An Introduction to Quantum Spin Systems[1]
Notes for Lecture 1

Bruno Nachtergaele and Robert Sims

Contents

1. Introduction

Non-relativistic quantum mechanics describes atoms, molecules, and both small and large systems composed of atoms and molecules. Its validity is well-established in a range of conditions that includes room temperature and atmospheric pressure as well as near-zero temperatures and low densities. The traditional way in which quantum spin systems arise is by a reduction of the Hilbert space of states for each atom or molecule to a finite-dimensional subspace. Such a reduction can often be justified on physical grounds. Other ways in which quantum spin models arises is as a truncation of a lattice quantum field theory for the purpose of numerical simulation. More abstractly, quantum spin systems describe collections of qubits in quantum information theory. Finally, quantum spin systems are also used as toy models in some theories of quantum gravity.

While there certainly are situations where a quantum spin system description would be inadequate, for example in conditions where relativistic effects are important, it is fair to say that almost all interesting features of quantum many-body physics are found in quantum spin models. These include the complex dynamics due to interactions between the components (be it particles or spins), the possibility of phase transitions, the important role played by symmetries and spontaneous symmetry breaking, the unique behavior typical of quantum phases of matter such as Bose-Einstein condensation and superfluidity, superconductivity, the integer and fractional quantum Hall effects, topological order, exotic quasi-particles called anyons etc. Quantum spin models provide the simplest framework in which all these phenomena can be studied in detail. It is also the setting that has proved to be most amenable to rigorous mathematical analysis. In fact, research on quantum spin systems has led to significant new development in functional analysis (e.g., the theory of operator algebras) and representation theory (e.g., quantum groups).

We have two goals in these lectures. The first is to provide a basic introduction to the mathematical framework for the rigorous study of quantum spin models and to introduce the most important models. The second goal is to discuss in sufficient detail some of the most important directions of research on quantum spin models today so that the course provides a foundation for graduate level research in quantum spin systems.

2. Quantum Spin Systems

2.1. **Spins and Qudits.** In these lectures, by *spin* we will be referring to any quantum system with a finite-dimensional, complex Hilbert space of states, i.e. $\mathbb{C}^d$. This could be the space of physical spin states of a particle, atom, or molecule. For example, electrons are spin 1/2 particles, meaning that in addition to its translational degrees of freedom, an electron also has a spin state described by a vector in $\mathbb{C}^2$. In other examples this finite-dimensional Hilbert space may be a subspace of an infinite dimensional Hilbert space, spanned by the most relevant states for the problem at hand. The finite-dimensional approximation may provide a convenient, more tractable description of the systems of interest, perhaps corresponding to finitely many orbitals in a molecule, or may be introduced for the purpose of simulating the system on a computer. The basic unit of quantum information, the *qubit*, has a two-dimensional state space. The d-dimensional generalization of a qubit is called a *qudit*.

We will commonly denote by $\mathcal{H}$ the complex Hilbert space of states of a quantum system, by $\langle\cdot,\cdot\rangle$ the inner-product, a sequilinear form, which is linear in its second argument and anti-linear in the first, following the convention standard in the physics literature. The norm induced by this inner-product is denoted by $\|\cdot\|$.

Unless stated otherwise, we use the standard inner product on $\mathcal{H}=\mathbb{C}^d$, given by

$$\langle u,v\rangle=\sum_{i=1}^{d}\overline{u_i}v_i. \tag{2.1}$$

To emphasize the relation with physical spin, one often writes the dimension d as $d=2S+1$ for half-integer values of the spin $S=0,1/2,1,3/2\ldots$. The smallest non-trivial dimension, $d=2$, corresponds to *spin 1/2*, $S=1/2$. Common notations for a choice of orthonormal basis in $\mathbb{C}^2$ are $\{|0\rangle,|1\rangle\}$, $\{|+\rangle,|-\rangle\}$, and $\{|+1/2\rangle,|-1/2\rangle\}$.

2.2. **Observables.** The *algebra of observables* of a quantum system with Hilbert space $\mathcal{H}$ is the set of all bounded linear operators on $\mathcal{H}$, denoted by $\mathcal{B}(\mathcal{H})$. In the physics literature, the term *observables* usually refers to the self-adjoint elements of $\mathcal{B}(\mathcal{H})$. Since the algebra structure of $\mathcal{B}(\mathcal{H})$ will be useful, we will refer to $\mathcal{B}(\mathcal{H})$ as the algebra of observables and single out the self-adjoint observables when necessary. The default notation for the algebra of observables will be $\mathcal{A}$.

For a qudit we have $\mathcal{H}=\mathbb{C}^d$ and, hence, $\mathcal{A}=\mathcal{B}(\mathcal{H})=M_d(\mathbb{C})$, the set of $d\times d$ matrices with entries in $\mathbb{C}$, which we will also write as M_d. Self-adjoint observables $A\in\mathcal{A}$, *i.e.* , A such that $A^*=A$, have *real spectrum*. In this case, the spectral values, $\mathrm{spec}(A)\subset\mathbb{R}$, correspond to measurable values that can be the outcome of a physical experiment.

Let us consider the case of $d=2$. In this case, the Hilbert space is $\mathcal{H}=\mathbb{C}^2$, and the set of observables is $\mathcal{A}=M_2$. It is convenient to have a basis for the set of observables. One such choice are the identity matrix and the three *Pauli matrices*:

$$\mathbb{1}=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad \sigma^1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad \sigma^2=\begin{pmatrix}0&-i\\i&0\end{pmatrix},\quad \sigma^3=\begin{pmatrix}1&0\\0&-1\end{pmatrix}. \tag{2.2}$$

In general, the observables $\mathcal{A}=M_d$ can be equipped with an inner-product

$$\langle A,B\rangle_{\mathrm{HS}}=\mathrm{Tr}(A^*B)\quad\text{for all } A,B\in\mathcal{A}, \tag{2.3}$$

where Tr denotes the trace. This inner product is often called the *Hilbert-Schmidt* inner product. With respect to $\frac{1}{2}\langle\cdot,\cdot\rangle_{\mathrm{HS}}$, the spin matrices (2.2) are orthonormal. The associated norm is the

Hilbert-Schmidt norm. Note, however, that standard norm on observables is the operator norm on $\mathcal{B}(\mathcal{H})$, defined by

$$\|A\| = \sup_{\psi \neq 0} \frac{\|A\psi\|}{\|\psi\|}. \tag{2.4}$$

2.3. **States.** A *state* of a quantum system with algebra of observables $\mathcal{A}$, which for now is given by $\mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$, is a *normalized, positive linear functional* on $\mathcal{A}$. This means ω is a state if it is a linear map $\omega : \mathcal{A} \to \mathbb{C}$ that satisfies

$$\omega(A^*A) \geq 0, \text{ for all } A \in \mathcal{A}, \text{ and } \omega(\mathbb{1}) = 1. \tag{2.5}$$

For $A \in \mathcal{A}$, $\omega(A)$ is the *expected value* or *expectation* of the observable A in the state ω. The expectation of self-adjoint observables is real and, in general, we have $\omega(A^*) = \overline{\omega(A)}$. The variance of A, $\mathrm{Var}(A)$, is given by the familiar formula:

$$\mathrm{Var}(A) = \omega((A - \omega(A)\mathbb{1})^*(A - \omega(A)\mathbb{1})) = \omega(A^*A) - |\omega(A)|^2. \tag{2.6}$$

For any unit vector $\psi \in \mathcal{H}$, one can define a state ω_ψ on $\mathcal{B}(\mathcal{H})$ by

$$\omega_\psi(A) = \langle \psi, A\psi \rangle \quad \text{for all } A \in \mathcal{A}. \tag{2.7}$$

States of this form are called *vector states*. An alternative expression for ω_ψ is

$$\omega_\psi = \mathrm{Tr} P_\psi A, \tag{2.8}$$

where P_ψ denotes the orthogonal projection defined by

$$P_\psi(\phi) = \langle \psi, \phi \rangle \psi, \quad \phi \in \mathcal{H}. \tag{2.9}$$

It follows from the definition of state given above that the set of states on $\mathcal{A}$ is convex. The extreme points of this convex set are called the *pure states*. In the finite-dimensional case, *i.e.* $\mathcal{A} = M_d$, the pure states are precisely the vector states and all states are finite convex combinations of vector states, *i.e.* , for any state ω, there are $t_1, \ldots, t_n \geq 0$ and unit vectors $\psi_1 \ldots, \psi_n \in \mathcal{H}$, such that

$$\omega = \sum_{i=1}^{n} t_i \omega_{\psi_i}. \tag{2.10}$$

It follows that there is a non-negative matrix $\rho \in M_d$ such that

$$\omega(A) = \mathrm{Tr}(\rho A), \quad \text{for all } A \in M_d, \tag{2.11}$$

with

$$\rho = \sum_{i=1}^{n} t_i P_{\psi_i}. \tag{2.12}$$

Matrices ρ of the form (2.12) are non-negative and, since the t_i are the coefficients in a convex combination, $\mathrm{Tr}\rho = \sum_{i=1}^{n} t_i = 1$. Non-negative matrices of unit trace are called *density matrices*.

