether he made the 'right' choice. If he did they can use the outcome as a bit of their shared key.

The presence of an eavesdropper will lead to errors in the shared key and can be detected with arbitrarily high probability by comparing (and then discarding) some of the key. This argument relies on the no cloning theorem, which states that the state of a quantum system cannot be copied. If quantum systems could be copied the eavesdropper could simply take copies of the photons and wait until Bob revealed his choices to measure them. The no cloning theorem is fundamental in many areas of QIP and was proven by Wootters and Zurek in 1982 [18].

A more general scheme was proposed by Ekert in 1991 [19]. The scheme is phrased in terms of *entanglement* - a quantum phenomenon involving a superposition of multiple particles. Instead of a stream of photons, pairs of entangled qubits are used as the key resource. Similar to Bennett and Brassard's scheme, measurements are made in a random basis, with basis choices later shared to establish the key. Bell's theorem [20] can be used to test for eavesdropping. The scheme has the benefit that it reduces the communication problem to that of distributing entangled pairs of qubits, which can be done from a central source.

Quantum communication is by far the most experimentally advanced of the QIP fields that we are concerned with [21], in the main part due to the comparatively few requirements it makes of the quantum systems involved. In 2004 a bank transfer in

Vienna was secured using QKD [22] and there are at least two commercially available quantum communication systems available on the market [23, 24]. In addition there are a growing number of quantum key distribution networks being created around the world [25, 26].

In practice there are a few ways in which the system can be vulnerable. One example is the *number splitting attack* [27]: if photons are occasionally emitted in pairs an attacker can split off one of these photons and save it until a time when the basis is revealed, thus being able to reconstruct some portion of the key. This can be prevented with a slight modification to the procedure [28] or with the development of better single photon sources. A more recent example is the *blinding attack* which exploits the specific photon detector design in two commercial QKD systems by constantly bombarding them with photons [29]. It is worth pointing out that both these examples target the deviation of certain real-world systems from the quantum ideal, rather than any inherent weakness in the protocol.

The field continues to progress the ability to establish keys over long distances. QKD was demonstrated between qubits separated by 100km in 2007 and 2008 [30, 31], over a noisy channel in 2012 [32] and more recently between an airplane travelling at 300km/hr and the ground [33]. It looks likely that satellite based quantum communication will be a reality in the near future.

2.1.3 Quantum Simulation

Feynman's initial contributions to quantum computing [1] were phrased in the terms of simulation: the existence of superpositions and entanglement makes it exponentially difficult to exactly simulate quantum systems using classical computers, so Feynman proposed using quantum systems instead. A big advance towards this goal was made by Lloyd, who in 1996 demonstrated the existence of universal quan-

tum simulators for systems with local interactions [34].

The short-term prospects for creating a useful quantum simulator are better than a quantum computer for two reasons [35]. First, quantum simulators appear to be more tolerant of errors due to decoherence effects: a small amount of noise can render a quantum computation useless whereas a quantum simulator can still give useful insights into the modelled system. Second, the size of system needed to obtain useful results is typically far smaller than for a quantum computer; to run Shor's algorithm for meaningfully large numbers would require thousands of qubits, whereas quantum systems containing a handful of qubits are already difficult to simulate classically.

An important area of application of quantum simulators is to quantum chemistry [36]. Quantum chemistry and band structure calculations currently account for up to 30% of computation time at supercomputing centres [37, 38]. Monte-Carlo and coupled-cluster methods, density functional theory, density renormalisation group theory and others have all been used to successfully solve a wide range of problems, however there are still whole classes of problems that cannot be tackled. Building on the phase estimation approach of Lloyd [39, 40], efficient quantum simulation algorithms for estimating the eigenvalues of many-body systems are known [41, 42].

Quantum simulators have been used to simulate quantum walks [43] with some experimental success [44]. Quantum walk type processes occur in many circumstances including exciton transfer in light harvesting biological systems. Recent experiments have shown the existence of long-lived coherences can exist in biological systems [45, 46, 47] making them a possible simulation target. There has also been some success in simulating in the field of condensed matter such as the simulation of the wavefunction of a frustrated Heisenberg spin system in 2011 [48].

2.2 Models of Quantum Computing

2.2.1 Circuit Model

The circuit model treats quantum computing as a sequence of operations, or gates, applied to qubits - and can therefore 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.

It is possible to construct any quantum operation from a sequence of two-qubit operations: two-qubit gates are universal for quantum computing [49] and are the only gate components we need to construct a circuit. In 2000 DiVincenzo produced five requirements [50] 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.

2.2.2 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 [51] 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 [52]. A universal set of Hamiltonians requiring only local terms was found in 2008 [53].

2.2.3 Measurement Based Quantum Computing

Measurement based quantum computation (MBQC) [54], or one-way quantum computation, is a computing paradigm proposed by Raussendorf and Briegel in 2001 [55]. 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 [56]. 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* [57]. The fundamental issue of which states could serve as universal resources for quantum computing was tackled by Van den Nest *et al.* in 2007 [58]. We will look at how such states can be created in Section 2.3.1.

