Entanglement and quantum information theory in the context of higher dimensional spin systems

A thesis

presented

by

Christopher Hadley

Department of Physics and Astronomy

University College London

In partial fulfillment

of the requirements of the

degree of

Doctor of Philosophy

of the

University of London

Final version

November 2008

Primary supervisor: Prof Sougato Bose

Secondary supervisor: Prof Andrew Fisher

ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

I, Christopher Andrew Hadley, confirm that the work presented in this thesis is my own. Where information has been derived from other sources, I confirm that this has been indicated; where work has been performed as part of a collaboration, this has also been indicated.

Abstract

Quantum information theory is an exciting, inter-disciplinary field, combining elements of condensed matter theory, quantum mechanics and information theory. In this thesis, I shall make a modest contribution to this field by examining entanglement in many-body systems with more than two levels.

In the first section, I consider the dynamics of a system of qutrits—three-level quantum systems—which are coupled through an SU(3)-invariant permutation Hamiltonian. Each term in this Hamiltonian is a nearest-neighbour permutation operator, and thus this Hamiltonian may be considered a generalisation of the standard SU(2)-invariant Heisenberg Hamiltonian, in which every term (up to the addition of the identity operator) is a nearest-neighbour permutation operator for two-level system. The system considered has the topology of a cross, and thus may be considered (to a limited extent) analogous to a beam-splitter. The aim of the study is to establish a Bell singlet state between two distant parties.

Building on this work, I shall go on to consider the ground state of a system made up of many-level systems coupled by the same Hamiltonian; I shall show that this state is a generalisation of the two-level singlet to many levels and many systems. It thus has a high degree of symmetry. I will consider its application in entanglement distribution through measurements (localisable entanglement), and discuss how it may be physically implemented in systems of ultracold atoms, through the Hubbard model.

I shall also show that in the famous valence bond solid (the ground state of the Affleck–Kennedy–Lieb–Tasaki spin chain), all the entanglement present in the state may be extracted from a single copy of the chain; this is in contrast to gapless, critical chains, in which only half the total entanglement is extractable from a single copy.

This thesis does not exceed 100,000 words.

Acknowledgements

I must first thank my supervisor, Sougato Bose, for giving me the opportunity to be his student. Throughout my PhD, I have appreciated his creativity, and have shared many fruitful discussions with him. I am particularly grateful for the high degree of autonomy and trust he granted me, allowing me to follow many of my own directions and frame my own questions for research, whilst still being able to answer my questions whenever they arose. Andrew Fisher, as my second supervisor, has also provided much encouragement, and has always been able to provide exceptionally clear and illuminating answers to my questions about condensed matter physics.

Aside from my official supervisors, Alessio Serafini has acted as an excellent teacher and mentor, both introducing me to many aspects of quantum information theory, and providing invaluable advice about such murky topics as dealing with referees. I must also thank James Munro for his assistance with computing issues (especially numerous instances of PEBKAC[1]), and his infectious enthusiasm; and Clark Downum for assistance with LaTeX.

During my studies, I have had the great pleasure of sharing many enjoyable discussions with members of the quantum information community, both in the UK and overseas. In particular, I must thank those whose ideas have influenced my own research; whilst it is not possible to name all such researchers, I would like to mention (in addition to those already named) Antonio Acín, Tom Boness, Daniel Burgarth, Ignacio Cirac, Heng Fan, Kurt Jacobs, Alastair Kay, Myungshik Kim, Vladimir Korepin, Mauro Paternostro, Robert Raussendorf and Mark Tame.

My understanding of physics, of course, owes a great deal to my undergraduate tutors. I am grateful to Geoff Brooker, Graham Ross and C. V. Sukumar not just for their teaching, but their conceptual insight, and ability to answer almost any question thrown at them. I must also thank my 'A' level physics teacher, Ian Taylor, without whose enthusiasm I may not have become a physicist. I have yet to meet a more inspirational teacher.

I must thank the many friends and colleagues who have provided support and encouragement over the years, particularly at those times when work was not flowing. And finally, I must thank my parents, for their love and support at this and every stage of my education.

My PhD was funded by an Engineering and Physical Sciences Research Council studentship; I am also grateful for assistance from the University of London Valerie Myerscough Prize Fund.

[1] 'Problem exists between keyboard and chair', a common problem in computer programming.

Foreword

The early twentieth century saw the development of two pillars of modern physics: *quantum mechanics* and *general relativity*. Together, they have revolutionised our world, paving the way for disruptive techologies such as transistor-based computation, satellite communication and, more recently, the internet. Whilst general relativity concerns itself with the very large (planets and galaxies, for example), quantum mechanics is the theory of the very small; indeed, the theory gives rise to a fundamental lengthscale (the Planck length), on which space may be considered 'grainy'. Ever since the idea of the 'atom' was first mooted by the ancient Greeks, scientists have been probing ever smaller particles and lengthscales; this strange, counter-intuitive world is the realm of the quantum theory.

Time and again the theory has passed the test of experimental falsification, and has given rise to many technological advances. From a practical point of view, then, the theory has been immensely successful. However, it forces scientists to radically overhaul their conceptual view of the universe. Phenomena wholly counter to mankind's experience of the everyday, 'classical' world (not least with respect to determinism and locality) are characteristic of the theory. Indeed, despite being one of the forefathers of the theory, Albert Einstein presented, with co-authors Boris Podolsky and Nathan Rosen, a 'paradox' purpotedly highlighting the inadequacies of quantum mechanics as a 'complete theory' of nature. He subsequently stated his dissatisfication with the probabilistic nature of the theory through the famous quote: 'God does not play dice'.

Erwin Schrödinger also considered the bizarre behaviour of composite systems predicted by quantum mechanics, and used the German word *Verschränkung* to describe the 'stronger-than-classical' correlations between particles. More recently, John Bell derived an inequality that any theory of nature should satisfy, were it to satisfy our intuitive concepts of locality and reality; quantum mechanics violates this inequality, and thus one must accept the non-local (or non-

realistic) nature of quantum mechanics[2]. This strong correlation—now named *entanglement*—cannot be avoided. Indeed, it is now regarded as the essential signature of quantum mechanics and routinely referred to as a 'resource': the power behind proposed *quantum computers.* Abstract notions of such machines were proposed independently by Paul Benioff and David Deutsch in the 1980s (building on the ideas of Yu Manin and Richard Feynman), and were intended to be a quantum analogue of the famous Turing machine in classical computer science (a machine that can solve any algorithmic process). Quantum computers are believed to be able to efficiently solve classically intractable problems, such as factoring, and cracking RSA cryptography. They may also be suitable for simulating other physical (quantum) systems.

In parallel, the idea that physics should be a theory of *information* arose: what one knows about the universe, and what information one can extract from it. Building on Claude Shannon's work on information theory in 1948, Edwin Jaynes described statistical mechanics (the physics of many-particle systems) in terms of information and the maximum-entropy principle. The modern field of quantum information theory now attempts to link quantum mechanics and information in an analogous manner.

Underlying both quantum computation and quantum information is the concept of entanglement. These endeavours have both blossomed in recent years, bringing together physicists, mathematicians, computer scientists and engineers, some motivated by a desire to build such a quantum computer, some by the promise that it will give scientists a deeper understanding of the physical world. This thesis makes a very modest contribution to this work by studying the entanglement that exists in, and may be extracted from, various many-body physical systems. The work included has been published in the following three papers:

'Entanglement creation and distribution on a graph of exchange-coupled qutrits'
Christopher Hadley, Alessio Serafini and Sougato Bose
Physical Review A, **72**, 052333 (2005)

'Multilevel multiparty singlets as ground states and their role in entanglement distribution'
Christopher Hadley and Sougato Bose
Physical Review A, **77**, 050308(R) (2008)

'Single-copy entanglement in a gapped quantum spin chain'
Christopher Hadley
Physical Review Letters, **100**, 177202 (2008)

[2] Although strictly, there are no loophole-free experiments!

The thesis is divided into five parts. In Part I, I introduce the modern notions of quantum mechanics and entanglement. The introduction begins from first principles, and only basic notions of physics and mathematics are assumed. I conclude by providing a brief overview of the central themes in quantum information theory and quantum computation, in order to provide the motivation for the study of entanglement in subsequent chapters.

In Part II, I propose a spin-based system which performs the tasks of entanglement generation and distribution, both essential for the development of a quantum computer. This work was performed in collaboration with Sougato Bose and Alessio Serafini. Part III is concerned with how much entanglement can be extracted from a single copy of a given system, as opposed to the usual asymptotic limit, and I show that for one type of system, this is equal to the entanglement extractable from an infinite number of copies. Finally, in Parts IV and V, I consider a state with a very high degree of permutational symmetry, characterise some of its properties, and discuss its implementation in various physical systems describable by the strong coupling limit of the Hubbard model. This work was performed in collaboration with Sougato Bose.

Full references to background literature are provided, and many of the introductory sections conclude with suggestions for further reading.

Christopher Hadley

London, November 2008

Contents

Part I

Introduction and context

In this part, I shall introduce the main concepts required for any work in the field of quantum information; specifically, quantum mechanics, entanglement, and the link between this and information processing. The introduction is written to be accessible to non-specialist physicists, and is relatively self-contained. Full references are given, including suggestions for further reading.

Chapter 1

Quantum mechanics

As anticipated in the foreword to this thesis, quantum mechanics is a highly counter-intuitive physical theory. It is also a highly successful description of nature. In this Chapter, I shall introduce the theory from first principles, along with the required mathematical notation, and attempt to show how many of the key concepts follow directy from the postulates. As one would expect for such a fundamental theory, many excellent introductory texts have been written, references to which are given in the 'further reading' section.

1.1 Postulates of modern quantum mechanics

Quantum mechanics is one of the two pillars of modern physics (the other being *general relativity*), and has been verified time and again in the laboratory. The origins of the theory lie in the early twentieth century, when Max Planck was studying *black-body radiation*; he considered what would happen if energy were divided into discrete quantities called *quanta*. This idea was further developed by Albert Einstein when he additionally quantised radiation, and applied it to the photoelectric effect. The modern conceptual understanding of quantum mechanics is quite different to what became know as the *old quantum theory*, but it was this idea of dividing physical quantities into discrete units that laid the foundation for the 'quantum revolution'.

Despite the incredibly complex phenomena that it describes (not to mention some of the more bizarre physical predictions and philosophical interpretations), the modern theory itself follows from only a handful of postulates. These are listed below in order to give a quick overview of the subject, and are subsequently discussed in more detail, along with many other key concepts and consequences of the postulates. The introduction I present here is driven by the desire to explain quantum mechanics from an information theoretic point of view, introducing operators, observables and other concepts from the point of view of what information can

be extracted from the system. The main consequence of this way of thinking about quantum mechanics is the elevation of 'entanglement' from a mere quirk (at best) or nuisance (at worst) to a central theme of the theory; indeed, it is now regularly described in the literature as a 'resource'. The approach is quite abstract, introducing a handful of postulates and the associated mathematics, rather than considering the more standard 'waves in boxes' or 'wave packet dynamics' more frequently encountered in undergraduate texts. This is motivated by, and intended to highlight, the fact that most results in quantum information theory are completely general; *i.e.* they are not peculiar to any particular physical implementation or system. In this introduction (and in the subsequent Chapter on entanglement), I wish to show how many of the key concepts arise without even considering which system the results may be applied to. It is for this reason that discussion of physical implementations is fairly cursory.

Postulate 1 (State vectors). *Any closed physical system has a complex vector space associated with it, called the state space. This space is an inner-product (Hilbert) space, usually denoted $\mathcal{H}$. A single state (a pure state) of the physical system is described by a vector $|\psi\rangle \in \mathcal{H}$ of unit length in this space, called the state vector. An ensemble of pure states (a mixed state) may be described by a density matrix ρ, an operator acting on the state space.*

Postulate 2 (Measurements). *Measurements of a physical quantity on a quantum system are represented by a set of measurement operators $\{M_i\}$ which act on the state space in question. This set of operators corresponds to a single physical quantity, where the index i refers to the possible outcomes of the measurement. When a measurement is made on a system in a mixed state ρ, the state of the system becomes*

$$\rho_i = \frac{M_i \rho M_i^\dagger}{\mathrm{tr}\left(M_i^\dagger M_i \rho\right)} \tag{1.1}$$

with probability $p(i) = \mathrm{tr}\,(M_i^\dagger M_i \rho)$. The operators satisfy the constraint $\sum_i M_i^\dagger M_i = \mathbb{I}$, reflecting the summation of probability to unity. For a measurement on a pure state $|\psi\rangle$, the post-measurement state Equation (1.1) reduces to

$$|\psi_i\rangle = \frac{M_i\,|\psi\rangle}{\sqrt{\left\langle\psi\middle|M_i^\dagger M_i\middle|\psi\right\rangle}}, \tag{1.2}$$

with probability $p(i) = \langle\psi_i\,|\,M_i^\dagger M_i\,|\,\psi_i\rangle$.

Postulate 3 (Unitary time evolution). *The time-evolution of a closed physical system described at time t_1 by a density matrix $\rho(t_1)$ is a unitary transformation depending solely on the times t_1, t_2; i.e. the state $\rho(t_2)$ of the system at time t_2 is*

$$\rho(t_2) = U(t_1, t_2)\,\rho(t_1)\,U(t_1, t_2)^\dagger. \tag{1.3}$$

For a pure state $|\psi(t_1)\rangle$*, this reduces to*

$$|\psi(t_2)\rangle = U(t_1, t_2)\,|\psi(t_1)\rangle\,. \tag{1.4}$$

Postulate 4 (Systems of many distinguishable bodies). *In a composite system of two or more particles, the state of each part will be represented by a vector in an appropriate vector space, as prescribed by the first postulate. The overall state of the system belongs to a larger vector space, formed by taking the tensor product (or direct product) of the these spaces. Namely, if a system consists of n smaller systems, where system j is prepared in the state* $|\psi_{i_j}\rangle_j \in \mathcal{H}_j$ *(for* $j \in [1, N]$*), the overall state will be*

$$|\psi_{i_1}\rangle_1 \otimes |\psi_{i_2}\rangle_2 \otimes \cdots \otimes |\psi_{i_n}\rangle_n \tag{1.5}$$

which resides in a composite vector space, denoted

$$\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n. \tag{1.6}$$

For brevity, the tensor product symbols are often omitted, and the state is denoted thus:

$$|\psi_{i_1}\rangle_1\,|\psi_{i_2}\rangle_2 \cdots |\psi_{i_n}\rangle_n\,. \tag{1.7}$$

Postulate 5 (Systems of many indistinguishable bodies). *Composite sytems of several indistinguishable particles should be eigenstates of all possible permutation operators, and must be either completely symmetric or antisymmetric under such operations. These are termed bosonic and fermionic statistics, respectively*[1]*. This gives rise to Pauli exclusion: no two fermions may exist in the same state at the same space*[2]*.*

Having introduced the postulates, it is now instructive to consider each in turn, and show how they give rise to other concepts in quantum mechanics.

1.1.1 Postulate 1: state space

Pure states

As already stated, a *pure state* is denoted $|\psi\rangle$ in *Dirac notation* (the notation $|\cdot\rangle$ is called a 'ket'). This object is a vector with unit norm. The simplest example is that of a two-level system, where there are two possible states: $|0\rangle$ and $|1\rangle$. The fundamental departure from classical mechanics here is that a quantum system can exist in a *superposition*, such as $\alpha\,|0\rangle + \beta\,|1\rangle$.

[1] More generally, states can have *parastatistics*, when identical particles transform according to Young tableaux other than those that are completely symmetric or completely antisymmetric; these, however, are not observed in nature. In two dimensions, quasi-particles called *anyons* can also exist.

[2] This is erroneously referred to as the Pauli exclusion *principle*, but it is a consequence of the permutational symmetry, *not* a principle!

This two level system is referred to as a *qubit*, to reflect its nature as a quantum generalisation of a *bit* (binary digit). In general, if a quantum mechanical degree of freedom has d possible values, it may be denoted by a vector $|\psi\rangle = \sum_{i=1}^{d} v_i |\psi_i\rangle$, in a vector space $\mathcal{H} \sim \mathbb{C}^d$. In this thesis, this will be referred to as a *qudit*. The complex numbers $v_i \in \mathbb{C}$ are *amplitudes*, onto which is imposed the *normalisation condition* $\sum_i^d v_i^* v_i = 1$ (where v_i^* is the complex conjugate of v_i), for reasons that will become clear later on. A general pure state of a d-level system thus has $2d - 1$ degrees of freedom (since a complex number is described by a real and imaginary number, and the normalisation constraint removes one degree of freedom). The set of vectors $\{|\psi_i\rangle\}$ is called a *basis set*, and may be used to expand any given vector $|\psi\rangle$ as above by choosing appropriate amplitudes.

Kets have counterpart objects called 'bras' $\langle\phi|$, which are complex-valued linear functions on the vector space $\mathcal{H}$; *i.e.* for any $\alpha, \beta \in \mathbb{C}$

$$\langle\phi| (\alpha |0\rangle + \beta |1\rangle) = \alpha \langle\phi|0\rangle + \beta \langle\phi|1\rangle . \tag{1.8}$$

These objects themselves form a basis for a different vector space $\mathcal{H}'$, the *adjoint space* of $\mathcal{H}$. By considering the number of vectors needed to expand an arbitrary state in both $\mathcal{H}$ and $\mathcal{H}'$, one can see that these spaces have the same dimension. Moreover, one can see that the counterpart of a vector $|\psi\rangle \in \mathcal{H}$ is $\langle\psi| \in \mathcal{H}'$. This allows us make the statement that basis sets (or *bases*) are *orthonormal* if $\langle\psi_i|\psi_j\rangle = \delta_{ij}$ for all $i, j \in [1, d]$. To simplify matters, physicists normally speak of a quantum system and its associated 'vector space', as opposed to the two spaces $\mathcal{H}$ and $\mathcal{H}'$.

A particularly useful function associated to a vector space $\mathbb{C}^d$ is the *inner product* $(\cdot, \cdot)$ which is a function $\mathbb{C}^d \times \mathbb{C}^d \to \mathbb{C}$, given by

$$\langle\psi|\phi\rangle := \left(\sum_i \psi_i |\psi_i\rangle , \sum_i \phi_i |\phi_j\rangle \right) = \sum_{i=1}^{d} \psi_i^* \phi_i . \tag{1.9}$$

The normalisation condition can therefore be denoted $\langle\psi|\psi\rangle = 1$. This vector space is hence referred to as an *inner product space*; for systems with finite d, this is identical to a *Hilbert space*. Physicists use these terms interchangeably, leaving mathematicians to argue over the difference! It is worth noting that the states $|\psi\rangle$ and $e^{i\phi} |\psi\rangle$ are physically indistinguishable (again, this will become clear after measurement has been introduced); the quantity $\phi \in \mathbb{R}$ is called a *global phase* and has no effect on physical reality. The state could thus equally well be described by the *ray* $e^{i\phi} |\psi\rangle$ for all ϕ.

Mixed states

The state vector is not the most general way of describing a state in quantum mechanics. The *density operator* approach allows for a description of an *ensemble* of pure states, which may

be used to describe the state of a physical system whose state is not completely known. The density operator for a system with an ensemble of state $\{|\psi\rangle\}$, each occurring with probability p_i is given by the operator

$$\rho := \sum_i p_i |\psi_i\rangle \langle\psi_i| . \tag{1.10}$$

Quantum mechanics can either be formulated in terms of density operators, regarding the pure state as a special case, or in terms of pure states, regarding the density operator as a way of describing ensembles through the above definition.

One might naively think of the density operator as describing a physical machine which creates the state $|\psi_i\rangle$ with probability p_i; physically, the state indeed being one of the $\{|\psi_i\rangle\}$, but with the experimenter ignorant of which i. However, this interpretation, whilst appealing, is not quite correct, since there is an infinite number of ensembles giving rise to the same density matrix, according to the following theorem given in Nielsen and Chuang [166] but originally discovered by Schrödinger [213] and extended by Jaynes [134, 135], and Hughston, Jozsa and Wootters [130].

Theorem 6 (Unitary freedom in ensembles). *The sets of states $\{|\psi_i\rangle\}$ and $\{|\phi_i\rangle\}$ generate the same density matrix ρ if and only if*

$$|\psi_i\rangle = \sum_j u_{ij} |\phi_j\rangle \tag{1.11}$$

where u_{ij} is a unitary matrix.

Linear algebra

It is clear from the preceeding two sections that the natural language for quantum mechanics is linear algebra. The reader is assumed to be familiar with basic concepts such as *vectors*, *basis sets* and elementary vector operations, which have been introduced implicitly above. For a basic overview, the reader is recommended to read the basic introduction in the textbook by Nielsen and Chuang [166].

1.1.2 Postulate 2: measurement and operators

One of the most radical departures of quantum mechanics from the classical world is that the observer becomes a central part of the description of nature. In classical mechanics, it is assumed that the physical state of a system is independent of whether it is being observed. However, quantum mechanics has a definite prescription for how observation affects a physical system.

In this thesis, I shall only consider the simplest form of measurement, the *projective*, or *von Neumann*, measurement. In this case, the observable A has the following *spectral decomposition*:

$$A = \sum_i a_i P_i \tag{1.12}$$

where $P_i = |a_i\rangle\langle a_i|$ is the *projector* onto the space with eigenvalue a_i (and eigenvector $|a_i\rangle$). The values $\{a_i\}$ are the possible outcomes of the measurement. If a system is initially in the pure state $|\psi\rangle$, then upon measurement of outcome a_i, the state of the system is projected to

$$\frac{P_i|\psi\rangle}{\sqrt{p(i)}}; \tag{1.13}$$

where $p(i) = \langle\psi|P_i|\psi\rangle$ is the probability of that outcome occurring. All physical observables have an associated Hermitian operator A, to guarantee that its eigenvalues are real (the converse is not true—there are Hermitian operators with no physical observable associated, since superselection rules often prohibit what can and cannot be measured).

A hugely important aspect of quantum mechanics is the existence of incompatible measurements. This means that there are sets of observables that any given state cannot simultaneously diagonalise. This concept is expressed through the *commutator*: if $[A, B] := AB - BA = 0$ then it is possible to simultaneously diagonalise A and B. It is this that gives rise to the *uncertainty principle*. If the 'uncertainty' in observables (given measurements on an infinite ensemble of systems identically prepared) is $(\Delta\alpha)^2 = \langle A^2\rangle - \langle A\rangle^2$ and $(\Delta\beta)^2 = \langle B^2\rangle - \langle B\rangle^2$, then

$$\Delta\alpha\,\Delta\beta \geq \frac{1}{2}\langle[A, B]\rangle\,. \tag{1.14}$$

The implication of this is that systems cannot simultaneously possess physical values of observables that do not commute. It is often asserted that there is a fundamental limit to the accuracy to which we can describe the physical world: an improvement in knowledge of A results in a decrease in knowledge of B; however, the true statement is not that we cannot observe these values with arbitrary precision, but that such precise values do not *exist*.

1.1.3 Postulate 3: unitary evolution

Schrödinger's Equation

In the case of continuous-time evolution, this postulate may be stated slightly differently, in the form of Schrödinger's Equation:

$$\mathrm{i}\hbar\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle\,, \tag{1.15}$$

where H is an Hermitian operator, and $\hbar$ is *Planck's constant*[3]. This has the solution (1.3), where $U(t_1, t_2) = \exp(-\mathrm{i}(t_2 - t_1)H/\hbar)$. There is thus a one-to-one correspondence between a

[3] $\hbar = 6.626\,19 \times 10^{-34}$ J s. It is because this constant is so small that quantum effects are negligible on the human scale. The fully classical limit of the theory can be obtained by setting $\hbar \to 0$.

continuous time evolution, and an evolution where the state is only described at the initial and final times t_1 and t_2.

The quantity H is called the *Hamiltonian*; it effectively provides a complete description of the system under consideration. Its form is not prescribed by quantum mechanics alone; in this formulation, quantum mechanics merely sets the stage on which phenomena occur, leaving the details of the physical interactions to theories such as quantum optics and quantum electrodynamics.

Quantum operations

Unitary evolutions can be combined with measurements, in the form of quantum operations. These are density matrix tranformations $\rho \rightarrow \rho' = \mathcal{E}(\rho)$ that can be written through the operator-sum representation:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger, \tag{1.16}$$

where E_k is a linear operator, and $\sum_k E_k^\dagger E_k \leq \mathbb{I}$ (where inequality means some information about the system has been obtained through measurement).

This form is often used for modelling decoherence (essentially the loss of 'quantumness') when a system interacts with an environment. In this context, the system under consideration is called *open*, whereas the unitary evolution above holds for *closed* systems.

1.1.4 Postulate 4: distinguishable particles and the tensor product

The *tensor product* is a way of joining vector spaces together into bigger spaces. As already stated, state vectors for composite systems live in such a space. One can also compose operators in this way: if an operator A acts on state $|v_1\rangle \in \mathcal{H}_1$, and B on state $|v_2\rangle \in \mathcal{H}_2$, then the overall effect is that of an operator $A \otimes B$ acting on $|v_1\rangle \otimes |v_2\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$.

It is worth noting that given a mixed state for a composite system, one can find a *reduced density matrix*, giving the best possible description of one's knowledge of that subsystem alone. This is given by the *partial trace*. Suppose two experimenters, Alice and Bob, share a state described by a density matrix ρ_{AB}; the best possible knowledge Alice could have about the system is given by

$$\rho_A = \mathrm{tr}_B \rho_{AB} \tag{1.17}$$

where tr_B denotes that the system is traced over Bob's system. The resultant matrix ρ_A is called the *reduced density matrix* of Alice's system[4].

[4]This anticipates the discussion of *entanglement* in the following Chapter: if the overall state is pure, then

Conversely to the partial trace, one can always find a *purification* to a mixed state; that is, one can find a pure state in a larger space, such that when the extra vector space is traced over, one retrieves the intial mixed state.

1.1.5 Postulate 5: indistinguishable particles and permutation symmetry

In the classical world, it is in principle possible to distinguish between every particle, and follow the dynamics of each (although computationally infeasible). For example, one could label all the balls on a pool table, and always be able to distinguish between them. However, in the quantum world, particles can be totally *indistinguishable*, with there being no possible measurements to distinguish between them (*i.e.* there is no way to physically 'label' them). Because of this, the tensor product structure is inadequate for indistinguishable particles, unless one confines the state to a particular subspace of the composite space.

Consider a set of particles at locations $\mathbf{r}_1, \cdots, \mathbf{r}_N$, described by a wavefunction $\psi(\mathbf{r}_1, \cdots, \mathbf{r}_N)$. One can define a *permutation operator* P_{ij} that performs the operation

$$P_{ij}\,\psi(\mathbf{r}_1, \cdots, \mathbf{r}_i, \cdots, \mathbf{r}_j, \cdots \mathbf{r}_N) = \psi(\mathbf{r}_1, \cdots, \mathbf{r}_j, \cdots, \mathbf{r}_i, \cdots \mathbf{r}_N); \tag{1.18}$$

i.e. it swaps the locations of particles i and j. For indistinguishable particles, one requires the overall physical wavefunction to be an eigenstate of this operator; otherwise one could use the permutation operator to distinguish between such particles. Since two applications of the permutation should bring the state back to the initial state[5], $P_{ij}P_{ij}\,|\Psi\rangle = \lambda^2\,|\Psi\rangle = |\Psi\rangle$ and thus $\lambda = \pm 1$. These eigenvalues correspond to completely symmetric ($\lambda = +1$) and antisymmetric states ($\lambda = -1$); particles with such wavefunctions are called *bosons* and *fermions*, respectively, after Satyendranath Bose and Enrico Fermi, respectively. Systems of many fermions thus have a wavefunction of the form

$$\Psi_F(\mathbf{r}_1, \cdots \mathbf{r}_N) = \frac{1}{\sqrt{N!}} \sum_{P \in S_N} \mathrm{sign}(P)\, P[\psi(\mathbf{r}_1) \cdots \psi(\mathbf{r}_N)]; \tag{1.19}$$

where the functions $\{\psi(\mathbf{r}_i)\}$ are one-particle wavefunctions; the operator P is an element of the permutation group S_N, and the sum is over all such operators. The function sign(P) gives $+1$

whether or not the reduced density matrix is pure indicates whether Alice and Bob's subsystems are separable or entangled; a separable pure state will have pure reduced density matrices, whereas an entangled pure state will have mixed reduced density matrices.

[5]This is not strictly true: it would be perfectly acceptable for two applications of the operator to introduce a global phase $e^{i\phi}$, as long as this is complemented by the presence of *superselection rules* forbidding the observation of this phase.

for even permutations, and -1 for odd permutations. The bosonic counterpart is

$$\Psi_B(\mathbf{r}_1, \cdots \mathbf{r}_N) = \sqrt{\frac{\prod_{k=1}^{\infty} n_k}{N!}} \sum_{P \in S_N} P[\psi(\mathbf{r}_1) \cdots \psi(\mathbf{r}_N)]. \tag{1.20}$$

A more convenient description of such states is the *second quantisation*. One defines *creation* and *annihilation* operators—denoted $c^\dagger$ and c, respectively—that add or remove a single particle to the system; one then replaces the above notation with the *occupation number* representation. A state of N fermions then becomes

$$|n_1; \cdots ; n_N\rangle = \prod_{k=1}^{\infty} \left(c_k^\dagger\right)^{n_k} |0\rangle\,, \tag{1.21}$$

where n_i is the occupation number of mode i (*i.e.* the number of particles in this state). Naturally for fermions (given the above definitions), n_i can only be 0 or 1. For bosons, the equivalent state is

$$|n_1; \cdots ; n_N\rangle = \prod_{k=1}^{\infty} \frac{\left(b_k^\dagger\right)^{n_k}}{\sqrt{n_k!}} |0\rangle\,. \tag{1.22}$$

It follows from the definition of these operators that they satisfy the following commutation and anticommutation relations

$$\text{fermions}: \qquad \{c_i, c_j^\dagger\} = \delta_{ij}; \tag{1.23}$$

$$\text{bosons}: \qquad [b_k, b_l^\dagger] = \delta_{kl}. \tag{1.24}$$

In both cases, the occupation of a mode is given by the *number* operator $n_k = c_k^\dagger c_k$ (or $n_k = b_k^\dagger b_k$).

1.1.6 Interactions, Hamiltonians and Lagrangians

The above formulation of quantum mechanics says nothing about forces, or the nature of any particular unitary evolution or measurement. This is because many of the ideas surrounding entanglement are independent of any particular physical implementation. Moreover, this formulation of quantum mechanics merely gives a mathematical framework; particular details of the *physics* of any given situation are left to theories such as quantum optics [19, 218], which specify the Hamiltonian (or, equivalently, the Lagrangian).

1.1.7 Further reading

An enjoyable account of the fascinating series of discoveries leading up to Einstein's 'photoelectric' paper are given in the textbook by Longair [160]. Standard introductory texts to the modern theory quantum mechanics include those by Sakurai [207] and Shankar [219], although

these mostly introduce quantum mechanics from the approach of wave mechanics. A more advanced, abstract introduction useful for the purposes of studying quantum information theory and the foundations of quantum mechanics is the insightful textbook by Peres [178]. A particularly clear introduction to the physics of indistinguishable particles is given by Gross *et al.* [99]. Contemporary introductions to quantum mechanics from a quantum information theoretic point of view are given by the excellent textbook by Nielsen and Chuang [166], and the lecture notes by Preskill [191].

Chapter 2

Entanglement

Quantum information theory promotes 'entanglement' from a paradox purpotedly highlighting the inadequacies of quantum mechanics, to a central pillar of our contemporary understanding of the natural world. In the Chapter that follows, I shall describe the historical development of our understanding of this concept, introduce from first principles the modern understanding of entanglement, discuss its quantification, and attempt to elucidate its role in the contemporary understanding of quantum mechanics and nonlocality. Its application in quantum computation and quantum information theory will be discussed in subsequent Chapters.

2.1 *Verschränkung* and 'spooky action at a distance'

The development of quantum theory in the twentieth century not only forced physicists to overhaul their scientific understanding of the world, but it also raised some uncomfortable philosophical questions. Many of the finest minds in the history of modern physics have struggled to interpret and answer these issues, and it has only been in recent years that satisfactory answers have been proposed. As Niels Bohr is reputed to have said: "anyone who is not shocked by quantum theory has not understood it"[1]. We are now, fortunately, enlightened enough to consider entanglement a resource, a concept to be embraced, but its history has certainly been problematic.

Einstein's dissatisfaction with quantum mechanics has been well-documented, and is famously encapsulated in the quote "God does not play dice"[2]. However, it was not the indeterminism of quantum theory that troubled him the most; rather, it was the position of the

[1] As quoted in Reference [245].

[2] This oft-quoted remark is paraphrased from a letter to Born in 1926: "Quantum mechanics is very impressive. But an inner voice tells me that it is not yet the real thing. The theory produces a good deal but hardly brings us closer to the secret of the Old One. I am at all events convinced that *He* does not play dice" [37].

notion of *objective reality*—or, as we shall see, lack of it—in a quantum theory. As Wolfgang Pauli states in a letter to Max Born [37], "Einstein's point of departure is 'realistic' rather than 'deterministic'". Einstein believed that every element of nature (objective reality) should have a counterpart in a complete description of nature. As recalled by Albert Pais [172, 173], "We often discussed his notions of objective reality. I recall that during one walk Einstein suddenly stopped, turned to me and asked whether I really believed that that the moon exists only when I look at it. The rest of this walk was devoted to a discussion of what a physicist should mean by the term 'to exist'".