As an example, we now describe the set of density matrices in the case $\mathcal{A} = M_2$. $\rho \in M_2$ is a density matrix if and only if

$$\rho = \begin{pmatrix} r & \mu \\ \overline{\mu} & 1 - r \end{pmatrix} \tag{2.13}$$

for some $r \in [0, 1]$ and $\mu \in \mathbb{C}$ satisfying

$$|\mu|^2 \leq r(1 - r) \tag{2.14}$$

Another useful parametrization of the 2×2 density matrices is obtained by expanding then in the orthornormal basis with respect the the Hilbert-Schmidt inner product given by the Pauli matrices and the identity, i.e. (2.2):

$$\rho = \frac{1}{2}\left(\mathbb{1} + \vec{x} \cdot \vec{\sigma}\right) \tag{2.15}$$

where $\vec{x} = (x_1, x_2, x_3) \in \mathbb{R}^3$ with $|\vec{x}| \leq 1$ and we have denoted by

$$\vec{x} \cdot \vec{\sigma} = x_1\sigma^1 + x_2\sigma^2 + x_3\sigma^3 \tag{2.16}$$

This provides a bijection between the set of all density matrices in M_2 and the unit ball in $\mathbb{R}^3$. The extreme points of the unit ball correspond to the pure states, and are in one-to-one correspondence with the unit vectors $\vec{x} \in \mathbb{R}^3 : \|\vec{x}\| = 1$. This set is often referred to as the *Bloch sphere*.

2.4. **Dirac notation.** The *Dirac bra- and ket notation* is very commonly used in quantum mechanics and quantum information theory. It is popular because it provides a convenient way to present the most frequently encountered operations in Hilbert space. Here, we only give a brief account of the Dirac notation in the case of finite-dimensional Hilbert spaces. Many aspects generalize without significant change to the case of infinite-dimensional spaces. We do not consider here the more liberal usage of the Dirac notation encountered in many physics texts, where it is extended beyond the Hilbert space context into distribution theory.

Let $\mathcal{H}$ be a finite-dimensional Hilbert space. With each $\phi \in \mathcal{H}$ we can associate two linear maps, which we denote by $|\phi\rangle$ and $\langle\phi|$.:

$$|\phi\rangle : \mathbb{C} \to \mathcal{H}, z \mapsto z\phi, \quad \langle\phi| : \mathcal{H} \to \mathbb{C} : \psi \mapsto \langle\phi, \psi\rangle. \tag{2.17}$$

In fact, since the linear maps define above depend linearly and anti-linearly on ϕ, we can consider $|\ \rangle$, pronounced *ket*, and $\langle\ |$, pronounced *bra*, as linear and antilinear maps themselves:

$$|\ \rangle : \mathcal{H} \to \mathcal{L}(\mathbb{C}, \mathcal{H}), \phi \mapsto |\phi\rangle, \quad \langle\ | : \mathcal{H} \to \mathcal{L}(\mathcal{H}, \mathbb{C}), \phi \mapsto \langle\phi|. \tag{2.18}$$

$\langle\ |$ is the antilinear map identifying $\mathcal{H}$ with its dual space $\mathcal{H}^*$, as guaranteed by the Riesz Representation Theorem. Since $\mathcal{H} \cong \mathbb{C}^d$, with $d = \dim(\mathcal{H})$, we can identify $|\phi\rangle$ with column vector of length d, and $\langle\phi|$ with a row vector of length d, and consider these vectors as the matrix representation of the linear maps defined in (2.17).

For any pair $\phi_1, \phi_2 \in \mathcal{H}$, we can define a rank-one linear map $\mathcal{H} \to \mathcal{H}$ by

$$\psi \mapsto \langle\phi_2, \psi\rangle\phi_1. \tag{2.19}$$

It is easy to see that this rank-one map is the composition of a $|\phi_1\rangle$ and $\langle\phi_2|$, which justifies the following elegant notation for it:

$$|\phi_1\rangle\langle\phi_2|(\psi) = |\phi_1\rangle(\langle\phi_2, \psi\rangle) = \langle\phi_2, \psi\rangle\phi_1. \tag{2.20}$$

It is now convenient to use the notation ψ and $|\psi\rangle$ for vectors interchangeably, and to use an alternate notation for the inner product as well:

$$\langle\phi, \psi\rangle = \langle\phi \mid \psi\rangle = \langle\phi||\psi\rangle. \tag{2.21}$$

Labeled sets of vectors, such as, *e.g.* , an orthonormal basis $\{e_1, \ldots, e_d\}$, can be written in Dirac notation using just the labels if this does not lead to confusion: $\{|1\rangle, \ldots, |d\rangle\}$.

Using the Dirac notation, orthonormality and completeness of the basis we can expressed by the following two equations:

$$\langle i \mid j\rangle = \delta_{i,j}, \quad \sum_{i=1}^{d} |i\rangle\langle i| = \mathbb{1}. \tag{2.22}$$

2.5. **Finite Quantum Spin Systems.** The observables of the quantum systems we have considered so far are given by the elements of $\mathcal{B}(\mathcal{H})$, the bounded linear operators on a complex Hilbert space. For a finite quantum spin system, $\mathcal{H}$ is finite-dimensional and the algebra of observables is the algebra of $d \times d$ matrices with complex entries, M_d, where d is the dimension of the Hilbert space. More generally, one can consider quantum systems with an infinite-dimensional complex Hilbert space. The algebra of observables will then consist of elements of $\mathcal{B}(\mathcal{H})$, the bounded linear operators on $\mathcal{H}$. $\mathcal{B}(\mathcal{H})$ is complete with respect to the metric topology derived from the operator norm defined in (2.4). It is straightforward to check that the operator norm satisfies $\|AB\| \leq \|A\|\|B\|$, for all $A, B \in \mathcal{B}(\mathcal{H})$, which in particular implies that the product of observables is continuous in the norm topology. The completeness and the continuity of the product make $\mathcal{B}(\mathcal{H})$ into a Banach algebra.

The operation of taking the adjoint of an operator A, denoted by A^*, is an anti-linear involution, meaning $(A^*)^* = A$, $(A+B)^* = A^* + B^*$, and $(zA)^* = \overline{z}A^*$, for all $A, B \in \mathcal{B}(\mathcal{H})$ and $z \in \mathbb{C}$, and is an algebra anti-morphism: $(AB)^* = B^*A^*$. One readily checks that $\|A^*\|$ and $\|A^*A\| = \|A\|^2$.

M_d and, more generally, $\mathcal{B}(\mathcal{H})$ are examples of C^*-algebras, which we introduce in the next section.

2.5.1. *C^*-algebras.* A C^*-algebra is a Banach algebra equipped with an involution, denoted by $*$, satisfying some special properties.

Definition 2.1. Let $\mathcal{A}$ be an associative algebra over $\mathbb{C}$ that is equipped with a norm $\|\cdot\|$. If $\mathcal{A}$ is complete with respect to this norm and

$$\|AB\| \leq \|A\|\|B\| \quad \text{for all } A, B \in \mathcal{A}, \tag{2.23}$$

then $\mathcal{A}$ is called a Banach algebra. A Banach algebra $\mathcal{A}$ is called unital if it has an identity element, which we denote by $\mathbb{1} \in \mathcal{A}$.

In this book the term *algebra*, unless explicitly stated otherwise, will always refer to an associative algebra over the complex numbers with a unit, which will routinely be denoted by $\mathbb{1}$. We will also assume that the algebra we consider are non-trivial, *i.e.* ., are not equal to $\{0\}$.

Definition 2.2. A C^*-algebra $\mathcal{A}$ is a Banach algebra with an anti-linear involution, which we will denote by $*$, satisfying the following properties:
i) $(AB)^* = B^*A^*$ for all $A, B \in \mathcal{A}$
ii) $\|A^*\| = \|A\|$ for all $A \in \mathcal{A}$ (This implies that the $*$ operation w.r.t. the norm $\|\cdot\|$.)
iii) $\|A^*A\| = \|A\|^2$ for all $A \in \mathcal{A}$. (This is called the C^*-property.)