2.2.4 Topological Quantum Computing

Topological quantum computing began as a new class of quantum error correcting 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 [59, 60] 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 the two topologically distinct ways to draw a loop that wraps a torus once. Further examples in the class of topological codes soon followed [61, 62].

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 [63], which was followed in 2007 with an approach from Raussendorf and Harrington which used braiding operations

on the code lattices [64, 65]. 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 [66, 67, 68, 69].

2.3 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’, remote interactions [70]. Bell’s work in 1964 [20] 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 [19] and the MBQC paradigm [55] show that entanglement can be viewed as a resource for both quantum communication and quantum computing. Entanglement purification schemes [71] 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 envisaging an entangled network of spatially separated computational nodes, we overcome many of the common barriers to scalability [72]. The problem of scaling the computation is reduced in part to that of entangling remote quantum systems.

2.3.1 Remote Entanglement Generation

Remote entanglement generation involves entangling two spatially separated quantum systems. One 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.* [73] 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 [74, 75, 76, 77] 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 [78] and was more recently used by Hanson *et al.* to entangle two NV⁻ centres [79]. 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].

2.4 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 best known approaches, noting interesting recent advances.

2.4.1 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 Chuang *et al.* had demonstrated a simple version of the Deutsch-Josza algorithm [82] and shortly after, in 2001, the same group managed to run Shor's algorithm to factorise the number fifteen [83].

The basic technique involved using electromagnetic pulses of precise frequencies to target particular transitions in order to perform a nuclear spin flip dependent on the position of a second spin. In this manner a two qubit CNOT gate was implemented. Initialisation into the lowest lying energy state was performed by taking a thermal state and equalising the populations in the higher energy states. The resulting mixture has a small excess of the target state, with the signals from the other states cancelling out. This state is said to be a *pseudo-pure state* and was later shown to have no true entanglement [84], calling into question whether early NMR experiments could really be considered quantum computations or whether they should be instead be viewed as simulations of quantum computations. The initialisation procedure also confers an inherent lack of scalability to the scheme; as the system size increases the excess in the target state, and therefore the signal from it, decreases exponentially.

In spite of these difficulties, pure NMR techniques remain at the forefront of what is possible on a quantum computer, as demonstrated by the factorisation of 143 using an adiabatic algorithm in 2012 [85]. However, the majority of the research in this area now focusses on the use of nuclear spins in hybrid systems - for example when coupled with an electronic spin that can be used for manipulation and cooling, as discussed in the next section.

2.4.2 Silicon based systems

There has been renewed interest in silicon based systems in recent years after the original proposal by Kane back in 1998 [86]. Qubits can be realised using the electronic and nuclear spin degrees of freedom in a system of an electron bound to a phosphorous donor. Using such a setup true entanglement was demonstrated in an large, NMR-type ensemble system for the first time in 2011 [87]. Unlike NMR, it is possible to make some measurements on individual spins in a single-shot manner, for example via spin to charge conversion [88].

Due to their weak environmental couplings nuclear spins make excellent candidates for quantum memories. Experiments in 2012 have shown spin coherence times in excess of $200\mu s$ [89, 90] at room temperature, with recent (unpublished) results apparently on the order of hours. It is likely that nuclear spins will play an important role in any solid state quantum computer.

2.4.3 Ion Traps

Ion trap approaches use ions trapped in electrical potentials with qubits often defined using low lying electronic states differentiated by spin, using optical processes for readout. The initial proposal was made by Cirac and Zoller in 1995 [91] and was followed with the implementation of a single qubit gate by Monroe *et al.* later that year [92]. After some theoretical advances [93] there was an implementation of the Deutsch-Josza algorithm in 2003 [94] and a successful quantum simulation using a single trapped atom in 2002 [95]. More recent success includes the demonstration of fourteen qubit entanglement by Blatt in 2011 [96]. Ion traps have also been used for the digital simulation of a range of spin systems using six qubits [97] and a system that can be used to simulate general open quantum system of up to five qubits [98].

Despite these successes the architecture has some weaknesses when it comes to

scaling: nearest neighbour interactions are commonly used to implement two-qubit gates which becomes problematic as the system size grows, with experimentalists forced to investigate approaches as the adiabatic transportation of ions along chip channels [99]. These concerns are less inhibitive in some simulation situations, such as the recent use of a 2D array of hundreds of ions to simulate large Ising systems [100].

2.4.4 Quantum Dots

Quantum dots are formed by confining a quantum particle in all three spacial directions, on a scale similar to its de Broglie wavelength. The resulting system has a series of discrete energy levels and can, to a good approximation, be viewed as an artificial atom. There are several physical systems that exhibit quantum dot behaviour; two of the most relevant systems for QIP are *self-assembled quantum dots* and *surface quantum dots*.