In 1935, along with Boris Podolsky and Nathan Rosen, Einstein published a now-classic paper entitled 'Can quantum-mechanical description of physical reality be considered complete?' [73]—often simply referred to as the 'EPR paper'—in which the three authors present an argument to answer the title question in the negative: that is, quantum mechanics must be considered an incomplete theory. They start from the assumption that *every element of physical reality must have a counterpart in the physical theory*, with the following definition of 'physical reality':

> "If without in any way disturbing a system, we can predict with certainty (*i.e.* with probability equal to unity) the value of a physical quantity, then there exists an element of physical reality corresponding to this physical reality".

The central thrust of their argument is the following *Gedankenexperiment*. Imagine two particles interacting at a time $t = 0$. The particles are subsequently moved to distinct regions of space, far apart (a *space-like interval*, in the language of relativity [67, 71, 72]) and have no further contact. The overall wavefunction of the two particles may be calculated by Schrödinger's Equation.

Now suppose an experimenter with access to system I wishes to measure a physical quantity A. Using the precepts of the conventional quantum theory, the outcomes of such an experiment are given by the set of eigenvalues $\{a_i\}_i$ and the eigenvectors $\{u_i(x_1)\}_i$, where x_1 is the set of variables describing the first system. The overall wavefunction Ψ of the two systems may then be written

$$\Psi(x_1, x_2) = \sum_{n=1}^{\infty} \psi_n(x_2) u_n(x_1), \tag{2.1}$$

when considered as a function of the first system. The functions $\{\psi_n(x_2)\}$ are merely the coefficients in this expansion. It is clear that if a measurement of A gives the outcome a_k, then the state of system I becomes $u_k(x_1)$, and that of system II, $\psi_k(x_2)$. The authors describe this as the *process of reduction of the wave packet*. Likewise, if the experimenter wishes to observe a physical quantity B, with eigenvalues $\{b_i\}_i$ and eigenvetors $\{\nu_i(x_1)\}$, the state should be

written

$$\Psi(x_1, x_2) = \sum_{s=1}^{\infty} \varphi_s(x_2)\nu_n(x_1). \tag{2.2}$$

In this case, it is clear that a measurement of B with outcome b_r, will leave system I in the state $\nu_r(x_1)$, and system II in state $\varphi_r(x_2)$.

The argument then proceeds by claiming that through two different possible measurements of the state of system I, system II is left in two different possible states. But, since the two systems no longer interact after $t = 0$, no real change of system II can take place, and thus it is possible to assign two different wave functions to the same ontic reality. Furthermore, since the choice of measurement cannot (by assumption) affect system II at all, the values of the physical observables must already have had physical existence.

If the two observables A and B are chosen to be non-commuting observables (the canonical example being position and momentum, which were known to be incapable of simultaneously possessing values in the theory), then there appears to be a problem. For, by the preceding argument, they must both have had values prior to measurement; but quantum mechanics is *incapable* of endowing these quantities with simultaneous values. Therefore, quantum theory must provide an incomplete description of physical reality. As EPR put it [73]:

> "either (1) the quantum-mechanical description of reality given by the wave function is not complete or (2) when operators corresponding to two physical quantities do not commute the two quantites cannot have simultaneous reality. Starting then with the assumption that the wave function does give a complete description of the physical reality, we arrived at the conclusion that two physical quantities, with noncommuting operators, can have simultaneous reality. Thus the negation of (1) leads to the negation of the only other alternative (2). We are thus forced to conlcude that the quantum-mechanical description of physical reality given by wave functions is not complete".

Quantum theory will, according to the authors, only ever be a partial description of the natural world. This, according to Léon Rosenfeld, had a deep impact on Bohr: "this onslaught came down to us as a bolt from the blue" [205].

It is often claimed that the paper dismisses quantum theory because the collapse of the wave function must allow *instantaneous* changes at system II when system I is measured (giving rise to so-called 'spooky action at a distance'). This, however, was *not* the argument of EPR, but a central assumption; indeed, they entirely dismiss the notion of observables only possessing reality when measured:

> "This makes the reality of P and Q depend upon the process of measurement carried out on the first system, which does not disturb the second system in any way. No reasonable definition of reality could be expected to permit this".

It is only later on that this objection surfaces.

Schrödinger subsequently corresponded intensely with Einstein, resulting in the publication, in 1935 and 1936, of a series of papers [211, 212, 213] in which he introduced the term 'entanglement' (or *Verschränkung* in German) to describe the special correlations between two particles that have previously interacted. He also introduced his own paradox, which has come to be known as *Schrödinger's cat*[3]. Instead of regarding entanglement as something to be circumvented if possible, he regarded it as a central theme of the quantum theory:

> "I would not call that *one* but rather *the* characteristic trait of quantum mechanics the one that enforces its entire departure from classical lines of thought. By the interaction the two representatives (of ψ-functions) have become entangled".

He then went on to develop an idea called *quantum steering*[4], in which two experimenters (now conventionally named 'Alice' and 'Bob') share a particular quantum state, and Alice attempts to prepare a state in Bob's laboratory be performing certain operations in her own laboratory. In some sense, this can be thought of as a generalisation of the modern idea of *teleportation* [26, 130]

> "Another way of expressing the peculiar situation is: the best possible knowledge of a *whole* does not necessarily include the best possible knowledge of all its *parts*, even though they may be entirely separated and therefore virtually capable of being *best possible known*, *i.e.* of possessing, each of them, a representative of its own ... It is rather discomforting that the theory should allow a system to be steered or piloted into one of the other type of state at the experimenter's mercy in spite of his having no access to it".

This now gives rise to more objections: if one accepts that quantum theory *is* complete, and that observables have ontic reality only after observation, then an entangled pair of particles might seem to cause problems for *causality*. Specifically, if Alice performs measurements on her half of an entangled state she shares with Bob (with a space-like separation), then the collapse would appear to involve information being transferred faster than the speed of light (*superluminal signalling*). Moreover, an observer can always find a frame of reference in which the collapse of Bob's system occurs *before* Alice's measurement.

[3] A discussion of this is beyond the scope of this exposition of nonlocality!

[4] The idea of steering has been put on a modern footing by Wiseman *et al.* [248].

In March 1947, Einstein writes again to Born [37], stating that he cannot seriously believe in the quantum theory because of the *spukhafte Fernwirkungen* ('spooky action at a distance') proposed by Schrödinger. A year later, in May 1948, Born tries to persuade Einstein [37] that

> "It seems to me that your axiom of the 'independence of spatially-separated objects A and B' is not as convincing as you make out. It does not take into account the fact of coherence; objects far apart in space which have a common origin need not be independent. I believe that this cannot be denied and simply has to be accepted."

Alas, Einstein did not live to see that matter approach resolution. In the 1960s, John Bell came close to doing so [20, 21, 22] by proposing a *Gedankenexperiment* based on the spin-singlet state $|\Psi^-\rangle = (|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B)/\sqrt{2}$, building on the work of David Bohm [34, 35]. In so doing, he put the problem on a much more rigorous footing. Bell's seminal paper [20] considered what would happen if one supplemented quantum mechanics with *hidden-variables*; the values of these variables have an objective, physical existence before measurement, and the outcome of a measurement depends on some function of these variables; such a model would be called a *local hidden-variable model.*

The brilliance of Bell's work was to forget about quantum mechanics, and to ask what constraints a theory of nature should satisfy were it *realistic* (*i.e.* observables have an objective reality before observation) and *local* (*i.e.* the outcome of one experiment can in no way affect the outcome of another, if there is a space-like separation between them). In the version of his thought experiment as refined by Clauser, Horne, Shimony and Holt [60], two observers, Alice and Bob, perform measurements on a spin-singlet state as above (now invariably referred to as a Bell, EPR, or EPR–Bohm, singlet state). By considering various combinations of the outcomes, one can derive an inequality that must be satisfied by all realistic, local theories. Then, by considering *average* outcomes in quantum mechanics, one can see that the inequality is *violated*; that is, nature cannot be described by a realistic, local theory! This result was first experimentally verified by Freedman and Clauser [89], and subsequently by Aspect *et al.* [16, 15], with the conclusion[5] that quantum mechanics does not permit local hidden-variable models! This counter-intuitive result has revolutionised modern physics, and paved the way for the contemporary studies of quantum information theory and the interpetation of quantum mechanics. Indeed, Bell's theorem has been dubbed "the most profound discovery of science" [224]. The Bell–CHSH argument was subsequently tightened up by Greenberger *et al.* [96], using a beautiful thought-experiment removing the need to consider average quantities or counterfactual reasing.

[5] These experiments, all subsequent experiments, contain *loopholes*, and thus strictly, one need not accept the nonlocal, nonrealistic nature of quantum mechanics.

The resolution of the problem of the instantaneous information transfer is that *no information is transmitted*! Since the outcome of the measurements is probabilistic, this effect cannot be used to deterministically send information, as forbidden by the special theory of relativity. In a recent critique [42] of EPR, Gilles Brassard and André Allan Méthot state that EPR were correct in asserting the unreasonableness of allowing instantaneous action, and claim that their mistake was claiming that quantum theory does not provide a description of the states of sytems I and II independently: only *pure* states were given ontic existence in their study. Through the density-matrix formalism, however, one can indeed partially describe the states of sytems I and II separately. If one takes the epistemological viewpoint that the state of system II is nothing more than the density matrix describing all possible knowledge of it, one can claim that it is only when this result is communicated to the experiment at system II that this system is updated, and this information transfer is strictly limited by the speed of light[6].

Research into nonlocality continues, and there are several open problems to answer, and loopholes to close. Nevertheless, the general consensus amongst physicists is that the universe cannot be described by a local hidden-variable model, and that Schrödinger was correct that entanglement is "*the* characteristic trait of quantum mechanics". Despite this consensus, however, nonlocality and Bell's theorem continue to cause conceptual difficulties, as can be seen in the following quote from a letter from an executive director of a Californian think-tank to the then US Under Secretary of Defense for Research and Engineering, informing him of the mind-boggling implications of nonlocal correlations [165]:

> "If in fact we can control the faster-than-light nonlocal effect, it would be possible ... to make an untappable and unjammable command-control-communication system at very high bit rates for use in the submarine fleet. The important point is that since there is no ordinary electromagnetic signal linking the encode with the decoder in such a hypothetical sytem, there is nothing for the enemy to tap or jam. The enemy would have to have actual possession of the "black box" decoder to intercept the message, whose reliability would not depend on separation from the encoder nor on ocean or weather conditions ... ".

2.2 Entanglement from first principles

Before proceeding to the quantification of entanglement, and its use in quantum computation, it would be instructive to introduce the contemporary understanding of entanglement from first principles: how does it arise physically and mathematically?

[6] This is similar to the final step in the teleportation protocol [26].

Physically, when independently-prepared systems interact, their statistical independence is destroyed. The systems become 'correlated'; *i.e.* a measurement of a quantity on one system will be correlated statistically with the outcome when a (possibly different) measurement is performed on the other system (that is, given an infinite ensemble of such pairs of systems). This is as much a classical concept as a physical one; the difference lies in the degree of the correlation. As we shall see, quantum mechanics permits 'stronger-than-classical' correlations. So what is the root of this?

The postulates of quantum mechanics state that the overall state of a composite system is the *tensor* product of the states of the subsystems. This is in contrast to the classical situation, where the overall state would be a *Cartesian* product. This, coupled with the existence of *superpositions*, allows the existence of *nonseparable* pure states (*i.e.* pure states that cannot be written as a direct product of other states). This can easily be demonstrated through a simple example: imagine a composite system of subsystems A and B in a pure state. Suppose their individual states reside in Hilbert spaces $\mathcal{H}_{A,B}$, respectively. Then their overall state (according to Posulate 4) resides in a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. If system A is in a pure state $|\psi\rangle_A$, and the system B in state $|\phi\rangle_B$, the overall state is $|\psi\rangle_A |\phi\rangle_B$. However, another, perfectly valid state is the superposition $(|\psi\rangle_A |\phi\rangle_B + |\phi\rangle_A |\psi\rangle_B)/\sqrt{2}$, and one can prove that it is impossible to find vectors $|\xi\rangle_A$ and $|\chi\rangle_B$ such that this can be written as a *product state* $|\xi\rangle_A |\chi\rangle_B$. This is termed an *entangled*—or *nonseparable*—pure state.

This notion can be tightened slightly through the *Schmidt decomposition*: it can be shown that all bipartite pure states can be brought to a standard form.

Theorem 7 (Schmidt decomposition [77, 208]). *For a general bipartite state* $|\Psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$, *where* $\dim \mathcal{H}_{A,B} = d_{A,B}$ *there exists a decomposition*

$$|\Psi\rangle = \sum_{i=1}^{d} \sqrt{\lambda_i}\, |e_i\rangle \otimes |f_i\rangle\,, \quad \lambda_i \geq 0 \; \forall i \tag{2.3}$$

where $d = \min(d_A, d_B)$. *The positive coefficients* λ_i *are called Schmidt coefficients, and the number of non-zero Schmidt coefficients is called the Schmidt rank.*

Proof. This follows directly from the *singular-valued decomposition*, an important result in linear algebra [114, 166]. □

The Schmidt decomposition is an incredibly useful and powerful tool in studying many-body quantum mechanics, giving rise directly to a number of important results. It is now clear why the superposition $(|\psi\rangle_A |\phi\rangle_B + |\phi\rangle_A |\psi\rangle_B)/\sqrt{2}$ given above cannot be written as a product state: it has Schmidt rank $d = 2$. It is straightforward to see that all product states have Schmidt rank $d = 1$; the Schmidt rank is thus clearly an indicator of the presence of entanglement. It

also follows directly from the decomposition that the entanglement properties depend only on the coefficients, since these are independent of *local basis changes* (equivalent to local unitary operations). Another consequence is that the reduced density matrices of the subsystems A and B have the same eigenvalues, since the reduced density matrices are $\rho_A = \sum_{i=1}^{d} \lambda_i |e_i\rangle \langle e_i|$ and $\rho_B = \sum_{i=1}^{d} \lambda_i |f_i\rangle \langle f_i|$.

The definition of a *separable* state can be made more rigorous by considering mixed, rather than pure, states, to allow for classical uncertainty.

Definition 8 (Classically-correlated states [244]). Let ρ be the density matrix of a bipartite system $A \otimes B$. If the state can be written

$$\rho = \sum_i p_i \rho_i^{(A)} \otimes \rho_i^{(B)}, \tag{2.4}$$

where the positive quantities p_i sum to unity, and the operators $\rho_i^{(A,B)}$ are valid density operators on $\mathcal{H}_{A,B}$, then the state is said to be *classically-correlated* or *separable*. This can trivially be generalised to systems with more than two subsystems.

The naming of this state as 'classically-correlated' is justified, since the correlations in the state can be very easily simulated by a state created through the following classical procedure. Suppose Alice and Bob are in distant laboratories, with state-prèparing devices. Each device prepares a physical systems in a particular state, dependent on some input i. Imagine now that elsewhere there is a random generator, which outputs the number j with probability p_j. This number is communicated to Alice and Bob's machines, which then prepare the respective states. If one understands the density operator to describe one's ignorance of the state as much as its physical reality, then one can see that the overall description of this state (if one does not know the outcome of the random number generator) is given by the probability distribution (2.4). It can also be seen that the expectation values of observable quantities $X^{(A)}$ and $X^{(B)}$ on the respective subsystems is given by

$$\mathrm{tr}\left[\rho\, X^{(A)} \otimes X^{(B)}\right] = \sum_i p_i \,\mathrm{tr}\left[\rho_i^{(A)} X^{(A)}\right] \mathrm{tr}\left[\rho_i^{(B)} X^{(B)}\right]. \tag{2.5}$$

The outcomes and correlations thus depend solely on the random number generator, which may be a purely classical device[7]. Note that this state does not have to be prepared using a classical device, but that its statistical properties may be simulated by a system that *is* purely classical. There is a *maximally-correlated state*, with the largest possible classical correlation [195]:

$$\rho = \sum_{i,j=1}^{d} a_{ij} |ii\rangle \langle jj| . \tag{2.6}$$

[7] Even though in reality it is believed to be impossible to build a perfectly *random* number generator classically.

2.2.1 Separability criteria

Deciding whether a given quantum state (represented by a density operator ρ) is separable or not is, in general, a tough mathematical problem [131, 230]. Indeed, it has been shown by Gurvits [100, 101] that the *separability problem* is computationally intractable (more specifically, it belongs to the complexity class NP-hard, thus making it as difficult as some of the most important problems in complexity theory[8]). This result at first glance might seem quite miserable, but it is this intractability that gives entanglement some of its mystique, and provides the power of a quantum computer.

Nevertheless, many important separability criteria have been obtained. Although I shall not make use of these in this thesis, I shall briefly state for completeness the Peres–Horodecki criterion—of paramount importance for its connection with *distillability* and *negativity*—and the definition of an *entanglement witness.*

Definition 9 (Peres–Horodecki criterion [116, 179]). The partial transpose of a multipartite density matrix is given by taking the tranpose of only one of the subsystems. Given a bipartite density matrix ρ of a state shared by Alice and Bob, the elements of the density matrix after a partial transpose has been taken with respect to Alice's subsystem are given by

$$(\rho^{T_A})_{m\mu,n\nu} = \rho_{n\mu,m\nu}, \tag{2.7}$$

where Latin indices refer to Alice's subsystem, and Greek indices to Bob's. Separable states have a positive partial transpose (*i.e.* $\rho^{T_A} \geq 0$), since the partially-transposed density matrix must still be a valid density matrix; thus the existence of a positive partial transpose ('PPT') is *necessary* for a state to be separable [179]. In some cases, it is also *sufficient*: this is true for density matrices on $\mathbb{C}^2 \otimes \mathbb{C}^2$ or $\mathbb{C}^2 \otimes \mathbb{C}^3$ [116].

Definition 10 (Entanglement witnesses [116]). A density matrix ρ is entangled if and only if there exists an Hermitian operator W such that

$$\mathrm{tr}\,(W\rho) < 0, \tag{2.8}$$

where $\mathrm{tr}\,(W\rho_S) \geq 0$ for *any* separable state ρ_S.

2.3 Quantifying entanglement

As we have seen, quantum mechanics permits the existence of nonseparable states that violate local realism, and there are many criteria to decide whether a general state is separable or

[8] A discussion of the different complexity classes relevant to quantum information theory is beyond the scope of this thesis, but an introduction accessible to physicists is given in Nielsen and Chuang [166].

not. However, there are in fact degrees of entanglement: some states are *more* entangled than others.

For the case of pure states, this was hinted at by the Schmidt decomposition. Considering the reduced density matrix of one of the subsystems, one can see that Schrödinger was justified in claiming that the best possible knowledge of a system is not the sum of the knowledge of its parts; if an experimenter only holds part of an entangled system, he or she will have incomplete knowledge of the state (since the reduced density matrix of his or her subsystem will be mixed). If the overall state is such that it gives rise to reduced density matrices of maximal ignorance—so-called *maximally-mixed* states, proportional to the identity operator—then these states may be considered as having the maximum amount of entanglement possible. These states are called *maximally-entangled states*, with all Schmidt coefficients equal to $1/d$.

Definition 11 (Maximally-entangled bipartite, pure states). A state $|\Psi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is maximally-entangled if its reduced density matrices are proportional to the identity operator; *i.e.* the state may be written

$$|\Psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle \tag{2.9}$$

At the other extreme, separable pure states will have pure reduced density matrices. Of course, for mixed states the situation is considerably more complicated. Indeed, as we shall see below, there is no unique measure of entanglement!

Insights from information theory

Why should physicists concern themselves with the degree to which a particular state is entangled, other than pure curiosity? With the rise of quantum information theory and quantum computation, physicists should *certainly* be concerned with such a question; through the insights of Feynman [84, 85, 86], Deutsch and others, entanglement has come to be considered a resource, allowing the solution of nonclassical problems. The first direct link between the amount of entanglement (or at least, the *entropy*, which as we shall see, is often a measure of entanglement) and the degree to which it is useful came with Schumacher's compression theorem [140, 217, 166]. This, and other results from information theory, along with uses of entanglement, will be briefly discussed in Chapter 3: for now, I shall just discuss the quantification of entanglement.

LOCC paradigm

So how should one go about quantifying entanglement? The modern theory of entanglement has the starting point of *entanglement manipulation*: how various entanged states can interconverted by spatially-separated parties, particularly through a class of protocols called *local operations and classical communications* ('LOCC').

This spatial separation was introduced earlier, along with classically-correlated states (2.4); in this case, Alice and Bob were assumed to be in *spatially-separated* laboratories. This separation is nearly always insisted upon, even though it is not strictly necessary. There are two reasons for doing so. Firstly, it avoids confusion with the apparent nonseparability of certain states of overlapping identical, indistinguishable particles. These states are often nonseparable by virtue of the requirement of symmetric (bosonic) or antisymmetric (fermionic) total wavefunctions (Postulate 5). However, there is no way that this apparent 'entanglement' can be exploited (which is the whole aim of quantum information theory) or destroyed, since to do so would violate the postulate that the states must have 'good' symmetry. One can see that in this case that these composite states do not have a true tensor product structure (in the case of fermions, the wedge product is more approriate). By enforcing that subsystems are spatially-separated, we avoid such misconceptions, since spatially-separated laboratories are, of course, physically distinguishable. Secondly, and more pragmatically, the aims of quantum cryptography, information theory and computation often involve sharing entanglement over long distances, as a resource for communication or computation.

In systems of more than two subsystems, there are of course several ways to group the subsystems. It is therefore important to state, when quantifying entanglement, which partition that quantity is with respect to. This gives rise to different types of entanglement when three or more particles are considered, a theme that will be explored in more detail in Section 2.4. For now, I shall focus on bipartite entanglement, the discussion of which will introduce most of the key concepts without the complication of having multiple subsystems.

The requirement of spatial separation gives rise to the *LOCC paradigm*. In its simplest setting, the bipartite case, this consists of two distant laboratories, where the experimenters (usually named Alice and Bob) have access to part of a shared quantum system (see Figure 2.3). On their part of their system, the experimenters can perform *local quantum operations*, described by completely-positive maps. In addition, Alice and Bob have access to a classical communication link. It is assumed that there is no 'cost' of communicating this way (*i.e.* there is no limit to the amount of classical information they can send). Whilst in practice, of course, they could not send an infinite amount of classical information, quantum information theory is concerned with quantifying and characterisation of the solely *quantum* resource (and of course, *classical* bits cannot be used to send *quantum* bits). This paradigm was originally recognised by Charles Bennett *et al.* to be the appropriate description of entanglement manipulation, since entanglement is nonincreasing under such operations [27, 29]. Within this paradigm, many results have been obtained, relating to entanglement manipulation of single copies of pure states, asymptotic state manipulation (*i.e.* given an infinite number of specimens of a state), and mixed state manipulation. Each of these will be discussed in turn below.

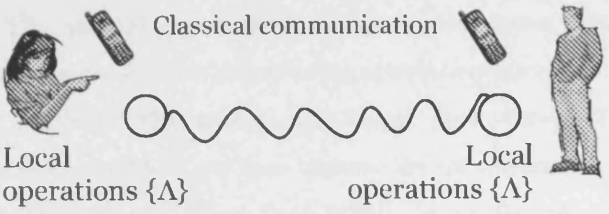


Figure 2.1: Local operations and classical communications: Alice and Bob share a quantum state described by some density matrix ρ, and have access to part of the state (denoted by the circles). They can perform local unitary or projective operations on these parts of the system, and can correlate their results through classical communications.

First, let us begin with the mathematical characterisation of such operations. Recall that the most general quantum operation is a probabilistic map

$$\rho \to \frac{\Lambda(\rho)}{\mathrm{tr}\,\Lambda(\rho)} \tag{2.10}$$

such that the trace does not increase, and the map is completely positive. That is,

$$\Lambda(\rho) = \sum_i V_i \rho V_i^\dagger. \tag{2.11}$$

The operators $\{V_i\}$ are called Kraus operators, and their domain and codomain are, in general, different. This operation takes place with probabilty $\mathrm{tr}\,\Lambda(\rho)$. If the map is trace-preserving, then the probability is equal to unity and $\sum_i V_i^\dagger V_i = \mathbb{I}$, and the map Λ is called a *quantum channel*.

Within this formalism, *local operations* can clearly be seen to have the form $\Lambda(\rho) = \Lambda_A \otimes \Lambda_B$; *i.e.* the operation is fully separable. What about classical communication? Clearly classical communication allows the outcomes to be classically-correlated, and analogously to a separable state, one can define *separable operations* as follows:

Definition 12 (Separable operations [193, 233]).

$$\Lambda(\rho) = \sum_i (A_i \otimes B_i)\,\rho\,(A_i^\dagger \otimes B_i^\dagger). \tag{2.12}$$

where $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i = \mathbb{I} \otimes \mathbb{I}$.

It was originally believed that LOCC operations are exactly the same as separable operations; it is now known that this is not the case. Bennett *et al.* gave in 1999 an example of a separable operation that requires a finite amount of quantum communcation[9]. Nevertheless, all LOCC protocols can be written as a separable operation, and such operations are useful

[9]The inequivalence of LOCC and separable operations follows from *nonlocality without entanglement* [28]; this is a mathematical quirk giving rise to the existence of global orthonormal bases that are not products of

as a tool to study LOCC, since the mathematical characterisation of LOCC is tricky [68], and moreover, LOCC protocols are a strict subset of separable operations.

There is a further ingredient that is often considered: *postselection*. This means that some possible outcomes are not considered, perhaps because the measurement performed is not complete (or 'ideal' in the language of Asher Peres [178]), or we discard some knowledge of the system. This gives rise to a *stochastic* separable operation.

Definition 13 (Stochastic separable operations [233, 193]).

$$\Lambda(\rho) = \frac{\sum_i (A_i \otimes B_i)\,\rho\,(A_i^\dagger \otimes B_i^\dagger)}{\mathrm{tr}\sum_i (A_i \otimes B_i)\,\rho\,(A_i^\dagger \otimes B_i^\dagger)}, \tag{2.13}$$

where now $\sum_i A_i^\dagger A_i \otimes B_i^\dagger B_i \leq \mathbb{I} \otimes \mathbb{I}$.

A special example of such an operation is the so-called *local-filtering operation*, which plays an important part in entanglement distillation [25, 93, 119], but which will not be discussed here. Analogously to LOCC, one can consider *stochastic LOCC* ('SLOCC'), where one performs LOCC with a certain probability.

2.3.1 Exact pure state manipulation

The question as to what degree a single pure state may be manipulated was originally considered by Lo and Popescu [159], who studied various optimal strategies for the inter-conversion of entangled states by local operations. Prior to that, all results pertained to the asymptotic limit, which will be discussed subsequently in this Chapter.

It was subsequently shown by Michael Nielsen [167] that the possibility of deterministically transforming one state to another is related to the Schmidt coefficients of those two states. A state $|\psi\rangle$ may be converted to a state $|\phi\rangle$ if and only if the nonincreasingly-ordered Schmidt coefficients $\{\lambda_j^{(\phi)\downarrow}\}$ *majorise* [30] the coefficients $\{\lambda_j^{(\psi)\downarrow}\}$; this means that for all $k \in [1, d]$ the following inequality holds:

$$\sum_{j=1}^{k} \lambda_j^{(\psi)\downarrow} \leq \sum_{j=1}^{k} \lambda_j^{(\phi)\downarrow}. \tag{2.14}$$

This statement means that the vector $\lambda^{(\phi)\downarrow}$ majorises the vector $\lambda^{(\psi)\downarrow}$, and may alternatively be denoted $\lambda^{(\psi)\downarrow} \prec \lambda^{(\phi)\downarrow}$. This result may be interpreted as stating that one state can be converted into another if and only if the subsystems of the initial state are more mixed than those of the desired target state; *i.e.* the first state is more entangled. This gives an intuitive

two local orthonormal bases—states described by such vectors cannot be distinguished by spatially-separated experimenters through LOCC! It is worth noting in passing that there is much evidence that nonlocality and entanglement are very different resources; indeed, there are states that no do not violate any Bell inequality, but may still be used for teleportation [188].

understanding of what is meant by one state being more entanged than another: here, a more entangled state is more 'powerful' in the sense that it may converted to a larger number of states than a less entangled state. Indeed, the maximally-entanged state (2.9) (with maximally-mixed subsystems) may be converted to any bipartite state, justifying its name[10]. One greatly-important consequence of the inequality (2.14) is that LOCC transformations are, in general, irreversible, since the process can only be reversed if and only if the Schmidt coefficients of the two states are equal (although, this irreversibility may be lifted in the asymptotic limit).

This result was then generalised to a strategy for converting arbitrary bipartite states by Guifré Vidal [240], who showed that the optimal probability of conversion is given by

$$P(\psi \to \phi) = \min_{k\in[1,d]} \frac{E_k(\psi)}{E_k(\phi)}, \qquad \text{where} \qquad E_k(\psi) = \sum_{j=k}^{d} \lambda_j^{(\psi)\downarrow}; \tag{2.15}$$

the quantities $\{E_k\}$ are a set of *entanglement monotones* [239], which will be discussed below, and in some sense may be considered a complete set of entanglement measures for bipartite, pure states. Further results in this direction were obtained by Jonathan and Plenio [138], including the surprising result of *entanglement catalysis*. This is the result that there are some transformations $|\psi\rangle \to |\phi\rangle$ which are impossible, but with the help of an extra state $|\xi\rangle$, the transformation $|\psi\rangle \otimes |\xi\rangle \to |\phi\rangle \otimes |\xi\rangle$ is possible! The state $|\xi\rangle$ plays a role reminiscent of that of a catalyst in chemical reactions.

2.3.2 Asymptotic state manipulation; operational measures

Of course, in realistic, physical situations (*i.e.* in the laboratory) one usually comes across mixed states. Entanglement in this setting may be considered 'noisy'. A question then naturally arising is whether this may be converted into a form of entanglement that we already understand, or is more useful. In 1996, Bennett *et al.* showed [25] that indeed it is possible to distill pure entanglement from noisy states in the asymptotic limit. At roughly the same time, Peter Shor and Andrew Steane developed *quantum error-correction*, with the aim of protecting quantum information from decoherence (which has the effect of making pure states into mixed states) [221, 225]; this was subsequently shown to be intimately related with distillation [29].

Can noisy entanglement always be distilled? In 1997, the Horodecki family showed [119] that all two-qubit states are distillable; however, in 1998, the same authors went on to prove the existence of entangled states that *cannot* be distilled [117]. Thus there are two types of entanglement: that which can be distilled, and that which cannot. The latter type is called *bound entanglement*, and gives rise to many questions relating to the fundamental nature of

[10] Majorisation may be further linked with entanglement; if a state is separable, then the density matrix of its subsystems must majorise that of the total state (*i.e.* $\lambda(\rho) \prec \lambda(\rho_A)$ and $\lambda(\rho) \prec \lambda(\rho_B)$), giving rise to the statement 'separable states are more disordered globally than locally' [168].

entanglement[11]. I shall mention here only one, which is whether bound entanglement is useful in the same sense of normal entangled states (as we shall see in the next Chapter), or whether it is just a curiosity; in fact, as shown by Lluis Masanes in 2005 [162, 163], *all* entangled states are useful for something. Thus, as suggested by the Horodecki family [122], instead of defining entangled states as nonseparable (Werner's original definition [244]), one could define them as those states that can perform some nonclassical task.

Definition 14 (Distillable entanglement, E_D). Consider a sequence of LOCC operations[12] $\{\Lambda_n\}$ acting on n input pairs in a collective state $\rho^{\otimes n}$, each in a space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, that map these states onto a state $\Lambda(\rho^{\otimes n}) \in (\mathbb{C}^2)^{\otimes m} \otimes (\mathbb{C}^2)^{\otimes m}$. We denote the set of operations $\mathcal{P}$ and call it a *protocol*; if the final state approaches m copies of the EPR singlet $|\Psi^-\rangle$, *i.e.* the fidelity

$$F\left(|\Psi^-\rangle^{\otimes m}\,,\,\Lambda(\rho^{\otimes n})\right) := \left\langle \Psi^{-\otimes m}\middle|\Lambda(\rho^{\otimes n})\middle|\Psi^{-\otimes m}\right\rangle \to 1 \tag{2.16}$$

in the limit $n \to \infty$ then we call $\mathcal{P}$ a *distillation protocol*. The distillable entanglement is defined as the supremum over all such protocols of the rate of singlets distillable in the asymptotic ($n \to \infty$) limit:

$$E_D(\rho) = \sup_{\mathcal{P}} D_{\mathcal{P}} \qquad \text{where} \qquad D_{\mathcal{P}} := \lim_{n\to\infty} \frac{m}{n}. \tag{2.17}$$

Qualitatively speaking, one may consider this quantity to measure the number of EPR singlets convertible from a given state per copy of that state, in the limit of an infinite number of copies;

Definition 15 (Entanglement cost, E_C). In the reverse situation, one may consider the amount of entanglement required (in terms of EPR singlets) to make an artibrary state. One starts from m copies of the EPR singlet $|\Psi^-\rangle$, and attempts to make n copies of a state ρ. If the output of the process is the state $\Lambda(|\Psi^-\rangle^{\otimes m})$, one requires the similarity of this state with ρ, measured again by the fidelity[13] $F(\Lambda(|\Psi^-\rangle^{\otimes m}), \rho^{\otimes n})$ tends to unity in the $n \to \infty$ limit. The cost is defined thus:

$$E_C(\rho) = \sup_{\mathcal{P}} C_{\mathcal{P}} \qquad \text{where} \qquad C_{\mathcal{P}}(\rho) := \lim_{n\to\infty} \frac{m}{n}. \tag{2.18}$$

The entanglement cost of a state may be considered the number of quantum bits an experimenter Alice needs to send to Bob in order for him to make a copy of that state [166] (in addition to LOCC). It is not known whether it is equal to the *entanglement of formation*, E_F, (an axiomatic measure, introduced below) for mixed states, although $E_F = E_C$ for pure states.