If the C^*-algebra $\mathcal{A}$ has a unit, denoted by $\mathbb{1}$, it is called unital. It follows from the properties stated the unit is unique, that $\mathbb{1}^* = \mathbb{1}$ and, if $\mathcal{A} \neq \{0\}$, that $\|\mathbb{1}\| = 1$.

If $\mathcal{A}$ and $\mathcal{B}$ are two C^*-algebras, a $*$-*morphism* (often simply called a morphism) $\pi : \mathcal{A} \to \mathcal{B}$ is an algebra morphism that preserves the involution, i.e., $\pi(A^*) = \pi(A)^*$ for all $A \in \mathcal{A}$. A morphism $\pi : \mathcal{A} \to \mathcal{B}$ is called *unit preserving* if $\pi(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$.

A *representation* of a C^*-algebra $\mathcal{A}$ on a Hilbert space $\mathcal{H}$ is a unit preserving morphism $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$. A representation π is called *faithful*, if $\ker \pi = \{0\}$, *i.e.* , if it is a $*$-isomorphism between $\mathcal{A}$ and $\pi(\mathcal{A})$. A morphism $\pi : \mathcal{A} \to \mathcal{A}$ is called an *automorphism* if π is invertible.

A *state* ω on $\mathcal{A}$ is a linear mapping $\omega : \mathcal{A} \to \mathbb{C}$ that is non-negative and normalized, i.e. $\omega(A^*A) \geq 0$, for all $A \in \mathcal{A}$, and $\omega(\mathbb{1}) = 1$.

In the finite dimensional case, i.e. $\mathcal{A} = M_d$, we already discussed that states are in one-to-one correspondence with density matrices. If $\mathcal{H}$ is infinite-dimensional, density matrices ρ, defined as positive operators of trace-class such that $\mathrm{Tr}\rho = 1$, also define states on $\mathcal{B}(\mathcal{H})$, by the formula $\omega(A) = \mathrm{Tr}\rho A$, but there are states on $\mathcal{B}(\mathcal{H})$ that are not of this form.

Let $\mathcal{A}$ be a C^*-algebra. $A \in \mathcal{A}$ is called *self-adjoint* if $A^* = A$. The set of all self-adjoint elements in $\mathcal{A}$ will be denoted by $\mathcal{A}_{\mathrm{sa}}$. $A \in \mathcal{A}$ is said to be *positive*, denoted by $A \geq 0$, if there exists $B \in \mathcal{A}$

such that $A = B^*B$. This notion of positivity allows one to define a partial order on $\mathcal{A}_{\rm sa}$, i.e. for any $A, B \in \mathcal{A}_{\rm sa}$, we write $A \geq B$ if and only if $A - B \geq 0$.

For the derivation of the following important properties see Appendix A, or consult a text on operator algebras such as [2], [11], or [5].

i) For any $A, B \in \mathcal{A}_{\rm sa}$,

$$A \geq B \quad \Rightarrow \quad C^*AC \geq C^*BC \quad \text{for all } C \in \mathcal{A}. \tag{2.24}$$

ii) For any $A \geq 0$, $A \leq \|A\|\mathbb{1}$, and as a consequence, for any state ω, we have that

$$\|\omega\| = \sup_{A \neq 0} \frac{|\omega(A)|}{\|A\|} = \omega(\mathbb{1}) = 1. \tag{2.25}$$

iii) Similarly, for a morphism π, we also have that

$$\|\pi\| = \|\pi(\mathbb{1})\| = 1 \quad \text{if } \pi \neq 0. \tag{2.26}$$

iv) Let $\mathcal{A}$ be a C^*-algebra and ω be a state on $\mathcal{A}$. The mapping from $\mathcal{A} \times \mathcal{A}$ to $\mathbb{C}$ given by

$$(A, B) \mapsto \omega(A^*B) \tag{2.27}$$

is a sesquilinear form. As a consequence, we have a Cauchy-Schwartz inequality:

$$|\omega(A^*B)|^2 \leq \omega(A^*A)\omega(B^*B) \quad \text{for all } A, B \in \mathcal{A}\,. \tag{2.28}$$

v) Let $\mathcal{A}$ be a C^*-algebra and ω be a state on $\mathcal{A}$. The bound

$$|\omega(A^*BA)| \leq \omega(A^*A)\|B\| \tag{2.29}$$

holds for all $A, B \in \mathcal{A}$. As a consequence, for all $A \in \mathcal{A}$ with $\omega(A^*A) \neq 0$,

$$\omega_A(B) := \frac{\omega(A^*BA)}{\omega(A^*A)} \quad \text{for all } B \in \mathcal{A} \tag{2.30}$$

defines a state ω_A on $\mathcal{A}$. This is the quantum analogue of starting with a measure, e.g. dx on $[0, 1]$, considering a non-negative function μ with $\int_0^1 \mu(x)dx < \infty$, and defining a new, normalized measure via

$$\frac{\mu(x)}{\int_0^1 \mu(x)dx} dx \tag{2.31}$$

2.5.2. *Composite systems.* Any two quantum systems described by Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ can be considered as one, composite system. The Hilbert space of the composite system is given by the tensor product of $\mathcal{H}_1$ and $\mathcal{H}_2$. The simplest way to describe the tensor product of two finite-dimensional Hilbert spaces, say with dimensions n and m and inner product $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_2$, respectively, is as the span of an orthonormal basis of simple tensors defined as follows. Let $e_1, \ldots, e_n$ and $f_1, \ldots, f_m$ be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$, then $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as the linear span of nm orthonormal vectors denoted $e_i \otimes f_j$, $1 \leq i \leq n, 1 \leq j \leq m$. The tensor notation is extended by linearity to identify $\phi_1 \otimes \phi_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$, for any $\phi_1 \in \mathcal{H}_1, \phi_2 \in \mathcal{H}_2$. Such vectors are called *simple tensors*. From the orthonormality of the basis it then follows that the the inner product is uniquely determined by the following formula for simple tensors:

$$\langle \phi_1 \otimes \phi_2, \psi_1 \otimes \psi_2 \rangle = \langle \phi_1, \psi_1 \rangle_1 \langle \phi_2, \psi_2 \rangle_2 \tag{2.32}$$

There are several ways to define the tensor product for infinite-dimensional, Hilbert spaces H_1 and H_2, all of which lead to a Hilbert space $\mathcal{H}$ with the following properties: (i) there is a bilinear bijection of $\mathcal{H}_1 \times \mathcal{H}_2$ into a subset of $\mathcal{H}$ (the set of simple tensors), (ii) the inner product of simple tensors factorizes as in (2.32), and (iii) the linear span of the simple tensors is dense in $\mathcal{H}$, which is unique up to unitary equivalence. See, e.g., [1, 9], for the details of a construction of the tensor product of two arbitrary Hilbert spaces. It is straightforward to extend the notion of tensor product from two to any finite number of Hilbert spaces.

The combination of two (or more) spins, meaning, considering a physical context in which both exist, is described as a composite systems using the tensor product of the Hilbert spaces of the individual systems.

Let us start by considering two spins, with Hilbert spaces of dimension d_1 and d_2. The Hilbert space for the composite system is then:

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \cong \mathbb{C}^{d_1 d_2} \tag{2.33}$$

Such a system is often referred to as *bipartite*. The algebra of observables is again given by $\mathcal{B}(\mathcal{H})$, and it can also be obtained as a tensor product since

$$M_{d_1 d_2} \cong M_{d_1} \otimes M_{d_2}, \tag{2.34}$$

where $M_{d_1} \otimes M_{d_2}$ is the linear span of the tensor products of two matrices $A = (a_{i,j}) \in M_{d_1}$, and $B = (b_{k,l}) \in M_{d_2}$, defined by

$$A \otimes B = (c_{i,k;j,l}), \text{ with } c_{i,k;j,l} = a_{i,j} b_{k,l}. \tag{2.35}$$

Systems 1 and 2 are called subsystems of the composite system. One can identify their algebra of observables with subalgebras of $M_{d_1 d_2}$. E.g., $M_{d_1} \cong M_{d_1} \otimes \mathbb{1}_2 \subset M_{d_1} \otimes M_{d_2}$.

One way to appreciate the uniquely quantum (versus classical) behavior of states is to consider marginals of pure states. Pure states of a classical bipartite system with a finite state space $\Omega = \Omega_1 \times \Omega_2$, are given by Dirac measures concentrated in a point $(\xi_1, \xi_2) \in \Omega$. The marginals of classical pure states are then Dirac measures in the points $\xi_i \in \Omega_i$, which are also pure. In contrast, what distinguishes quantum from classical structure states (quantum probability versus classical probability) can be seen as exactly the property that *any* state of system 1 is the marginal of a pure state on for composite system containing system 1 as a tensor factor [3].