Self-assembled quantum dots are semiconductor structures consisting of a nanoscale region of a low band gap material embedded in higher band gap surroundings, the resulting 3D potential providing the confinement. There are two main approaches to defining qubits in self-assembled quantum dot systems. Spin qubits use the spin of the electronic ground state and have good coherence properties (ms) [101, 102] but relatively slow (ns) gating times [103]. Excitonic qubits use the existence of an electron-hole pair, or *exciton*, to define the qubit and have very fast (ps) gating times [104] but suffer from rapid (ns) decoherence due to strong environmental interactions. Some of the more promising proposals seek to combine the desirable features from both these schemes, for example by spin selective creation of an exciton to allow fast manipulation of the spin qubit [105, 106, 107]. There have been several successful demonstrations of initialisation [108, 109], control [110] and measurement

[111] of quantum dot qubits.

Self-assembled quantum dots are hindered by their random nature as optical characteristics vary wildly between dots. Surface quantum dots overcome this problem by using surface electrodes positioned on the surface of a thin semi-conductor film to define the dot. Using such systems, state initialisation, coherent manipulation and measurement via spin-to-charge conversion have been demonstrated [112]. Unlike self-assembled quantum dots, surface quantum dots are not typically optically active, and multiple qubit operations have been a challenge due to the geometrical constraints in placing multiple qubits in close proximity.

2.4.5 Photonic Systems

Due to weak interactions with their environment, photonic qubits show excellent coherence properties. The information can be encoded in various ways, including in the photon's polarisation and also in the 'dual-rail' representation - where the qubit is defined by the absence or presence of a qubit in a given mode [113]. In both these representations single qubit operations can be carried out by well understood linear optical gates [114, 115]. The difficulty with the scheme comes in implementing the two-qubit entangling gates. Non-linear effects, such as the Kerr effect, are very weak, making entanglement generation a challenge [116].

In 2001 Knill, Laflamme and Milburn proposed a system using projective measurements to implement two-qubit gates probabilistically [117]. By using a teleportation type approach these gates can be incorporated into the system with high probability. Combined with theoretical advances to reduce resources [118], the approach has been the basis of some exciting recent developments. In 2009 a team at Bristol managed to implement Shor's algorithm using 4 optical qubits to factorise 15 [119] and then in 2011 used qubit recycling schemes to factorise 21 [120].

Dealing with photon loss is still a key challenge but advances in the fields of efficient photon detectors [121] and sources [122] should go some way to improve the situation.

2.4.6 NV^- Centres

NV centers are defects in diamond consisting of a nitrogen and a neighbouring vacancy in the place of two carbon atoms. The NV^- system is formed when an additional electron is trapped at the site. The system is optically active and the spin projections of the electron ground state have promising properties for use as a qubit, including good coherence times at room temperature [123, 124].

In 2012 Grover's algorithm was implemented using the degrees of freedom in a single NV^- center to define two qubits [125], with gate fidelities of over 90%. There has been much recent progress in generating entanglement between different centers. In 2013 Hanson *et al.* demonstrated the non-deterministic entanglement of an NV^- center and a ^{13}C atom [79], and Wrachtrup *et al.* demonstrated deterministic entanglement between two neighbouring NV^- centres [126]. It has also been shown possible to entangle two NV^- centres on different pieces of diamond [127] - a promising step towards a distributed quantum computing architecture.

2.4.7 Superconducting Devices

Superconducting devices represent one of the most attractive systems for quantum computing [128]. A common proposal is to encode the qubit state in the direction of a current flowing in a superconducting ring with non-linear Josephson Junction [129] effects harnessed for two-qubit gates. Other possibilities include using charge or phase properties to define the qubit.

There has been much progress since first implementation of a superconducting

qubit in 1999 [130]. An increase in coherence times [131] has allowed the demonstration of two and three qubits control and entanglement [132, 133]. There have also been successful implementations of quantum computing algorithms, such as a two-qubit versions of the Deutsch-Josza and Grover algorithms in 2009 [134]. It is thought that superconducting qubits can now be made with coherence times approaching those needed for fault tolerant quantum computing [135].

Superconducting devices are also the system of choice of DWave Systems - the only commercial company claiming to offer quantum computing technology. In 2011 DWave published an article in *Nature* demonstrating the use of their superconducting computing device to find the ground state of an artificial Ising system using a quantum annealing technique [136]. At the time of writing it remains a controversial question exactly to what extent the DWave devices harness true quantum phenomena.