[11] The reader is referred to the review by the Horodecki family [122] and references therein.

[12] One could similarly restrict attention to PPT operations, and obtain the *PPT-distillable entanglement* [196, 197]

[13] In fact, in the case of both E_C and E_D one may equivalently use either the trace-norm, the Uhlmann fidelity or the Bures norm [194].

Transformation of general states

The notions of entanglement distillation and cost may be generalised to general asymptotic state transformations via LOCC. If Alice and Bob want to convert n copies of a state ρ to m copies of a state σ, and $F(\Lambda(\rho^{\otimes n}), \sigma^{\otimes m}) \to 1$ as $n \to \infty$ (where $\Lambda(\rho^{\otimes n})$ is the output state of their protocol), then the largest possible asymptotic ratio m/n is the rate of conversion, denoted $R(\rho \to \sigma)$; *i.e.*

$$R(\rho \to \sigma) := \sup_{\mathcal{P}} \lim_{n\to\infty} \frac{m}{n}. \tag{2.19}$$

One can then see that Equations (2.17) and (2.18) are special cases: $E_D(\rho) = R(\rho \to |\Psi^-\rangle\langle\Psi^-|)$ and $E_C = 1/R(|\Psi^-\rangle\langle\Psi^-| \to \rho)$

Reversibility and bound entanglement

The procedures of distilling entanglement from noise, and making a general state from maximally-entanged states are defined in a mutually-dual way; but are they really two facets of the same phenomenon? For pure bipartite states, the processes are reversible, and $E_C = E_D$. This reversibility is reminiscent of Carnot cycles in thermodynamics [83, 189], which seems all the more compelling when one recasts quantum mechanics in terms of accessible information, and the power to perform some nonclassical task.

Alas, these processes in general are not reversible, and the thermodynamical analogy is not quite rigorous. This is due to the existence of bound states, as mentioned above. These states require entanglement for their creation, but no entanglement can subsequently be distilled. There is a fundamental irreversibility here, the most profound consequence being the absence of a unique measure of entanglement [120, 251]. Within the thermodynamical analogy, bound entangled states can be considered as heat baths [229]: energy is needed to create the bath, but no work can be extracted from it.

Nevertheless, in the bipartite pure state (due to the non-existence of bound states), the processes are reversible. Thus one might expect that $E_C = E_D$, and the amount of entanglement is characterised by a single number. Indeed, this is true [189]. Using the thermodynamical analogy and considering the extractable mechanical work, it can be shown that for a bipartite state both quantities are equal to the *von Neumann entropy* of one of either of the subsystems.

Definition 16 (von Neumann entropy). The von Neumann entropy of a state ρ of a d-level system is defined

$$S(\rho) = -\mathrm{tr}\,\rho\log\rho = -\sum_{i=1}^{d} \lambda_i \log \lambda_i, \tag{2.20}$$

(where $\{\lambda_i\}$ are the eigenvalues of ρ), analogously to the Shannon entropy of a classical probability distribution X, $H(X) = -\sum_i p_i \log p_i$. Throughout this thesis logarithms are taken to

the base 2, which have an interpertation in terms of the number of *bits* or *qubits* that may be transmitted using classical or quantum channels.

The Schmidt decomposition (2.3) ensures that the entropy of either subsystem in a bipartite state is equal (since the density matrix eigenvalues of each part are equal). This gives rise to the definition of the *ebit* as a fundamental unit of bipartite entanglement: a subsystem of maximally-entangled qubit state has von Neuman entropy equal to unity, and thus these state may be considered a 'unit' (or even 'building block') of entanglement: a state with a von Neumann entropy $S(\rho)$ would require $S(\rho)$ singlets to be shared between Alice and Bob for its construction via asymptotic LOCC. Note that the irreversibilty in the regime of single copies implied by the majorisation criterion (2.14) is lifted when one has an infinite number of copies of states. More generally, a maximally-entangled state of dimension d has entropy $\log d$.

2.3.3 Axiomatic measures

Since there is no unique measure of entanglement, how should physicists proceed? So far, two of the entanglement measures introduced have 'operational meanings'; that is, they quantify the possibility of performing some specific task. One could invent a whole class of measures relating to such tasks. But is it possible to define generic measures?

One direction would be to consider what constraints such measures would satisfy, were they to exist. This approach was first used by Vlatko Vedral *et al.* [233, 234], who put forward a class of distance-based measures, and subsequently by Vidal [239], who proposed the idea that the only criterion required was *monotonicity*. In fact, all other reasonable criteria can be shown to follow directly from this. The definition given is quite general, and works for both bipartite and multipartite systems, although for most of the discussion below I shall focus on the bipartite case.

Definition 17 (Entanglement monotone [239]). An entanglement monotone is any scalar $\mu(\rho)$ that does not increase on average under local quantum operations.

$$\mu(\Lambda(\rho)) \leq \mu(\rho). \tag{2.21}$$

This is directly equivalent to two conditions. Firstly, the entanglement monotone cannot increase by local quantum operations (or deterministically in the case of stochastic local quantum operations); *i.e.*

$$\mu(\rho) \geq \sum_k p_k \mu(\rho_k), \tag{2.22}$$

where $p_k = \operatorname{tr} \epsilon_{ik}(\rho)$ and $\rho_k = \epsilon_{ik}(\rho)/p_k$ for some operation ϵ_{ik} performed on the ith party Secondly, the entanglement shared between Alice and Bob cannot be increased by discarding

(or 'forgetting') knowledge obtained about the system:

$$\sum_k q_k \mu(\rho_k) \geq \mu\left(\sum_k q_k \rho_k\right), \tag{2.23}$$

where $\{q_k, \rho_k\}$ is some ensemble of state such that $\rho = \sum_k q_k \rho_k$.

Together, these conditions imply that separable states have a constant value of μ, since all separable states are interconvertible by LOCC. This value must clearly be the minimal value, and can be taken to be zero, since we are only interested in differences in entanglement between states. Also note that the nonincreasing value of the monotone refers to the average; there may be operations that probabilitically increase entanglement[14], but these cannot be used to increase entanglement determinisitically.

Since any separable operation[15] may be written as a combination of local unitary operations, local von Neumann measurements, and the addition and dismissal of ancilliary particles, the condition (2.23) may be seen to be equivalent to the following more intuitive criteria: μ must be

(i) invariant under separable unitaries U

$$\mu(\rho) = \mu(U \rho U^\dagger); \tag{2.24}$$

(ii) nonincreasing under local von Neumann measurements with outcomes $\{\rho_k, p_k\}$

$$\mu(\rho) \geq \sum_k p_k \mu(\rho_k); \tag{2.25}$$

(iii) invariant under the addition of ancilliary particles Q

$$\mu(\rho) = \mu(\rho \otimes \rho_Q); \tag{2.26}$$

(iv) nonincreasing under the dismissal of part Q of the system

$$\mu(\rho) \geq \mu(\mathrm{tr}_Q \rho). \tag{2.27}$$

Optimal local conversion rates

The above list of criteria allows us to see that the conversion probability (2.15) of two bipartite, pure states as a special case of condition (2.22). Indeed, suppose Alice and Bob started with the state ρ, and wished to make the state ρ', using a LOCC strategy with outcomes $\{\rho_k\}$ with probabilities $\{p_k\}$. One of the possible outcomes is the desired state: $\rho_1 := \rho'$. Clearly

$$\mu(\rho) \geq \sum_k p_k \mu(\rho_k) \geq p_1 \mu(\rho_1); \tag{2.28}$$

[14] This is called 'gambling with entanglement' [40].

[15] Bear in mind that physically we are interested in LOCC, rather than separable, operations, but it has already been noted that for most purposes the study of separable operations suffices to give some insight into the problem; also, in this case, if a measure is a monotone for separable operations, it will be a monotone for LOCC.

from which it immediately follows that the probability of success $p(\rho \to \rho')$ is given by

$$p(\rho \to \rho') \leq \frac{\mu(\rho)}{\mu(\rho')}. \tag{2.29}$$

Therefore the maximal probablity of success for general strategies is given by

$$p(\rho \to \rho') = \min_{\mu} \frac{\mu(\rho)}{\mu(\rho')}, \tag{2.30}$$

for some choice of monotone μ. The choice of monotone that saturates the inequality (2.30) gives the optimal strategy. Conversely, the inequality indicates that there is at least one monotone that is conserved during any optimal strategy.

The study of monotones suggest that in in the nonasymptotic, exact regime of single specimens, one needs an entire family of measures to fully describe the power of the entanglement present in a state. Since we have previously considered entropic measures, the set of α-entropies might be a candidate for such a family. These quantities are a set of measures of uncertainty used in differing circumstances, of which the von Neumann entropy (2.20) is a special case. They are defined $S_\alpha(\rho) = \log \operatorname{tr} \rho^\alpha/(1-\alpha)$, and are sometimes referred to as Rényi entropies [203]. However, by considering the interconversion of several copies of states (although still a finite number of them), one can show that the entropy does not suffice to describe the entanglement properties of a state.

One attractive property of the α-entropies S_α is *additivity*. This is the property that for some state ρ, $S_\alpha(\rho^{\otimes n}) = n S_\alpha(\rho)$. Therefore, using this choice of monotone, the inequality (2.29) reads

$$p(\rho \to \rho') \leq \frac{S_\alpha(\rho^{\otimes n})}{S_\alpha(\rho'^{\otimes n})} = \frac{S_\alpha(\rho)}{S_\alpha(\rho')}. \tag{2.31}$$

Therefore, the expectation value of the number N' of copies of the target state successfully made by the protocol $\langle N' \rangle := \sum_{N'} p(\rho \to \rho') N'$ can be seen to be upper-bounded by the ratio of the entropies:

$$\frac{\langle N' \rangle}{N} \leq \frac{S_\alpha(\rho)}{S_\alpha(\rho')}, \tag{2.32}$$

where the initial number of copies is N. This has the startling implication that in general, the rate of conversion N'/N of N copies of ρ to N' copies of ρ' is *not* given by the ratio of their von Neumann entropies for finite N and N', as is the case for the asymptotic regime [25, 189] (as we saw in Section 2.3.2).

Entanglement monotones: asymptotic versus exact regimes

So what about the asymptotic limit? This regime is important, as it is the natural description for both quantum channel capacities [25] and the 'thermodynamics' of entanglement [189]. How does one reconcile the existence of a multitude of measures in the finite regime with the

unique (in the bipartite case, at least) measure—the entropy—in the asymptotic regime? This apparent problem is resolved by the addition of further requirements in the asymptotic regime: those of *partial additivity* and *continuity*.

Definition 18 (Asymptotic entanglement measure [68, 118]). In addition to the requirements to be an entanglement monotone, a good asymptotic entanglement measure must satisfy:

(i) partial additivity:

$$E(\rho^{\otimes n}) = n\,E(\rho); \tag{2.33}$$

(ii) continuity: if $\lim_{n\to\infty} \langle\psi^{\otimes n}|\rho_n|\psi^{\otimes n}\rangle = 1$, then

$$\frac{1}{n}|E(\psi^{\otimes n}) - E(\rho_n)| \to 0, \tag{2.34}$$

where ρ_n is a joint state of n pairs.

Partial additivity means that if Alice and Bob share a stationary, memoryless source, producing pairs of states ρ, then the total entanglement grows linearly with the number n of pairs produced. Plenio and Vedral [183] originally considered *full* additivity as an essential requirement: *i.e.* $E(\rho\otimes\sigma) = E(\rho) + E(\sigma)$. However, the existence of bound entanglement gives indications that the entanglement of distillation is not fully additive [121], so according to the Horodeckis' rule that 'entanglement of distillation is a good measure' (*i.e.* any postulate not satisfied by E_D should be rejected [118]), this additivity need not be imposed (in fact, a lot of measures are *subadditive*: $E(\rho\otimes\sigma) \leq E(\rho) + E(\sigma)$).

Asymptotic continuity was considered as a requirement by Vidal [239], who considered the behaviour of the family of α-entropies in the asymptotic regime, and showed that the von Neumann entropy occupies a privileged position, in agreement with Popescu and Rohrlich's result for pure states [189]. The continuity requirement allows for a completed *uniqueness theorem*, stating that for pure states, any measure of entanglement satisfying all the axioms listed above must be equal to the entanglement of formation E_F.

The Horodecki family subsequently showed that for mixed states, any measure of entanglement satisfying all these axioms lies between the entanglements of distillation and formation [118] (*i.e.* $E_D \leq E \leq E_F$). These results were further sharpened by Donald *et al.* [68].

Example of axiomatic measures

There are a whole host of axiomatic measures in the literature, constructed to give the desired properties. An exhaustive list and discussion of such measures is well beyond the scope of this thesis, but for reference I shall list a few well-known examples. For a more comprehensive list, the reader is advised to consult the review by the Horodecki family [122].

Distance-based measures—This class of measures assumes that the closer (according to some measure of 'distance') a state is to the set of fully separable states, the less entanglement it contains. Thus

$$E_D(\rho) = \inf_{\sigma \in \mathcal{S}} D(\rho, \sigma) \tag{2.35}$$

for some distance measure[16] $D(\cdot, \cdot)$, and the set of separable states $\mathcal{S}$. An important example is the *relative entropy of entanglement* [233]: $S(\rho|\sigma) = \operatorname{tr} \rho(\log \rho - \log \sigma)$, which plays an important role in quantum information theory [166].

Convex roof measures—Starting from a good measure for pure states E, one can extend it to a mixed state $\rho = \sum_i p_i |\psi_i\rangle \langle\psi_i|$ through the following:

$$E(\rho) = \inf \sum_i p_i E(|\psi_i\rangle), \tag{2.36}$$

where the infimum is taken over all ensembles that reconstruct the state ρ. All such measures are monotonic [239]. The most important measure built in this way is the *entanglement of formation* E_F, where the measure used for pure states is the von Neumann entropy of the reduced density matrix of $|\psi_i\rangle$.

Logarithmic negativity—Given a bipartite state ρ, one can calculate the partial transpose, and sum its negative eigenvalues, λ_i. This gives the negativity, $\mathcal{N} = \sum_{\lambda_i < 0} \lambda_i$ [243, 255]. This can be used to form the *logarithmic negativity*:

$$E_{\mathcal{N}} = \log \frac{\mathcal{N} + 1}{2}, \tag{2.37}$$

which is monotonic, and an upper-bound to the entanglement of distillation.

2.4 Multipartite entanglement

Entanglement in systems of many parties exhibits a vastly richer structure, due in large part to the increasing number of parameters required to describe a state fully. The notion of tripartite entanglement was first discussed in the case of $N = 3$ qubits by Coffman *et al.* [61]. It was noticed that if two parties are entangled, the degree to which either of them can be entangled to a third party is limited. Specifically, if parties A, B and C are entangled, the following holds:

$$E_{A|B} + E_{A|C} \leq E_{A|(BC)} \tag{2.38}$$

where $E_{i|j}$ is the entanglement between i, j, as measured by the concurrence-squared. The difference between the two sides of the inequality gives a quantity that cannot be accounted for

[16] Although this need not be a metric in the standard sense.

$$|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle ,$$

for $n \leq N$, then the system may be said to be n-separable; *i.e.* the parts of be separated by large distances, and there will be no entanglement between the state may be said to be *fully separable*. One may also consider what s be required to *make* a larger entangled state. If in this case each of the $|\psi_i$ more than k systems ($n \geq N/k$), then the state is 'k-producible'. If a state by $(k-1)$-party entangled states, the state is said to be genuinely k-partite

The simplest example of multipartite entanglement is the tripartite, qu shown by Dür *et al.* [70] that in this case there are two inequivalent types not producible from bipartite entanglement (*i.e.* the right-hand side of the in nonzero). These states are the Greenberger–Horne–Zeilinger state

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|0,0,0\rangle + |1,1,1\rangle);$$

and the W-state

$$|W\rangle = \frac{1}{\sqrt{3}}(|0,0,1\rangle + |0,1,0\rangle + |1,0,0\rangle).$$

The inequivalence here refers to the fact that these states may not be intercon This was shown by considering the number of parameters required to describe the number of parameters that can by changed by LOCC.

The inequality (2.38) may be generalised to more than three parties, givin degrees of residual entanglement [1]. For more than three parties, there is i number of inequivalent types of entanglement [70].

2.5 Further reading

The study of nonlocality in physics, and its connection to the interpretation chanics, continues to provoke argument, and the interested reader is directe Bub [45], Dickson [66], d'Espagnat [64], and Grib and Rodrigues [98] for a many of the philosophical issues in this area. The more general quantum me

by Peres also contains an insightful, thorough discussion [178]. The recent volume of Bell's papers on the subject (including that which introduces what we now call *Bell's theorem*) is also illuminating [22].

The study of the quantification of entanglement has also blossomed in recent years (driven by the application to quantum information theory), and there are still many open problems regarding its characterisation. Particularly clear review articles include those by Bruß [44], the Horodecki family [115, 122], and Plenio and Virmani [187]. The usual texts on quantum information also include good introductions [166, 191], particularly to 'operational measures'. The thesis by Christandl [54] also includes a thorough description of the various measures of entanglement, their relationships, and applications to information theory.

Chapter 3

Quantum information theory

In this Chapter, I shall briefly introduce some of the main concepts in the newly developed fields of quantum information theory and quantum computation. These fields provide the motivation for the study of entanglement (aside from its fundamental interest), and give rise to the concept of entanglement as a physical resource.

3.1 Simulation of physical systems; the quantum computer

As we have seen in the preceeding two Chapters, quantum mechanics provides a qualitatively different description of the physical world to classical mechanics. However, could one (in principle) simulate a quantum system through purely classical means? That is, could one build a computer operating on classical principles, that could efficiently simulate the quantum world? The answer is believed to be *no* (although this remains an unsettled matter). Whilst small quantum systems (systems of a handful of particles) can be simulated (inefficiently) on classical computers, the number of parameters required to decribe such a state grows exponentially with the number of particles. In fact, with each additional qubit added to a system in a pure state, the number of possible states doubles, rendering efficient classical simulation infeasible.

Indeed, there are some problems that are not just infeasible to solve using a classical computer, but impossible[1]. The notion of what may or may not be computed was made rigorous by Alonzo Church and Alan Turing, two pioneers of computer science. Turing proposed an abstract computer called a Turing machine; the set of problems this machine can solve is exactly the same as the set of problems one can solve through an algorithm. Moreover, there

[1] Following the work of Kurt Gödel and others, we know that the answer to Hilbert's *Entscheidungsproblem*—whether there is an algorithm to solve any problem—is 'no'.

is a universal Turing machine that can efficiently simulate any other Turing machine. In this context, 'efficiently' means that the problem is solved in a time that scales only polynomially in the length of the problem. This gives rise to the strong Church–Turing thesis: *a universal Turing machine can efficiently simulate any algorithm.* This thesis is now further strengthed to allow for a probabilistic Turing machine.

In 1985 David Deutsch attempted to discover whether or not there were systems of computation that could not be simulated by a Turing machine. And, since the universe is quantum, his starting point was quantum mechanics, and the simulability of physical systems. In the process of doing this, he introduced the universal *quantum* Turing machine[2]. It remains an open question as to whether such a device can simulate arbitrary physical systems, but its theoretical existence proved that computers built on quantum principles are in principle more powerful than standard, classical computers.

Following Deutsch's work, a handful of quantum algorithms have been discovered. These fall into two classes: those based on the quantum Fourier transform (such as Peter Shor's famous algorithm for finding prime factors, and algorithms for breaking RSA cryptography), and those based on Lov Grover's search algorithm; these offer exponential and quadratic reduction, respectively, in computational resources. The *complexity class* of problems solvable on a quantum computer remains to be seen.

3.2 Entanglement as a resource

What differentiates quantum and classical computers? While there are many unanswered issues surrounding this question, it is generally agreed that entanglement is the essential ingredient. Perhaps this is not surprising in light of Schrödinger's assertion: "I would not call that *one* but rather *the* characteristic trait of quantum mechanics" [212]. In the standard picture of quantum computers, the circuit model, the computer is initialised in a particular state, and a standard set of operations is performed on this state: single particle unitary operations, together with the *controlled* NOT operation (in the *computational basis* $\{|0\rangle, |1\rangle\}$ this is $|0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes \sigma_x$). Together, these suffice to perform any computation. In such a model, the entanglement is effectively inserted into the system through the controlled NOT operations.

A completely different, but essentially equivalent, model of computation has been developed much more recently: *measurement-based* quantum computation [198, 199, 200]. In such a model, a highly-entangled state (a *cluster state* [43]) is initially prepared, and the computation proceeds through measurements on individual qubits in various measurement bases. In this model, the role of entanglement is much clearer than in the circuit model, since one starts with a highly

[2] Quantum Turing machines were independently proposed by Benioff [23].

entangled state, and entanglement is 'consumed' during the computation.

3.3 Information theory

In parallel to developments in computer science, the twentieth century also saw considerable work on *information theory*, the theory of communication. This began in earnest in 1948 when Claude Shannon mathematically defined the notion of 'information' [220]. The concept of entropy initially arose in the fields of statistical mechanics and thermodynamics, but Shannon considered questions from the viewpoint of information theory: how much knowledge does one possess of an information source?

Definition 19 (Shannon entropy [220]). The Shannon entropy of a random variable X producing a value x_i with probability p_i is

$$H(X) = -\sum_i p_i \log p_i. \tag{3.1}$$

The interpretation of this quantity is two-fold: on the one hand, one may consider it to be the 'amount' of information one gains, on average, by measuring the value of the variable X; on the other, one may regard it as the uncertainty of one's knowledge of the value of X before a measurement is taken. Building on the first interpretation is *Shannon's noiseless coding theorem*, which states that the number of 'bits' (binary digits) required to store the value of the variable X is given, on average, by $H(X)$. This can be extended to strings of variables, giving rise to Shannon's noiseless *channel* coding theorem. Analogously, a theorem for noisy (lossy) channels also exists, and Shannon showed that the probability of error in transmitting information through such channels can be limited by error-correcting codes.

In 1995, Ben Schumacher proved *Schumacher's noiseless channel coding theorem* [217], which quantifies the amount of classical information that can be sent through a quantum channel (or equivalently, the resources required to store or send a given piece of information), and in 1996, Schumacher's noisy channel coding theorem [216], the analogous case for noisy channels[3]. These theorems give rise to the notion of a 'qubit' as the quantum counterpart of the 'bit'.

Shannon's work was built upon by Edwin Jaynes in 1957 [134, 135], who recast statistical mechanics from an information theoretic point of view. His main result (now known as *Jaynes's principle*, or the *principle of maximum entropy*) was that the physical state of a statistical ensemble is that which maximises the entropy. The work of Shannon and Jaynes paved the

[3] No such theorem is yet known for quantum information through noisy quantum channels, although quantum error correcting codes have been developed.

way for the modern way of describing the physical world in terms of what one knows of it, and what can be inferred of it.

3.4 Quantum information theory

As we have seen, two strands of thought emerged in the twentieth century unifying computer science and physics: that computation is essentially a physical process, and one should quantify the physical resources required to solve mathematical problems ('information is physical'[4]); and that physics can be considered to be a theory of our knowledge of the universe ('physics is informational' [139]). Underlying both of these ideas is the notion of *entanglement*, the fundamental departure of quantum mechanics from the classical world. It is the aim of quantum information theory to rigorously understand and quantify entanglement, much as the aim of thermodynamics in the nineteenth century was to understand energy; and it is the aim of quantum computation to harness it as a resource.

Much research effort is also being directed into quantifying the entanglement that exists naturally, and can be controlled, in naturally occuring physical systems, or those studied in condensed matter physics. The aim here is to see which physical systems can be exploited for quantum computation, and to see whether knowledge of entanglement increase one's knowledge of the physics of such situations. The research in this thesis is in this direction.

3.5 Further reading

The idea that computers operating according to quantum rules might simulate physical systems more efficiently than classical computers was developed independently by Manin and Feynman [84, 85, 86].

An excellent introduction to the ideas of the quantum Turing machine, complexity classes of problems, the circuit model, and the modern quantum algorithms is given in the textbook by Nielsen and Chuang [166], and the lecture notes by Preskill [191]. Deutsch's book [65] also contains a discussion of quantum computers. A basic introduction to computer science is the textbook by Goldschlager and Lister [94].

Further work on the link between physics and information theory was undertaken by Bennett [24], Landauer [155] and Szilard [228].

[4]This phrase was coined by Rolf Landauer.

Part II

Extraction of entanglement through dynamics

For entanglement to be useful as a resource, it needs to be shared between laboratories separated by large distances. In this Chapter, I shall propose a scheme to extract entanglement through the natural dynamics of a system of coupled three-level quantum systems. The interactions between nearest-neighbours creates entanglement, which then propogates through the system, and is extracted through local measurements.

This Chapter is based on the work in Reference [104].

Chapter 4

Creation and distribution of entanglement

In this Chapter, I shall propose a scheme that performs entanglement generation and distribution, both essential for distributed quantum computation. This system used is a graph of three-level spin systems, coupled through a permutation Hamiltonian.

4.1 Introduction

In any potential realisation of a quantum computer, or a system that performs some quantum information theoretic task, the establishment of entanglement between spatially separated systems is vitally important. To date, a great deal of research has been undertaken into performing these the creation and distribution of entanglement *separately*, *i.e.* entangling some quantum systems through some process, and then distributing those systems through some other process.

The latter aspect of this has been studied extensively in the context of *state transfer*. This is the process of moving a quantum state from one spatial location to another, without disturbing or observing it: quantum states by their very nature are fragile, and hence difficult to move without inadvertently performing a measurement. The state cannot even be observed and re-created at a distant location, since this would only be possible with an infinite number of identically-prepared systems. Such state transfer protocols usually start by initialising a spin chain in a particular state (not an eigenstate of the Hamiltonian), and then placing an additional spin at one extreme of the chain in the desired state to be transferred. At a certain time $t = 0$, the Hamiltonian is 'switched on', including a coupling between the additional spin and the end spin of the chain. After some time has elapsed, the state will have arrived at the spin at the end chain with some probability.

Imperfect state transfer in homogeneous (*i.e.* all nearest-neighbour couplings) has been studied by Sougato Bose [38] and V. Subrahmanyam [226], and it has also been shown by Daniel Burgarth *et al.* that pair of such chains permit perfect state transfer, given sufficient time [46, 47, 48]. Other schemes for perfect state transfer have been proposed, relying on engineered couplings [55, 56, 145, 169, 252], state inversion [7], graph state generation [59], multiqubit encoding [108, 171], and spin ladders [156].

Imperfect state transfer has also been studied for other systems: chains of harmonic oscillators [186], imperfect artificial spin networks [176], spin rings with flux [39] many-particle states [157], quantum dot arrays [63, 169], Josephson junction arrays [204], photons in cavity QED [57] and flying atoms [31]. Related studies have also been undertaken on the dynamical propagation of entangled states [11], the 'superballistic' distribution of entanglement [87] and the realisation of quantum memories [92, 222].

A natural corollary of state transfer is *entanglement transfer*. By transferring one half of an entangled state through such a procedure, entanglement can be established over long distances. However, such schemes say nothing about how the entanglement might be created. The ability to create *and* distribute entanglement within the same protocol would be a useful development. Such schemes have indeed been proposed for chains of harmonic oscillators (systems with continuous degrees of freedom at each lattice site) [76, 175, 177, 185]. In the context of discrete variable systems (*i.e.* spin chains), it is straightforward to see that if a single spin in a homogeneous chain of spin-1/2 systems is 'flipped' (*i.e.* its state is inverted), any other two spins in the sytem will be very slightly entangled at some subsequent time. However, this, in general, will be mixed-state entanglement, and far from maximal. Ideally, one would like to establish maximally-entangled states, enabling greater communication or computational capacity. In principle, this could be achieved by entanglement distillation [25], although this would only work perfectly in the asymptotic limit. Another possiblity, also difficult, would be to use chains with engineered couplings; that is, nearest-neighbour couplings artificially chosen to give perfect state transfer and hence perfect entanglement transfer [253]. However, these chains would be harder to produce than those with uniform couplings. So, a naturally arising question, then, is the following: is it possible to create a Bell state between spatially separated parties using chains of quantum systems with homogeneous couplings?

4.2 SU(3) permutation Hamiltonian

In this Chapter, I shall consider a spin graph-based scheme that performs *both* the conclusive creation *and* distribution of entanglement, avoiding the difficulties of interfacing systems performing these tasks separately. I shall propose a protocol, the result of which shall be that two

distant parties, Alice and Bob, share a maximally-entangled Bell state

$$|\Phi^+_{AB}\rangle = \frac{1}{\sqrt{2}}\left[|+1\rangle_A|-1\rangle_B + |-1\rangle_A|+1\rangle_B\right], \tag{4.1}$$

which may then subsequently be used for some quantum information theoretic task. I shall only consider maximally-entangled states, in order to avoid the requirement of distillation and purificiation.

Most protocols studied in the general area of state or entanglement transfer start with the Heisenberg model, given by the Hamiltonian

$$H = J\sum_{\langle i,j\rangle} \mathbf{s}_i \cdot \mathbf{s}_j; \tag{4.2}$$

where the $\mathbf{s}_i = (s_i^x, s_i^y, s_i^z)$ is the quantum spin satisfying

$$[s_i^\mu, s_i^\nu] = \mathrm{i}\epsilon^{\mu\nu\pi}s_i^\pi \qquad\qquad \mathbf{s}^2 = s(s+1). \tag{4.3}$$

When the identity operator is added to Equation (4.2), this Hamiltonian becomes the *permutation Hamiltonian*. That is, each term is a permutation operator P_{ij}, which exchanges the qubit states at lattice sites i and j: $P_{ij}|\psi\rangle_i|\phi\rangle_j = |\phi\rangle_i|\psi\rangle_j$. This Hamiltonian will be discussed in more detail in Chapter 9.

However, in this Chapter, I shall consider a graph of *qutrits* (three-level quantum objects, with states labelled $\{-1, 0, +1\}$ coupled by SU(3) permutation operators. This is a generalisation of the Heisenberg Hamiltonian (4.2). I shall consider two graphs—a cross and loop—for comparison. Let each vertex of the graph be labelled by an index $n \in [1, N]$, and let $\{S^\alpha_\beta(n)\}$ be the generators of the group SU(3) at the nth qutrit satisfying the algebra [148]

$$\left[S^\beta_\alpha(m), S^\rho_\sigma(n)\right] = \delta^m_n\left\{\delta^\rho_\alpha S^\beta_\sigma(n) - \delta^\beta_\sigma S^\rho_\alpha(n)\right\}. \tag{4.4}$$

The indices α, β refer to the states, and $S^\alpha_\beta(n)$ swaps the states labelled by α and β at vertex n. The Hamiltonian is thus [148, 201, 227]

$$H = J\sum_{\langle m,n\rangle} P_{mn}, \tag{4.5}$$

where the operator

$$P_{mn} = \sum_{\alpha,\beta} S^\beta_\alpha(m)S^\alpha_\beta(n) \tag{4.6}$$

permutes the states at vertices m and n and the sum is taken over all neigbouring vertices[1] m, n and all states α, β. An important point to note is that the generators may be given either

[1] The sign of J is unimportant, as this only sets the energetic ordering of the states—the initial state here is not an eigenstate of the Hamiltonian, and thus dynamics is the important issue.

bosonic [13] or fermionic [148] representations in terms of creation and annihilation operators according to $S^{\alpha}_{\beta}(n) = c^{\dagger}_{\alpha}(n)c_{\beta}(n)$. The physics is representation independent, giving rise to a variety of potential physical implementations: implementations of the permutation Hamiltonian will be considered in Part V.

The state of the whole system may be described in terms of basis vectors $|\psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_N\rangle$, residing in a Hilbert space of dimension 3^N, where $|\psi_n\rangle$ is the state at the nth site. However, since the Hamiltonian merely permutes states, the numbers of $+1$ and -1 excitations are individually conserved; thus one may describe the state in terms of a smaller basis. I shall here consider the case where there is always one qutrit in either of the states ± 1, and thus for convenience use the compact basis $\{|i,j\rangle\}_{i\neq j=1}^{N}$, where i,j are respectively the indices of the lattice sites where the states $+1$ and -1 reside; this basis has size ${}^{N}P_2 = N(N-1)$.

The scheme requires minimal control, requiring only the encoding of two qutrits in a pure state by a third party, Charlie (a local unitary), a local projective measurement by both Alice and Bob, and a global 'resetting' of the lattice. The scheme shares some of the advantages of the dual-rail based scheme [46, 47, 48], which, although interpretable as a single SU(3) chain, is only a scheme for transmitting quantum states or entanglement already generated. The scheme proposed here differs in that it additionally generates the entanglement during the protocol.

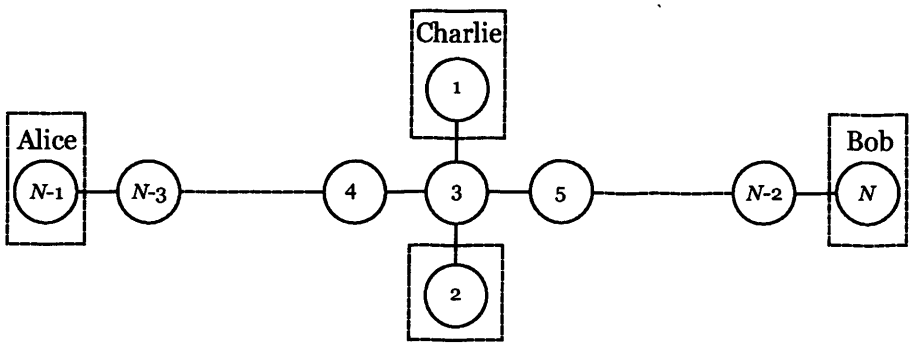


Figure 4.1: The 'cross' graph of qutrits: each circle represents a three-level quantum system with states $\{-1, 0, +1\}$, and the number inside the circle is the vertex index $n \in [1, N]$; lines between qutrits represent the permutation operator (4.6). The qutrits are numbered such that all the even indices are in Alice's arm of the graph, and all the odd indices are in Bob's arm of the cross. The rectangles show the limitations of each party's control.