The marginals of a pure state for a bipartite quantum system given by a unit vector $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$, are pure iff the pure state is separable, *i.e.* , ψ is a simple tensor [10]. The marginals of the Bell states coincide with the maximally mixed state described by the density matrix $\frac{1}{2}\mathbb{1}_2$ (see the Example below).

Considering the marginals of a state of a bipartite system is simply considering its restrictions from $\mathcal{A}_1 \otimes \mathcal{A}_2$ to the subalgebras $\mathcal{A}_1 \otimes \mathbb{1}$ and $\mathbb{1} \otimes \mathcal{A}_2$. In the case of finite-dimensional state spaces, all states are uniquely represented by a density matrix. Hence there is a corresponding well-defined operation on density matrices describing the restriction process. For all density matrices $\rho \in M_{d_1} \otimes M_{d_2}$ there is a unique density matrix ρ_1 in M_{d_1}, such that

$$\mathrm{Tr}\rho(A \otimes \mathbb{1}) = \mathrm{Tr}\rho_1 A \tag{2.36}$$

The map $\rho \mapsto \rho_1$ is often denoted by Tr_2 and is called the *partial trace*.

Example: Take $d_1 = d_2 = 2$. Denote by $\{|0\rangle, |1\rangle\}$ an orthonormal basis of $\mathbb{C}^2$. Let $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2 = \mathbb{C}^2 \otimes \mathbb{C}^2$ be the normalized vector

$$\psi = \frac{1}{\sqrt{2}} \left(|0\rangle \otimes |1\rangle + |1\rangle \otimes |0\rangle \right) \tag{2.37}$$

Note that ψ is a maximally entangled state. For $A \in \mathcal{A}_1$, $A \otimes \mathbb{1} \in \mathcal{A}$. The restriction (or marginal) of the state defined by ψ is easily calculated:

$$\begin{aligned} \mathrm{Tr}|\psi\rangle\langle\psi|(A \otimes \mathbb{1}) &= \langle \psi, (A \otimes \mathbb{1})\psi \rangle \\ &= \frac{1}{2} \left(\langle 0|A|0\rangle + \langle 1|A|1\rangle \right) = \frac{1}{2}\mathrm{Tr}A. \end{aligned} \tag{2.38}$$

Hence

$$\mathrm{Tr}_2|\psi\rangle\langle\psi| = \frac{1}{2}\mathbb{1}. \tag{2.39}$$

Vector states given by simple tensors are product states. More generally, a state ω on an algebra of observables of the form $\mathcal{A} = \mathcal{A}_1 \otimes \mathcal{A}_2$, is called a *product state* if there exist states ω_1 on $\mathcal{A}_1$ and ω_2 on $\mathcal{A}_2$, such that for all $A_1 \in \mathcal{A}_1$ and $A_2 \in \mathcal{A}_2$, one has $\omega(A_1 \otimes A_2) = \omega_1(A_1)\omega_2(A_2)$.

Definition 2.3. A state on a tensor product algebra $\mathcal{A}_1 \otimes \mathcal{A}_2$ is called separable if it is a convex combination of product states. A state is called entangled if it is not separable.

If $d_1, d_2 \geq 2$ not all vectors $\psi \in \mathcal{H}$ can be written as $\psi = \psi_1 \otimes \psi_2$, and only those that are of this form define separable states. A vector state is either a product state or entangled. There is no analogue of entangled states for classical systems. Quantum information theory is of interest exactly due to the existence of entangled states.

One of the most commonly used measures of entanglement for a bipartite system is the *entanglement entropy*. For a pure state given by a unit vector $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$, the entanglement entropy, $S_E(\psi)$, is defined as the entropy of the restriction of the state to either one of its subsystems (the value is the same for both subsystems). Concretely:

$$S_E(\psi) = -\mathrm{Tr}\rho_1 \log \rho_1, \text{ with } \rho_1 = \mathrm{Tr}_{\mathcal{H}_2} |\psi\rangle\langle\psi|. \tag{2.40}$$

For a general state given by a density matrix ρ, the entanglement entropy is defined by the following minimization problem:

$$S_E(\rho) = \inf\{\sum t_i S_E(\psi_i) \mid \rho = \sum t_i |\psi_i\rangle\langle\psi_i|\} \tag{2.41}$$

which is an infinum over all decompositions of ρ as a convex combination of pure states. This measure of entanglement is also called *entanglement of formation*, because of an equivalent operational definition [6]. One can easily check that $S_E(\rho) = 0$ iff ρ is separable. The maximum value of S_E is $\min(\log d_1, \log d_2)$, and it is easy to construct states that attain this maximal value. Such states are called *maximally entangled*. In the case $d_1 = d_2 = 2$, the maximally entangled states are the so-called Bell states of the form $(e_1 \otimes f_1 + e_2 \otimes f_2)/\sqrt{2}$, for two arbitrary orthonormal bases $\{e_1, e_2\}$ and $\{f_1, f_2\}$ of $\mathbb{C}^2$.

2.5.3. *Dynamics.* One to the most important observables of any quantum spin system is the *Hamiltonian*, which has the physical interpretation of the total energy of the system. For a system consisting of N spins, the Hilbert space is

$$\mathcal{H}_N = \bigotimes_{j=1}^{N} \mathcal{H}_j \tag{2.42}$$

and the algebra of observables is

$$\mathcal{A}_N = \bigotimes_{j=1}^{N} \mathcal{A}_j \tag{2.43}$$

where $\mathcal{A}_j = \mathcal{B}(\mathcal{H}_j)$. The Hamiltonian is a selfadoint element $H^* = H \in \mathcal{A}_N$. Its importance stems from its role as generator of the *dynamics* of the system. For any pure state of the system at time $t = 0$, given by $\psi_0 \in \mathcal{H}_N$, the state at any time $t \in \mathbb{R}$ is given by the solution of the Schrödinger equation:

$$i\frac{d}{dt}\psi(t) = H\psi(t) \quad \text{with} \quad \psi(0) = \psi_0. \tag{2.44}$$

As is well-known, the solution of this vector-valued linear equation is given by

$$\psi(t) = U_t \psi_0, \text{ with } U_t = e^{-itH}. \tag{2.45}$$

Since H is self-adjoint, U_t is unitary for all $t \in \mathbb{R}$ and it is easy to see that $U_t^* = U_{-t}$, and that $U_t U_s = U_{t+s}$, $t, s \in \mathbb{R}$, *i.e.* , $\{U_t \mid t \in \mathbb{R}\}$ is a one-parameter group of unitaries.

Denote by $\rho_0 = |\psi_0\rangle\langle\psi_0|$. Then the density matrix corresponding to the solution of (2.44), i.e. (2.45), is

$$\rho(t) = |\psi(t)\rangle\langle\psi(t)| = U_t \rho_0 U_t^*. \tag{2.46}$$

This is the solution of the operator-valued equation

$$i\frac{d}{dt}\rho(t) = [H, \rho(t)] \quad \text{with} \quad \rho(0) = \rho_0 \tag{2.47}$$

This is sometimes called the *Schrödinger-Liouville equation.* It has a unique solution ρ_t which, for an arbitrary initial density matrix ρ_0, is a density matrix for all t.

The dynamics of a finite spin system can equivalently be described in the so-called *Heisenberg picture*, by evolving the observables rather than the states. This change of perspective is particularly useful in the context of infinite systems because, while there is no a priori infinite volume Hilbert space, there is a well-defined observable algebra for the infinite system (see following lectures). The equivalence of the Schrödinger and Heisenberg descriptions of the dynamics is established by the following relations:

$$\omega_{\rho(t)}(A) = \mathrm{Tr}\rho(t)A = \mathrm{Tr}U_t\rho_0 U_t^* A = \mathrm{Tr}\rho_0 U_t^* A U_t = \omega_{\rho_0}(U_t^* A U_t), \tag{2.48}$$

for any observable $A \in \mathcal{A}$. This justifies the following definition of time-evolved observables:

$$A(t) = U_t^* A U_t \quad \text{for any } A \in \mathcal{A} \quad \text{and } t \in \mathbb{R}. \tag{2.49}$$

These time-dependent observables satisfy the *Heisenberg equation*:

$$\frac{d}{dt}A(t) = i[H, A(t)] \quad \text{with } A(0) = A, \tag{2.50}$$

and (2.48) becomes, for any $A \in \mathcal{A}$,

$$\mathrm{Tr}\rho(t)A = \mathrm{Tr}\rho_0 A(t). \tag{2.51}$$

Example: The Quantum Heisenberg Model, introduced by Heisenberg almost a century ago [4].