Bibliography

- [1] Feynman, R. (1982) Simulating physics with computers. *Int. J. Theor. Phys.*, **21**, 467–488.
- [2] Deutsch, D. (1985) Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. A*, **400**, 97–117.
- [3] Deutsch, D. and Jozsa, R. (1992) Rapid solution of problems by quantum computation. *Proceedings: Mathematical and Physical Sciences*, **439**, 553–558.
- [4] Simon, D. R. (1994) On the power of quantum computation. *Siam J. Comput.*, **26**, 116–123.
- [5] Grover, L. K. (1996) A fast quantum mechanical algorithm for database search. *Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC)*, pp. 212–219.
- [6] Shor, P. (1997) Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Siam J. Comput.*, **26**, 1484–1509.
- [7] Rivest, R., Shamir, A., and Adleman, L. (1978) A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**, 120–126.
- [8] Landauer, R. (1996) The physical nature of information. *Phys. Lett. A*, **217**, 188–193.
- [9] Ladd, T. D., Jelezko, F., Laflamme, R., Nakamura, Y., Monroe, C., and O’Brien, J. L. (2010) Quantum computers. *Nature*, **464**, 45–53.
- [10] Shor, P. W. (1995) Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, **52**, 2493–2496.
- [11] Steane, A. (1996) Error correcting codes in quantum theory. *Phys. Rev. Lett.*, **77**, 793–797.
- [12] Steane, A. (1996) Multiple-particle interference and quantum error correction. *Proc. R. Soc. A*, **452**, 2551–2577.

- [13] Laflamme, R., Miquel, C., Paz, J. P., and Zurek, W. H. (1996) Perfect quantum error correcting code. *Phys. Rev. Lett.*, **77**, 198–201.
- [14] Aharonov, D. and Ben-Or, M. (1997) Fault-tolerant quantum computation with constant error. *Proc. 29th ann. ACM symp. Th. comp.*, pp. 176–188.
- [15] Knill, E. (2005) Quantum computing with realistically noisy devices. *Nature*, **434**, 39–44.
- [16] Singh, S. (1999) *The Code Book: The Secret History of Codes and Code-breaking*. Doubleday.
- [17] Bennett, C. and Brassard, G. (1984) Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, **175**.
- [18] Wootters, W. K. and Zurek, W. H. (1982) A single quantum cannot be cloned. *Nature*, **299**, 802–803.
- [19] Ekert, A. K. (1991) Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.*, **67**, 661–663.
- [20] Bell, J. (1964) On the Einstein-Podolsky-Rosen paradox. *Physics*, **1**, 195–200.
- [21] Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002) Quantum cryptography. *Rev. Mod. Phys.*, **74**, 145–195.
- [22] World premiere: Bank transfer via quantum cryptography based on entangled photons. ”http://www.secoqc.net/downloads/pressrelease/Banktransfer_english.pdf”.
- [23] Id quantique. <http://www.idquantique.com/>.
- [24] Quantum key distribution system (q-box). <http://www.magiqtech.com/MagiQ/Products.html>.
- [25] Peev, M., et al. (2009) The SECOQC quantum key distribution network in vienna. *New J. Phys.*, **11**, 075001.
- [26] Sasaki, M., et al. (2011) Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, **19**, 10387–10409.
- [27] Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. (2000) Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, **85**, 1330–1333.
- [28] Hwang, W.-Y. (2003) Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, **91**, 057901.

-
- [29] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., and Makarov, V. (2010) Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.*, **4**, 686–689.
 - [30] Tanaka, A., et al. (2008) Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Opt. Express*, **16**, 11354–11360.
 - [31] Schmitt-Manderbach, T., et al. (2007) Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, **98**, 010504.
 - [32] Patel, K. A., Dynes, J. F., Choi, I., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Pentty, R. V., and Shields, A. J. (2012) Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Phys. Rev. X*, **2**, 041010.
 - [33] Nauerth, S., Moll, F., Rau, M., Fuchs, C., Horwath, J., Frick, S., and Weinfurter, H. (2013) Air-to-ground quantum communication. *Nat. Photon.*, pp. –.
 - [34] Lloyd, S. (1996) Universal quantum simulators. *Science*, **273**, 1073–1078.
 - [35] Blatt, R. and Roos, C. F. (2012) Quantum simulations with trapped ions. *Nat. Phys.*, **8**, 277–284.
 - [36] Buluta, I. and Nori, F. (2009) Quantum simulators. *Science*, **326**, 108–111.
 - [37] Aspuru-Guzik, A. and Walther, P. (2012) Photonic quantum simulators. *Nat. Phys.*, **8**, 285–291.
 - [38] of Energy, U. D. (2010), National energy research supercomputing center annual report. <http://www.nersc.gov/assets/Annual-Reports/annrep2010.pdf>.
 - [39] Abrams, D. S. and Lloyd, S. (1999) Quantum algorithm providing exponential speed increase for finding eigenvalues and eigenvectors. *Phys. Rev. Lett.*, **83**, 5162–5165.
 - [40] Abrams, D. S. and Lloyd, S. (1997) Simulation of many-body fermi systems on a universal quantum computer. *Phys. Rev. Lett.*, **79**, 2586–2589.
 - [41] Aspuru-Guzik, A., Dutoi, A. D., Love, P. J., and Head-Gordon, M. (2005) Simulated quantum computation of molecular energies. *Science*, **309**, 1704–1707.
 - [42] Whitfield, J. D., Biamonte, J., and Aspuru-Guzik, A. (2011) Simulation of electronic structure hamiltonians using quantum computers. *Molecular Physics*, **109**, 735–750.