4.3 Protocol: one measurement

Initially, each lattice site is set to the state $|0\rangle$. For the cross (Figure 4.2), Charlie has control of sites 1 and 2, and encodes these in the state $|+1\rangle_1 |-1\rangle_2$ (or equivalently $|1,2\rangle$ in the reduced

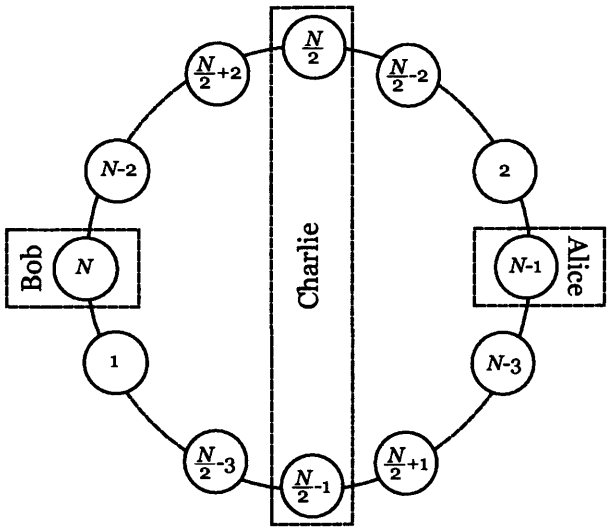


Figure 4.2: The 'loop' graph of qutrits: as before, each circle represents a qutrit, labelled n. Note that the Charlie's qutrits could be close together, with Alice and Bob separated by a large distance, or Charlie could be replaced by two distant parties, each in control of one of the qutrits $N/2$ and $N/2-1$.

basis). For the loop (Figure 4.2), Charlie has control of vertices $N/2$ and $N/2-1$ and encodes these in the similar state $|N/2, N/2-1\rangle$.

The system is then allowed to evolve under the Hamiltonian (4.5). Under this evolution—as it only swaps states of neighbouring qutrits—the system is always in a state with exactly one qutrit in $|+1\rangle$, one in $|-1\rangle$ and the remainder in $|0\rangle$. After a given time Alice and Bob perform at their respective qutrits the composite, local projective measurement

$$M = [|+1\rangle_A\langle+1|_A + |-1\rangle_A\langle-1|_A] \otimes [|+1\rangle_B\langle+1|_B + |-1\rangle_B\langle-1|_B], \tag{4.7}$$

which effectively tests for the Bell state $|\Phi^+_{AB}\rangle$, since the terms $|\pm1\rangle_A\langle\pm1|_A \otimes |\pm1\rangle_B\langle\pm1|_B$ always give null results. This allows the presence of a *global* state to be tested through *local* measurements. Each of the parentheses of M performs a *coarse-grained measurement* at either Alice or Bob's qutrit which differentiates between states $|\pm1\rangle$ and $|0\rangle$, but does not distinguish between $|+1\rangle$ and $|-1\rangle$; *i.e.* it gives the *same* eigenvalue $+1$ for *both* outcomes $|+1\rangle$ and $|-1\rangle$, while it gives a different eigenvalue 0 for the outcome $|0\rangle$. I shall not discuss precise details of such a coarse-grained measurement but only mention the fact that it is allowed by quantum mechanics[2]. After the measurement, Alice and Bob perform classical communication to compare measurement outcomes. If both have positive measurements (*i.e.* both of their mea-

[2]The precise mechanism may vary from one physical implementation of our protocol to another. In optical lattices, for example, if three internal atomic levels are being used to represent the states $|0\rangle$, $|+1\rangle$ and $|-1\rangle$, then by applying a laser of appropriate frequency and polarisation Alice or Bob can *selectively* send an atom

surements register $|\pm 1\rangle$, Alice and Bob conclusively[3] share the state (4.1); if the wavefunction in the $\{|i,j\rangle\}$ basis is $\sum_{i\neq j=1}^{N} a_{i,j}\,|i,j\rangle$ immediately before the measurement this occurs with a probability

$$p^{(1)}(t) = \frac{1}{2}\left|a_{N,N-1} + a_{N-1,N}\right|^2. \tag{4.8}$$

I have calculated numerically this probability for both the cross and the loop, for various sizes N of these. The probability is plotted against time in units of $1/J$ (Figures 4.3 and 4.4).

Results for the cross show a characteristic initial peak shortly after the state for all $N \neq 5$ (the case $N = 5$ is special due to the symmetry of the system in this case). The time at which the peak occurs would be the optimum time to measure. For the loop, there is less of a characteristic pattern, although there remains a large peak. The simplest case $N = 4$ has a periodic peak probability of $1/2$. For both graphs, the peak probability decreases with N (see Figure 4.5).

4.4 Protocol: repeated measurements I

In order to improve the probability of success, one can repeat the protocol many times until success occurs. If the peak probability of success is p, the cumulative probability after n repetitions of this protocol is

$$P(n) = \sum_{k=1}^{n} p(1-p)^{k-1}. \tag{4.9}$$

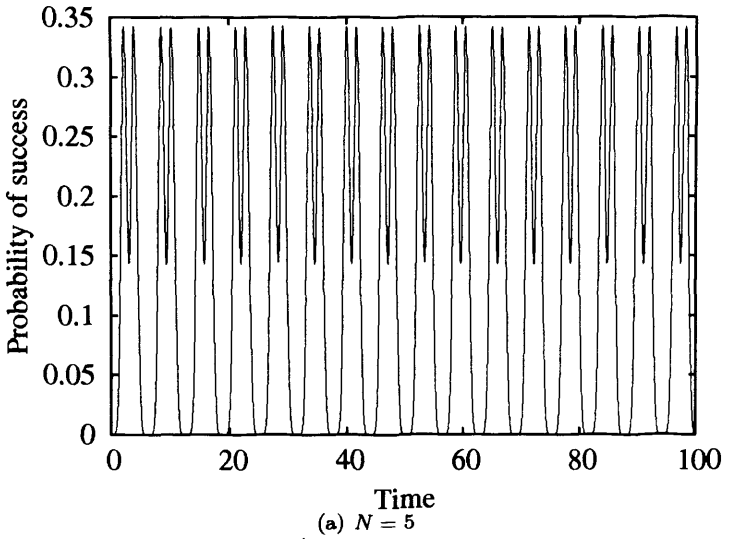
Since this is a geometric progression, it is clear that $\lim_{n\to\infty} P(n) = 1$. The question is how quickly this converges. In Tables 4.1 and 4.2 I have calculated the number of measurements required to obtain success with a probability of at least 0.90, 0.95 and 0.99 for the cross and loop respectively, when measurements are taken at the peak of the probability. In general it is clear that to obtain success with probability in excess of some q, the number of measurements n must satisfy

$$n \geq \frac{\log(1-q)}{\log(1-p)}. \tag{4.10}$$

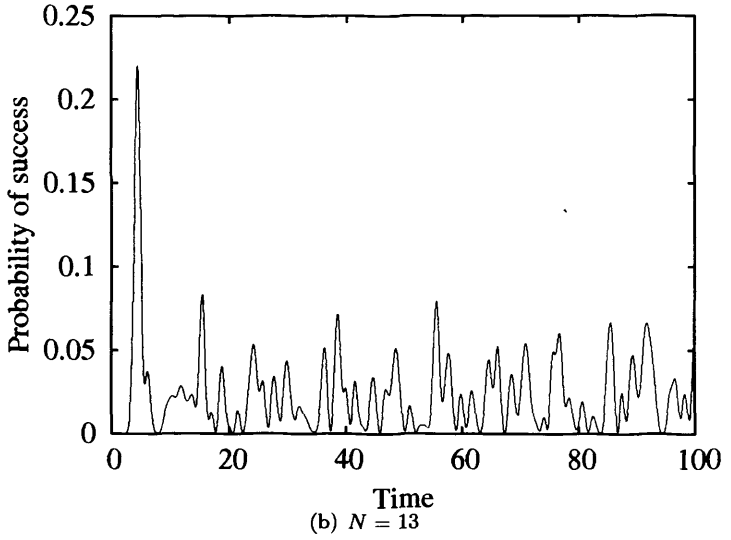
One can see that the probability of success converges relatively quickly; however, the system needs to be reset at each stage after an unsuccessful measurement. If the three levels of each qutrit are represented by hyperfine levels of atoms, with energy of atoms in $|0\rangle$ lower in a magnetic field than atoms in $|\pm 1\rangle$, then the resetting can be achieved by applying a uniform

in the state $|0\rangle$ to an unstable excited state. When this state spontaneously decays (rather immediately), the fluorescence will tell us that the atom was in the state $|0\rangle$. The absence of fluorescence would imply that the atom was in either of the states $|+1\rangle$ or $|-1\rangle$ but not reveal whether it was actually $|+1\rangle$ or $|-1\rangle$.

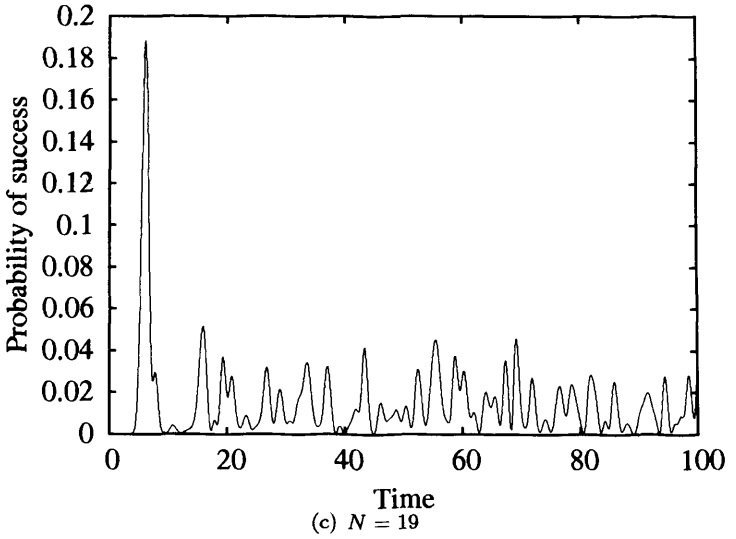
[3] In this context, 'conclusive' means that when success occurs, Alice and Bob are aware of this.



(a) $N = 5$

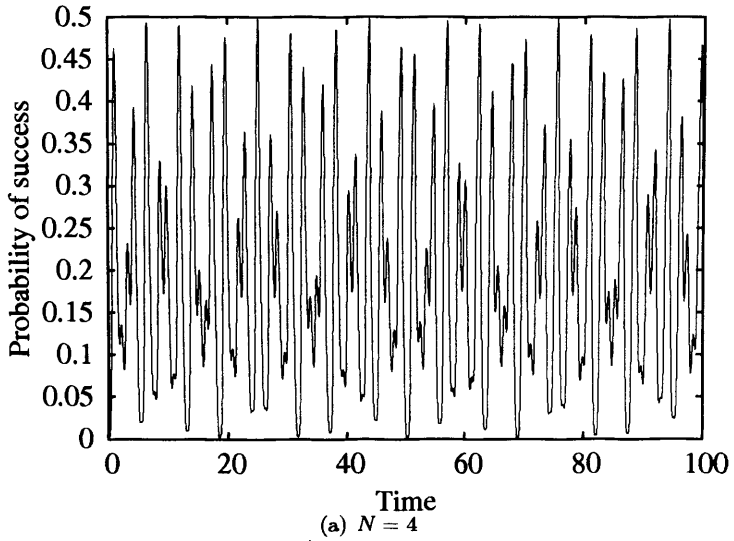


(b) $N = 13$

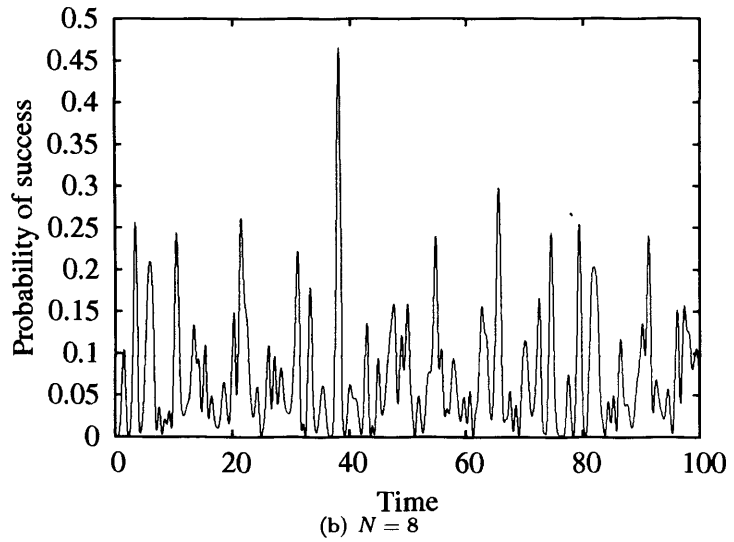


(c) $N = 19$

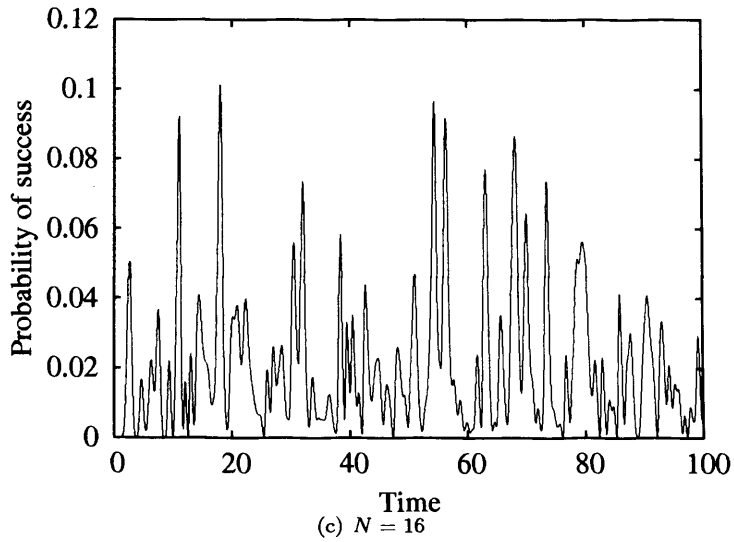
Figure 4.3: Probability of success (*i.e.* probability that measurement (4.7) results in Alice and Bob sharing a Bell state (4.1)) for various N for the cross topology



(a) $N = 4$



(b) $N = 8$



(c) $N = 16$

Figure 4.4: Probability of success (*i.e.* probability that measurement (4.7) results in Alice and Bob sharing a Bell state (4.1)) for various N for the loop topology

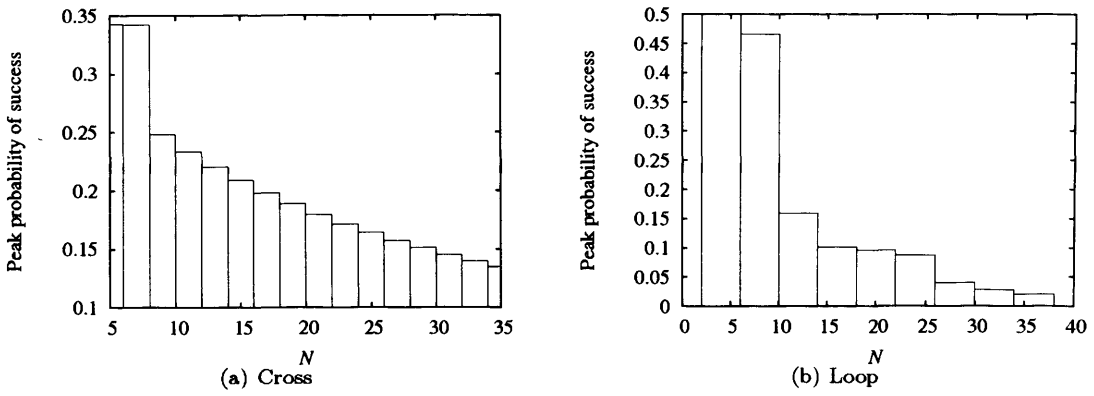


Figure 4.5: Peak probability of success as a function of N for one measurement

magnetic field to the system and bringing it to its ground state (this resetting process, of course, is not unitary). Optical pumping, as used to initialise quantum registers in optical lattices, can also be used [210]. In other physical implementations, dissipatively cooling the system to a ground state could be possible.

Note that in principle, resetting could be achieved through local actions of Alice and Bob. Upon unsuccessful measurement, Alice and Bob continue to measure periodically, and when one of them receives an excitation, he or she swaps the qutrit out of the system for a new qutrit in the state $|0\rangle$. Alice and Bob continue until two excitations have been removed in this way; they then know that the whole lattice is in the initial state.

4.5 Protocol: repeated measurements II

In order to reduce the number of times the system is reset, I shall now consider a slightly different protocol. First, let us consider in more detail what happens when the measurement (4.7) is applied. This measurement distinguishes between $|\pm 1\rangle$ and $|0\rangle$ at each site. There are thus four possible outcomes:

(i) both measurements are negative, giving the state $|0\rangle_A |0\rangle_B$, with the excitations remaining elsewhere in the system;

(ii) Alice's measurement is positive, and Bob's negative, giving one of the states[4] $|\pm 1\rangle_A |0\rangle_B$;

(iii) Alice's is negative, and Bob's positive, giving one of the states $|0\rangle_A |\pm 1\rangle_B$;

(iv) both are positive, and Alice and Bob share the state $|\Phi^+_{AB}\rangle$.

In each case, the resultant overall wavefunction will be different. If the wavefunction in

[4]The measurement cannot distinguish between these.

	N	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35
	0.90	6	6	9	9	10	10	11	12	12	13	13	14	15	15	16	16
q	0.95	8	8	11	12	13	13	14	15	16	16	17	18	19	20	20	21
	0.99	11	11	17	18	19	20	21	23	24	25	26	27	29	30	31	32

Table 4.1: Cross: number of measurements required to obtain at least the desired probability of success q for various N.

	N	4	8	12	16	20	24	28	32	36
	0.90	4	4	14	22	23	26	57	81	110
q	0.95	5	5	18	28	30	33	73	105	143
	0.99	7	8	27	44	46	51	113	161	220

Table 4.2: Loop: number of measurements required to obtain at least the desired probability of success q for various N.

the $\{|i,j\rangle\}$ basis is $\sum_{i\neq j=1}^{N} a_{i,j}\,|i,j\rangle$ immediately before the measurement, these will be for the both cross and the loop, respectively:

$$|\psi_1\rangle = \frac{\sum_{i\neq j=1}^{N-2} a_{i,j}\,|i,j\rangle}{\sqrt{\sum_{i\neq j=1}^{N-2}|a_{i,j}|^2}}; \qquad |\psi_2\rangle = \frac{\sum_{j=1}^{N-2}(a_{N-1,j}\,|N-1,j\rangle + a_{j,N-1}\,|j,N-1\rangle)}{\sqrt{\sum_{j=1}^{N-2}(|a_{N-1,j}|^2+|a_{j,N-1}|^2)}};$$

$$|\psi_3\rangle = \frac{\sum_{j=1}^{N-2}(a_{N,j}\,|N,j\rangle + a_{j,N}\,|j,N\rangle)}{\sqrt{\sum_{j=1}^{N-2}(|a_{N,j}|^2+|a_{j,N}|^2)}}; \quad |\psi_S\rangle = \frac{1}{\sqrt{2}}\left[|N-1,N\rangle + |N,N-1\rangle\right]; \tag{4.11}$$

where Alice's qutrit is at vertex $N-1$ and Bob's at N, and of course $\sum_{i\neq j=1}^{N}|a_{i,j}|^2 = 1$.

If the measurement is unsuccessful, one ends up with one of the states $|\psi_{1\text{-}3}\rangle$. Since the measurement has not totally destroyed the amplitude of the excitations existing in the system, another measurement may be taken some time later. However, it is difficult numerically to consider simultaneously the separate evolutions of the states $|\psi_{1\text{-}3}\rangle$. Since the states $|\psi_{2,3}\rangle$ are asymmetric (*i.e.* Alice and Bob do not have the same local states), let us consider taking repeated measurements on the outcome $|\psi_1\rangle$, which posseses the same symmetry at the target state and thus seems most likely that it will lead to this.

Consider now the protocol where at each measurement, if the outcomes $|\psi_{2,3}\rangle$ occur, Alice, Bob and Charlie reset all qutrits to $|0\rangle$ and start again. All possible outcomes are represented diagrammatically in Figure 4.5. It is clear that the cumulative probability of success occurring by the nth measurement without having to re-start is then

$$\bar{P}_n(t_1,\ldots,t_n) = p_S^{(1)}(t_1) + \sum_{j=2}^{n} p_S^{(j)}(t_j)\prod_{i=1}^{j-1} p_1^{(i)}(t_i) \tag{4.12}$$

for n measurements at times $t_{1\text{-}n}$. Alice and Bob's strategy should be to attempt to maximise

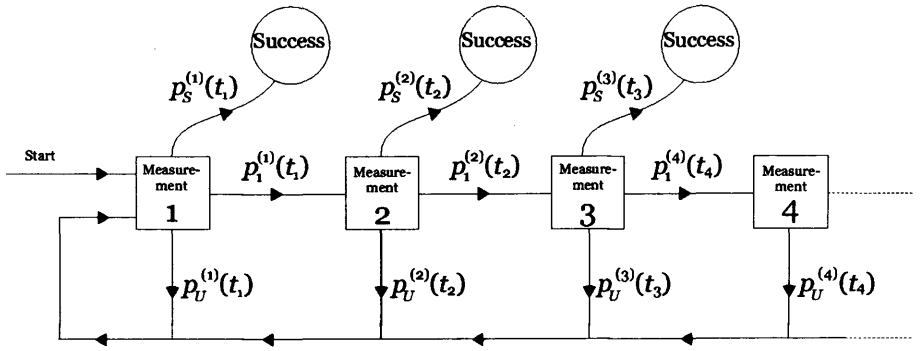


Figure 4.6: Diagrammatic representation of protocol discussed in Section 4.5. Alice and Bob's route through the diagram starts on the left. At each measurement, there are three types of outcome: success, a state $|\psi_1\rangle$ (upon which they carry on, represented by rightwards arrows), or state $|\psi_{2,3}\rangle$ (upon which they reset and start again, represented by downwards arrows).

this with respect to t_{1-n}, where $p_k^{(i)}(t_i)$ is the probability of outcome $k \in \{1, 2, 3, S\}$ at the ith measurement.

When considering only one measurement, the optimum strategy is to measure when the probability of success was at a peak. Here however, three strategies naturally present themselves when considering at what time each successive measurement should be taken:

(i) measure when the probability of success is at a peak, as above;

(ii) measure when the probability of states $|\psi_{2,3}\rangle$ is at a minimum, so we are minimising the amount of wavefunction one is 'throwing away';

(iii) measure when the difference between the probability of success and the probability of receiving the states $|\psi_{2,3}\rangle$ is maximised.

There is an important point to notice here: since one is taking measurements when the single event probability of success is at a maximum, the time of the nth measurement depends on the route taken through all the possibilities in Figure 4.5. Any problems caused by this could be rectified by taking measurements at regular time intervals, such that $t_k = k\tau$ for all k, where τ is some interval of time. However, I shall continue to optimise the probabilities at each stage according to the three strategies (i)–(iii), since taking measurements at regular intervals may cause some measurements to be taken at troughs in the success probability, thus causing the system to require more measurements.

A moment's thought should convince one that the cumulative probability of success will tend towards unity with increased number of measurements, since Alice and Bob should receive the state eventually. Let us denote single event probabilities by lower-case p's, and joint probabilities with upper-case P's. Now, one resets the state on measurement of either of the

states $|\psi_{2,3}\rangle$. The probability of receiving either of these and thus requiring re-starting at the ith measurement is $p_U^{(i)}(t_i) = p_2^{(i)}(t_i) + p_3^{(i)}(t_i)$.

The total probability of receiving the state by the n^{th} measurement is then

$$\begin{aligned} P_n(t_1,\ldots,t_n) &= \bar{P}_n(t_1,\ldots,t_n) + p_U^{(1)}(t_1)P_{n-1}(t_2,\ldots,t_n) \\ &\quad + \sum_{j=2}^{n-1}\left\{\prod_{i=1}^{j-1} p_1^{(i)}(t_i)\right\} p_U^{(j)}(t_j)P_{n-j}(t_{j+1},\ldots,t_n) \qquad (4.13) \\ &= \bar{P}_n(t_1,\ldots,t_n) + p_U^{(1)}(t_1)P_{n-1}(t_1,\ldots,t_{n-1}) \\ &\quad + \sum_{j=2}^{n-1}\left\{\prod_{i=1}^{j-1} p_1^{(i)}(t_i)\right\} p_U^{(j)}(t_j)P_{n-j}(t_1,\ldots,t_{n-j}), \qquad (4.14) \end{aligned}$$

where the last line follows from the fact that $P_{n-j}(t_{j+1},\ldots,t_n) = P_{n-j}(t_1,\ldots,t_{n-j})$. This formula for the total cumulative probability can be found iteratively, since one can find $P_{n+1}(t_1,\ldots,t_{n+1})$ from knowledge of $P_1(t_1),\ldots,P_n(t_1,\ldots,t_n)$. Note that the $\bar{P}_n$ are already known from previous numerical calculations.

For this protocol to work with arbitrary precision, one would like it be to the case that

$$\lim_{n\to\infty} P_n(t_1,\ldots,t_n) = 1. \qquad (4.15)$$

I shall give now a simple argument that this is indeed the case. Let m be the number of times the system has to be reset, and n the number of measurements taken, and make the assumption that the probability p_U of having to reset is non-zero a finite number of times, such that as $n \to \infty$, so too does $m \to \infty$. It is then possible to say that the probability of success occurring between the jth and $(j+1)$th resettings is always greater than or equal to the probability p of the initial peak, since measuring again can only increase or have no effect on the cumulative probability. This then implies

$$\lim_{n\to\infty} P_n(t_1,\ldots,t_n) \geq \lim_{m\to\infty} \sum_{k=0}^{m} p(p-1)^{k-1}, \qquad (4.16)$$

but the right-hand side of (4.16) is equal to unity, and thus (4.15) is satisfied.

I have found the quantity $P_n(t_1,\ldots,t_n)$ for various values of n and N, and found that this quantity does indeed converge to unity, but much more slowly than the simple repetition proposed in Section 4.4. For small systems though, the rate of convergence using the two protocols is comparable (see Tables 4.3 and 4.4); however, the protocol based on the conditional resetting of the system has the obvious advantage that the system does not need to be reset at each stage.

It was noted above that there was an initial peak in the success probability, after which the probability was much diminished. This peaks becomes much diminished on subsequent measurements, causing the convergence of the success probability to slow as the excitation disperses over the system.

	Protocol II			Protocol I		
Measurement	$N = 5$	$N = 7$	$N = 9$	$N = 5$	$N = 7$	$N = 9$
1	0.3429	0.3426	0.2482	0.3429	0.3426	0.2482
2	0.5294	0.5091	0.3966	0.5682	0.5679	0.4735
3	0.6667	0.5937	0.4794	0.7162	0.7160	0.6216
4	0.7620	0.6614	0.5344	0.8136	0.8133	0.7189
5	0.8280	0.7061	0.5737	0.8775	0.8772	0.7828
6	0.8741	0.7461	0.6065	0.9195	0.9192	0.8248
7	0.9066	0.7857	0.6311	0.9471	0.9468	0.8524
8	0.9301	0.8214	0.6510	0.9652	0.9649	0.8705
9	0.9478	0.8481	0.6678	0.9771	0.9769	0.8825
10	0.9608	0.8687	0.6831	0.9850	0.9847	0.8903

Table 4.3: Cross: convergence of probabilities under protocol proposed in Section 4.5 compared with simple repetition, as discussed in Section 4.4.

	Protocol II			Protocol I		
Measurement	$N = 4$	$N = 8$	$N = 12$	$N = 4$	$N = 8$	$N = 12$
1	0.4998	0.4658	0.1586	0.4998	0.4658	0.1586
2	0.7333	0.5566	0.2485	0.7498	0.7146	0.2920
3	0.8578	0.6085	0.3234	0.8748	0.8475	0.4042
4	0.9242	0.6522	0.3959	0.9374	0.9186	0.4987
5	0.9596	0.7056	0.4623	0.9687	0.9565	0.5782
6	0.9785	0.7350	0.5179	0.9843	0.9768	0.6451
7	0.9885	0.7740	0.5676	0.9922	0.9876	0.7013
8	0.9939	0.8061	0.6128	0.9961	0.9934	0.7487
9	0.9967	0.8424	0.6509	0.9981	0.9965	0.7885
10	0.9983	0.8646	0.6863	0.9990	0.9981	0.8221

Table 4.4: Loop: convergence of probabilities under protocol proposed in Section 4.5 compared with simple repetition, as discussed in Section 4.4.

4.6 Summary

I have proposed a system that performs *both* the creation *and* distribution of entanglement. These tasks are fundamental to any physical realisation of a quantum computer or quantum 'circuit', where the ability to create entanglement *in situ* without needing to interfacing different physical systems would be ideal. The protocol, for example, could be used to establish a shared Bell state between two optical lattice quantum computers or two quantum dot quantum computers without interfacing atomic systems or quantum dot systems with photons. It is also directly motivated by schemes of entanglement transfer and entanglement generation and transfer with minimal control cited in the introduction. As opposed to the previous protocols of the latter class, here we conditionally establish a perfect Bell state between Alice and Bob.

The system conclusively creates a maximally-entangled Bell state with a certain probability, which varies with the size of the lattice. This probability may be improved by repeating the measurement, or using the more complicated protocol for small lattices. Advantages of the scheme include the ability to continue to take measurements without destroying the information, and the fact that Alice and Bob test for a global state using local measurements and classical communication. The only stage that requires a global action is the resetting of the lattice, though in principle this may also be performed through local actions.

The probability of success can be slightly lower than desired, for larger lattices, but it is possible for this to tend to unity upon repetition, and it may be the case in future work that the inclusion of the states $|\psi_{2,3}\rangle$ causes the system to converge without needing to reset. With the existing protocols qutrits separated by a distance of 33 lattice sites (for a cross of $N = 35$) can share a Bell state with 90 percent probability of success in just 16 measurements. This might be a reasonable separation of two distinct quantum processors which need to be connected for greater processing power.

Part III

Extraction of entanglement from a single specimen

As we have seen in the introduction, the amount of entanglement present in a physical system is often measured with respect to the amount of entanglement one can distill from this system (i.e. the number of EPR singlets it can be converted into), in the asymptotic limit. However, in realistic, physical scenarios one often only has access to a single copy of a physical system. How much entanglement can be extracted from a single specimen? How is this related to the amount of entanglement accessible in the asymptotic limit?

In this part, I shall introduce a system for which all the entanglement present may be extracted from a single-copy in the thermodynamic limit (i.e. in the limit of a large number of subsystems), along with many of the background concepts, such as gapped and gapless spin chains, the Haldane conjecture, and the paridgmatic Affleck–Kennedy–Lieb–Tasaki spin chain.

This Chapter is based on the work published in Reference [102].

Chapter 5

Valence bond solids

In this chapter, I shall introduce the valence bond solid, the ground state of famous Affleck–Kennedy–Lieb–Tasaki Hamiltonian, which was given as the first example of a one dimensional system satisfying the famous Haldane conjecture. I shall review several background results, and discuss the recent extension of the notion of valence bond solids to matrix-product states.

5.1 1D spin chains and the Haldane conjecture

The behaviour of quantum mechanical ferro- and antiferromagnets is an incredibly important area of research for a variety of reasons. Not only do such models provide explanations of a wide variety of physical phenomena (such as magnetism and superconductivity), but provide the simplest models with which to test quantum mechanics. These models are naturally considered in condensed matter physics, but are also attracting a lot of attention from quantum information theorists looking for candidate systems for quantum computers, and to understand the entanglement that arises naturally in many common physical systems.

The simplest such system is a 'spin chain'; a one dimensional array of quantum spins localised at regular intervals. Each spin is given an index, and usually interacts with its nearest-neighbours through some Hamiltonian. The starting point for most discussion of spin chains is the *Heisenberg model*, with the Hamiltonian

$$H = J \sum_{\langle i,j \rangle} \mathbf{s}_i \cdot \mathbf{s}_j; \tag{5.1}$$

where the $\mathbf{s}_i = (s_i^x, s_i^y, s_i^z)$ is the quantum spin satisfying

$$[s_i^\mu, s_i^\nu] = \mathrm{i}\epsilon^{\mu\nu\pi} s_i^\pi \qquad\qquad \mathbf{s}^2 = s(s+1), \tag{5.2}$$

located at the lattice site with label i, and $\langle i,j \rangle$ denotes that the summation is over nearest-neighbour spins. The constant J is termed an *exchange constant*, since its physical origin is

the exchange interaction (itself arising from the electrostatic Couloumb interaction and Pauli exclusion) [33].