To each $x \in \mathbb{Z}$ associate the single-site Hilbert space $\mathcal{H}_x = \mathbb{C}^2$. For any finite interval $\Lambda = [a, b] \subset \mathbb{Z}$, consider the Hilbert space

$$\mathcal{H}_\Lambda = \bigotimes_{x=a}^{b} \mathbb{C}^2 = \mathbb{C}^{2^{b-a+1}} \tag{2.52}$$

and the corresponding observable algebra

$$\mathcal{A}_\Lambda = \bigotimes_{x=a}^{b} M_2 = M_{2^{b-a+1}} \tag{2.53}$$

To each $i = 1, 2, 3$, and any $x \in \Lambda$ associate a self-adjoint observable $\sigma_x^i \in \mathcal{A}_\Lambda$ by setting

$$\sigma_x^i = \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \sigma^i \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1} \tag{2.54}$$

where the only non-trivial operator, σ^i above, occurs in the xth factor of $\mathcal{A}_\Lambda$. The quantum Heisenberg Hamiltonian on volume Λ is then the self-adjoint observable

$$\begin{aligned} H_\Lambda &= -J \sum_{j=a}^{b-1} \vec{\sigma}_x \cdot \vec{\sigma}_{x+1} \\ &= -J \sum_{x=a}^{b-1} \left(\sigma_x^1 \sigma_{x+1}^1 + \sigma_x^2 \sigma_{x+1}^2 + \sigma_x^3 \sigma_{x+1}^3 \right) \end{aligned} \tag{2.55}$$

with $J \in \mathbb{R}$ a parameter.

If $J > 0$, this is called the (quantum) *ferromagnetic* Heisenberg chain.

If $J < 0$, this is called the (quantum) *anti-ferromagnetic* Heisenberg chain.

In the Exercises you are asked to prove some basic properties of the Heisenberg chain with periodic boundary conditions.

3. Appendix: C^*-algebras

It this appendix, we review some of the basic properties of abstract C^*-algebras. These properties are familiar when the C^*-algebra is a subalgebra of $\mathcal{B}(\mathcal{H})$, for some Hilbert space $\mathcal{H}$. Since the algebra of observables of an infinite quantum spin system, introduced in **??**, is *a priori* not represented on a Hilbert space, it is important to understand the basic properties of abstract C^*-algebras. This appendix is based on Sections 2.1-2.3 - of [2], to which we refer the reader for complete details and further information.

3.1. **C^*-algebras.** A complex vector space $\mathcal{A}$ is an *associative algebra* if it is equipped with a bilinear product, i.e. to each pair $A, B \in \mathcal{A}$ there corresponds a unique element $AB \in \mathcal{A}$, in such a way that:

i) $A(BC) = (AB)C$ for all $A, B, C \in \mathcal{A}$,
ii) $A(B + C) = AB + AC$ for all $A, B, C \in \mathcal{A}$,
iii) $\alpha\beta(AB) = (\alpha A)(\beta B)$ for all $\alpha, \beta \in \mathbb{C}$ and all $A, B \in \mathcal{A}$.

If an algebra $\mathcal{A}$ contains an identity element, i.e., $\mathbb{1} \in \mathcal{A}$ such that $\mathbb{1}A = A = A\mathbb{1}$, for all $A \in \mathcal{A}$, $\mathcal{A}$ is called *unital*. A subspace $\mathcal{B} \subset \mathcal{A}$ that is also an algebra with respect to the operations of $\mathcal{A}$ is called a subalgebra of $\mathcal{A}$.

An associative algebra $\mathcal{A}$ is a $*$-algebra if it has a map $A \mapsto A^*$ with the properties:

i) $(A^*)^* = A$ for all $A \in \mathcal{A}$ (* is an *involution*),
ii) $(AB)^* = B^*A^*$ for all $A, B \in \mathcal{A}$ (* is an *antimorphism*),
iii) $(\alpha A + \beta B)^* = \overline{\alpha}A^* + \overline{\beta}B^*$ for all $\alpha, \beta \in \mathbb{C}$ and all $A, B \in \mathcal{A}$ (* is *antilinear*).

Here, and below, we will denote by $\overline{z}$ and $|z|$ the complex conjugate and modulus of $z \in \mathbb{C}$, respectively. A subset $\mathcal{B}$ of a $*$-algebra A is called *self-adjoint* if $A \in \mathcal{B}$ implies $A^* \in \mathcal{B}$.

An algebra $\mathcal{A}$ is called a *normed algebra* if there is a mapping $\|\cdot\| : \mathcal{A} \to \mathbb{R}$ with the properties:

i) $\|A\| \geq 0$ for all $A \in \mathcal{A}$ and $\|A\| = 0$ if and only if $A = 0$,
ii) $\|\alpha A\| = |\alpha|\|A\|$ for all $\alpha \in \mathbb{C}$ and all $A \in \mathcal{A}$,
iii) $\|A + B\| \leq \|A\| + \|B\|$ for all $A, B \in \mathcal{A}$,
iv) $\|AB\| \leq \|A\|\|B\|$ for all $A, B \in \mathcal{A}$.

For any $A \in \mathcal{A}$, the quantity $\|A\|$ is called the norm of A. The norm on a normed algebra $\mathcal{A}$ defines a metric topology on $\mathcal{A}$, called the *uniform topology* or *norm topology*, and if $\mathcal{A}$ is complete with respect to this topology, then $\mathcal{A}$ is called a *Banach algebra*. A $*$-algebra $\mathcal{A}$ is a normed $*$-algebra $\mathcal{A}$ if one has $\|A^*\| = \|A\|$ for all $A \in \mathcal{A}$. A normed $*$-algebra is a *Banach $*$-algebra* if it is complete with respect to its norm topology.

The main object of interest in the section can now be defined.

Definition 3.1. A C^*-algebra is a Banach $*$-algebra $\mathcal{A}$ with the property that

$$\|A^*A\| = \|A\|^2 \quad \text{for all } A \in \mathcal{A}. \tag{3.1}$$

The condition (3.1) is called the *C^*-property*. It is easy to see that (3.1) implies the $*$ property of the norm: $\|A^*\| = \|A\|$ for all $A \in \mathcal{A}$. Here are some important examples.

Example: Let $\mathcal{H}$ be a complex Hilbert space and denote by $\mathcal{A} = \mathcal{B}(\mathcal{H})$ the set of bounded linear operators over $\mathcal{H}$. With the $*$ operation given by the adjoint operation and the norm corresponding to the operator norm, $\mathcal{A}$ is a C^*-algebra. □

Example: Let X be a topological space and let $C(X)$ denote the space of bounded and continuous complex-valued functions on X. $C(X)$ is a an commutative algebra for the pointwise multiplication of functions. Equipped with the supremum norm and the $*$-operation given by complex conjugation, $C(X)$ becomes a C^*-algebra. □

Example: Let $\mathcal{H}$ be a complex Hilbert space and denote by $\mathcal{C} \subset \mathcal{B}(\mathcal{H})$ the set of compact operators over $\mathcal{H}$. One easily checks that any uniformly closed subalgebra of $\mathcal{B}(\mathcal{H})$ that is also a self-adjoint subset, is a C^*-sub-algebra of $\mathcal{B}(\mathcal{H})$. This is the case with the algebra of compact operators $\mathcal{C}$. Note that $\mathbb{1} \notin \mathcal{C}$. □

The following theorem shows that, as in the last example, any C^* algebra can be regarded as a closed subalgebra of $\mathcal{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$.

Theorem 3.2. *Any C^*-algebra $\mathcal{A}$ is isomorphic to a norm-closed self-adjoint algebra of bounded linear operators on a Hilbert space $\mathcal{H}$.*

For a proof of this theorem see, e.g., [2, Theorem 2.1.10].

The availability of an identity in a C^*-algebra describing the observables of a physical system is important. Let $\mathcal{A}$ be a C^*-algebra. If $\mathcal{A}$ has an indentity, it is necessarily unique; if both $\mathbb{1}$ and $\mathbb{1}'$ are identities, then $\mathbb{1} = \mathbb{1}\mathbb{1}' = \mathbb{1}'$. It is easy to verify that $\mathbb{1}^*$ is an identity, and hence we must have $\mathbb{1}^* = \mathbb{1}$. Moreover,

$$\|\mathbb{1}\| = \|\mathbb{1}^*\mathbb{1}\| = \|\mathbb{1}\|^2 \quad \text{and} \quad \|A\| = \|\mathbb{1}A\| \leq \|\mathbb{1}\|\|A\|. \tag{3.2}$$

Thus either $\|\mathbb{1}\| = 1$ or $\mathcal{A} = \{0\}$, which is a trivial case we shall ignore; we will always assume that $\|\mathbb{1}\| = 1$. A C^*-algebra $\mathcal{A}$ with an identity is called a *unital* C^*-algebra.