- [43] Farhi, E. and Gutmann, S. (1998) Quantum computation and decision trees. *Phys. Rev. A*, **58**, 915–928.
- [44] Perets, H. B., Lahini, Y., Pozzi, F., Sorel, M., Morandotti, R., and Silberberg, Y. (2008) Realization of quantum walks with negligible decoherence in waveguide lattices. *Phys. Rev. Lett.*, **100**, 170506.
- [45] Engel, G. S., Calhoun, T. R., Read, E. L., Ahn, T.-K., Mancal, T., Cheng, Y.-C., Blankenship, R. E., and Fleming, G. R. (2007) Evidence for wavelike energy transfer through quantum coherence in photosynthetic systems. *Nature*, **446**, 782–786.
- [46] Collini, E., Wong, C. Y., Wilk, K. E., Curmi, P. M. G., Brumer, P., and Scholes, G. D. (2010) Coherently wired light-harvesting in photosynthetic marine algae at ambient temperature. *Nature*, **463**, 644–647.
- [47] Panitchayangkoon, G., Hayes, D., Fransted, K. A., Caram, J. R., Harel, E., Wen, J., Blankenship, R. E., and Engel, G. S. (2010) Long-lived quantum coherence in photosynthetic complexes at physiological temperature. *Proceedings of the National Academy of Sciences*, **107**, 12766–12770.
- [48] Ma, X.-s., Dakic, B., Naylor, W., Zeilinger, A., and Walther, P. (2011) Quantum simulation of the wavefunction to probe frustrated heisenberg spin systems. *Nat. Phys.*, **7**, 399–405.
- [49] DiVincenzo, D. P. (1995) 2-bit gates are universal for quantum computation. *Phys. Rev. A*, **51**, 1015–1022.
- [50] DiVincenzo, D. P. (2000) The physical implementation of quantum computation. *Fortschritte der Physik*, **48**, 771–783.
- [51] Farhi, E., Goldstone, J., Gutmann, S., and Sipser, M. (2000) Quantum computation by adiabatic evolution. *arXiv:quant-ph/0001106*.
- [52] Mizel, A., Lidar, D. A., and Mitchell, M. (2007) Simple proof of equivalence between adiabatic quantum computation and the circuit model. *Phys. Rev. Lett.*, **99**, 070502.
- [53] Biamonte, J. D. and Love, P. J. (2008) Realizable hamiltonians for universal adiabatic quantum computers. *Phys. Rev. A*, **78**, 012352.
- [54] Jozsa, R. (2005) An introduction to measurement based quantum computation. *arXiv:quant-ph/0508124*.
- [55] Raussendorf, R. and Briegel, H. (2001) A one-way quantum computer. *Phys. Rev. Lett.*, **86**, 5188–5191.
- [56] Daniel Gottesman, I. L. C. (1999) Quantum teleportation is a universal computational primitive. *Nature*, **402**, 390–393.

- [57] Raussendorf, R., Browne, D. E., and Briegel, H. J. (2003) Measurement-based quantum computation on cluster states. *Phys. Rev. A*, **68**, 022312.
- [58] den Nest, M. V., Duer, W., Miyake, A., and Briegel, H. J. (2007) Fundamentals of universality in one-way quantum computation. *New J. Phys.*, **9**, 204.
- [59] Kitaev, A. (2003) Fault-tolerant quantum computation by anyons. *Annals of Physics*, **303**, 2–30.
- [60] Kitaev, A. Y. (1997) Quantum computations: algorithms and error correction. *Russian Math. Surveys*, **52**, 1191–1249.
- [61] Bravyi, S. B. and Kitaev, A. Y. (1998) Quantum codes on a lattice with boundary. *arXiv:quant-ph/9811052*.
- [62] Freedman, M. H. and Meyer, D. A. (2001) Projective plane and planar quantum codes. *Foundations of Computational Mathematics*, **1**, 325–332.
- [63] Wang, C., Harrington, J., and Preskill, J. (2003) Confinement-higgs transition in a disordered gauge theory and the accuracy threshold for quantum memory. *Annals of Physics*, **303**, 31–58.
- [64] Raussendorf, R. and Harrington, J. (2007) Fault-tolerant quantum computation with high threshold in two dimensions. *Phys. Rev. Lett.*, **98**, 190504.
- [65] Raussendorf, R., Harrington, J., and Goyal, K. (2007) Topological fault-tolerance in cluster state quantum computation. *New J. Phys.*, **9**, 199.
- [66] Fowler, A. G., Whiteside, A. C., McInnes, A. L., and Rabbani, A. (2012) Topological code autotune. *Phys. Rev. X*, **2**, 041003.
- [67] Duclos-Cianci, G. and Poulin, D. (2010) Fast decoders for topological quantum codes. *Phys. Rev. Lett.*, **104**, 050504.
- [68] Duclos-Cianci, G. and Poulin, D. (2010) A renormalization group decoding algorithm for topological quantum codes. *Information Theory Workshop (ITW), 2010 IEEE*, pp. 1–5.
- [69] Wootton, J. R. and Loss, D. (2012) High threshold error correction for the surface code. *Phys. Rev. Lett.*, **109**, 160503.
- [70] Einstein, A., Podolsky, B., and Rosen, N. (1935) Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, **47**, 777–780.
- [71] Bennett, C. H., Bernstein, H. J., Popescu, S., and Schumacher, B. (1996) Concentrating partial entanglement by local operations. *Phys. Rev. A*, **53**, 2046–2052.