If the spins in Equation (5.1) were *classical* spins (*i.e.* vectors that can point in any direction), then its ground state (5.1) would be with all spins parallel for $J < 0$ (*ferromagnetic*), and nearest-neighbours antiparallel for $J > 0$ (*antiferromagnetic*). This antiferromagnetic state spontaneously breaks the spatial symmetry (since there are two ways in which it can occur), and possesses what is known as *Néel order*. For quantum spins, the true antiferromagnetic ground state is slightly different, due to quantum fluctuations (and the fact that the *Néel state* is not an eigenstate of the Hamiltonian), but the Néel state captures the essential qualitative features of the state. For the large s limit, the ground sate approaches the Néel state, since the spins become 'classical' (in the sense of the Bohr correspondence principle).

In this model, excitations are essentially described by spin-flips (*i.e.* a spin pointing in the opposite direction to that in which it would point in the ground state) 'smeared' across the chain. These are called spin waves. These are described in some detail (for both the ferro- and antiferromagnetic cases) in the review by Affleck [2]), and are a simple form of the Bethe *ansatz* [141, 142, 143, 151]. This picture predicts that the two-point correlation functions (*i.e.* quantities such as $\langle s_i^z s_j^z \rangle$) have a power-law decay, and that there are excitations with arbitrarily low energy (*i.e.* there is no gap in the energy spectrum immediately above the ground state) in the limit of an infinite chain, often referred to as the *infinite volume* or *thermodynamic* limit.

What should one expect the behaviour to be for other isotropic, one dimensional quantum antiferromagnets? One might naively expect all such systems to behave in the same manner. However, in 1983, Haldane conjectured that integer-spin antiferromagnetic Heisenberg chains have a finite gap above the ground state (and exponential decay of correlation functions), and only the half-odd-integer are gapless (and power-law decay of correlation functions) [105, 106, 107]. This has since become known as the *Haldane conjecture*. Indication of the correctness of this conjecture were given experimentally and numerically, and, in 1986, it was shown that the Lieb–Shultz–Mattis theorem [158] can be extended to all half-odd-integer systems, but fails for those with integer spin [5]. This theorem states that for spin-1/2 chains, the energy gap in the thermodynamic limit is zero.

The first example of a spin chain satisfying the Haldane conjecture were given by Affleck, Kennedy, Lieb and Tasaki [3, 4]. They proved that the ground state of the Majumdar–Ghosh Hamiltonian [161] has a gap in the energy spectrum, and it also has exponential decay of correlation functions. However, the ground state is degenerate, and the choice of ground state breaks the translational invariance of the Hamiltonian. Affleck *et al.* went on to show that there exists an antiferromagnet with exponentially decaying correlation functions, a gap in the

spectrum, a unique ground state *and* translational invariance. This is the *valence bond solid* (VBS).

The Haldane conjecture remains a conjecture, although the extension of the Lieb–Schultz-Mattis theorem mentioned above has been proved rigorously [5], and it has been shown that all gapped systems have exponentially decaying correlations [109, 111].

5.2 Valence bond solids

The valence bond solid is the ground state of the Hamiltonian

$$H = \sum_{i=1}^{N} \left[\mathbf{s}_i \cdot \mathbf{s}_{i+1} - \beta (\mathbf{s}_i \cdot \mathbf{s}_{i+1})^2 \right], \tag{5.3}$$

for the value $\beta = -1/3$. The case $\beta = 0$ is the standard Heisenberg Hamiltonian (5.1), and the case $\beta = 1$ can be solved the by Bethe *ansatz* and shown to have a unique ground state [17, 18]. This Hamiltonian for $\beta = -1/3$ is often referred to as the AKLT model, or AKLT chain, after the authors who discovered its connection with the Haldane conjecture.

Consider this Hamiltonian acting on a finite lattice of size N. At each lattice site, there is a spin of magnitude 1 (*i.e.* there are three possible spin states). The total spin of two adjacent lattice sites can add up to 0, 1 or 2. The projection of the spins i and $i+1$ on to the space of total spin S can be denoted $P_S(\mathbf{s}_i + \mathbf{s}_{i+1})$. Now,

$$P_2(\mathbf{s}_i + \mathbf{s}_{i+1}) = \frac{1}{2} \mathbf{s}_i \cdot \mathbf{s}_{i+1} + \frac{1}{6} (\mathbf{s}_i \cdot \mathbf{s}_{i+1})^2 + \frac{1}{3}. \tag{5.4}$$

Suppose one makes the Hamiltonian

$$H = \sum_{i=1}^{N} H_i \qquad\qquad H_i = P_2(\mathbf{s}_i + \mathbf{s}_{i+1}); \tag{5.5}$$

then since $H \geq 0$, if a state $|\Psi\rangle$ exists such that $H_i |\Psi\rangle = 0$ for all i, then this will be the ground state. Remarkably, such a state exists. This state is known as the valence bond solid, and can be represented in terms of 'virtual spins'. Suppose at each lattice site one places two virtual spins, each with two possible states (*i.e.* spin-1/2), maximally-entangled with the nearest virtual spin on an adjacent lattice site. At each lattice site, the two virtual spins are projected on to the totally symmetric subspace—recall that two spin-1/2 systems can be added up to a symmetric ($S = 1$) and antisymmetric space ($S = 0$). As can be seen from the diagram (Figure 5.2), there are two spin-1/2's at the extremeties of the chain, which are not part of any 'bond'. There is freedom in these spins' choice of state, and there is thus a four-fold degeneracy in the ground state of the Hamiltonian (5.3) with $\beta = -1/3$. In the thermodynamic limit, the

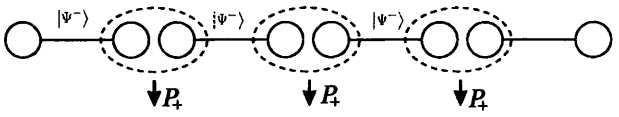


Figure 5.1: The VBS state has an interpretation in terms of 'bonds' between spins, where each bond is a maximally-entangled state of two spin-$S/2$'s, and at each bulk spin the state is projected (dotted circles) to the symmetric space of total spin.

ground state is unique. For the finite case, removing these spin-1/2's makes the final state:

$$|\Psi\rangle = \bigotimes_{k=1}^{N} P_{k,k'} \bigotimes_{i=0}^{N} |\Psi^-\rangle_{i',i+1}\,, \tag{5.6}$$

where $P_{k,k'}$ projects virtual spins k, k' on to the symmetric subspace (spanned by the Bell states $\{|\Psi^+\rangle, |\Phi^\pm\rangle\}$). This state is then the *unique* ground state of the modified Hamiltonian [80]

$$H = \sum_{i=1}^{N-1} \left[\mathbf{s}_i \cdot \mathbf{s}_{i+1} + \frac{1}{3}(\mathbf{s}_i \cdot \mathbf{s}_{i+1})^2 \right] + \pi_{0,1} + \pi_{N,N+1}, \tag{5.7}$$

where the extra terms project the end-most spin-1 and spin-1/2 onto a spin-3/2 space:

$$\pi_{0,1} = \frac{2}{3}(1 + \mathbf{s}_0 \cdot \mathbf{s}_1) \qquad \pi_{N,N+1} = \frac{2}{3}(1 + \mathbf{s}_N \cdot \mathbf{s}_{N+1}). \tag{5.8}$$

There is no problem in removing the end spin-1/2's, since their removal makes no difference in the thermodynamic limit[1]. It can be shown that the above system is gapped, and that the correlation functions in the thermodynamic limit are [3, 4]

$$\lim_{N\to\infty} \langle s_i^\mu s_j^\nu \rangle = \delta_{\mu\nu} \left(-\frac{1}{3}\right)^{|j-i|} \frac{4}{3}. \tag{5.9}$$

A further representation of this state arises if one replaces the spins with *Schwinger bosons*. In this representation, two bosonic modes are associated with each bulk spin; the 'spin' is represented by the difference in the occupation numbers of these modes. The state may then be written [14]

$$|\mathrm{VBS}\rangle = \prod_{i=0}^{N} (a_i^\dagger b_{i+1}^\dagger - b_i^\dagger a_{i+1}^\dagger)\,|0\rangle\,, \tag{5.10}$$

[1] In fact, all 'finite size effects' decay exponentially [81, 90], which makes sense in the light of Hastings's result that correlations in gapped systems always decay exponentially [109, 111].

where $a_i^\dagger$, $b_i^\dagger$ are bosonic operators, and the spin operators are defined as

$$S_i^+ = a_i^\dagger b_i \tag{5.11}$$

$$S_i^- = a_i b_i^\dagger \tag{5.12}$$

$$S_i^z = (a_i^\dagger a_i - b_i^\dagger b_i)/2 \tag{5.13}$$

with the constraint $a_i^\dagger a_i + b_i^\dagger b_i = 2S$. This representation will be discussed further in the next Chapter.

The AKLT spin chain can be extended to the case of larger spins. In this case, one replaces the EPR singlets between virtual spins with maximally-entangled states of size $S \times S$, and projects on to the space of symmetric subspace of total spin J. The chain then consists of N spins of magnitude S, with two spin-$S/2$'s at either end. In the Schwinger boson representation this is written

$$|\text{VBS}\rangle = \prod_{i=0}^{N} (a_i^\dagger b_{i+1}^\dagger - b_i^\dagger a_{i+1}^\dagger)^S \, |0\rangle \,, \tag{5.14}$$

where now $a_i^\dagger a_i + b_i^\dagger b_i = 2S$. This is the unique ground state of the Hamiltonian

$$H = \sum_{j=1}^{N-1} \sum_{J=S+1}^{2S} A_J P_{j,j+1}^J + \pi_{0,1} + \pi_{N,N+1}, \tag{5.15}$$

where the operator $P_{j,j+1}$ projects bond spins j, $j+1$ onto the (symmetric) subspace of total spin J, and the A_J are arbitrary positive coefficients. The boundary terms $\pi_{0,1}$, $\pi_{N,N+1}$ are similarly defined to project the end spin S and $S/2$ onto the total spin J subspace.

5.3 Matrix-product states; simulability

In the original AKLT papers [3, 4], Hamiltonians were constructed to give valence bond structures as the exact ground state for different dimensions and geometries. Inspired by this, Fannes *et al.* extended this formalism to the case of infinite translationally-invariant 1D systems, and termed such states *finitely-correlated states* [82]. This idea can be extended yet further to finite systems, and those without translational invariance, through the notion of *matrix-product states* (MPS) [181, 241]. This class of states provides a neat representation of many states naturally arising in both condensed matter and quantum information theory, and can often be used to efficiently describe such a state *classically*. I shall follow the notation of Reference [181].

Consider a general multipartite state $|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}$, describing a 1D array of N quantum systems, each with d states (*i.e.* there is a d dimensional Hilbert space at every lattice site). At every lattice site, two 'virtual spins' are assigned, each of dimension D. Each virtual spin shares a maximally-entangled state (unnormalised) $|I\rangle = \sum_{\alpha=1}^{D} |\alpha, \alpha\rangle$ with the nearest virtual spin

on an adjacent lattice site. This is called a *bond*, and D the *bond dimension*. In an analogous manner to the VBS state, a projection operator is applied at every lattice site (or 'bulk spin'):

$$A = \sum_{i=1}^{d} \sum_{\alpha,\beta=1}^{D} A_{i,\alpha,\beta} |i\rangle \langle \alpha, \beta| . \tag{5.16}$$

Greek indices are used for the virtual systems, Roman indices for the bulk systems. Identifying $A_{i,\alpha,\beta}$ as the component $\langle \alpha | A_i | \beta \rangle$ of the matrix A_i, one can see that repeated application of this map at adjacent lattice sites gives

$$|\psi\rangle = \sum_{i_1,\cdots,i_N=1}^{d} \mathrm{tr}\left[A_{i_1} \cdots A_{i_N}\right] |i_1, \cdots, i_N\rangle . \tag{5.17}$$

In general, the bond dimension can vary from bond to bond, and the projection matrix can also vary. Allowing for site-dependent maps $A_i^{[k]}$ of size $D_k \times D_{k+1}$ corresponding to site k and bond dimensions D_k and D_{k+1}, one obtains the most general form of a matrix-product state[2]:

$$|\psi\rangle = \sum_{i_1,\cdots,i_N=1}^{d} \mathrm{tr}\left[A_{i_1}^{[1]} \cdots A_{i_N}^{[N]}\right] |i_1, \cdots, i_N\rangle .. \tag{5.18}$$

As an example of an MPS representation, one can see clearly that the spin-1 valence bond solid (5.6) is represented in this form by the matrices [231]

$$A_1 = \sigma^z \qquad A_2 = \sqrt{2}\sigma^+ \qquad A_3 = -\sqrt{2}\sigma^- . \tag{5.19}$$

Part of the difficulty of simulating the dynamics (or even calculating ground state properties) of a many-body system in condensed matter physics is that the number of parameters requried to describe the state grows exponentially with the number of constituent systems in the overall state. This, of course, is what gives a quantum system the potential to act as a quantum computer, since it has the potential to store a much larger number of parameters than a classical device. However, many quantum systems can be efficiently simulated by a classical device, and knowing when this is possible is useful for two reasons: first, it allows physicists to easily calculate expectation values of certain properties of such systems; and second, it gives some insight in to what properties of states make them amenable to being a resource for quantum computation.

Indeed, the main motivation behind the introduction of MPS was to be able to efficiently describe the low-energy dynamics of certain Hamiltonians with small-range interactions. All multipartite states can be represented in the form (5.18) if one allows for large enough bond dimensions; if the bond dimension D grows only polynomially with the number of subsystems N, then one can efficiently simulate the dynamics and properties of this system with a classical device, and exactly calculate various properties of the state. Fortunately, many of states of

[2] A given representation is not neccessarily unique, although there is often a canonical form [181].

interest in condensed matter theory have such a representation, including the ground states of various physically interesting Hamiltonians. MPS thus provide a powerful tool with which to study various 1D systems, and it turns out that it is very easy to calculate certain global properties to a reasonable accuracy (although not, of course, entanglement).

These states can be used to represent ground state of various physical systems [236] (particularly gapped systems, but also some critical systems), are a suitable variational basis for the highly successful *density matrix renormalisation group* technique [209, 246, 247], and can be extended to two or more dimensions (as *projected entangled pair states*—PEPS [129, 180]). The computational complexity of finding MPS and PEPS, and their computational power has also been extensively studied [214, 215], and *stabilizer states* are known to have an interpretation in terms of a valence bond solid [58, 235]. In fact, the study of MPS, DMRG and PEPS is a flourishing field, and it would be impossible to provide a comprehensive summary of their various uses.

5.4 Entanglement properties of valence bond solids; area laws

The entanglement naturally present in the ground states of various physics systems is of great interest. There are several ways this can be investigated. One is to calculate the entanglement between two spins in a spin chain; this is nearly always a mixed state, and must be quantified through a quantity such as negativity. Another is to calculate how much entanglement can be 'localised' between certain spins by performing local measurements on the remaining spins (this gives rise to the notion of *localisable entanglement*[3], which I shall consider in Chapter 8). However, the most common way is to calculate the *block entropy* (see figure 5.4).

The ideal situation for quantum information processing is to possess an entangled *pure* state; thus the best way to 'use' the entanglement present in the ground state of a physical system is to bipartition the system, and measure the bipartite entanglement present. Since one is usually interested in the thermodynamic limit, the system is normally bipartitioned into a block in the middle of the chain, and the remainder (see Figure 5.4). Since the state should be pure, the *block entropy*, should be equal to the entanglement of the block with the remainder, because of the Schmidt decomposition (2.3). This idea can be extended to lattice systems in two or more dimensions; indeed, an early motivation for the study of block entropies was the discovery that the entropy of a black hole scales with the surface area of the event horizon (approximately one bit of information per Planck area) [36, 41, 113, 223]. This is called an *area law*. Whether

[3]This quantity has been calculated for deformed AKLT chains by Verstraete *et al.* [237].

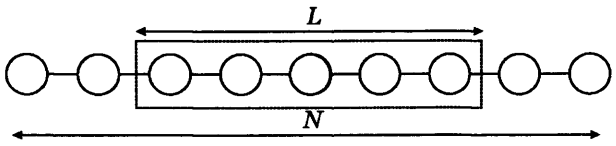


Figure 5.2: The *block entropy* measures the entanglement of a block (typically of size L) with the remainder of the chain (typically of length N). A more useful partitioning from the point of view of entanglement distribution might be to 'cut' the chain in half, and then to give either half to distant experimenters, Alice and Bob. However, partitioning the system into a block and the remainder is useful from a mathematical point of view; one can consider the scaling of the block and the chain separately, without having to worry about the effects of having 'half-infinite chains'. The single-copy entanglement considered here is measured with respect to this partitioning of the system.

or not the zero temperature entropy (*i.e.* the entanglement) of a block of a two dimensional spin lattice also scales with the area is thus an interesting question (it is believed that most quantum states exhibit a volume scaling [249]).

In fact, gapped systems do indeed satisfy an area law; the leading term in the entropy is proportional to the 'area' of the boundary between the two regions. This can be understood as being related to the number of EPR singlets 'cut' by the partitioning [8, 53]. For the case of 1D systems, this is of course a constant. The block entropy thus saturates to a constant bound as the length of the chain and block increase (the area law holds in the thermodynamic limit) [80, 144, 181, 242]. Indeed, the scaling of the Rényi entropy is given by [52, 137, 146, 147, 242]

$$S_\alpha(\rho_L) \sim \frac{c}{6}\left(1+\frac{1}{\alpha}\right)\log\xi, \tag{5.20}$$

where ρ_L is the reduced density matrix of a block of length L, and ξ is the correlation length. In the gapless case, the block entropy violates the area law by a logarithmic correction:

$$S_\alpha(\rho_L) \sim \frac{c}{6}\left(1+\frac{1}{\alpha}\right)\log L; \tag{5.21}$$

i.e. the entropy diverges logarithmically with the block length, although this is still exponentially smaller than one would expect for most quantum states.

Area laws [62, 110, 184, 249] indicate that the correlations in a system are very short-ranged, and that the entanglement is somehow 'localised' around the boundary between regions[4]. Since gapped quantum systems have markedly short-ranged entanglement, the area laws hold particularly accurately in this case; gapless systems can have slightly longer correlation lengths,

[4]This (heuristic) argument has recently been made rigorous by considering the *mutual information* between two regions in a system [249].

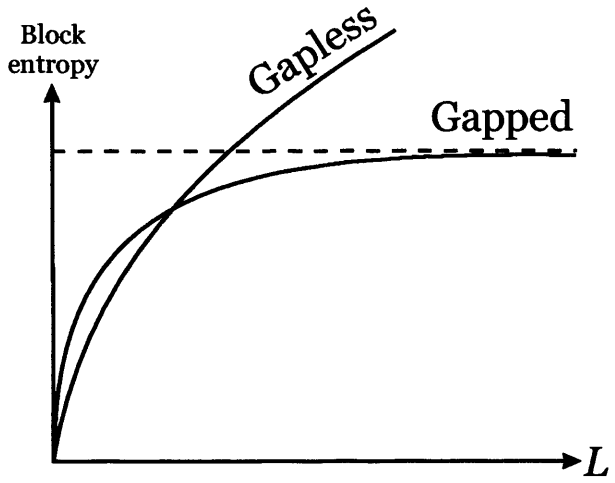


Figure 5.3: Scaling of block entropy: for *gapped* systems, the block entropy scales to a constant bound related to the number of singlets 'cut'; for *gapless* systems, it diverges logarithmically with the length of the block.

and thus the area law is slightly violated, as above. In fact, the existence of a strict area law in a given 1D system indicates the existence of an efficient matrix-product representation of that system [249], and the short correlation lengths in gapped systems explains why they are so amenable to simulation as MPS.

Chapter 6

Single-copy entanglement

In this chapter, I shall review the formal definition of the single-copy entanglement, along with results obtained by others relating to critical, gapless spin systems. I shall then show that for the AKLT chain, the single-copy entanglement is equal to the von Neumann entropy in the thermodyamic limit. That is, all the entanglement present (according to the asymptotic measure) may be distilled from a single specimen of the chain.

6.1 Introduction

As we have seen in the previous chapter, an important quantity in many-body system is the *block entropy*. This is equal to the entanglement between the block and the remainder of the system in the asymptotic limit. Of course in realistic, physical situations one might only have access to a single specimen of a particular system, and the von Neumann entropy in this case gives merely an upper bound to the distillable entanglement. An interesting question then arising is how much entanglement can be deterministically distilled from a single-copy of a system.

As mentioned in Chapter 2, the entanglement of a single specimen has been considered before, in terms of the types of state another can be converted to via LOCC. Nielsen's majorisation theorem (2.14) gives a rigorous criterion for the possibility of conversion of a pure state $|\psi\rangle$ to another pure state $|\phi\rangle$. However, only recently was the distillable entanglement in the exact regime formally defined. In the asymptotic limit, this is defined as the number of maximally-entangled states one can distill; analogously, Jens Eisert and Marus Cramer [75], and Roman Orús *et al.* [170] defined the *single-copy entanglement* as the number of EPR singlets deterministically distillable from a single specimen of a given system. They further showed that for gapless quantum spin chains close to criticality this is exactly half the von Neumann

entropy: that is, *half the entanglement present may be distilled in a single process*[1].

However, a large class of spin chains of interest are *gapped.* These have substantially different entanglement properties, as mentioned in the previous chapter. It would therefore be interesting to know whether gapped chains also exhibit different behaviour in the context of single specimens. While this remains an open problem in general, I shall in this chapter provide an example giving indications that this is indeed the case. Specifically, I shall show that the celebrated spin-S AKLT chain [2, 3, 4] introduced previously has a single-copy entanglement *equal* to the von Neumann entropy for all S; *i.e. all the entanglement present in the spin chain may be distilled in a single process.*

Definition 20 (Single-copy entanglement [75]). The single-copy entanglement (with respect to a particular bipartition) is defined [75] as the maximal number of singlets one can deterministically distill from a single-copy of a specimen in a single process; *i.e.* the single-copy entanglement is $E_1 = \log M$, if M is the largest m for which the transformation

$$\rho \longrightarrow |\psi_m\rangle \langle\psi_m| \tag{6.1}$$

is possible under local operations and classical communication with unit probability (where $|\psi_m\rangle = \sum_{i=1}^{m} |i,i\rangle / \sqrt{m}$, the maximally-entangled state of dimension $m \times m$)[2]. Applying Nielsen's majorisation criterion (2.14) to a bipartition of a spin-S chain into a block of length L and the remainder, this holds if and only if

$$\sum_{k=1}^{K} \alpha_k^{\downarrow} \leq \frac{K}{M} \qquad \text{for all} \qquad K \in [1, M], \tag{6.2}$$

where $\{\alpha_1^{\downarrow}, \cdots, \alpha_{(2S+1)^L}^{\downarrow}\}$ are the nonincreasing eigenvalues of the reduced density matrix of the block of length L. As pointed out by Eisert and Cramer [75], this is contained within the stronger criterion that $\alpha_1^{\downarrow} \leq 1/M$; *i.e.* the majorisation reduction of the $(2S+1)^L$-level system (the block) must be at least as mixed as the reduced density matrix of one half of the $M \times M$ maximally-entangled state. One can then define the single-copy entanglement

$$E_1(\rho) = \log \left\lfloor 1/\alpha_1^{\downarrow} \right\rfloor = -\log \alpha_1^{\downarrow}. \tag{6.3}$$

Note that this may alternately be found from the α-entropy (also called the Rényi entropy) $S_\alpha(\rho) = \log \operatorname{tr} \rho^\alpha / (1-\alpha)$ by taking the limit $\alpha \longrightarrow \infty$ [203] (by allowing α to take many values, this may be used as a class of entanglement monotones—called the α-entropies—with the desired additivity properties [122]).

[1] The single-copy entanglement has also been studied recently by Peschel and Zhao [182], and Zhou *et al.* [254].

[2] A maximally-entangled state of two M-level systems is equivalent to $\log M$ qubit singlets, as these have the same Schmidt decomposition [159].

6.2 Critical, gapless systems

Using the tools of conformal field theory, Orús *et al.* found that for all translationally-invariant quantum spin systems that can be mapped onto an isotropic, quadratic system of fermions (via the Jordan–Wigner transformation), the single-copy entanglement of a block of length L is exactly *half* the von Neumann entropy in the thermodynamic ($L \to \infty$) limit: both logarithmically diverge with L [170]. Explicitly,

$$E_1(\rho_L) = \frac{c}{6} \ln L - \frac{c}{6} \frac{\pi^2}{\ln L} + O(1/L), \tag{6.4}$$

where c is the conformal field theoretic central charge.

6.3 Non-critical, gapped systems

As we saw in the previous chapter, it is known that for gapped systems, the block entropy saturates to a constant bound [80, 144, 181, 242]. This qualitatively different behaviour of the entropy suggests that the single-copy entanglement might also have substantially different behaviour in gapped systems. As a first step in obtaining a general statement regarding gapped systems, it would be instructive to consider the VBS ground state of the AKLT chain, the first example of a chain satisfying the Haldane conjecture [2, 3, 4], and introduced in the previous chapter. To perform this calculation, I shall use the Schwinger boson representation.

6.4 Coherent spin state approach to the VBS

The ground state of the spin-S AKLT chain (5.15) may be written in the *Schwinger boson representation* [14] as

$$|\text{VBS}\rangle = \prod_{i=0}^{N} (a_i^\dagger b_{i+1}^\dagger - b_i^\dagger a_{i+1}^\dagger)^S |0\rangle , \tag{6.5}$$

where $a_i^\dagger$ and $b_i^\dagger$ are bosonic creation and annihilation operators, and the spin operators are defined as

$$S_i^+ = a_i^\dagger b_i \tag{6.6}$$

$$S_i^- = a_i b_i^\dagger \tag{6.7}$$

$$S_i^z = (a_i^\dagger a_i - b_i^\dagger b_i)/2 \tag{6.8}$$

with the constraint $a_i^\dagger a_i + b_i^\dagger b_i = 2S$ (where S is the spin eigenvalue given by $\mathbf{S}^2 = S(S+1)$). This representation effectively replaces spins of largest eigenvalue S with two bosonic modes,

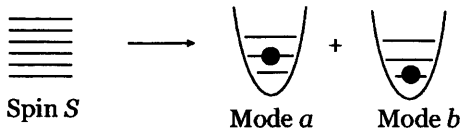


Figure 6.1: Schwinger boson representation: each spin of magnitude S is replaced by two bosonic modes. Half the difference in the occupation of these modes gives the z-component of spin, S_z.

whose collective state encodes the spin (see Figure 6.4). The eigenstates of the spin operators $\mathbf{S}^2$ and S_z are then given by (see the Appendix for more details)

$$|S,m\rangle = \frac{(a^\dagger)^{S+m}(b^\dagger)^{S-m}}{\sqrt{(S+m)!(S-m)!}}\,|0\rangle\,, \tag{6.9}$$

An alternative representation of state (6.5) is given in terms of *coherent spin states*, the less well-known relative of the *coherent oscillator states* often studied in quantum optics [19, 218] and considered the most 'classical' of quantum states. The coherent oscillator state is defined to be an eigenstate of the bosonic annihilation operator a; analogously, the coherent spin state is defined as an eigenstate of the spin raising operator S^+ [192] as

$$|\theta,\phi\rangle = \frac{1}{(1+|\mu|^2)^{2S}}\exp(\mu S^-)\,|S,S\rangle\,, \tag{6.10}$$

where $|S,m\rangle$ is the spin state with $\langle\mathbf{S}^2\rangle = S(S+1)$ and $\langle S_z\rangle = m$, and μ is a complex number. Parametrising this with $\mu = \mathrm{e}^{\mathrm{i}\phi}\tan(\theta/2)$ gives

$$|\theta,\phi\rangle = \sum_{m=-S}^{S} u^{S+m}v^{S-m}\sqrt{\binom{2S}{S+m}}\,|S,m\rangle\,, \tag{6.11}$$

where $(u,v) := (\mathrm{e}^{\mathrm{i}\phi/2}\cos(\theta/2)\,,\ \mathrm{e}^{-\mathrm{i}\phi/2}\sin(\theta/2))$. This state has a clear geometric interpretation: the state $|\theta,\phi\rangle$ may be represented by the unit vector $\mathbf{\Omega} = (\theta,\phi)$ (*i.e.* a point on the unit sphere). Therefore the overlap between two such states may be found geometrically to be

$$\langle\theta,\phi|\theta',\phi'\rangle = \left[\cos\frac{\theta}{2}\cos\frac{\theta'}{2} + \sin\frac{\theta}{2}\cos\frac{\theta'}{2}\mathrm{e}^{\mathrm{i}(\phi-\phi')}\right]^{2S}, \tag{6.12}$$

and thus

$$|\langle\theta,\phi|\theta',\phi'\rangle| = \left(\frac{1+\mathbf{\Omega}\cdot\mathbf{\Omega}'}{2}\right)^{S}. \tag{6.13}$$

Note that these states form an overcomplete set, and have the following completeness relation:

$$\frac{2S+1}{4\pi}\int \mathrm{d}\Omega\,|\Omega\rangle\,\langle\Omega| = \mathbb{I}. \tag{6.14}$$

We thus have

$$\langle\Omega|S,m\rangle = \sqrt{\binom{2S}{S+m}}u^{S+m}v^{S-m}. \tag{6.15}$$

For $S = 1/2$ this representation gives the well-known Bloch sphere.

Comparing Equation (6.11) to the form of the eigenstates of $\mathbf{S}^2$ and S_z given by the Schwinger boson representation 6.9, one can clearly see that an alternative representation of a state may be made by making the replacement

$$a^\dagger \to u, \qquad b^\dagger \to v, \qquad a \to \frac{\partial}{\partial u}, \qquad b \to \frac{\partial}{\partial v} \tag{6.16}$$

and multiplying by $\sqrt{(2S)!}$ wherever operators occur in pairs. Therefore, denoting the coherent state $|\Omega\rangle$ one may write [14, 90]

$$\langle\Omega|\mathrm{VBS}\rangle = \prod_{i=0}^{N}\sqrt{(2S)!}(u_i v_{i+1} - v_i u_{i+1})^S; \tag{6.17}$$

and hence

$$|\langle\Omega|\mathrm{VBS}\rangle|^2 = \prod_{i=0}^{N}(2S)!|u_i v_{i+1} - v_i u_{i+1}|^{2S} \tag{6.18}$$

$$= \prod_{\langle ij\rangle}(2S)!\left(\frac{1-\mathbf{\Omega}_k\cdot\mathbf{\Omega}_{k+1}}{2}\right)^S. \tag{6.19}$$

This approach was used by Freitag and Müller-Hartman [90] to calculate all two-spin correlation functions, and more recently by Katsura *et al.* [144] to calculate the block entropy of the VBS state.

6.5 Single-copy entanglement of the valence bond solid

Having introduced the coherent spin state representation, I shall now go on to apply it to the calculation of the single-copy entanglement for the VBS state. As we have already seen, a standard measure of the bipartite entanglement present in a many-body system is given by the block entropy; *i.e.* the entanglement of a block of L contiguous spins with the remainder of the chain. I shall use the same partition to calculate the single-copy entanglement. In order to calculate this, one first needs to find the reduced density matrix ρ_L of these L spins. Beginning with the density operator for the whole system, one may use the partial trace to find the reduced density matrix

$$\rho_L = \mathrm{tr}_{j\notin\mathcal{B}_L}\rho, \tag{6.20}$$

where the notation $j \notin \mathcal{B}_L$ denotes that the trace is taken over all spins not contained within the block $\mathcal{B}_L$ of L spins.

The trace of any operator in the coherent spin representation is

$$\mathrm{tr}\,\mathcal{A} = \frac{2S+1}{4\pi}\int \mathrm{d}\Omega\,\langle\Omega|\mathcal{A}|\Omega\rangle\,, \tag{6.21}$$

and therefore one obtains

$$\rho_L = \int \prod_{j\notin L}\frac{\mathrm{d}\Omega}{4\pi}\frac{\langle\Omega_j|\mathrm{VBS}\rangle\,\langle\mathrm{VBS}|\Omega_j\rangle}{\langle\mathrm{VBS}|\mathrm{VBS}\rangle} \tag{6.22}$$

$$= \frac{\int\prod_{i=1}^{L}\frac{\mathrm{d}\Omega_i}{4\pi}\prod_{k=1}^{L-1}T_{k,k+1}\,|\Omega_1\rangle_0\,\langle\Omega_1|\otimes|\Omega_L\rangle_{L+1}\,\langle\Omega_L|}{\int\prod_{j=1}^{L}\frac{\mathrm{d}\Omega_j}{4\pi}\prod_{k=1}^{L-1}T_{k,k+1}}, \tag{6.23}$$

where the transfer matrix

$$T_{k,k+1} := (1-\mathbf{\Omega}_k\cdot\mathbf{\Omega}_{k+1})^S/2^S \tag{6.24}$$

and in the first line I have omitted numerical factors. Katsura *et al.* found [144] that this is independent of the length of the total chain N, and therefore without loss of generality one can set $L = N$. Following the methods of Katsura *et al.* and Freitag and Müller-Hartmann [90, 144], one may find the eigenvalues of this matrix (replacing $S \to S/2$ for the end spins)

The following decomposition in terms of Legendre polynomials may be used [90, 95]

$$\left(\frac{1+x}{2}\right)^S = \sum_{l=0}^{S}(2l+1)\frac{S!S!}{(S-l)!(S+l+1)!}P_l(x), \tag{6.25}$$

from whence it follows that

$$\rho_L = \frac{4\pi}{(S+1)^2}\sum_{l=0}^{S}\lambda(l)^{L-1}I_l(\mathbf{s}_0\cdot\mathbf{s}_{L+1}), \tag{6.26}$$

where

$$\lambda(l) := (-)^l\frac{S!(S+1)!}{(S-l)!(S+l+1)!}, \tag{6.27}$$

and $I_l(X)$ is an lth order polynomial in X determined recursively through the relationship

$$I_{j+1}(X) = \frac{2j+3}{(S+j+2)^2}\left(\frac{4X}{j+1}+j\right)I_j(X) - \frac{j}{j+1}\frac{2j+3}{2j-1}\left(\frac{S-j+1}{S+j+2}\right)^2 I_{j-1}(X), \tag{6.28}$$

with $I_0(X) = 1/4\pi$, $I_1(X) = 3X/4\pi(S/2+1)^2$. These polynomials form a complete set of isotropic, two-site tensor operators.