It is not the case that all C^*-algebras possess an identity. As mentioned above, the C^*-algebra of the compact operators on a Hilbert space $\mathcal{H}$ has an identity if and only if $\mathcal{H}$ is finite-dimensional. In general, it is possible to *adjoin an identity* to any C^*-algebra. We briefly describe this procedure.

Let $\mathcal{A}$ be a C^*-algebra with no identity. Consider the collection of pairs

$$\tilde{\mathcal{A}} = \{(\alpha, A) : \alpha \in \mathbb{C} \text{ and } A \in \mathcal{A}\}\,. \tag{3.3}$$

Equip $\tilde{\mathcal{A}}$ with the vector space properties

$$(\alpha, A) + (\beta, B) = (\alpha + \beta, A + B) \quad \text{and} \quad \alpha(\beta, B) = (\alpha\beta, \alpha B) \tag{3.4}$$

In addition, declare a product and involution by setting

$$(\alpha, A)(\beta, B) = (\alpha\beta, \alpha B + \beta A + AB) \quad \text{and} \quad (\alpha, A)^* = (\overline{\alpha}, A^*) \tag{3.5}$$

One can check, see also Proposition 2.1.5 in [2], that the quantity

$$\|(\alpha, A)\| = \sup\{\|\alpha B + AB\| : B \in \mathcal{A}, \|B\| = 1\} \tag{3.6}$$

defines a norm on $\tilde{\mathcal{A}}$ and with respect to this norm, $\tilde{\mathcal{A}}$ is a C^*-algebra. The algebra $\mathcal{A}$ can be identified with the C^*-subalgebra of $\tilde{\mathcal{A}}$ formed by the pairs $(0, A)$. $\tilde{\mathcal{A}}$ is often called the C^*-algebra obtained by adjoining an identity to $\mathcal{A}$. The notation $\tilde{\mathcal{A}} =: \mathbb{C}\mathbb{1} + \mathcal{A}$ and similarly $(\alpha, A) =: \alpha\mathbb{1} + A$ is common.

With this construction in mind, we will only work with unital C^*-algebras in these notes.

3.2. **Spectral theory in a C^*-algebra.** The goal of this section is to provide quick introduction to the basic facts of spectral theory in a C^*-algebra. For more details and more general statements, we refer the interested reader to, e.g., [2, Section 2.2.1]. Unless otherwise state, we will assume $\mathcal{A}$ is a unital C^*-algebra..

An element $A \in \mathcal{A}$ is said to be *invertible* if there exists an element $A^{-1} \in \mathcal{A}$, called the *inverse* of A, which satisfies

$$AA^{-1} = A^{-1}A = \mathbb{1}\,. \tag{3.7}$$

One readily checks that if A is invertible, then the inverse is unique. A number of other properties also immediately follow:

i) If A is invertible, then so is A^{-1} and $(A^{-1})^{-1} = A$.
ii) If A is invertible, then so is A^* and $(A^*)^{-1} = (A^{-1})^*$.
iii) If A and B are invertible, then so is AB and $(AB)^{-1} = B^{-1}A^{-1}$.

Definition 3.3. The resolvent set of an element $A \in \mathcal{A}$, denoted by $\mathrm{res}_{\mathcal{A}}(A)$, is the set of all $\lambda \in \mathbb{C}$ for which $\lambda \mathbb{1} - A$ is invertible. The spectrum of any $A \in \mathcal{A}$, denoted by $\mathrm{spec}_{\mathcal{A}}(A)$, is then defined to be the complement of $\mathrm{res}_{\mathcal{A}}(A)$ in $\mathbb{C}$. Given $A \in \mathcal{A}$ and $\lambda \in \mathrm{res}_{\mathcal{A}}(A)$, the inverse $(\lambda \mathbb{1} - A)^{-1}$ is called the resolvent of A at λ.

For a non-unital C^*-algebras $\mathcal{A}$, one can still define the notion of spectrum by setting $\mathrm{spec}_{\mathcal{A}}(A) := \mathrm{spec}_{\tilde{\mathcal{A}}}(A)$, where $\tilde{\mathcal{A}}$ is the unique algebra obtained from $\mathcal{A}$ by adjoining an identity.

For all $A \in \mathcal{A}$ and any $\lambda \in \mathbb{C}$ with $\|A\| < |\lambda|$, it is easy to see that

$$\frac{1}{\lambda} \sum_{n=0}^{\infty} \left(\frac{A}{\lambda} \right)^n \tag{3.8}$$

defines a norm-convergent sum. It is then readily checked that this element is the inverse of $\lambda \mathbb{1} - A$. Hence, $\lambda \in \mathrm{res}_{\mathcal{A}}(A)$ and thus $\mathrm{spec}_{\mathcal{A}}(A)$ is a bounded subset of $\mathbb{C}$; namely

$$\mathrm{spec}(A) \subset \{ \lambda \in \mathbb{C} : |\lambda| \leq \|A\| \} . \tag{3.9}$$

Straightforward manipulations with Neumann series, defined similarly to (3.8), allow one to show that for any $A \in \mathcal{A}$, $\mathrm{res}_{\mathcal{A}}(A)$ is open, and thus $\mathrm{spec}_{\mathcal{A}}(A)$ is closed. One readily verifies that the mapping $\lambda \mapsto (\lambda \mathbb{1} - A)^{-1}$ is continuous on $\mathrm{res}_{\mathcal{A}}(A)$. It is also important to observe that for every $A \in \mathcal{A}$, $\mathrm{spec}_{\mathcal{A}}(A)$ is non-empty. This fact is a consequence of the next result.

First, an important definition. For any $A \in \mathcal{A}$ define the *spectral radius* of A by

$$\rho(A) = \sup\{ |\lambda| : \lambda \in \mathrm{spec}_{\mathcal{A}}(A) \} . \tag{3.10}$$

Proposition 3.4. *For any $A \in \mathcal{A}$, one has that*

$$\rho(A) = \lim_{n \to \infty} \|A^n\|^{1/n} = \inf_n \|A^n\|^{1/n} \leq \|A\| . \tag{3.11}$$

In particular, the above limit exists and if the righthand side of (3.11) vanishes, then $0 \in \mathrm{spec}(A)$. Therefore, the spectrum of any $A \in \mathcal{A}$ is a non-empty compact set.

A proof of this result can be found, e.g., in [2, Proposition 2.2.2].

One can characterize the spectrum of certain special classes of elements $A \in \mathcal{A}$. An element $A \in \mathcal{A}$ is said to be *normal* if $A^* A = A A^*$, and $A \in \mathcal{A}$ is called *self-adjoint* if $A^* = A$. The set of all self-adjoint elements of $\mathcal{A}$ will be denoted by $\mathcal{A}_{\mathrm{sa}}$. It is often useful to observe that each $A \in \mathcal{A}$ can be written as a linear combination of self-adjoint elements:

$$A = A_1 + i A_2 \quad \text{with } A_1 = \frac{A + A^*}{2} \text{ and } A_2 = \frac{A - A^*}{2i} \tag{3.12}$$

and A_1 and A_2 are commonly referred to as the real and imaginary parts of A respectively.

An element $A \in \mathcal{A}$ is called an *isometry* if $A^* A = \mathbb{1}$, and $A \in \mathcal{A}$ is said to be *unitary* if $A^* A = \mathbb{1} = A A^*$.

The following statement collects some facts proven, e.g., [2, Theorem 2.2.5].

Theorem 3.5. *Let $\mathcal{A}$ be a unital C^*-algebra.*

i) If $A \in \mathcal{A}$ is normal, then $\rho(A) = \|A\|$.

ii) If $A \in \mathcal{A}$ is unitary, then

$$\mathrm{spec}_{\mathcal{A}}(A) \subset \{ \lambda \in \mathbb{C} : |\lambda| = 1 \} .$$

iii) If $A \in \mathcal{A}$ is self-adjoint, then

$$\mathrm{spec}_{\mathcal{A}}(A) \subset [-\|A\|, \|A\|] .$$

iv) For any $A \in \mathcal{A}$ and any polynomial P,

$$\mathrm{spec}_{\mathcal{A}} \left(P(A) \right) = P \left(\mathrm{spec}_{\mathcal{A}}(A) \right) .$$

Two important consequences follow now from the results previously stated.