- [72] Denchev, V. S. and Pandurangan, G. (2008) Distributed quantum computing: a new frontier in distributed systems or science fiction? *SIGACT News*, **39**, 77–95.
- [73] Cabrillo, C., Cirac, J., Garcia-Fernandez, P., and Zoller, P. (1999) Creation of entangled states of distant atoms by interference. *Phys. Rev. A*, **59**, 1025–1033.
- [74] Duan, L.-M. and Kimble, H. J. (2003) Efficient engineering of multiatom entanglement through single-photon detections. *Phys. Rev. Lett.*, **90**, 253601.
- [75] Feng, X.-L., Zhang, Z.-M., Li, X.-D., Gong, S.-Q., and Xu, Z.-Z. (2003) Entangling distant atoms by interference of polarized photons. *Phys. Rev. Lett.*, **90**, 217902.
- [76] Barrett, S. D. and Kok, P. (2005) Efficient high-fidelity quantum computation using matter qubits and linear optics. *Phys. Rev. A*, **71**, 060310.
- [77] Lim, Y. L., Beige, A., and Kwek, L. C. (2005) Repeat-until-success linear optics distributed quantum computing. *Phys. Rev. Lett.*, **95**, 030505.
- [78] Moehring, D. L., Maunz, P., Olmschenk, S., Young, K. C., Matsukevich, D. N., Duan, L.-M., and Monroe, C. (2007) Entanglement of single-atom quantum bits at a distance. *Nature*, **449**, 68–71.
- [79] Pfaff, W., Taminiau, T. H., Robledo, L., Bernien, H., Markham, M., Twitchen, D. J., and Hanson, R. (2013) Demonstration of entanglement-by-measurement of solid-state qubits. *Nat. Phys.*, **9**, 29–33.
- [80] Benjamin, S. C., Browne, D. E., Fitzsimons, J., and Morton, J. J. L. (2006) Brokered graph-state quantum computation. *New J. Phys.*, **8**, 141.
- [81] Gershenfeld, N. A. and Chuang, I. L. (1997) Bulk spin-resonance quantum computation. *Science*, **275**, 350–356.
- [82] Chuang, I., Vandersypen, L., Zhou, X., Leung, D., and Lloyd, S. (1998) Experimental realization of a quantum algorithm. *Nature*, **393**, 143–146.
- [83] Vandersypen, L., Steffen, M., Breyta, G., Yannoni, C., Sherwood, M., and Chuang, I. (2001) Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance. *Nature*, **414**, 883–887.
- [84] Braunstein, S., Caves, C., Jozsa, R., Linden, N., Popescu, S., and Schack, R. (1999) Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, **83**, 1054–1057.
- [85] Xu, N., Zhu, J., Lu, D., Zhou, X., Peng, X., and Du, J. (2012) Quantum factorization of 143 on a dipolar-coupling nuclear magnetic resonance system. *Phys. Rev. Lett.*, **108**, 130501.