To find the block entropy for general S, one can use this method to find the eigenvalues of the reduced density matrix, and use the standard formula (2.20) for the von Neumann entropy. This was found to approach $2\log(S+1)$ exponentially fast in L (the thermodynamic limit) [144], confirming the conjecture of Vidal *et al.* that the block entropy of a gapped integer spin chain reaches saturation for all S [242]. For the purposes of finding the single-copy entanglement, only the *largest* eigenvalue is required.

The density matrix is diagonal in the basis of the total spin of spins 0 and $L+1$. These spins, of course, add up to several multiplets in the usual manner of spin addition, and so there will be degeneracy in the eigenvalues. One thus requires the largest value of

$$\langle P_\sigma \rangle = \mathrm{tr}\ \{P_\sigma \rho_L\}, \tag{6.29}$$

where P_σ is the projector on to the subspace of total spin σ. This multiplet distribution (*i.e.* the eigenvalues multiplied by their weight) is given by [90]

$$\langle P_\sigma \rangle = 4\pi(2\sigma+1)\sum_{j=0}^{S} \frac{(S+j+1)!(S-j)!}{(S+1)!(S+1)!}\lambda(j)^{L+1} I_j[X(\sigma)], \tag{6.30}$$

where $X(\sigma) := \mathbf{s}_0 \cdot \mathbf{s}_{L+1} = \sigma(\sigma+1)/2 - S/2(S/2+1)$. The calculation of the single-copy entanglement only requires the eigenvalues, and thus one omits the weights $(2\sigma+1)$.

This distribution is found recursively, determined by the coefficients $I_j[X(\sigma)]$. The largest values are given by the cases $\sigma = S$ and $\sigma = 0$ for L even and odd, respectively. For even L, the required value is

$$\langle P_S \rangle = (2S+1)\sum_{j=0}^{S} \frac{2j+1}{(S+1)^2}\lambda(j)^{L+1} \tag{6.31}$$

and thus the largest eigenvalue is

$$\Lambda_1 = \sum_{j=0}^{S} \frac{2j+1}{(S+1)^2}\lambda(j)^{L+1} \tag{6.32}$$

$$= \frac{1}{(S+1)^2}\left\{1 + \sum_{j=0}^{S}\lambda(j)^{L+1}(2j+1)\right\}. \tag{6.33}$$

This gives the single-copy entanglement:

$$\begin{aligned} E_1 &= -\log \Lambda_1 \\ &= 2\log(S+1) - \log\left\{1 + \sum_{j=1}^{S}\lambda(j)^{L+1}(2j+1)\right\} \qquad (6.34) \\ &= 2\log(S+1) - \log\lambda(0)^{L+1}\left\{1 + \sum_{j=1}^{S}\frac{\lambda(j)^{L+1}}{\lambda(0)^{L+1}}(2j+1)\right\}. \qquad (6.35) \end{aligned}$$

Since $\lambda(j) < \lambda(j+1)$ for all j, and $\lambda(0) = 1$, it is clear that in the thermodynamic limit $L \to \infty$ (as considered in the critical, gapless case [170]), this becomes

$$E_1 \to 2\log(S+1), \tag{6.36}$$

which is exactly equal to the von Neumann entropy, as found by Katsura *et al.* [144]. The proof for L odd follows analogously.

It therefore is the case that *all* the entanglement present in the VBS state (the ground state of the gapped spin-S AKLT Hamiltonian) may be distilled from a single-copy: one can distill with certainty a maximally-entangled state, the dimension of which is related to S; of course, in the case the $\log(S+1)$ is not an integer, the dimension of the maximally-entangled state would be given by $2\lfloor\log(S+1)\rfloor$. This would appear to have an intuitive explanation in terms of the valence bond picture of the state: the entanglement between a block and the remainder of the chain is related to the number of bonds 'cut' by the boundary (indeed, this is similar to the reasoning behind area laws [62, 110, 184, 249] although the analogy is not strict in this case, since the entanglements of formation and distillation are only equal in the asymptotic limit), and is further evidence of the qualitatively different behaviour of gapped chains to gapless chains. One should contrast this with the critical case [170], from whence one can distill with certainty (in the $L \rightarrow \infty$ limit) a maximally-entangled state of arbitrary dimension (*i.e.* an infinite single-copy entanglement); the crucial, qualitative difference is that this is still only *half* the total amount of entanglement present.

6.6 Summary and open problems

In this chapter, I have demonstrated that all the entanglement present in the valence bond solid ground state of the gapped AKLT Hamiltonian for arbitrary S may be distilled with certainty in a single process. This qualitative difference to the behaviour of gapless, critical chains provides further evidence that the entanglement present in gapped systems is of a fundamentally different nature.

It is an open problem as to the behaviour of single-copy entanglement in general gapped systems, but this result provides the first indication that the behavoiur is quite a departure from the case of gapless systems, and I hope that this will provide a stepping-stone to a statement for general gapped systens.

Part IV

Antisymmetric states

Symmetry plays an important role in physics; symmetric states often correspond to physically important states, and have curious properties by virtue of their symmetry. In this section, I shall consider a specific multipartite state with a high degree of symmetry under the permutation of its subsystems. I shall consider its behaviour under local projective measurements, and elucidate its entanglement properties.

This Chapter is based on the work published in Reference [103].

Chapter 7

Multi-party, multi-level singlets

In this chapter, I shall introduce some highly symmetric many-body states called 'multi-party, multi-level singlets', or 'qudit singlets'. I shall show that local measurements on some of these qudits project the unmeasured qudits onto a smaller singlet, regardless of the choice of measurement basis at each measurement, and the outcome of that measurement. It follows that the entanglement is highly persistent, and that through local measurements, a large amount of entanglement may be established between spatially-separated parties for subsequent use in distributed quantum computation.

7.1 Introduction

Entanglement between spatially-separated systems is a pivotal resource in quantum information theory, enabling distributed or networked quantum computation. There is thus an enormous interest in extracting this resource from various many-body systems [10], in particular through measurements [238]. In such schemes, the measurement bases have to be carefully optimised. Could there be other systems offering a more flexible method of entanglement extraction, and could the amount of entanglement exceed the currently-known limits? This is indeed the case for a particular quantum state, the *qudit singlet*, which I shall consider in this chapter.

I shall first show that if N parties share an N-level singlet, and M parties perform successive measurements (each in a random basis), the remaining parties share a singlet of $N - M$ systems, regardless of the choice of measurement bases (measurement in the same basis has been previously considered [49]). A direct consequence of this is that these states have a very high *localisable entanglement* (without the need to optimise the local measurement basis), and the highest possible *persistency of entanglement* (the robustness of a multi-party entangled state to local measurements [43]).

7.2 Qudit singlets: definition

A qudit is a generic d-level system; *qudit singlets* $|S_N^{(d)}\rangle$ are N-partite states with the property $U^{\otimes N}|S_N^{(d)}\rangle = |S_N^{(d)}\rangle$ (up to a global phase), where U is an arbitrary one-qudit unitary operation. For the case $d = N$, they may be written

$$\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle = \frac{1}{\sqrt{N!}} \sum_{\{n_l\}} \epsilon_{n_1,\cdots,n_N} |\alpha_{n_1}, \cdots, \alpha_{n_N}\rangle , \tag{7.1}$$

where $\epsilon_{n_1,\cdots,n_N}$ is the generalised Levi-Civita symbol, and the state is written in the basis $\{|\alpha_i\rangle\}_{i=1}^d$ at each qudit. The sum is taken over all permutations of incides $\{n_1, \cdots, n_N\}$, and crucially, is antisymmetric with respect to the permutation (or 'exchange') of any two qudits; that is,

$$P_{ij} \left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle = - \left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle \tag{7.2}$$

for $i, j \in [1, N]$, where for given states $|\psi\rangle_i \in \mathcal{H}_i, |\phi\rangle_j \in \mathcal{H}_j$, the *permutation operator* P_{ij} swaps the states according to

$$P_{ij} |\psi\rangle_i |\phi\rangle_j = |\phi\rangle_i |\psi\rangle_j , \tag{7.3}$$

and has eigenvalues ± 1. This operator was introduced in the postulates of quantum mechanics, since Posulate 4 asserts that multipartite states must be eigenstates of this operator. However, it must be emphasised that this postulate holds for states of identical, indistinguishable particles; although the state here is an eigenstate of such permutation operators, the particles are 'localised' at particular vertices on a lattice, and thus are physically distinguishable. This is of particular importance when, in Part V, I shall discuss the possible realisation of such a state using identical particles that are made distinguishable by confining their locations to lattice vertices.

The qudit singlet has some curious properties and applications. It was previously shown by Adan Cabello[1] that it may be used to solve problems lacking classical solutions (such as *liar detection*, the N *strangers problem*, and *secret sharing* [49, 50, 51]. It has also been shown to be applicable in multiparty remote state preparation [6], and for encoding qubits in decoherence-free subspaces [150].

7.3 The effect of local measurements

I shall show that when N parties share such a state, and some of them perform measurements on their qudits in randomly chosen bases (varying from party to party), a qudit singlet is

[1] Cabello has termed such states 'supersinglets' [51].

still established between those unmeasured qudits, in a basis related to that used for the last measurement. To demonstrate this, I will make use of the property [6] $U \otimes \mathbb{I}^{\otimes N-1}|S_N^{(N)}\rangle = \mathbb{I} \otimes U^{\dagger\otimes N-1}|S_N^{(N)}\rangle$ and introduce the notation $|S_{N-1}^{(N-1)}(\boldsymbol{\beta};\beta_l)\rangle$ to denote an $(N-1)$-singlet written in the basis $\{|\beta_i\rangle\}_{i=1}^N$ at each qudit, with level $|\beta_l\rangle$ absent (*i.e.* $\mathrm{tr}\,\rho_i|\beta_l\rangle\langle\beta_l| = 0$ for all i where ρ_i is the reduced density matrix of the ith qudit).

Theorem 21. *When an N-singlet $|S_N^{(N)}(\boldsymbol{\alpha})\rangle$ written in a basis $\{|\alpha_i\rangle\}$ is measured at one site using an arbitrary basis $\{|\beta_i\rangle\} := \{U|\alpha_i\rangle\}$, the state obtained is a product of a state $|\beta_i\rangle$ at the measured site and a smaller singlet $|S_{N-1}^{(N-1)}(\boldsymbol{\beta};\beta_i)\rangle$ written in the basis $\{|\beta_i\rangle\}$.*

Proof. Consider the outcome when one performs a von Neumann measurement $\{|\beta_i\rangle\langle\beta_i|\}$ at one qudit. Without loss of generality, let this measurement be on the qudit labelled 1. Since $|\beta_i\rangle\langle\beta_i| = U|\alpha_i\rangle\langle\alpha_i|U^\dagger$ we may write

$$\begin{aligned}
&|\beta_i\rangle\langle\beta_i| \otimes \mathbb{I}^{\otimes N-1}\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle \\
&\quad = U|\alpha_i\rangle\langle\alpha_i|U^\dagger \otimes \mathbb{I}^{\otimes N-1}\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle \\
&\quad = U|\alpha_i\rangle\langle\alpha_i| \mathbb{I} \otimes U^{\otimes N-1}\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle. \qquad (7.4)
\end{aligned}$$

To proceed, note that the N-singlet may be re-written in the form

$$\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}(-)^{i+1}|\alpha_i\rangle_1\left|S_{N-1}^{(N-1)}(\boldsymbol{\alpha};\alpha_i)\right\rangle_{2,\cdots,N},$$

and it thus follows that

$$\mathbb{I} \otimes U^{\otimes N-1}\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle_{1,\cdots,N} = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}(-)^{i+1}|\alpha_i\rangle_1 \otimes U^{\otimes N-1}\left|S_{N-1}^{(N-1)}(\boldsymbol{\alpha};\alpha_i)\right\rangle_{2,\cdots N}. \qquad (7.5)$$

Whilst $|S_{N-1}^{(N-1)}(\boldsymbol{\alpha};\alpha_i)\rangle$ is a singlet written in the $\{|\alpha_l\rangle\}_{l\neq i}$ basis at each qudit, one can see that the term $U^{\otimes N-1}|S_{N-1}^{(N-1)}(\boldsymbol{\alpha};\alpha_i)\rangle$ is a singlet written in the $\{|\beta_l\rangle\}_{l\neq i}$ basis[2]. Thus if the measurement outcome is $|\beta_i\rangle$, the overall state is projected to

$$\frac{|\beta_i\rangle\langle\beta_i| \otimes \mathbb{I}^{\otimes N-1}\left|S_N^{(N)}(\alpha)\right\rangle_{1,\cdots,N}}{||\cdots||} = (-)^{i+1}|\beta_i\rangle_1 \otimes \left|S_{N-1}^{(N-1)}(\beta;\beta_i)\right\rangle_{2,\cdots,N}, \qquad (7.6)$$

where $||\cdots||$ denotes the norm of the state in the numerator of the fraction, in order to normalise the state. This completes the proof. □

The significance of the above theorem is revealed when one considers successive measurements at different qudits. Indeed, by iterating the above proof, it becomes apparent that by measuring in a different basis at each qudit, the remaining, unmeasured qudits will be projected to a singlet in a basis related to that used for the final measurement.

[2]These are *not* the same state, since the bases are not complete in the N-dimensional space.

Corollary 22. *If M parties perform successive measurements in arbitrary bases (where the mth party uses the basis $B_m = \{|\alpha_i^{(m)}\rangle\}_{i\neq 1,\cdots,m-1} = \{\prod_{l=1}^{m} U^{(l)}|\alpha_i^{(0)}\rangle\}$), the remaining parties share an $(N-M)$-singlet in the B_M basis at each qudit, with the restriction that at each measurement, the basis transformation operates on a space whose dimension is one less than the previous transformation; i.e. at the lth measurement the basis may be transformed by any $U^{(l)}$ acting on the subspace $\mathbb{C}^{N-l}$.*

Proof. Consider measuring in the basis $\{|\alpha_i^{(2)}\rangle\}$ on the state resulting from the previous measurement, namely, $|\alpha_i^{(1)}\rangle_1 |S_{N-1}^{(N-1)}(\boldsymbol{\alpha}^{(1)}; \alpha_i^{(1)})\rangle_{2,\cdots,N}$. Applying Theorem 21 on the smaller singlet, one can see that the final state is

$$\left|\alpha_i^{(1)}\right\rangle_1 \left|\alpha_j^{(2)}\right\rangle_2 \left|S_{N-2}^{(N-2)}(\boldsymbol{\alpha}^{(2)}; \alpha_i^{(2)}, \alpha_j^{(2)})\right\rangle_{3,\cdots,N}. \tag{7.7}$$

In general, if M measurements are taken, we have (upto a global phase)

$$\left|\alpha_{n_1}^{(1)}\right\rangle_1 \cdots \left|\alpha_{n_M}^{(M)}\right\rangle_M \left|S_{N-M}^{(N-M)}(\boldsymbol{\alpha}_{n_M}^{(M)}; \mathbf{n}^{(M)})\right\rangle_{M+1,\cdots,N}, \tag{7.8}$$

where $\mathbf{n} = (n_1, \cdots, n_M)$ is a vector, the elements of which are the indices of the vectors of the basis B_M excluded from the $(N-M)$-singlet. □

It must be noted that the proof—see Equation (7.4)—makes use of the property $U^{\otimes N}|S_N^{(N)}\rangle = |S_N^{(N)}\rangle$. This holds only when the $U^{\otimes N}$ operates on the space occupied by the singlet $|S_N^{(N)}\rangle$; if one were to put this state within a larger space, a separable unitary operation on the whole n-partite space would not (in general) give this invariance. Thus in order to iterate the proof, it is essential to make the restriction that at each successive measurement the dimension of the unitary transformation decreases by one. So, at the lth measurement, one would be able to transform the basis by a unitary $U^{(l)}$, such that there is a submatrix operating on $N-l$ levels (which levels are operated on depends on the previous outcomes), and '1' on all diagonal elements corresponding to the remaining levels.

In fact, this restriction may be lifted slightly. It is well known [202] that any $d \times d$ unitary matrix can be written as a product of two-level unitaries through the decomposition $U_d = V_1 \cdots V_k$, where the operators $\{V_i\}$ are two-level operators, and $k \leq d(d-1)/2$. The original proof of this was intended to show how to break down a d-level operator into a series of beam splitters [218]. This then gives

$$U_d \otimes U_d = (V_1 \otimes V_1) \cdots (V_k \otimes V_k), \tag{7.9}$$

allowing one to use at measurement the subset of $d \times d$ unitaries that factorise such that the two-level matrices $\{V_i\}$ either act within the subspace supporting the singlet, or its complement (*i.e.* the matrix element linking the singlet subspace to the rest of the space is zero). This is

because those factors operating on the complement act as the identity on the singlet, and those operating on the singlet subspace have the rotational invariance property.

But what would happen if one measured in an arbitrary basis? To answer this, one should consider the effect of operating on a 2-singlet with a more general unitary operator, written in the form (7.9). Those factors $V_i \otimes V_i$ that do not operate on any part of the singlet subspace can be removed successively from the right of the operator (7.9), until the right-most factor links one of the levels of the singlet with a different level. Suppose the ith factor in (7.9) operates on levels j, k in a basis $\{|l\rangle\}_{l=1}^{d}$, and the whole operator $U_d \otimes U_d$ is applied to a singlet of levels j, m. Then

$$(V_1 \otimes V_1) \cdots (V_i \otimes V_i)(|jm\rangle - |mj\rangle) = (V_1 \otimes V_1) \cdots (V_{i-1} \otimes V_{i-1}) \left((V_i |j\rangle) |m\rangle - |m\rangle (V_i |j\rangle) \right). \tag{7.10}$$

This remains a singlet, albeit in a different subspace. In general, when an n-singlet is operated on by a separable unitary $U_d^{\otimes n}$ (where $d > n$), the state remains an n-singlet, but (in general) lies within a different subspace of the n^n-dimensional n-partite Hilbert space acted on by $U_d^{\otimes n}$. Thus one can conclude that for any measurement, one still obtains a singlet, but for those measurement bases not satisfying the constraints given above, the singlet moves into a different subspace.

Chapter 8

Entanglement properties

In this chapter, I shall consider some of the entanglement properties of the qudit singlet. Specifically, I shall show that the measurement property proven in the previous chapter implies that the state has a very high localisable entanglement (the amount of entanglement available to be concentrated between two subsystems through local measurements), and the highest possible persistency of entanglement (the robustness of the entanglement to local measurements).

8.1 Localisable entanglement

As we saw in the chapter on entanglement, there is a vast array of entanglement measures, each best suited for different purposes. Perhaps the most physically-relevant is the amount of entanglement one can establish between spatially-separated subsystems for subsequent use in networked quantum computation. Indeed, it was with this motivation that *localisable entanglement* was introduced [238].

Definition 23 (Localisable entanglement [190, 238]). The localisable entanglement is defined as the maximum amount of entanglement establishable between two subsystems i and j in a multipartite state by performing local measurements on the other spins. If measuring in a given basis M establishes the bipartite state $|\psi_s\rangle$ between i and j with a probability p_s, then the localisable entanglement is

$$E_{ij} = \max_{\epsilon} \sum_{s} p_s E(|\psi_s\rangle), \tag{8.1}$$

where $\epsilon := \{p_s, |\psi_s\rangle\}$ is an ensemble of pure states of at least 2^{N-2} elements, associated with the choice of measurement basis M, and $E(\cdot)$ is some measure of entanglement. For pure states, the von Neumann entropy (2.20) is the unique asymptotic entanglement monotone, although a measure called *concurrence* is also easy to calculate in this context [136, 190, 238]. The

definition can be extended to mixed states in a straightforward way [190], where the choice of entanglement measure $E(\cdot)$ could be (for example) the entanglement of formation.

Through numerical calculations, it has been shown that a maximally-entangled state of a 2×2 system (*i.e.* a standard EPR singlet $|\Psi^-\rangle = (|0,1\rangle - |1,0\rangle)/\sqrt{2}$) can be established in this way. However, any realistic scheme for distributed quantum computation would require a much larger amount of entanglement.

Using the above measurement related properties of qudit singlets, one can now consider the role of N-singlets in entanglement distribution. As mentioned above, the establishment of successively smaller singlets at each measurement is *independent* of the choice of measurement basis, and the outcome of the measurement. Thus, it is *always* possible to establish a maximally-entangled state between any two subsystems of the state. This is a qualitative difference in mechanism of entanglement localisation to those systems studied previously, since maximisation of the localisable entanglement in general requires careful optimisation of the local measurement bases, and averaging over all possible outcomes. This then gives the maximum *avergage* entanglement localisable by measurements. However, for the singlet, even if one selected the basis *randomly* at each measurement, one can always establish a maximally-entangled state between the unmeasured parties.

Moreover, another important difference emerges if one considers the entanglement establishable between two *subsystems* (*i.e.* groups of constituent systems), rather than two individual constituents, of a system (*e.g.* blocks of spins in a 1D chain, rather than individual spins). In models studied so far, the entanglement establishable between two subsystems has no reason to differ from that of two individual parts; however, by performing local measurements on a qudit singlets, a larger amount of entanglement can be established in this way. Suppose that Alice and Bob each hold n qudits of an N-singlet. By measuring the remaining qudits, they can establish a $2n$-singlet between them. This is equivalent to sharing a maximally-entangled state of dimension $D \times D$ (where $D := \binom{2n}{n}$) or $\log D$ EPR singlets [189], since the $2n$-singlet can be written in a Schmidt decomposition of $\binom{2n}{n}$ terms of equal amplitude (see figure 8.1), and upto local unitaries this is equivalent to $\sum_{i=1}^{D} |i\rangle |i\rangle / \sqrt{D}$. Thus the localisable entanglement of qudit singlets (when the notion is generalised to two subsystems) can be much larger in comparison to those systems studied so far.

8.2 Persistency of entanglement

An important consideration from a practical point of view is the ease of destroying the entanglement present. This can be quantified by the *persistency of entanglement*

Definition 24 (Persistency of entanglement [43]). For a state of N qudits, the persistency

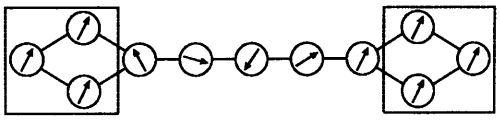


Figure 8.1: Two subsystem localisable entanglement. Here, Alice and Bob have access to the boxed qudits. By performing arbitrary measurements on the other qudits (in random directions), they can establish a 6-singlet between them.

of entanglement P is defined as the minimum number of local von Neumann measurements such that, regardless of the measurement outcome, the state is completely separable. For a pure state, it is clear that $0 \leq P \leq N-1$.

This quantity may be used to model an environment that interacts with a system through random, local measurements. Since the establishment of successively smaller singlets is *independent* of both the basis choice and outcome, it is easy to see that $N-1$ measurements always need to be performed to completely disentangle the state (there is no way to optimise the basis to reduce this number). Thus these states have the highest possible persistency of an N-partite state (for comparison, the multi-qubit cluster, GHZ and W states have persistencies $\lfloor N/2 \rfloor$, 1 and $N-1$, respectively [43]).

8.3 Block entropy

I shall briefly mention the scaling of the *block entropy*. As mentioned in Section 5.4, this is the entanglement of a block of spins with the remainder of the system. By taking a Schmidt decomposition across an arbitrary partitioning of qudits, one can see that the *block entropy* of this state is $\log \binom{N}{L}$. This is in contrast to the usual behaviour for gapped systems, where the entropy is usually proportional to the block's 'area', and to the case of gapless spin chains in 1D where it is proportional to $\log L$.

This suggests that the state does not admit an efficient matrix-product state decomposition; Vidal's criterion [241] for efficient classical simulability is that the number of parameters does not scale any faster than $\log N$ (where N is the number of subsystems) when more subsystems are added. This suggests that these singlet states may have some use in solving nonclassical problems, although this remains an open problem.

8.4 Multipartite entanglement

As we have seen, qudit singlets may be used to distribute a large amount of entanglement between two parties, but what is the nature of this entanglement? Is the state *genuinely*

multipartite entangled, or is producible from bipartite entanglement alone? Here I shall show that a singlet of N parties and N levels is indeed N-partite entangled.

A natural first step in understanding multipartite entanglement would seem to be to attempt to extend the Schmidt decomposition to an arbitary number of systems. Such a generalisation does not really exist: one can take a similar decomposition, but the number of terms is not the minimum of the dimensions of each subsystem. However, one can write an N-partite state in the form

$$|\psi\rangle = \sum_{i=1}^{R} c_i |i_1\rangle \cdots |i_N\rangle , \tag{8.2}$$

and define a quantity called the Schmidt measure P_S [74], which quantifies the minimum number of product terms required to expand the state: $P_S = \log \min R$. However, this measure is, in general, very difficult to compute. More importantly, it does not quantify *genuine* multipartite entanglement: it only distinguishes entangled and completely separable states with respect to a particular partioning of subsystems. In order to use it to make statements regarding multipartite entanglement, one must compute this quantity with respect to every possible partition of the state's subsystems.

Instead, I shall take here a different, but related, approach. The approach is strongly related to the iterative method first used by Dür *et al.* [70] to show the existence of two different types of tripartite entanglement (the so-called GHZ and W states), and also the more recent work by Lamata *et al.* [153, 154] to rederive the same result from a slightly different perspective.

Imagine taking a bipartition of an N-partite system, with one part being a single spin or qudit (a d-level quantum system), and the other being the remainder of the system. One may write a bipartite Schmidt decomposition for this state. If the state is separable with respect to this partition, the Schmidt number (equivalently, the rank of the reduced density matrix of either subsystem) will be unity; otherwise, it will be an integer greater than or equal to two. If all such bipartitions of the state into a single subsystem and the remainder have rank unity, then the state is fully separable: one need not investigate the entanglement properties of the state further.

If there exists at least one such bipartition for which the Schmidt number is greater than unity (equivalently, the von Neumann entropy of either part of the partition is greater than zero) then the state has some degree of entanglement present. However, at this stage one cannot state whether this is bipartite, tripartite, or generally n-partite, entangled; all that can be said is that this state contains 'at least' bipartite entanglement with respect to this partitioning. It may be 2-producible (*i.e.* it may be produced from bipartite entanglement alone), or it may be k-producible (*i.e.* it may be produced from k-partite entangled states, where $2 < k \leq N$).

Using the information obtained thus far, one can 'discard' those subsystems that are not

entangled with the remainder of the system (those with reduced density matrices of rank unity) and investigate these no further. Now take a further bipartition of the remainder of the state, with part A containing two subsystems, and part B the remaining, entangled subsystems. Again, one can find the rank of this decomposition. If it is unity, then the two subsystems in part A of the decomposition are bipartite entangled. This can be repeated with part B, by considering all possible bipartitions into two subsystems and the remainder. This method can be iterated, taking all bipartitions with one part containing n subsystems, increasing n incrementally, until all partitions with larger subsystems give separable states. The system may be said to contain between n_1- and n_2-partite entanglement, where n_1 is the smallest value of n giving rise to bipartitions with Schmidt number unity, and n_2+1 the value for which all bipartitions containing n_2+1 subsystems in one part of the partition have rank unity. It must be said that this method will, for general states, be very laborious. One might expect it to be intractable for large N in the light of the fact that deciding whether or not a state is separable is computationally intractable [100, 101, 131]. However, clearly for highly symmetric states the number of partitions to be taken is greatly reduced.

One may thus use the Schmidt number of bipartitions to detect genuine multipartite entanglement. However, this method merely detects whether the entanglement in a particular state may be made up of smaller entangled states, and their size; it does not detect which entanglement *class* the state belongs to. As stated by Dür *et al.* [70] there are, in fact, an infinite number of entanglement classes for systems of more than four particles, even for a given producibility—since the number of parameters that need to be changed in order to transform one state in to another grows exponentially with the number of subsystems, whereas the number of parameters used to describe an invertible, linear operator (these correspond to stochastic operations and local communications) grows linearly.

What may be said of the nature of the entanglement in multilevel multiparty singlets using this method? Fortunately the state is highly symmetric, making the investigation considerably simpler. In fact, since the singlet may be written in terms of smaller ones (due to the permutation group S_{N-1} being a subgroup of S_N), one may perform the argument by iteration, in the spirit of the work by Lamata *et al.* [153, 154]. One begins by writing the N-singlet as

$$\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle = \frac{1}{\sqrt{N}}\sum_{i=1}^{N}(-)^{i+1}\left|\alpha_i\right\rangle_1\left|S_{N-1}^{(N-1)}(\boldsymbol{\alpha};\alpha_i)\right\rangle_{2,\ldots,N}.$$

One can show that this is the smallest Schmidt decomposition across the $1|2\ldots N$ partition by taking the single-valued decomposition with respect to the coefficient matrix as split between sites 1 and the remainder [114, 153, 154]. Thus the state is maximally-entangled across the split $1|2\ldots N$, since the state is supported in $\mathbb{C}^N$ on both sides of the split and so the maximal Schmidt rank is N. The crucial observation here is that if the $(N-1)$-singlet $|S_{N-1}\rangle$ is $(N-1)$-

partite entangled, then so is the N-singlet, since the number of subsystems entangled can not decrease with the addition of another subsystem, and the new subsystem is entangled with the remainder. So, if the $(N-1)$-singlet is $(N-1)$-partite entangled, the N-singlet is N-partite entangled However, we know that the 2-singlet is bipartite entangled, and therefore by induction on N, all N-singlets are N-partite entangled.

Part V

Physical realisation of antisymmetric states

In this part, I shall review the Hubbard model, and briefly discuss its importance in both condensed matter physics and the growing field of ultracold atoms. I shall go on to show that in a particular regime of this model in one spatial dimension, it effectively becomes a permutation Hamiltonian, and thus its ground state is the qudit singlet considered in Part IV.

This Chapter is based on the work published in Reference [103].

Chapter 9

Permutation Hamiltonians

In this Chapter, I shall briefly introduce permutation Hamitonians, and show that they may be considered a generalisation of the Heisenberg model. I shall then go on to prove that the qudit singlets studied in the previous Chapter arise naturally as the ground states of this Hamiltonian.

9.1 The Heisenberg and permutation Hamiltonians

The familiar isotropic Heisenberg Hamiltonian ($\boldsymbol{\sigma}^i \cdot \boldsymbol{\sigma}^j$) acting on two qubits i, j is equivalent (when the two-qubit identity operator is added) to the permutation operator P_{ij}. The natural generalisation of this Hamiltonian for d-level systems is a sum of permutation operators P_{ij} [227]. For a general network of qudits (some arrangement of qudits connected by permutation operators) one may use the language of *graph theory* and ascribe a finite graph $G := \{V(G), E(G)\}$, where $V(G)$ denotes its set of vertices and $E(G)$ its set of edges—if (i,j) are adjacent vertices, $(i,j) \in E(G)$. At each vertex we associate a d-level Hilbert space. I shall avoid the term *lattice* at this stage, since this implies a regular arrangement of qudits; the following results hold for more general networks, making graph theory the natural description. The Hamiltonian is then written

$$H = \sum_{i,j \in E(G)} J_{ij} P_{ij}. \tag{9.1}$$

The operator

$$P_{ij} = \sum_{\alpha,\beta=1}^{d} S_\alpha^\beta(i) S_\beta^\alpha(j) \tag{9.2}$$

permutes the states of the Hilbert spaces at vertices i and j, where $\{S_\beta^\alpha(n)\}$ are the generators of the group SU(d) at vertex n satisfying the algebra

$$\left[S_\alpha^\beta(m), S_\sigma^\rho(n)\right] = \delta_n^m \left\{\delta_\alpha^\rho S_\sigma^\beta(n) - \delta_\sigma^\beta S_\alpha^\rho(n)\right\}, \tag{9.3}$$

where the indices α, β refer to the state labels, and the operator $S^{\alpha}_{\beta}(n)$ destroys the state β and creates α at the vertex labelled n. As noted in Chapter 4, an important point is that the generators of SU(d) may be constructed from either fermionic or bosonic creation and annihilation operators, $S^{\alpha}_{\beta}(n) = c^{\dagger}_{\alpha}(n)c_{\beta}(n)$. There are thus many potential realisations of such a Hamiltonian (this will be discussed in Chapter 10).

9.2 Qudit singlets as ground states

The ground state of quantum spin chains are generally very hard to find. For the permutation Hamiltonian

$$H = \sum_{i,j \in E(G)} J_{ij} P_{ij}, \tag{9.4}$$

the solution is, in general, very complicated, and requires the use of the Bethe *ansatz* [227]. However, as with most physical systems, there is a particular regime of the model that can be solved with ease. Specifically, this is the case where the number of vertices of the graph G is *equal* to the number of levels at each graph site i (*i.e.* if there are N graph vertices, there is at each graph vertex a Hilbert space of dimension N, and thus the whole state space is $(\mathbb{C}^N)^{\otimes N}$). I shall now provide a simple proof that the qudit singlet (7.1) arises as the ground state in this case, for all couplings $J_{ij} > 0$ (antiferromagnetic); this proof relies on some straightforward lemmata.