First, if $\mathcal{A}$ is a $*$-algebra and there exists a norm on $\mathcal{A}$ with the C^* property and with respect to which $\mathcal{A}$ is closed, then this norm is unique. Hence the norm on a C^*-algebra is unique.

Next, let $\mathcal{B}$ be a C^*-sub-algebra of some C^*-algebra $\mathcal{A}$. Then, for any $A \in \mathcal{B}$,

$$\mathrm{spec}_{\mathcal{A}}(A) = \mathrm{spec}_{\mathcal{B}}(A)$$

Thus, there is no ambiguity in the definition of the spectrum of an element A in a C^*-algebra, and so we may simply write $\mathrm{spec}(A)_{\mathcal{A}} = \mathrm{spec}(A)$.

3.3. **Positive elements.** In this section, we review some of their basic properties of positive elements a unital C^*-algebra $\mathcal{A}$. As we shall see, the cone of positive elements introduces a partial order on $\mathcal{A}$.

Definition 3.6. An element $A \in \mathcal{A}$ is said to be *positive* if A is self-adjoint and $\mathrm{spec}(A) \subset [0, \infty)$. We will denote by $\mathcal{A}_+$ the set of all positive elements $A \in \mathcal{A}$.

As a consequence of Theorem 3.5 iii), we actually know that if $A \in \mathcal{A}$ is positive, then

$$\mathrm{spec}(A) \subset [0, \|A\|] \,.$$

In fact, since it is easy to verify that

$$\mathrm{spec}(\lambda \mathbb{1} - A) = \lambda - \mathrm{spec}(A) \quad \text{for all } \lambda \in \mathbb{C} \text{ and } A \in \mathcal{A} \,,$$

we immediately conclude that

$$A \in \mathcal{A}_+ \quad \Rightarrow \quad \|A\| \mathbb{1} - A \in \mathcal{A}_+ \,. \tag{3.13}$$

Similar arguments allow one to prove that if $A \in \mathcal{A}_{\mathrm{sa}}$, then A is positive if and only if

$$\left\| \mathbb{1} - \frac{A}{\|A\|} \right\| \leq 1 \,. \tag{3.14}$$

Positive elements allow for the definition of a square root, which is an important building block for developing functional calculus in C^*-algebras. A first result in this direction is the following.

Theorem 3.7. *[2, Theorem 2.2.10] $A \in \mathcal{A}_{\mathrm{sa}}$ is positive if and only if $A = B^2$ for some $B \in \mathcal{A}_{\mathrm{sa}}$. In fact, for each $A \in \mathcal{A}_+$, there is a unique $B \in \mathcal{A}_+$ for which $A = B^2$.*

Given the above result, we can now make the following definitions. For any $A \in \mathcal{A}_+$, the *square-root of A*, which we denote by $A^{1/2}$, is defined by $A^{1/2} = B$, where $B \in \mathcal{A}_+$ is the unique element described in Theorem 3.7 above. Moreover, for any $A \in \mathcal{A}_{\mathrm{sa}}$, it is clear that $\mathrm{spec}(A^2) \subset [0, \|A\|^2]$, combine e.g. Theorem 3.5 iii) and iv). Thus $A^2 \in \mathcal{A}_+$, and so we may therefore define the *modulus of A*, which we denote at $|A|$, by setting $|A| = (A^2)^{1/2}$.

The following fact is a useful observation about the set of positive operators.

Proposition 3.8. *The set $\mathcal{A}_+ \subset \mathcal{A}$ of positive elements is a uniformly closed convex cone satisfying $\mathcal{A}_+ \cap (-\mathcal{A}_+) = \{0\}$. Moreover, if $A \in \mathcal{A}_{\mathrm{sa}}$, then with $A_\pm = (|A| \pm A)/2$ one sees that*

i) $A_\pm \in \mathcal{A}_+$,
ii) $A = A_+ - A_-$,
iii) $A_+ A_- = 0$.

The elements $A_\pm$ are the unique elements with these properties.

A proof of Proposition 3.8 can be found e.g. in [2, Proposition 2.2.11]. The decomposition for $A \in \mathcal{A}_{\mathrm{sa}}$, i.e. $A = A_+ - A_-$ in ii) above, is called the *orthogonal decomposition of A*.

The following fact is crucial.

Theorem 3.9. *$A \in \mathcal{A}_+$ if and only if $A = B^* B$ for some $B \in \mathcal{A}$.*

A proof of this result can be found in [2, Theorem 2.2.12].

Given Theorem 3.9, one can now extend the notion of modulus to all $A \in \mathcal{A}$. In fact, for any $A \in \mathcal{A}$, it is clear that $A^*A \in \mathcal{A}_+$. In this case, we define $|A| = (A^*A)^{1/2}$ to be the modulus of A. Moreover, if $A \in \mathcal{A}$ is invertible, then an analogue of the polar decomposition holds:

$$A = U|A| \quad \text{with} \quad U = A|A|^{-1} \tag{3.15}$$

and one can check that the U given above is unitary. One final result on decompositions is occasionally of use.

Lemma 3.10. *Every $A \in \mathcal{A}$ can be written as*

$$A = \sum_{j=1}^{4} a_j U_j \text{ where each } a_j \in \mathbb{C} \text{ satisfies } |a_j| \leq \frac{\|A\|}{2}\,, \tag{3.16}$$

and each U_j is unitary.

The proof of the above follows from (3.12) and the observation that for any $A \in \mathcal{A}_{\mathrm{sa}}$ with $\|A\| \leq 1$, one can readily check that

$$A = \frac{U_+ + U_-}{2} \quad \text{with unitaries} \quad U_\pm = A \pm i\sqrt{\mathbb{1} - A^2}\,. \tag{3.17}$$

Using the fact that $\mathcal{A}_+$ is a convex cone, one can introduce an order relation on the self-adjoint elements of $\mathcal{A}$. If $A, B \in \mathcal{A}_{\mathrm{sa}}$, we write that $A \geq B$, or $B \leq A$, if $A - B \in \mathcal{A}_+$.

The following proposition identifies some important features of this partial order.

Proposition 3.11. *Let $\mathcal{A}$ be a unital C^*-algebra.*
i) If $A \geq 0$ and $A \leq 0$, then $A = 0$.
ii) If $A \geq B$ and $B \geq C$, then $A \geq C$.
iii) If $A \geq 0$, then $\|A\|\mathbb{1} \geq A$.
iv) If $A \geq B \geq 0$, then $C^*AC \geq C^*BC \geq 0$ for all $C \in \mathcal{A}$.

3.4. **Representations.** It is often useful to consider mappings between C^*-algebras that preserve the structure. These are $*$-morphism. A particularly important sub-class of these are the representations. We introduce these notions in this subsection.

Definition 3.12. Let $\mathcal{A}$ and $\mathcal{B}$ be unital C^*-algebras. A mapping $\pi : \mathcal{A} \to \mathcal{B}$ is called a $*$-morphism between $\mathcal{A}$ and $\mathcal{B}$ if it satisfies:
i) $\pi(\alpha A + \beta B) = \alpha\pi(A) + \beta\pi(B)$ for all $\alpha, \beta \in \mathbb{C}$ and $A, B \in \mathcal{A}$,
ii) $\pi(AB) = \pi(A)\pi(B)$ for all $A, B \in \mathcal{A}$,
iii) $\pi(A^*) = \pi(A)^*$ for all $A \in \mathcal{A}$.

Remarks:
1) The phrase *morphism* may refer to mappings satisfying only properties i) and ii) above. Property iii) makes π a $*$-morphism. We only consider $*$-morphisms below.
2) A $*$-morphism $\pi : \mathcal{A} \to \mathcal{B}$ is said to be *unit preserving* if $\pi(\mathbb{1}_{\mathcal{A}}) = \mathbb{1}_{\mathcal{B}}$.
3) Any $*$-morphism π from $\mathcal{A}$ to $\mathcal{B}$ necessarily preserves positivity in the sense that: $\pi : \mathcal{A}_+ \to \mathcal{B}_+$. Indeed, for any $A \in \mathcal{A}_+$, $A = B^*B$ and hence,

$$\pi(A) = \pi(B^*B) = \pi(B^*)\pi(B) = \pi(B)^*\pi(B) \in \mathcal{B}_+\,.$$

The following proposition demonstrates that $*$-morphism are bounded, hence continuous.