-
- [86] Kane, B. E. (1998) A silicon-based nuclear spin quantum computer. *Nature*, **393**, 133–137.
- [87] Simmons, S., Brown, R., Riemann, H., Abrosimov, N., Becker, P., Pohl, H., Thewalt, M., Itoh, K., and Morton, J. (2011) Entanglement in a solid-state spin ensemble. *Nature*, **470**, 69–72.
- [88] Morello, A., et al. (2010) Single-shot readout of an electron spin in silicon. *Nature*, **467**, 687–691.
- [89] Pla, J. J., Tan, K. Y., Dehollain, J. P., Lim, W. H., Morton, J. J. L., Jamieson, D. N., Dzurak, A. S., and Morello, A. (2012) A single-atom electron spin qubit in silicon. *Nature*, **489**, 541–545.
- [90] Tyryshkin, A. M., et al. (2012) Electron spin coherence exceeding seconds in high-purity silicon. *Nat. Mater.*, **11**, 143–147.
- [91] Cirac, J. I. and Zoller, P. (1995) Quantum computations with cold trapped ions. *Phys. Rev. Lett.*, **74**, 4091–4094.
- [92] Monroe, C., Meekhof, D. M., King, B. E., Itano, W. M., and Wineland, D. J. (1995) Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.*, **75**, 4714–4717.
- [93] Wineland, D., Monroe, C., Itano, W. M., Leibfried, D., King, B. E., and Meekhof, D. M. (1998) Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Technol.*, **103**, 259–328.
- [94] Gulde, S., Riebe, M., Lancaster, G., Becher, C., Eschner, J., Haffner, H., Schmidt-Kaler, F., Chuang, I., and Blatt, R. (2003) Implementation of the deutsch-jozsa algorithm on an ion-trap quantum computer. *Nature*, **421**, 48–50.
- [95] Leibfried, D., et al. (2002) Trapped-ion quantum simulator: Experimental application to nonlinear interferometers. *Phys. Rev. Lett.*, **89**, 247901.
- [96] Monz, T., Schindler, P., Barreiro, J. T., Chwalla, M., Nigg, D., Coish, W. A., Harlander, M., Hänsel, W., Hennrich, M., and Blatt, R. (2011) 14-qubit entanglement: Creation and coherence. *Phys. Rev. Lett.*, **106**, 130506.
- [97] Lanyon, B. P., et al. (2011) Universal digital quantum simulation with trapped ions. *Science*, **334**, 57–61.
- [98] Barreiro, J. T., Muller, M., Schindler, P., Nigg, D., Monz, T., Chwalla, M., Hennrich, M., Roos, C. F., Zoller, P., and Blatt, R. (2011) An open-system quantum simulator with trapped ions. *Nature*, **470**, 486–491.

-
- [99] Stick, D., Hensinger, W., Olmschenk, S., Madsen, M., Schwab, K., and Monroe, C. (2006) Ion trap in a semiconductor chip. *Nat. Phys.*, **2**, 36–39.
- [100] Britton, J. W., Sawyer, B. C., Keith, A. C., Wang, C. C. J., Freericks, J. K., Uys, H., Biercuk, M. J., and Bollinger, J. J. (2012) Engineered two-dimensional ising interactions in a trapped-ion quantum simulator with hundreds of spins. *Nature*, **484**, 489–492.
- [101] Kroutvar, M., Ducommun, Y., Heiss, D., Bichler, M., Schuh, D., Abstreiter, G., and Finley, J. (2004) Optically programmable electron spin memory using semiconductor quantum dots. *Nature*, **432**, 81–84.
- [102] Greilich, A., Yakovlev, D. R., Shabaev, A., Efros, A. L., Yugova, I. A., Oulton, R., Stavarache, V., Reuter, D., Wieck, A., and Bayer, M. (2006) Mode locking of electron spin coherences in singly charged quantum dots. *Science*, **313**, 341–345.
- [103] Burkard, G., Loss, D., and DiVincenzo, D. (1999) Coupled quantum dots as quantum gates. *Phys. Rev. B*, **59**, 2070–2078.
- [104] Li, X., Wu, Y., Steel, D., Gammon, D., Stievater, T., Katzer, D., Park, D., Piermarocchi, C., and Sham, L. (2003) An all-optical quantum gate in a semiconductor quantum dot. *Science*, **301**, 809–811.
- [105] Calarco, T., Datta, A., Fedichev, P., Pazy, E., and Zoller, P. (2003) Spin-based all-optical quantum computation with quantum dots: Understanding and suppressing decoherence. *Phys. Rev. A*, **68**, 012310.
- [106] Chen, G., Bonadeo, N., Steel, D., Gammon, D., Katzer, D., Park, D., and Sham, L. (2000) Optically induced entanglement of excitons in a single quantum dot. *Science*, **289**, 1906–1909.
- [107] Yokoi, T., Adachi, S., Sasakura, H., Muto, S., Song, H., Usuki, T., and Hirose, S. (2005) Polarization-dependent shift in excitonic Zeeman splitting of self-assembled $\text{In}_{0.75}\text{Al}_{0.25}\text{As}/\text{Al}_{0.3}\text{Ga}_{0.7}\text{As}$ quantum dots. *Phys. Rev. B*, **71**, 041307.
- [108] Atatüre, M., Dreiser, J., Badolato, A., Högele, A., Karrai, K., and Imamoglu, A. (2006) Quantum-dot spin-state preparation with near-unity fidelity. *Science*, **312**, 551–553.
- [109] Gerardot, B. D., Brunner, D., Dalgarno, P. A., Ohberg, P., Seidl, S., Kroner, M., Karrai, K., Stoltz, N. G., Petroff, P. M., and Warburton, R. J. (2008) Optical pumping of a single hole spin in a quantum dot. *Nature*, **451**, 441–444.