Lemma 25. *The lowest possible energy state of a permutation Hamiltonian has energy equal to that of an eigenstate of all* $\{P_{ij} | i, j \in E(G)\}$ *with eigenvalue* -1.

Proof. By definition, the ground state must minimise the energy $\langle\psi|H|\psi\rangle$. Now

$$\min_{|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}} \langle\psi|H|\psi\rangle \geq \sum_{i,j \in E(G)} \min_{|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}} \langle\psi|J_{ij}P_{ij}|\psi\rangle \,. \tag{9.5}$$

The smallest eigenvalue of P_{ij} is -1, thus $\min \langle\psi|P_{ij}|\psi\rangle = -1$; it follows that

$$\min_{|\psi\rangle \in (\mathbb{C}^d)^{\otimes N}} \langle\psi \,|\, H \,|\, \psi\rangle \geq -\sum_{i,j} J_{ij}. \tag{9.6}$$

Equality exists for an eigenstate of all terms in the Hamiltonian (*i.e.* the set of operators $\{P_{ij} | i, j \in E(G)\}$) and if this state exists, it is the ground state. □

Lemma 26. *If a state is an eigenstate of all operators in the set* $\{P_{ij} | i, j \in E(G)\}$, *it is an eigenstate of all operators* $\{P_{ij} | i, j \in [1, N]\}$.

Proof. Consider first a linear chain with nearest-neighbour permutations. Any other permutation may be written as a product of an odd number of nearest-neighbour permutations, *e.g.*

$$P_{13} = P_{23}P_{12}P_{23}; \tag{9.7}$$

in general

$$P_{1,k} = P_{1,k-1}P_{k-1,k}P_{1,k-1}. \tag{9.8}$$

Thus an eigenstate of all nearest-neighbour permutations must also be an eigenstate of *all* possible permutations. This can be readily generalised to any connected graph, since any 'path' through the graph is equivalent to a 1D chain of nearest-neigbour connections; thus any permutation in any graph can be written as a product of an odd number of nearest-neighbour permutations. □

Theorem 27. *The ground state of a permutation Hamiltonian on N N-level systems is an N-singlet.*

Proof. The above lemmata show that a state antisymmetric under all permutations is a valid ground state; since a qudit singlet for $d = N$ by definition satisfies this, it is a valid ground state. It can easily be shown to be the *unique* ground state by assuming the existence of another distinct ground state $|\phi\rangle \neq |S_N^{(N)}\rangle$. Being a ground state, $|\phi\rangle$ must minimise the total energy, leading to $\langle\phi|P_{ij}|\phi\rangle = -1$ for all i, j. This implies $|\phi\rangle = |S_N^{(N)}\rangle$. This is a contradiction and thus there cannot be another ground state. □

Therefore, the completely antisymmetric state 7.1 arises as the ground state of the antiferromagnetic Hamiltonian. What about the ferromagnetic case? In this regime, all couplings $J_{ij} < 0$; following the argument of the above proof, the ground state must be the completely *symmetric* state

$$\left|S_N^{(N)}(\boldsymbol{\alpha})\right\rangle = \frac{1}{\sqrt{N!}} \sum_{\{n_l\}} |\alpha_{n_1}, \cdots, \alpha_{n_N}\rangle, \tag{9.9}$$

i.e. the sum of all possible permutations, with a coefficient of $+1$ in front of each term.

Chapter 10

Hubbard model

The permutation Hamiltonian considered in the previous Chapter may seem a natural extension of the Heisenberg Hamiltonian, or a natural Hamiltonian to consider when one has particles hopping around on an otherwise empty lattice. However, how does this Hamiltonian arise from already known physical models? In this Chapter, I shall show how this Hamiltonian arises from a strong coupling regime of the well-known Hubbard model, for the fermionic case, and briefly discuss how it can also arise in the bosonic case. I shall first introduce the Hubbard model, then discuss the strong-repulsion limit, and finally discuss the preparation method for obtaining the singlet as the ground state in one spatial dimension.

10.1 Introduction

Recent years have seen much development at the interface of condensed matter theory and the theory of ultracold atoms, and both fields have also been studied from the vantage point of quantum information. One of the central models in condensed matter theory is the Hubbard model, with both bosonic and fermionic varieties. This model has many fascinating phases, and provides physicists with a way of understanding many physical phenomena, ranging from magnetism to superconductivity. Recent experimental demonstrations that one can implement a traditional condensed matter model in *optical lattices* have provided physicists with the potential to simulate tailor-engineered 'spin' models [97, 232], opening up the possibilty of engineering systems suitable for quantum computation.

It is already well-known [78, 88] that the Heisenberg Hamiltonian (ferromagnetic or antiferromagnetic) may be obtained as an effective Hamiltonian in the strong coupling regime of the two-level Hubbard model (either fermionic or bosonic), a paradigm in condensed matter physics [79] and more recently considered with ultracold atoms in optical lattices [69, 152].

I shall in this Chapter extend this perturbation theoretic calculation to systems with larger number of energy levels, and show that the SU(d)-invariant permutation Hamiltonian may be obtained as an effective Hamiltonian in the strong coupling regime of the d-species Hubbard model Hamiltonian. The derivation given is for the fermionic case, but with the addition of a hard-core interaction, and fine tuning of the inter-species interactions, one may obtain the same result from the bosonic case.

10.2 The Hubbard model

The behaviour of individual particles in a quantum solid is incredibly complex. There are huge numbers of particles, interacting in myriad ways; a full description of their behaviour is intractable, both analytically and numerically. Fortunately, however, there are several simple approximate models serving to give physicists detailed insight into the behaviour of such systems. One of the simplest is the *Hubbard model.*

This model is named after John Hubbard, who published a series of articles introducing the Hamiltonian in order to describe the behaviour of electrons in narrow energy bands in condensed matter systems [123, 124, 125, 126, 127, 128]. The original articles assumed that electrons moved around on a static lattice (formed by a regular distribution of ions). The dynamics of the N electrons are given by the Hamiltonian

$$H = \sum_{i=1}^{N} \left(\frac{\mathbf{p}_i^2}{2m} + V_I(\mathbf{x}_i) \right) + \sum_{i \neq j} V_C(\mathbf{x}_i - \mathbf{x}_j), \tag{10.1}$$

where V_I is the periodic potential given by the ions, V_C the electrostatic Coulomb repulsion $e^2/4\pi\epsilon_0|\mathbf{x}_i - \mathbf{x}_j|^2$ between the electrons, and $\mathbf{p}_i^2/2m$ the kinetic energy operator. By making a 'mean-field' approximation (assuming each electron moves in an 'average' field set up by the dynamics of the others) and second-quantising the equations, one ends up with the following Hamiltonian:

$$H = -\sum_{\langle ij \rangle} \sum_{\sigma=\uparrow,\downarrow} t_{ij}^{\sigma} \left(c_{\sigma i}^{\dagger} c_{\sigma j} + c_{\sigma j}^{\dagger} c_{\sigma i} \right) + U_{\uparrow\downarrow} \sum_{i=1}^{N} n_{\uparrow i} n_{\downarrow i}. \tag{10.2}$$

The notation $\langle ij \rangle$ denotes that the sum is taken over some lattice (with ions localised at its vertices), and the two possible spin states of the electrons are labelled with the pseudospin notation: $\uparrow$, $\downarrow$. The operator $c_{\sigma i}^{\dagger}$ is the creation operator for the electron in state σ at lattice site i. The first term in the Hamiltonian (10.2), which I shall denote H_0, is the 'hopping' term, where t_{ij}^{σ} is the hopping integral between lattice sites i and j for species σ; and the second term, H_1, is the on-site interaction, where $U_{\uparrow\downarrow} > 0$. Full details of this derivation are given in the standard texts on the Hubbard model [79, 88].

This is the original form of the Hubbard model, although there are now countless variations. The term 'Hubbard model' is often used as a generic term for all such models. The importance of these models stem from their applicability to a variety of physical phenomena. One of the most relevant is to condensed matter theory is *superexchange*. The standard exchange interaction occurs when wavefunctions of atoms 'overlap', and the Coulomb interaction between their electrons, coupled with Pauli exclusion, causes an effective spin–spin interaction between the atoms, without the spins physically interacting [33]. This wavefunction overlap is typically very short-ranged; however, on a lattice such interactions can be mediated over longer distances by *virtual hopping* processes. These are thus called *super*-exchange interactions, due to the longer range. These have recently been directly observed experimentally [232], and are the underlying mechanism by which the Hubbard model can 'simulate' magnetic systems (including spin chains). Since these effective interactions are mediated by quantum tunneling (and influenced by particle statistics), such magnetism is often referred to as *quantum* magnetism [206]. It has also been proposed by Anderson that these interactions may play an important role in high temperature superconductivity [12], adding further interest to such models.

The bosonic version of the Hubbard model (the *Bose–Hubbard model*) has also been extensively studied, predominantly in the field of optical lattices [9, 32, 91, 132, 133]. Although fermions can also be studied in such systems, bosons are easier to cool for practical reasons, and thus the Bose–Hubbard model has itself become the focus of much interest at the so-called 'interface' between condensed matter and atomic physics. Such systems offer great potential to realise many exotic phases of matter, but also are a strong candidate for the realisation of a universal quantum computer.

10.3 Strong-repulsion: effective Heisenberg antiferromagnet

Before considering the d-species case, it would be instructive to review the well-known derivation of the Heisenberg Hamiltonian (5.1) from the strong-coupling limit of the two-level Hubbard model, as considered by Emery [78] and Fradkin [88]. A slightly different, but effectively identical, derivation for the fermionic case is given in the book by Essler *et al.* [79]; a generalised Schrieffer–Wolff derivation also gives the same result [69, 112].

Consider the standard one-band Hubbard model:

$$H = -\sum_{\langle ij \rangle} \sum_{\sigma=\uparrow,\downarrow} t_{ij}^{\sigma} \left(c_{\sigma i}^{\dagger} c_{\sigma j} + c_{\sigma j}^{\dagger} c_{\sigma i} \right) + U_{\uparrow\downarrow} \sum_{i=1}^{N} n_{\uparrow i} n_{\downarrow i}. \tag{10.3}$$

This model need not just describe the evolution of electrons, but may be used to describe the evolution of a two-species system encoded in internal energy levels of atoms located at vertices

in a network, labelled with 'pseudospin' notation: $\uparrow$, $\downarrow$. The notation corresponds to that used in Equation (10.2).

Whilst the value of the interaction $U_{\uparrow\downarrow}$ cannot really be tuned once the atom used to encode the 'species' has been chosen, the hopping integrals could fluctuate due to slight fluctuations in the inter-atomic spacing; therefore I shall allow for general hopping integrals t_{ij}. I shall also allow for hopping integrals to vary for 'up' and 'down', in a similar manner to Kuklov and Svistunov [152] and Duan *et al.* [69]. The sum is taken over some network of N vertices, each of which has a two-level system (a qubit) and $\langle ij \rangle$ denotes the set of lattice sites that are connected (*i.e.* qubits placed in these lattice sites interact).

The derivation takes place in the half-filled regime (*i.e.* there are no unoccupied sites, and no sites with doubly occupancy) in the strong coupling limit $U_{\uparrow\downarrow} \gg t_{ij}$ for all t_{ij} (*i.e.* the chemical potential has been tuned such that the number fluctuations have been eliminated, and the energy cost of leaving this subspace is very large). In this limit, H_0 may be treated as a perturbation to H_1 and one obtains an expansion in terms of powers of t_{ij}^2/U.

Let $|\alpha\rangle$ be any of the 2^N states with every lattice site singly occupied by a spin (either up or down). Now $H_1 |\alpha\rangle = E_1 |\alpha\rangle$ and $H |\Psi\rangle = E |\Psi\rangle$ for any eigenstate $|\Psi\rangle$. Thus we can write

$$(E - H_1) |\Psi\rangle = H_0 |\Psi\rangle , \tag{10.4}$$

which has the formal solution

$$|\Psi\rangle = \frac{1}{E - H_1} H_0 |\Psi\rangle \tag{10.5}$$

$$= \frac{P}{E - H_1} H_0 |\Psi\rangle + \sum_\alpha |\alpha\rangle \frac{\langle \alpha | H_0 | \Psi \rangle}{E - E_1}, \tag{10.6}$$

where $H_1 |\alpha\rangle = E_1 |\alpha\rangle$, and $P = \mathbb{I} - \sum_\alpha |\alpha\rangle \langle\alpha|$ projects onto the space of perturbed states. Defining $|\Psi_\alpha\rangle$ as the solution of

$$|\Psi_\alpha\rangle = |\alpha\rangle + \frac{P}{E - H_1} H_0 |\Psi_\alpha\rangle . \tag{10.7}$$

and $a_\alpha := \langle \alpha | H_0 | \Psi \rangle / (E - E_1)$, it is clear that $|\Psi\rangle = \sum_\alpha a_\alpha |\Psi_\alpha\rangle$. This gives a recursive relation for $|\Psi_\alpha\rangle$. Iterating to first order, one obtains

$$|\Psi_\alpha\rangle \simeq |\alpha\rangle + \frac{P}{E - H_1} H_0 |\alpha\rangle \tag{10.8}$$

$$\simeq |\alpha\rangle - \frac{1}{U} H_0 |\alpha\rangle . \tag{10.9}$$

Since $\langle \alpha' | H_0 | \alpha \rangle = 0$, this gives

$$(E - E_1) a_\alpha = -\frac{1}{U} \sum_{\alpha'} \langle \alpha | H_0^2 | \alpha' \rangle \, a_{\alpha'} . \tag{10.10}$$

This is the same as the Schrödinger Equation for Hamiltonian $H_0' = -H_0^2/U$, where H_0' is the effective spin–spin interaction. This can be shown by expanding H_0^2/U:

$$H' = -\frac{H_0^2}{U} = -\sum_{\alpha,\beta=\uparrow,\downarrow}\sum_{\langle ij\rangle,\langle kl\rangle}\frac{t_{ij}^{\alpha}t_{kl}^{\beta}}{U}\left(c_{\alpha i}^{\dagger}c_{\alpha j}+c_{\alpha j}^{\dagger}c_{\alpha i}\right)\left(c_{\beta k}^{\dagger}c_{\beta l}+c_{\beta l}^{\dagger}c_{\beta k}\right). \tag{10.11}$$

Upon expansion of the two parentheses, one must bear in mind the hard-core constraint: since we have assumed that the energy $U_{\uparrow\downarrow}$ is very large, states with double-occupancy (with opposite pseudospin) at any given lattice site will have an extra energy U relative to those with single-occupation everywhere, and by assumption this is a large energy cost. States with the same pseudospin are forbidden by Pauli exclusion in the fermionic case; and can be neglected in the bosonic case by adding a large on-site interaction for particles of the same species (at this stage, this need not be 'hard-core' in the sense that the probability is strictly zero; as long as the probability of this is comparable to the probability of double-occupation of species of opposite pseudospin).

This constraint implies that if the operator $\left(c_{\beta k}^{\dagger}c_{\beta l}+c_{\beta l}^{\dagger}c_{\beta k}\right)$ moves a particle from site k to site l, the application of the operator $\left(c_{\alpha i}^{\dagger}c_{\alpha j}+c_{\alpha j}^{\dagger}c_{\alpha i}\right)$ must either move it back, or more a particle of the opposite pseudospin from l to k. Thus, upon expansion, one only keeps terms such that $(i,j)=(k,l)$ or $(i,j)=(l,k)$. This gives:

(i) $(i,j)=(k,l)$

$$\left(c_{\alpha i}^{\dagger}c_{\alpha j}+c_{\alpha j}^{\dagger}c_{\alpha i}\right)\left(c_{\beta i}^{\dagger}c_{\beta j}+c_{\beta j}^{\dagger}c_{\beta i}\right)$$

$$= \underbrace{c_{\alpha i}^{\dagger}c_{\alpha j}c_{\beta i}^{\dagger}c_{\beta j}}_{\text{double occupancy}} + \underbrace{c_{\alpha i}^{\dagger}c_{\alpha j}c_{\beta j}^{\dagger}c_{\beta i}}_{=\xi c_{\alpha i}^{\dagger}c_{\beta i}c_{\beta j}^{\dagger}c_{\alpha j}} + \underbrace{c_{\alpha j}^{\dagger}c_{\alpha i}c_{\beta i}^{\dagger}c_{\beta j}}_{=\xi c_{\beta i}^{\dagger}c_{\alpha i}c_{\alpha j}^{\dagger}c_{\beta j}} + \underbrace{c_{\alpha j}^{\dagger}c_{\alpha i}c_{\beta j}^{\dagger}c_{\beta i}}_{\text{double occupancy}} \tag{10.12}$$

$$= \xi\left\{c_{\alpha i}^{\dagger}c_{\beta i}c_{\beta j}^{\dagger}c_{\alpha j}+c_{\beta i}^{\dagger}c_{\alpha i}c_{\alpha j}^{\dagger}c_{\beta j}\right\}; \tag{10.13}$$

(ii) $(i,j)=(l,k)$

$$\left(c_{\alpha i}^{\dagger}c_{\alpha j}+c_{\alpha j}^{\dagger}c_{\alpha i}\right)\left(c_{\beta j}^{\dagger}c_{\beta i}+c_{\beta i}^{\dagger}c_{\beta j}\right)$$

$$= \underbrace{c_{\alpha i}^{\dagger}c_{\alpha j}c_{\beta j}^{\dagger}c_{\beta i}}_{=\xi c_{\alpha i}^{\dagger}c_{\beta i}c_{\beta j}^{\dagger}c_{\alpha j}} + \underbrace{c_{\alpha i}^{\dagger}c_{\alpha j}c_{\beta i}^{\dagger}c_{\beta j}}_{\text{double occupancy}} + \underbrace{c_{\alpha j}^{\dagger}c_{\alpha i}c_{\beta i}^{\dagger}c_{\beta j}}_{\text{double occupancy}} + \underbrace{c_{\alpha j}^{\dagger}c_{\alpha i}c_{\beta i}^{\dagger}c_{\beta j}}_{=\xi c_{\beta i}^{\dagger}c_{\alpha i}c_{\alpha j}^{\dagger}c_{\beta j}} \tag{10.14}$$

$$= \xi\left\{c_{\alpha i}^{\dagger}c_{\beta j}c_{\beta i}^{\dagger}c_{\alpha j}+c_{\beta j}^{\dagger}c_{\alpha i}c_{\alpha j}^{\dagger}c_{\beta i}\right\}; \tag{10.15}$$

where ξ denotes the particles statistics ($\xi=+1$ for bosons, $\xi=-1$ for fermions[1]). This thus

[1] This allows the bosonic commutation relation $[c_{\alpha i},c_{\beta j}^{\dagger}]=\delta_{ij}\delta_{\alpha\beta}$ and the fermionic anticommutation relation $\{c_{\alpha i},c_{\beta j}^{\dagger}\}=\delta_{ij}\delta_{\alpha\beta}$ to be written together as $c_{\alpha i}^{\dagger}c_{\beta j}-\xi c_{\beta j}^{\dagger}c_{\alpha i}=\delta_{ij}\delta_{\alpha\beta}$.

gives the effective Hamiltonian

$$H' = -\frac{H_0^2}{U} = -\sum_{\alpha,\beta=\uparrow,\downarrow}\sum_{\langle ij\rangle}\frac{2\xi t_{ij}^{\alpha}t_{ij}^{\beta}}{U}\left(c_{\alpha i}^{\dagger}c_{\beta i}c_{\beta j}^{\dagger}c_{\alpha j} + c_{\beta i}^{\dagger}c_{\alpha i}c_{\alpha j}^{\dagger}c_{\beta j}\right) \tag{10.16}$$

$$= -\sum_{\alpha,\beta=\uparrow,\downarrow}\sum_{\langle ij\rangle}\frac{4\xi t_{ij}^{\alpha}t_{ij}^{\beta}}{U}c_{\alpha i}^{\dagger}c_{\beta i}c_{\beta j}^{\dagger}c_{\alpha j}. \tag{10.17}$$

For the case of isotropic couplings ($t_{ij}^{\uparrow} = t_{ij}^{\downarrow}$) this is in fact the two-body, two-level exchange operator [227], which is equivalent to the spin-1/2 Heisenberg Hamiltonian (5.1) (when the identity operator is added). The identity term may be neglected, since this just adds a constant to the ground state energy, and the remaining Hamiltonian is

$$H_0' = -\sum_{\langle ij\rangle} J_{ij}\mathbf{s}_i \cdot \mathbf{s}_j, \tag{10.18}$$

with exchange couplings $J_{ij} = 4\xi t_{ij}^2/U$. It is clear that the bosonic case gives the ferromagnetic regime, and the fermionic case the antiferromagnetic regime. The bosonic case may also be shown to be equal to the *anti*-ferromagnetic Heisenberg Hamiltonian, if one allows for general species-dependent tunneling integrals, and adds a hard-core interaction [69, 152] (the above derivation assumed that the on-site repulsion was large, but not neccessarily 'hard-core', and gave the ferromagnet for the bosonic case). Without this extra term, and with isotropic couplings, the bosonic case gives the ferromagnetic counterpart to the above Hamiltonian.

As previously noted by Duan *et al.* the ability to simulate the full range of Hamiltonians (both ferromagnetic and antiferromagnetic) with bosons alone is important, since bosonic atoms are generally easier to cool in an optical lattice [69].

10.4 Strong-repulsion: d-species permutation

It is straightforward to extend the above analysis to an SU(d)-invariant permutation Hamiltonian. As previously mentioned, such a Hamiltonian may be considered a generalisation of the Heisenberg model, where the Pauli matrices are replaced with the generators of the group SU(d). As we have already seen, such a Hamiltonian may be written (allowing for general couplings)

$$H = \sum_{\langle ij\rangle} J_{ij}P_{ij}. \tag{10.19}$$

The sum is taken over some network of qudits. Generalising the Hubbard Hamiltonian (10.3) to a model allowing for d species gives:

$$H = -\sum_{i,j}\sum_{\sigma=1}^{d} t_{ij}^{\sigma}\left(c_{\sigma i}^{\dagger}c_{\sigma j} + c_{\sigma j}^{\dagger}c_{\sigma i}\right) + \sum_{i}\sum_{\sigma\neq\sigma'} U_{\sigma,\sigma'}n_{\sigma i}n_{\sigma' i}. \tag{10.20}$$

We continue to consider the model in the limit $U \gg t_{ij}$, this time in the $1/d$-filling regime (to ensure single-site occupancy). The analysis continues analogously to the spin-1/2 case, but the effective Hamiltonian in the case of isotropic tunneling integrals ($t_{ij}^{\sigma} = t_{ij}$ for all σ) is now

$$H' = -\sum_{\alpha,\beta=1}^{d} \sum_{\langle ij \rangle} \frac{4\xi t_{ij}^2}{U} c_{\alpha i}^{\dagger} c_{\beta i} c_{\beta j}^{\dagger} c_{\alpha j}, \tag{10.21}$$

which is exactly the exchange Hamiltonian (10.19) required, for fermions ($\xi = -1$) or bosons ($\xi = +1$).

10.5 Preparation of qudit singlets in 1D

The Hubbard model has been used to describe many physical systems; the regime relevant here is realisable with ultracold atoms in optical lattices. Two-level atoms at 1/2-filling realise the Heisenberg model [152], and atoms with d degenerate levels—*e.g.* d hyperfine levels [174] where $d = 10$ is routine with ^{40}K [149] and much higher d is possible with Er [164]—can realise the permutation Hamiltonian. The fermonic case is straightforward: as shown above, isotropic couplings suffice to realise the permutation Hamiltonian. The bosonic case, however, requires the addition of a hard-core repulsion (to completely eliminate double-occupancy), and careful tuning of species-dependent tunneling integrals, since the isotropic case in the bosonic regime gives the ferromagnetic permutation Hamiltonian, rather than the *anti*-ferromagnetic Hamiltonian.

To prepare the singlet, a d-site optical lattice is first loaded with d-level atoms in the translationally-invariant state $|1\rangle^{\otimes d}$ (with all $t_{ij} \sim 0$). An inhomogenous B-field coupled to the hyperfine levels is applied to select this as the unique ground state within the $1/d$-filling regime and to allow parity to be broken in the subsequent evolution. The ratios t_{ij}/U are then increased adiabatically (the standard method for ground state preparation in optical lattices [97]) to reach finite, but small $t_{ij} \ll U$ (still in the Mott insulator regime); similarly the B-field is slowly tuned to zero. The system's state evolves to the final ground state: the singlet.

Part VI

Summary

Chapter 11

Summary

In this thesis, I have made a very modest contribution to the field of quantum information theory by studying the entanglement extractable from several many-body systems, and the properties of the entanglement naturally present. I have listed below the main results of each section of the thesis.

Part II: Extraction of entanglement from dynamics

For entanglement to be useful as a resource, it needs to be shared between laboratories separated by large distances. In this section, I proposed a scheme to extract entanglement through the natural dynamics of a system of coupled three-level quantum systems. The interactions between nearest-neighbours creates entanglement, which then propogates through the system, and is extracted through local measurements.

This work is published in Reference [104].

Part III: Extraction of entanglement from a single specimen

The amount of entanglement present in a physical system is often quantified with respect to the number of EPR-singlets it can be converted into, in the *asymptotic* limit. However, in realistic, physical scenarios one often only has access to a single-copy of a physical system. How much entanglement can be extracted from a single specimen, and how is this related to the amount of entanglement accessible in the asymptotic limit?

In this section, I introduced the formal definition of the *single-copy entanglement*, and showed that for paridgmatic Affleck–Kennedy–Lieb–Tasaki chain, the single-copy entanglement is equal to the von Neumann entropy in the thermodynamic limit, in contrast to the case of gapless chain close to criticality.

This work is published in Reference [102].

Part IV: Antisymmetric states

In this section, I considered a specific multipartite state with a high degree of symmetry under the permutation of its subsystms. I showed that local measurements on some of these qudits project the unmeasured qudits onto a smaller singlet, regardless of the choice of measurement basis at each measurement, and the outcome of that measurement. It follows that the entanglement is highly *persistent*, and that through local measurements, a large amount of entanglement may be established between spatially-separated parties for subsequent use in distributed quantum computation.

This work is published in Reference [103].

Part V: Physical realisation of antisymmetric states

In the section, I review the Hubbard model and its importance in many-body physics, and showed that in a particular regime of this model in one spatial dimension, it effectively becomes a permutation Hamiltonian, and thus its ground state is the qudit singlet considered in Part IV.

Chapter 12

Open problems

Following on from the work in this thesis, a number of open problems present themselves; all these avenues for future research lie within the broader area of symmetry and entanglement of many-body systems.

Single-copy entanglement

The behaviour of the single-copy entanglement for gapped systems remains an open problem, and the initial motivation for studying the single-copy entanglement of a bipartition of a valence bond solid was as a first step in obtaining a more general statement regarding the relationship between this quantity and the presence of absence of a gap in the energy spectrum. An immediately apparent problem, then, for future work is to extend this analysis to general gapped systems; presumably this would be done through the formalism of matrix-product states.

Since gapped systems are particularly amenable to efficient classical simulation through matrix-product states, it would appear that there would thus be an indirect relation between the simulability of a given state and its single-copy entanglement.

Implementation of the permutation Hamiltonian in optical lattices

In Part V, I showed that the permutation Hamiltonian can be obtained from the Hubbard model in the strong-coupling limit, in principle. However, it is unclear whether this is physically realistic, given current experimental technology. In future work, I would like to explore the feasibility of this implementation, especially in the light of recent observations of superexchange interactions in optical lattices. The fact that these states can be used to encode many qubit states is decoherence-free subspaces suggests that one could implement a quantum 'memory' in an optical lattice, if one had the ability to generate such states.

Symmetry in many-body systems and entanglement classes

The qudit states studied in Part IV are highly antisymmetric, and one of my aims for future

research is to obtain a deeper understanding of this symmetry, and that of related states. In particular, I wish to explore the connection between symmetries present in physical states of many-body systems, the entanglement class to which that state belongs, and its robustness to environmental noise (modelled by local measurements).

Use of many-body systems as a resource for quantum computation

A fruitful avenue for future research is to find out what physical states that are already known may be used for such measurement-based quantum computation. The qudit singlets might be useful as a potential resource, since they do not admit an efficient classical approximation (according to Vidal's criterion [241]). I wish to understand whether this is indeed the case, and whether there is a connection between the permutational symmetry of a given state, and its power as a computational resource.

I intend the central themes of my future research to be

- to quantify the amount of entanglement occurring in physical systems, particularly with the aim of sharing entanglement over large distances for subsequent use as a communication or computational resource;
- to see whether the study of such entanglement may be used to understand the structure of such states, and provide any physical insight;
- to find out what sort of state interesting in quantum information theory may be feasibly generated in regimes of well-known physical models, particularly in systems of ultracold atoms;
- to understand the connection between the symmetry of a physical state, its physical properties, and its interest in quantum information theory.

Part VII

Appendix

Appendix A

Spin coherent states

The coherent state for oscillators [19, 218] is defined in terms of the number basis $\{|n\rangle\}$ thus:

$$|\alpha\rangle = \frac{1}{\sqrt{\pi}} e^{-|\alpha|^2/2} \exp(\alpha a^\dagger) |0\rangle ; \tag{A.1}$$

this is defined to be an eigenstate of the annihilation operator a. By anology, the *spin* coherent state [192] is defined to be an eigenstate of the spin raising operator S_+ thus:

$$|\mu\rangle = \frac{1}{(1+|\mu|^2)^{2S}} \exp(\mu S_-) |S, S\rangle , \tag{A.2}$$

where $|S, m\rangle$ is the spin state with $\mathbf{S}^2 = S(S+1)$ and $S_z = m$, and μ is a parameter. Parametrizing this with $\mu = \tan\theta/2$ gives

$$|\Omega\rangle = \left(\cos\frac{\theta}{2}\right)^{2S} \exp\left\{\tan\frac{\theta}{2} e^{i\phi} S_-\right\} |S, S\rangle \tag{A.3}$$

$$= \left(\cos\frac{\theta}{2}\right)^{2S} \sum_{m=0}^{\infty} \left(\tan\frac{\theta}{2}\right)^m \frac{e^{i\phi}}{m!} \sqrt{\frac{m!(2S)!}{(2S-m)!}} |S, S-m\rangle \tag{A.4}$$

$$= \sum_{m=-S}^{S} u^{S+m} v^{S-m} \sqrt{\binom{2S}{S+m}} |S, m\rangle , \tag{A.5}$$

where the state is now denoted $|\Omega\rangle$ to make it obvious that there is a geometric interpretation: each state defined by (θ, ϕ) is equivalent to a point on the unit sphere. In the last line I have used the definitions $(u, v) = (e^{i\phi/2}\cos(\theta/2), e^{-i\phi/2}\sin(\theta/2))$.

We thus have

$$\langle\Omega|S, m\rangle = \sqrt{\binom{2S}{S+m}} u^{S+m} v^{S-m} . \tag{A.6}$$

Comparing this to the Schwinger boson representation

$$|S, m\rangle = \frac{(a^\dagger)^{S+m} (b^\dagger)^{S-m}}{\sqrt{(S+m)!(S-m)!}} |0\rangle , \tag{A.7}$$

we see that one can replace the operators $a^\dagger$ and $b^\dagger$ by the numbers u and v, respectively, and multiplying by $\sqrt{(2S)!}$ when they occur in pairs.

Note that these states form an overcomplete set, and have the following completeness relation:

$$\frac{2S+1}{4\pi}\int \mathrm{d}\Omega\, |\Omega\rangle\langle\Omega| = \mathbb{I} \tag{A.8}$$

In this representation, for any operator $\mathcal{A}$

$$\langle\mathcal{A}\rangle = \frac{2S+1}{4\pi}\int \mathrm{d}\Omega\, \langle\Omega|\mathcal{A}|\Omega\rangle\,. \tag{A.9}$$

Further properties of this state are given in Reference [192].

Bibliography

[1] G. Adesso and F. Illuminati. Strong monogamy of bipartite and genuine multipartite entanglement: the Gaussian case. *Physical Review Letters*, 99:150501, 2007.

[2] I. Affleck. Quantum spin chains and the Haldane gap. *Journal of Physics: Condensed Matter*, 1:3047, 1989.

[3] I. Affleck, T. Kennedy, E. Lieb, and H. Tasaki. Rigorous results on valence-bond ground states in antiferromagnets. *Physical Review Letters*, 59:799, 1987.

[4] I. Affleck, T. Kennedy, E. Lieb, and H. Tasaki. Valence bond ground states in isotropic quantum antiferromagnets. *Communications in Mathematical Physics*, 115:477, 1988.

[5] I. Affleck and E. H. Lieb. A proof of part of Haldane's conjecture on spin chains. *Letters in Mathematical Physics*, 12:57, 1985.

[6] P. Agrawal, P. Parashar, and A. K. Pati. Exact remote state preparation for multiparticles. *quant-ph/0304006*, 2003.

[7] C. Albanese, M. Christandl, N. Datta, and A. Ekert. Mirror inversion of quantum states in linear registers. *Physical Review Letters*, 93:230502, 2004.

[8] F. Alet, S. Capponi, N. Laflorencie, and M. Mambrini. Valence bond entanglement entropy. *Physical Review Letters*, 99:117204, 2007.

[9] E. Altman, W. Hofstetter, E. Demler, and M. D. Lukin. Phase diagram of two-component bosons on an optical lattice. *New Journal of Physics*, 5:113, 2003.