- [110] Press, D., Ladd, T. D., Zhang, B., and Yamamoto, Y. (2008) Complete quantum control of a single quantum dot spin using ultrafast optical pulses. *Nature*, **456**, 218–221.
- [111] Berezovsky, J., Mikkelsen, M. H., Gywat, O., Stoltz, N. G., Coldren, L. A., and Awschalom, D. D. (2006) Nondestructive optical measurements of a single electron spin in a quantum dot. *Science*, **314**, 1916–1920.
- [112] Hu, Y., Kuemmeth, F., Lieber, C. M., and Marcus, C. M. (2012) Hole spin relaxation in ge-si core-shell nanowire qubits. *Nat. Nano.*, **7**, 47–50.
- [113] Kok, P., Munro, W. J., Nemoto, K., Ralph, T. C., Dowling, J. P., and Milburn, G. J. (2007) Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, **79**, 797.
- [114] Fox, A. M. (2006) *Quantum Optics: An Introduction*. Oxford University Press.
- [115] Walls, D. and Milburn, G. (2008) *Quantum Optics*. Springer, 2 edn.
- [116] Shapiro, J. H. (2006) Single-photon Kerr nonlinearities do not help quantum computation. *Phys. Rev. A*, **73**, 062305.
- [117] Knill, E., Laflamme, R., and Milburn, G. (2001) A scheme for efficient quantum computation with linear optics. *Nature*, **409**, 46–52.
- [118] O’Brien, J. L. (2007) Optical quantum computing. *Science*, **318**, 1567–1570.
- [119] Politi, A., Matthews, J. C. F., and O’Brien, J. L. (2009) Shor’s quantum factoring algorithm on a photonic chip. *Science*, **325**, 1221.
- [120] Martin-Lopez, E., Laing, A., Lawson, T., Alvarez, R., Zhou, X.-Q., and O’Brien, J. L. (2012) Experimental realization of Shor’s quantum factoring algorithm using qubit recycling. *Nat. Photon.*, **6**, 773–776.
- [121] Hadfield, R. H. (2009) Single-photon detectors for optical quantum information applications. *Nat. Photon.*, **3**, 696–705.
- [122] Grangier, P., Sanders, B., and Vuckovic, J. (2004) Focus on single photons on demand. *New J. Phys.*, **6**.
- [123] Kok, P. and Lovett, B. W. (2006) Materials science - qubits in the pink. *Nature*, **444**, 49–49.
- [124] Jelezko, F., Gaebel, T., Popa, I., Gruber, A., and Wrachtrup, J. (2004) Observation of coherent oscillations in a single electron spin. *Phys. Rev. Lett.*, **92**, 076401.

-
- [125] van der Sar, T., Wang, Z. H., Blok, M. S., Bernien, H., Taminiau, T. H., Toyli, D. M., Lidar, D. A., Awschalom, D. D., Hanson, R., and Dobrovitski, V. V. (2012) Decoherence-protected quantum gates for a hybrid solid-state spin register. *Nature*, **484**, 82–86.
 - [126] Dolde, F., Jakobi, I., Naydenov, B., Zhao, N., Pezzagna, S., Trautmann, C., Meijer, J., Neumann, P., Jelezko, F., and Wrachtrup, J. (2013) Room-temperature entanglement between single defect spins in diamond. *Nat. Phys.*, **9**, 139–143.
 - [127] Bernien, H., et al. (2012) Heralded entanglement between solid-state qubits separated by 3 meters. *arXiv:1212.6136*.
 - [128] Steffen, M. (2011) Superconducting qubits are getting serious. *Physics*, **4**, 103.
 - [129] Josephson, B. D. (1974) The discovery of tunnelling supercurrents. *Rev. Mod. Phys.*, **46**, 251–254.
 - [130] Nakamura, Y., Pashkin, Y. A., and Tsai, J. S. (1999) Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature*, **398**, 786–788.
 - [131] Chiorescu, I., Nakamura, Y., Harmans, C. J. P. M., and Mooij, J. E. (2003) Coherent quantum dynamics of a superconducting flux qubit. *Science*, **299**, 1869–1871.
 - [132] Ansmann, M., et al. (2009) Violation of Bell’s inequality in Josephson phase qubits. *Nature*, **461**, 504–506.
 - [133] DiCarlo, L., Reed, M. D., Sun, L., Johnson, B. R., Chow, J. M., Gambetta, J. M., Frunzio, L., Girvin, S. M., Devoret, M. H., and Schoelkopf, R. J. (2010) Preparation and measurement of three-qubit entanglement in a superconducting circuit. *Nature*, **467**, 574–578.
 - [134] DiCarlo, L., et al. (2009) Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature*, **460**, 240–244.
 - [135] Paik, H., et al. (2011) Observation of high coherence in Josephson junction qubits measured in a three-dimensional circuit qed architecture. *Phys. Rev. Lett.*, **107**, 240501.
 - [136] Johnson, M. W., et al. (2011) Quantum annealing with manufactured spins. *Nature*, **473**, 194–198.