[10] L. Amico, R. Fazio, A. Osterloh, and V. Vedral. Entanglement in many-body systems. *Reviews of Modern Physics*, 80:517, 2007.

[11] L. Amico, A. Osterloh, F. Plastina, R. Fazio, and G. M. Palma. Dynamics of entanglement in one-dimensional spin systems. *Physical Review A*, 69:022304, 2004.

[12] P. W. Anderson. The resonating valence bond state in La_2CuO_4 and superconductivity. *Science*, 235:1196, 1987.

[13] D. P. Arovas and A. Auerbach. Functional integral theories of low-dimensional quantum Hubbard models. *Physical Review B*, 38:316, 1988.

[14] D. P. Arovas, A. Auerbach, and F. D. M. Haldane. Extended Heisenberg models of antiferromagnetism: analogies to the fractional quantum Hall effect. *Physical Review Letters*, 60:531, 1988.

[15] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Physical Review Letters*, 49:1804, 1982.

[16] A. Aspect, P. Grangier, and G. Roger. Experimental realization of Einstein–Podolsky–Rosen–Bohm *gedankenexperiment*: a new violation of Bell's inequalities. *Physical Review Letters*, 49:91, 1982.

[17] J. Babudjian. Exact solution of the one-dimensional isotropic Heisenberg chain with arbitrary spins S. *Physics Letters A*, 90:479, 1982.

[18] J. Babudjian. Exact solution of the isotropic Heisenberg chain with arbitrary spins: thermodynamics of the model. *Nuclear Physics B*, 215:317, 1983.

[19] S. M. Barnett and P. M. Radmore. *Methods in theoretical quantum optics.* Oxford University Press, 1997.

[20] J. S. Bell. On the Einstein–Podolsky–Rosen paradox. *Physics*, 1:195, 1964. Reproduced in Reference [22].

[21] J. S. Bell. Bertlmann's socks and the nature of reality. *Journal de Physique*, 3:C2 41, 1981. Reproduced in Reference [22].

[22] J. S. Bell. *Speakable and unspeakable in quantum mechanics.* Cambridge University Press, second edition, 2004.

[23] P. Benioff. The computer as a physical system: a microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22:563, 1980.

[24] C. H. Bennett. Demons, engines and the second law. *SIAM Journal of Computing*, 18:766, 1989.

[25] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Physical Review A*, 53:2046, 1996.

[26] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. *Physical Review Letters*, 70:1895, 1993.

[27] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 78:2031, 1996.

[28] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. Smolin, and W. K. Wootters. Quantum nonlocality without entanglement. *Physical Review A*, 59:1070, 1999.

[29] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54:3824, 1996.

[30] R. Bhatia. *Matrix analysis.* Springer-Verlag, 1997.

[31] A. Biswas and G. S. Agarwal. Transfer of an unknown quantum state, quantum networks, and memory. *Physical Review A*, 70:022323, 2004.

[32] I. Bloch, J. Dalibard, and W. Zwerger. Many-body physics with ultracold gases. *Reviews of Modern Physics*, 80:885, 2008.

[33] S. J. Blundell. *Magnetism in condensed matter.* Oxford University Press, 2001.

[34] D. Bohm. *Quantum theory.* Prentice Hall, 1951.

[35] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Physical Review*, 108:1070, 1957.

[36] L. Bombelli, R. K. Koul, J. Lee, and R. D. Sorkin. Quantum source of entropy for black holes. *Physical Review D*, 34:373, 1986.

[37] M. Born. *The Born–Einstein letters: friendship, politics and physics in uncertain times.* Walker, New York, 1971.

[38] S. Bose. Quantum communication through an unmodulated spin chain. *Physical Review Letters*, 91:207901, 2003.

[39] S. Bose, B.-Q. Jin, and V. E. Korepin. Quantum communication through a spin-ring with twisted boundary conditions. *Physical Review A*, 72:022345, 2005.

[40] S. Bose, V. Vedral, and P. L. Knight. Multiparticle generalization of entanglement swapping. *Physical Review A*, 57:822, 1998.

[41] R. Bousso. The holographic principle. *Reviews of Modern Physics*, 74:825, 2002.

[42] G. Brassard and A. A. Méthot. Can quantum-mechanical description of physical reality be considered *in*complete? *International Journal of Quantum Information*, 4:45, 2006.

[43] H. J. Briegel and R. Raussendorf. Persistent entanglement in arrays of interacting particles. *Physical Review Letters*, 86:910, 2001.

[44] D. Bruß. Characterizing entanglement. *Journal of Mathematical Physics*, 43:4237, 2002.

[45] J. Bub. *Interpreting the quantum world.* Cambridge University Press, 1997.

[46] D. Burgarth and S. Bose. Conclusive and arbitrarily perfect quantum state transfer using parallel spin chain channels. *Physical Review A*, 71:052315, 2005.

[47] D. Burgarth and S. Bose. Perfect quantum state transfer with randomly coupled quantum chains. *New Journal of Physics*, 7:135, 2005.

[48] D. Burgarth, V. Giovanetti, and S. Bose. Efficient and perfect state transfer in quantum chains. *Journal of Physics A: Mathematical and General*, 38:6793, 2005.

[49] A. Cabello. N-particle N-level singlet states: some properties and applications. *Physical Review Letters*, 89:100402, 2002.

[50] A. Cabello. Solving the liar detection problem using the four-qubit singlet state. *Physical Review A*, 68:012304, 2003.

[51] A. Cabello. Supersinglets. *Journal of Modern Optics*, 50:1049, 2003.

[52] P. Calabrese and J. Cardy. Entanglement entropy and quantum field theory. *Journal of Statistical Mechanics: Theory and Experiment*, page P06002, 2004.

[53] R. W. Chhajlany, Tomczak P., and A. Wójcik. Topological estimator of block entanglement for Heisenberg antiferromagnets. *Physical Review Letters*, 99:167204, 2007.

[54] M. Christandl. *The structure of bipartite quantum states: insights from group theory and cryptography.* PhD thesis, University of Cambridge, 2006.

[55] M. Christandl, N. Datta, T. C. Dorlas, A. Ekert, A. Kay, and A. J. Landahl. Perfect transfer of arbitrary states in quantum spin networks. *Physical Review A*, 71:032312, 2005.

[56] M. Christandl, N. Datta, A. Ekert, and A. J. Landahl. Perfect state transfer in quantum spin networks. *Physical Review Letters*, 92:187902, 2004.

[57] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi. Quantum state transfer and entanglement distribution among distant nodes in a quantum network. *Physical Review Letters*, 78:3221, 1997.

[58] S. Clark. Valence bond solid formalism for d-level one-way quantum computation. *Journal of Physics A: Mathematical and General*, 39:2701, 2006.

[59] S. Clark, C. Moura Alves, and D. Jaksch. Efficient generation of graph states for quantum computation. *New Journal of Physics*, 7:124, 2005.

[60] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23:880, 1969.

[61] V. Coffman, J. Kundu, and W. K. Wootters. Distributed entanglement. *Physical Review A*, 61:052306, 2000.

[62] M. Cramer, J. Eisert, M. B. Plenio, and J. Dreißig. Entanglement-area law for general bosonic harmonic lattice systems. *Physical Review A*, 73:012309, 2006.

[63] F. de Pasquale, G. Giorgi, and S. Paganelli. Teleportation on a quantum dot array. *Physical Review Letters*, 93:120502, 2004.

[64] B. d'Espagnat. *Conceptual foundations of quantum mechanics.* Perseus, second edition, 1999.

[65] D. Deutsch. *The fabric of reality.* Penguin, 1997.

[66] W. M. Dickson. *Quantum chance and non-locality.* Cambridge University Press, 1998.

[67] P. A. M. Dirac. *General theory of relativity.* Princeton University Press, 1975.

[68] M. Donald, M. Horodecki, and O. Rudolph. The uniqueness theorem for entanglement measures. *Journal of Mathematical Physics*, 43:4252, 2002.

[69] L.-M. Duan, E. Demler, and M. D. Lukin. Controlling spin exchange interactions of ultracold atoms in optical lattices. *Physical Review Letters*, 91:090402, 2003.

[70] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Physical Review A*, 62:062314, 2000.

[71] A. Einstein. *Relativity.* Dover, fifteenth edition, 1954.

[72] A. Einstein, H. A. Lorentz, H. Weyl, and H. Minkowski. *The principle of relativity.* Dover, 1932.

[73] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:780, 1935.

[74] J. Eisert and H. J. Briegel. The Schmidt measure as a tool for quantifying multi-particle entanglement. *Physical Review A*, 64:022306, 2001.

[75] J. Eisert and M. Cramer. Single-copy entanglement in critical quantum spin chains. *Physical Review A*, 72:042112, 2005.

[76] J. Eisert, M. B. Plenio, S. Bose, and J. Hartley. Towards quantum entanglement in nanoelectromechanical devices. *Physical Review Letters*, 93:190402, 2004.

[77] A. Ekert and P. L. Knight. Entangled quantum systems and the Schmidt decomposition. *American Journal of Physics*, 63:415, 1994.

[78] V. J. Emery. Theory of the quasi-one-dimensional electron gas with strong "on-site" interactions. *Physical Review B*, 14:2989, 1976.

[79] F. H. L. Essler, H. Frahm, F. Gohmann, A. Klumper, and V. E. Korepin. *The one-dimensional Hubbard model.* Cambridge University Press, 2005.

[80] H. Fan, V. Korepin, and V. Roychowdhury. Entanglement in a valence-bond solid state. *Physical Review Letters*, 93:227203, 2004.

[81] H. Fan, V. Korepin, V. Roychowdhury, C. Hadley, and S. Bose. Boundary effects to entropy and entanglement of the spin-1 valence-bond solid. *Physical Review B*, 76:014428, 2007.

[82] M. Fannes, B. Nachtergaele, and R. F. Werner. Finitely correlated states on quantum spin chains. *Communications in Mathematical Physics*, 144:443, 1992.

[83] E. Fermi. *Thermodynamics.* Dover, 1936.

[84] R. P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 21:467, 1982.

[85] R. P. Feynman. Quantum mechanical computers. *Optics News*, 11:11, 1985.

[86] R. P. Feynman. *Feynman lectures on computation.* Penguin, 1996.

[87] J. Fitzsimons and J. Twamley. Superballistic diffusion of entanglement in disordered spin chains. *Physical Review A*, 72:050301, 2005.

[88] E. Fradkin. *Field theories of condensed matter systems.* Addison Wesley, 1991.

[89] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variables theories. *Physical Review Letters*, 28:938, 1972.

[90] W.-D. Freitag and E. Müller-Hartmann. Complete analysis of two spin correlations of valence bond solid chains for all integer spins. *Zeitschrift für Physik B: Condensed Matter*, 83:381, 1991.

[91] J. J. Garcá-Ripoll and J. I. Cirac. Spin dynamics for bosons in an optical lattice. *New Journal of Physics*, 5:76, 2003.

[92] S. M. Giampaolo, F. Illuminati, A. Di Lisi, and S. De Siena. Engineering massive quantum memories by topologically time-modulated spin rings. *Laser Physics*, 16:1411, 2006.

[93] N. Gisin. Hidden quantum nonlocality revealed by local filters. *Physics Letters A*, 210:151, 1996.

[94] L. Goldschlager and A. Lister. *Computer science: a modern introduction.* Prentice Hall, second edition, 1988.

[95] I. S. Gradshteyn and I. M. Rhyzhik. *Tables of integrals, series, and products.* Academic Press, 1980.

[96] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger. Bell's theorem without inequality. *American Journal of Physics*, 58:1131, 1990.

[97] M. Greiner, O. Mandel, T. Esslinger, T. W. Hänsch, and I. Bloch. Quantum phase transition from a superfluid to a Mott insulator ina gas of ultracold atoms. *Nature*, 415:39, 2002.

[98] A. A. Grib and W. A. Rodrigues, Jr. *Nonlocality in quantum physics.* Kluwer Academic, 1999.

[99] E. K. U. Gross, E. Runge, and O. Heinonen. *Many-particle theory.* Institute of Physics Publishing, 1991.

[100] L. Gurvits. Quantum matching theory (with new complexity theoretic, combinatorial and topological insights on the nature of the quantum entanglement). *quant-ph/0201022*, 2002.

[101] L. Gurvits. Classical deterministic complexity of Edmunds' problem and quantum entanglement. *quant-ph/0303055*, 2003.

[102] C. Hadley. Single-copy entanglement in a gapped quantum spin chain. *Physical Review Letters*, 100:177202, 2008.

[103] C. Hadley and S. Bose. Multi-level, multi-party singlets as ground states and their role in ententanglement distribution. *Physical Review A*, 77:050308(R), 2008.

[104] C. Hadley, A. Serafini, and S. Bose. Entanglement creation and distribution on a graph of exchange-coupled qutrits. *Physical Review A*, 72:052333, 2005.

[105] F. D. M. Haldane. Continuum dynamics of the 1D Heisenberg antiferromagnet: Identification with the O(3) nonlinear sigma model. *Physics Letters A*, 93:464, 1983.

[106] F. D. M. Haldane. Nonlinear field theory of large-spin Heisenberg antiferromagnets: semiclassically quantized solitons of the one-dimensional easy-axis Néel state. *Physical Review Letters*, 50:1153, 1983.

[107] F. D. M. Haldane. 'theta physics' and quantum spin chains. *Journal of Applied Physics*, 57:3359, 1985.

[108] H. Haselgrove. Optimal state encoding for quantum walks and quantum communication over spin systems. *Physical Review A*, 72:062326, 2005.

[109] M. B. Hastings. Locality in quantum and Markov dynamics on lattices and networks. *Physical Review Letters*, 93:140402, 2004.

[110] M. B. Hastings. An area law for one-dimensional quantum systems. *Journal of Statistical Mechanics: Theory and Experiment*, page P08024, 2007.

[111] M. B. Hastings and T. Koma. Spectral gap and exponential decay of correlations. *Communications in Mathematical Physics*, 265:781, 2004.

[112] A. C. Hewson. *The Kondo problem to heavy fermions.* Cambridge University Press, 1993.

[113] C. Holzhey, F. Larsen, and F. Wilczek. Geometric and renormalized entropy in conformal field theory. *Nuclear Physics B*, 424:443, 1994.

[114] R. A. Horn and C. R. Johnson. *Topics in matrix analysis.* Cambridge University Press, 1991.

[115] M. Horodecki. Entanglement measures. *Quantum Information and Computation*, 1:3, 2001.

[116] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223:1, 1996.

[117] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: Is there a "bound" entanglement in nature? *Physical Review Letters*, 80:5239, 1998.

[118] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *Physical Review Letters*, 84:2014, 2000.

[119] M. P. Horodecki, P. Horodecki, and R. Horodecki. Inseparable two spin-1/2 density matrices can be distilled to a singlet form. *Physical Review Letters*, 78:574, 1997.

[120] P. Horodecki, M. Horodecki, and R. Horodecki. Entanglement and thermodynamical analogies. *Acta Physica Slovenia*, 47:128, 1998.

[121] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Physical Review Letters*, 82:1056, 1999.

[122] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki. Quantum entanglement. *quant-ph/0702225*, 2007.

[123] J. Hubbard. Electron correlations in narrow energy bands. *Proceedings of the Royal Society of London*, 276:238, 1963.

[124] J. Hubbard. Electron correlations in narrow energy bands. II. Degenerate band case. *Proceedings of the Royal Society of London*, 277:237, 1964.

[125] J. Hubbard. Electron correlations in narrow energy bands. III. Improved solution. *Proceedings of the Royal Society of London*, 281:401, 1964.

[126] J. Hubbard. Electron correlations in narrow energy bands. IV. Atomic representation. *Proceedings of the Royal Society of London*, 285:542, 1965.

[127] J. Hubbard. Electron correlations in narrow energy bands. V. A perturbation expansion about atomic limit. *Proceedings of the Royal Society of London*, 296:82, 1967.

[128] J. Hubbard. Electron correlations in narrow energy bands. VI. Connexion with many-body perturbation theory. *Proceedings of the Royal Society of London*, 296:100, 1967.

[129] R. Hübener, C. Kruszynska, L. Hartmann, W. Dür, F. Verstraete, J. Eisert, and M. B. Plenio. Renormalization algorithm with graph enhancement. *arXiv:0802.1211*, 2008.

[130] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density operator. *Physics Letters A*, 183:14, 1993.

[131] L. M. Ioannou. Computational complexity of the quantum separability problem. *Quantum Information and Computation*, 7:335, 2007.

[132] D. Jaksch, C. Bruder, J. I. Cirac, C. W. Gardiner, and P. Zoller. Cold bosonic atoms in optical lattices. *Physical Review Letters*, 81:3108, 1998.

[133] D. Jaksch and P. Zoller. The cold atom Hubbard toolbox. *Annals of Physics*, 315:52, 2005.

[134] E. T. Jaynes. Information theory and statistical mechanics. *Physical Review*, 106:620, 1957.

[135] E. T. Jaynes. Information theory and statistical mechanics II. *Physical Review*, 108:171, 1957.

[136] B.-Q. Jin and V. E. Korepin. Localizable entanglement in antiferromagnetic spin chains. *Physical Review A*, 69:062314, 2004.

[137] B.-Q. Jin and V. E. Korepin. Quantum spin chain, Toeplitz determinants and the Fisher–Hartwig conjecture. *Journal of Statistical Physics*, 116:79, 2004.

[138] D. Jonathan and M. B. Plenio. Minimal conditions for local pure-state manipulation. *Physical Review Letters*, 83:1455, 1999.

[139] R. Jozsa. Illustrating the concept of quantum information. *IBM Journal of Research and Development*, 48:79, 2004.

[140] R. Jozsa and B. Schumacher. A new proof of the quantum source coding theorem. *Journal of Modern Optics*, 41:2343, 1994.

[141] M. Karbach, K. Hu, and G. Müller. Introduction to the Bethe ansatz II. *cond-mat/9809163*, 1998.

[142] M. Karbach, K. Hu, and G. Müller. Introduction to the Bethe ansatz III. *cond-mat/0008018*, 2000.

[143] M. Karbach and G. Müller. Introduction to the Bethe ansatz I. *cond-mat/9809162*, 1998.

[144] H. Katsura, T. Hirano, and Y. Hatsugai. Exact analysis of entanglement in gapped quantum spin chains. *Physical Review B*, 76:012401, 2007.

[145] A. Kay and M. Ericsson. Geometric effects and computation in spin networks. *New Journal of Physics*, 7:143, 2005.

[146] J. P. Keating and F. Mezzadri. Random matrix theory and entanglement in quantum spin chains. *Communications in Mathematical Physics*, 252:543, 2004.

[147] J. P. Keating and F. Mezzadri. Entanglement in quantum spin chains, symmetry classes of random matrices anad conformal field theory. *Physical Review Letters*, 94:050501, 2005.

[148] M. N. Kiselev, H. Feldmann, and R. Oppermann. Semi-fermionic representation of SU(N) Hamiltonians. *European Physical Journal B*, 22:53, 2001.

[149] M. Köhl, H. Moritz, T. Stöferle, K. Günter, and T. Esslinger. Fermionic atoms in a three dimensional optical lattice: Observing Fermi surfaces, dynamics, and interactions. *Physical Review Letters*, 94:080403, 2005.

[150] P. Kok, K. Nemoto, and W. J. Munro. Properties of multi-particle dark states. *quant-ph/0201138*, 2002.

[151] V. E. Korepin, N. M. Bogoliubov, and A. G. Izergin. *Quantum inverse scattering method and correlation functions.* Cambridge University Press, 1993.

[152] A. B. Kuklov and B. V. Svistunov. Counterflow superfluidity of two-species ultracold atoms in a commensurate optical lattice. *Physical Review Letters*, 90:100401, 2003.

[153] L. Lamata, J. Léon, D. Salgado, and E. Solano. Inductive classification of multipartite entanglement unders stochastic local operations and classical communication. *Physical Review A*, 74:052336, 2006.

[154] L. Lamata, J. Léon, D. Salgado, and E. Solano. Inductive entanglement classification of four qubits under stochastic local operations and classical communication. *Physical Review A*, 75:022318, 2007.

[155] R. Landauer. Irreversibility and heat generation in the computing process. *IBM Journal of Research and Development*, 5:183, 1961.

[156] Y. Li, T. Shi, B. Chen, Z. Song, and C. P. Sun. Quantum-state transmission via a spin ladder as a robust data bus. *Physical Review A*, 71:022301, 2005.

[157] Y. Li, Z. Song, and C. P. Sun. Perfect transfer of many-particle quantum state via high-dimensional systems with spectrum-matched symmetry. *quant-ph/0504175*, 2005.

[158] E. H. Lieb, T. Schultz, and D. J. Mattis. Two soluble models of an antiferromagnetic chain. *Annals of Physics*, 16:407, 1961.

[159] H.-K. Lo and S. Popescu. Concentrating entanglement by local actions: beyond mean values. *Physical Review A*, 63:022301, 2001.

[160] M. S. Longair. *Theoretical concepts in physics.* Cambridge University Press, 1984.

[161] C. K. Majumdar and D. K. Ghosh. On next-nearest-neighbor interaction in linear chain I. *Journal of Mathematical Physics*, 10:1388, 1967.

[162] L. Masanes. All bipartite entangled states are useful for information processing. *Physical Review Letters*, 96:150501, 2005.

[163] L. Masanes. Useful entanglement can be extracted from all nonseparable states. *Journal of Mathematical Physics*, 49:022101, 2008.

[164] J. J. McClelland and J. L. Hanssen. Laser cooling without repumping: A magneto-optical trap for Erbium atoms. *Physical Review Letters*, 96:143005, 2006.

[165] N. D. Mermin. Is the moon there when nobody looks? Reality and the quantum theory. *Physics Today*, April 1985:38, 1985.

[166] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[167] M. A. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436, 1999.

[168] M. A. Nielsen and J. Kempe. Separable states are more disordered globally than locally. *Physical Review Letters*, 86:5184, 2001.

[169] G. M. Nikolopoulos, D. Petrosyan, and P. Lambropoulos. Coherent electron wavepacket propagation and entanglement in array of coupled quantum dots. *Europhysics Letters*, 65:297, 2004.

[170] R. Orús, J. I. Latorre, J. Eisert, and M. Cramer. Half the entanglement in critical systems is distillable from a single specimen. *Physical Review A*, 73:060303(R), 2006.

[171] T. J. Osborne and N. Linden. Propagation of quantum information through a spin system. *Physical Review A*, 69:052315, 2004.

[172] A. Pais. Einstein and the quantum theory. *Reviews of Modern Physics*, 51:863, 1979.

[173] A. Pais. *Subtle is the Lord: the science and the life of Albert Einstein*. Oxford University Press, 1982.

[174] A. S. Parkins, P. Marte, P. Zoller, O. Carnal, and H. J. Kimble. Quantum-state mapping between multilevel atoms and cavity light fields. *Physical Review A*, 51:1578, 1995.

[175] M. Paternostro, M. S. Kim, E. Park, and J. Lee. Entanglement generation in harmonic chains: tagging by squeezing. *Physical Review A*, 72:052307, 2005.

[176] M. Paternostro, G. M. Palma, M. S. Kim, and G. Falci. Quantum-state transfer in imperfect artificial spin networks. *Physical Review A*, 71:042311, 2005.

[177] Á. Perales and M. B. Plenio. Manipulating quantum information by propagation. *Journal of Optics B: Quantum and Semiclassical Optics*, 7:S601, 2005.

[178] A. Peres. *Quantum theory: concepts and methods.* Kluwer Academic, 1993.

[179] A. Peres. Separability criterion for density matrices. *Physical Review Letters*, 77:1413, 1996.

[180] D. Pérez-Garcia, F. Verstraete, J. I. Cirac, and M. M. Wolf. PEPS as unique ground states of local Hamiltonians. *Quantum Information and Computation*, 8:0650, 2007.

[181] D. Pérez-Garcia, F. Verstraete, M. M. Wolf, and J. I. Cirac. Matrix product state representations. *Quantum Information and Computation*, 7:401, 2007.

[182] I. Peschel and J. Zhao. On single-copy entanglement. *Journal of Statistical Mechanics: Theory and Experiment*, page P11002, 2005.

[183] M. Plenio and V. Vedral. Teleportation, entanglement and thermodynamics in the quantum world. *Contemporary Physics*, 39:431, 2000.

[184] M. B. Plenio, J. Eisert, J. Dreißig, and M. Cramer. Entropy, entanglement, and area: analytical results for harmonic lattice systems. *Physical Review Letters*, 94:060503, 2005.

[185] M. B. Plenio, J. Eisert, and J. Hartley. Dynamics and manipulation of entanglement in coupled harmonic systems with many degrees of freedom. *New Journal of Physics*, 6:36, 2004.

[186] M. B. Plenio and F. L. Semiao. High efficiency transfer of quantum information and multiparticle entanglement generation in translation-invariant quantum chains. *New Journal of Physics*, 7:73, 2005.

[187] M. B. Plenio and S. Virmani. An introduction to entanglement measures. *Quantum Information and Computation*, 7:1, 2007.

[188] S. Popescu. Bell's inequalities versus teleportation: what is nonlocality? *Physical Review Letters*, 72:797, 1994.

[189] S. Popescu and D. Rohrlich. Thermodynamics and the measure of entanglement. *Physical Review A*, 56:R3319, 1997.

[190] M. Popp, F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac. Localizable entanglement. *Physical Review A*, 71:042306, 2005.

[191] J. Preskill. *Lecture notes.* California Institute of Technology, 2008.

[192] J. M. Radcliffe. Some properties of coherent spin states. *Journal of Physics A: General*, 4:313, 1971.

[193] E. M. Rains. Entanglement purification via separable superoperators. *quant-ph/9707002*, 1997.

[194] E. M. Rains. A rigorous treatment of distillable entanglement. *quant-ph/9809078*, 1998.

[195] E. M. Rains. Bounds on distillable entanglement. *Physical Review A*, 60:179, 1999.

[196] E. M. Rains. Rigorous treatment of distillable entanglement. *Physical Review A*, 60:173, 1999.

[197] E. M. Rains. Erratum: Bound on distillable entanglement [Phys. Rev. A 60, 179 (1999)]. *Physical Review A*, 63:019902(E), 2001.

[198] R. Raussendorf and H. J. Briegel. A one-way quantum computer. *Physical Review Letters*, 86:5188, 2001.

[199] R. Raussendorf and H. J. Briegel. Computational model underlying the one-way quantum computer. *Quantum Information and Computation*, 2:443, 2002.

[200] R. Raussendorf, D. E. Browne, and H. J. Briegel. Measurement-based quantum computation on cluster states. *Physical Review A*, 68:022312, 2003.

[201] N. Read and S. Sachdev. Some features of the phase diagram of the square lattice SU(N) antiferromagnet. *Nuclear Physics B*, 316:609, 1988.

[202] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73:58, 1994.

[203] A. Rényi. *Probabilty theory*. North Holland, 1970.

[204] A. Romito, R. Fazio, and C. Bruder. Solid-state quantum communication with Josephson arrays. *Physical Review B*, 71:100501(R), 2005.

[205] L. Rosenfeld. Niels Bohr in his thirties. In S. Rozental, editor, *Niels Bohr: his life and work seen by his friends and colleagues*. Interscience, 1964.

[206] S. Sachdev. Quantum magnetism and criticality. *Nature Physics*, 4:173, 2008.

[207] J. J. Sakurai. *Modern quantum mechanics*. Addison Wesley, revised edition, 1994.

[208] E. Schmidt. Zur Theories der linearen und nichtlinearan Integralgleichungen. *Mathematische Annalen*, 63:433, 1906.

[209] U. Schollwöck. The density-matrix renormalization group. *Reviews of Modern Physics*, 77:259, 1992.

[210] D. Schrader, I. Dotsenko, M. Khudaverdyan, Y. Miroshnychenko, A. Rauschenbeutel, and D. Meschede. Neutral atom quantum register. *Physical Review Letters*, 93:150501, 2004.

[211] E. Schrödinger. Die gegenwärtige Situation der Quantenmechanik. *Naturwissenschaften*, 23:807, 1935.

[212] E. Schrödinger. Discussion of probability distributions between separated systems. *Proceedings of the Cambridge Philosophical Society*, 31:555, 1935.

[213] E. Schrödinger. Probability relations between separated systems. *Proceedings of the Cambridge Philosophical Society*, 32:446, 1936.

[214] N. Schuch, I. Cirac, and F Verstraete. The computational difficulty of finding MPS ground states. *Physical Review Letters*, 100:250501, 2008.

[215] N. Schuch, M. M. Wolf, F. Verstraete, and J. I. Cirac. The computational complexity of PEPS. *Physical Review Letters*, 98:140506, 2007.

[216] B. Schuhmacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54:2614, 1996.

[217] B. Schumacher. Quantum coding. *Physical Review A*, 51:2738, 1995.

[218] M. O. Scully and M. S. Zubairy. *Quantum optics.* Cambridge University Press, 1997.

[219] R. Shankar. *Principles of quantum mechanics.* Kluwer Academic, second edition, 1994.

[220] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[221] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A*, 52:2493, 1995.

[222] Z. Song and C. P. Sun. Quantum information storage and state transfer based on spin systems. *Fizika Nizkik Temperature*, 31:907, 2005.

[223] M. Srednicki. Entropy and area. *Physical Review Letters*, 71:666, 1993.

[224] H. Stapp. Are superluminal connections necessary? *Nuovo Cimento*, 40B:191, 1977.

[225] A. Steane. Error correcting codes in quantum theory. *Physical Review Letters*, 77:793, 1996.

[226] V. Subrahmanyam. Entanglement dynamics and quantum-state transport in spin chains. *Physical Review A*, 69:034304, 2004.

[227] B. Sutherland. Model for a multicomponent quantum system. *Physical Review B*, 12:3795, 1975.

[228] L. Szilard. Über die Entropieverminiderung in einen thermodynamischen System bei eingriffen intelligenter Wesen. *Zeitschrift für Physik*, 53:840, 1929.

[229] B. Terhal, M. M. Wolf, and A. C. Doherty. Quantum entanglement: A modern perspective. *Physics Today*, 56:46, 2003.

[230] B. M. Terhal. Detecting quantum entanglement. *Theoretical Computer Science*, 287:313, 2002.

[231] K. Totsuka and M. Suzuki. Matrix formalism for the VBS-type models and hidden order. *Journal of Physics: Condensed Matter*, 7:1639, 1995.

[232] S. Trotzky, P. Cheinet, S. Fölling, M. Feld, U. Schnorrberger, A. M. Rey, A. Polkovnikov, E. A. Demler, M. D. Lukin, and I. Bloch. Time-resolved observation and control of superexchange interactions with ultracold atoms in optical lattices. *Science*, 319:29, 2008.

[233] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57:1619, 1998.

[234] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight. Quantifying entanglement. *Physical Review Letters*, 78:2275, 1997.

[235] F. Verstraete and J. I. Cirac. Valence bond solids for quantum computation. *Physical Review A*, 70:060302(R), 2004.

[236] F. Verstraete and J. I. Cirac. Matrix product states represent ground states faithfully. *Physical Review B*, 73:094423, 2006.

[237] F. Verstraete, M. A. Martín-Delgado, and J. I. Cirac. Diverging entanglement length in gapped quantum spin systems. *Physical Review Letters*, 92:087201, 2004.

[238] F. Verstraete, M. Popp, and J. I. Cirac. Entanglement versus correlations in spin systems. *Physical Review Letters*, 92:027901, 2004.

[239] G. Vidal. Entanglement monotones. *Journal of Modern Optics*, 47:355, 1999.

[240] G. Vidal. Entanglement of pure states for a single copy. *Physical Review Letters*, 83:1046, 1999.

[241] G. Vidal. Efficient classical simulation of slightly entangled quantum computations. *Physical Review Letters*, 91:147902, 2003.

[242] G. Vidal, J. I. Latorre, E. Rico, and A. Kitaev. Entanglement in quantum critical phenomena. *Physical Review Letters*, 90:227902, 2003.

[243] G. Vidal and R. F. Werner. Computable measure of entanglement. *Physical Review A*, 65:032314, 2002.

[244] R. F. Werner. Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40:4277, 1989.

[245] M. J. Wheatley. *Leadership and the new science: discovering order in a chaotic world.* Berrett-Koehler, 1999.

[246] S. White. Density matrix formulation for quantum renormalization groups. *Physical Review Letters*, 69:2863, 1992.

[247] K. G. Wilson. The renormalization group and critical phenomena. *Reviews of Modern Physics*, 47:773, 1975.

[248] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the Einstein–Podolsky–Rosen paradox. *Physical Review Letters*, 98:140402, 2007.

[249] M. M. Wolf, F. Verstraete, M. B. Hastings, and J. I. Cirac. Area laws in quantum systems: mutual information and correlations. *Physical Review Letters*, 100:070502, 2008.

[250] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:80, 1982.

[251] D. Yang, M. Horodecki, R. Horodecki, and B. Synak-Radtke. Irreversibility for all bound entangled states. *Physical Review Letters*, 95:190501, 2005.

[252] M.-H. Yung and S. Bose. Perfect state transfer, effective gates, and entanglement generation in engineered bosonic and fermionic networks. *Physical Review A*, 71:032310, 2005.

[253] M.-H. Yung, D. Leung, and S. Bose. An exact effective two-qubit gate in a chain of three spins. *Quantum Information and Computation*, 4:174, 2004.

[254] H.-Q. Zhou, T. Barthel, J. O. Fjærestad, and U. Schollwöck. Entanglement and boundary critical phenomena. *Physical Review A*, 74:050305(R), 2006.

[255] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Physical Review A*, 58:883, 1998.