Proposition 3.13. *Let $\mathcal{A}$ and $\mathcal{B}$ be unital C^*-algebras. Any $*$-morphism $\pi : \mathcal{A} \to \mathcal{B}$ is bounded, in fact*

$$\|\pi(A)\| \leq \|A\| \quad \text{for all } A \in \mathcal{A}. \tag{3.18}$$

In addition, the range of π, namely $\pi(\mathcal{A}) := \{\pi(A) : A \in \mathcal{A}\}$, is a C^*-subalgebra of $\mathcal{B}$.

Proof. We begin with the following observation. Let $P = \pi(\mathbb{1}_{\mathcal{A}})$. It is easy to check that $P \in \mathcal{B}_{\text{sa}}$ and moreover, $P^2 = P$, i.e. P is a projection. As a consequence, $\mathcal{B}' = P\mathcal{B}P$ is a C^*-subalgebra of $\mathcal{B}$. On this C^*-sub-algebra, P acts as the identity, and it is also the case that $\pi(\mathcal{A}) \subset \mathcal{B}'$.

Now, it is sufficient to check (3.18) for $A \in \mathcal{A}_{\text{sa}}$. In fact, suppose this bound holds for all $A \in \mathcal{A}_{\text{sa}}$. Then, for any $A \in \mathcal{A}$,

$$\|\pi(A)\|^2 = \|\pi(A)^*\pi(A)\| = \|\pi(A^*A)\| \leq \|A^*A\| = \|A\|^2 \tag{3.19}$$

where we have used the C^*-property in both $\mathcal{A}$ and $\mathcal{B}'$.

Now, suppose $A \in \mathcal{A}_{\text{sa}}$. It is clear then that $\pi(A) \in \mathcal{B}'_{\text{sa}}$, i.e. $\pi(A)^* = \pi(A^*) = \pi(A)$. Using Theorem 3.5 i), the norm of $\pi(A)$ can be calculated using the spectral radius, i.e.,

$$\|\pi(A)\| = \rho(\pi(A)) = \sup\{|\lambda| : \lambda \in \text{spec}_{\mathcal{B}'}(\pi(A))\}\,. \tag{3.20}$$

One readily checks that

$$\text{spec}_{\mathcal{B}'}(\pi(A)) \subset \text{spec}_{\mathcal{A}}(A)\,, \tag{3.21}$$

and therefore,

$$\|\pi(A)\| \leq \sup\{|\lambda| : \lambda \in \text{spec}_{\mathcal{A}}(A)\} = \|A\| \tag{3.22}$$

since $A \in \mathcal{A}_{\text{sa}}$. An argument for the remainder of this proof can be found in [2, Proposition 2.3.1]. □

Let $\mathcal{A}$ and $\mathcal{B}$ be unital C^*-algebras. A $*$-morphism π from $\mathcal{A}$ to $\mathcal{B}$ is said to be a *$*$-isomorphism* if it is one-to-one and onto. Clearly π is a $*$-isomorphism if and only if $\ker(\pi) = \{0\}$, where

$$\ker(\pi) := \{A \in A : \pi(A) = 0\}\,.$$

Definition 3.14. Let $\mathcal{A}$ be a C^*-algebra. A representation of $\mathcal{A}$ is a pair $(\mathcal{H}, \pi)$ where $\mathcal{H}$ is a complex Hilbert space and π is a $*$-morphism from $\mathcal{A}$ to $\mathcal{B}(\mathcal{H})$. The representation $(\mathcal{H}, \pi)$ is said to be faithful if and only if π is a $*$-isomorphism from $\mathcal{A}$ to $\pi(\mathcal{A})$, i.e., if and only if $\ker(\pi) = \{0\}$.

If $\mathcal{A}$ is a C^*-algebra and $(\mathcal{H}, \pi)$ is a representation, then $\mathcal{H}$ is called the *representation space*; the operators $\pi(A) \in \mathcal{B}(\mathcal{H})$ are called the *representatives of* $\mathcal{A}$, and π is often referred to as a *representation of* $\mathcal{A}$ *on* $\mathcal{H}$.

Proposition 3.15. *Let $(\mathcal{H}, \pi)$ be a representation of a C^*-algebra $\mathcal{A}$. The representation is faithful if and only if it satisfies each of the following equivalent conditions:*
i) $\ker(\pi) = \{0\}$,
ii) $\|\pi(A)\| = \|A\|$ *for all* $A \in \mathcal{A}$,
iii) for all $A \in \mathcal{A}_+$, $A \neq 0$, *we have* $\pi(A) \geq 0$ *and* $\pi(A) \neq 0$.

A proof of this result can be found in [2, Proposition 2.3.3].

Definition 3.16. Let $\mathcal{A}$ be a C^*-algebra. A $*$-isomorphism τ from $\mathcal{A}$ to $\mathcal{A}$ is called an automorphism on $\mathcal{A}$.

An immediate consequence of Proposition 3.15 and Definition 3.16 is the following.

Corollary 3.17. *Let $\mathcal{A}$ be a C^*-algebra and τ be an automorphism on $\mathcal{A}$. τ is norm-preserving, i.e.*

$$\|\tau(A)\| = \|A\| \quad \textit{for all } A \in \mathcal{A}. \tag{3.23}$$

3.5. **States.** Another notion of crucial importance for the theory of C^*-algebras is that of states. States are essential, of course, also in applications to physical systems. Again, let $\mathcal{A}$ be a unital C^*-algebra.

The *dual* of $\mathcal{A}$, which we denote by $\mathcal{A}^*$, is the collection of all continuous linear functionals over $\mathcal{A}$. For any $f \in \mathcal{A}^*$, we define the *norm* of f to be

$$\|f\| := \sup\{|f(A)| : A \in \mathcal{A} \text{ and } \|A\| = 1\}. \tag{3.24}$$

Definition 3.18. A linear functional ω over $\mathcal{A}$ is said to be positive if

$$\omega(A^*A) \geq 0 \quad \text{for all } A \in \mathcal{A}.$$

A positive linear functional ω over a C^*-algebra $\mathcal{A}$ is said to be a state if $\|\omega\| = 1$.

Recall that $A \in \mathcal{A}_+$ if and only if $A = B^*B$ for some $B \in \mathcal{A}$. Moreover, for $A, B \in \mathcal{A}_{\text{sa}}$, $A \geq B$ if and only if $A - B \in \mathcal{A}_+$. It follows that $\omega(A) \in \mathbb{R}$ if $A \in \mathcal{A}_{\text{sa}}$, and $A \geq B$ implies $\omega(A) \geq \omega(B)$.

States and representations are intimately connected. To see this, let $\mathcal{A}$ be a unital C^*-algebra, and let $(\mathcal{H}, \pi)$ be a representation of $\mathcal{A}$. For any non-zero $\Omega \in \mathcal{H}$, define

$$\omega_\Omega(A) = \langle \Omega, \pi(A)\Omega \rangle \quad \text{for all } A \in \mathcal{A}\,. \tag{3.25}$$

It is clear that any such ω_Ω is linear on $\mathcal{A}$. In addition,

$$\omega_\Omega(A^*A) = \langle \Omega, \pi(A^*A)\Omega \rangle = \|\pi(A)\Omega\|^2 \geq 0 \tag{3.26}$$

and so ω_Ω is positive as well. If $\|\Omega\| = 1$ and π is non-degenerate, then one can check that $\|\omega_\Omega\| = 1$. In this case, then ω_Ω is a state on $\mathcal{A}$. States of this type are called *vector states* of the representation $(\mathcal{H}, \pi)$. In fact, one can prove that every state over a C^*-algebra is a vector state in a suitable representation **??**.

The following lemma underlies the most basic properties of states .

Lemma 3.19 (Cauchy-Schwarz)**.** *Let ω be a positive linear functional over $\mathcal{A}$. It follows that*
i) $\omega(A^*B) = \overline{\omega(B^*A)}$ for all $A, B \in \mathcal{A}$,
ii) $|\omega(A^*B)|^2 \leq \omega(A^*A)\omega(B^*B)$ for all $A, B \in \mathcal{A}$.

Proof. Let $A, B \in \mathcal{A}$ and $\lambda \in \mathbb{C}$. By positivity of ω

$$\omega\left((\lambda A + B)^*(\lambda A + B)\right) \geq 0\,. \tag{3.27}$$

Using linearity, one finds that this is equivalent to

$$|\lambda|^2\omega(A^*A) + \overline{\lambda}\omega(A^*B) + \lambda\omega(B^*A) + \omega(B^*B) \geq 0 \tag{3.28}$$

The necessary and sufficient conditions for the positivity of this quadratic form on λ are exactly the conditions given above. ☐

There are a number of immediate and important consequences.

Corollary 3.20. *Let ω be a positive linear functional over $\mathcal{A}$. It follows that*
i) $\omega(A^*) = \overline{\omega(A)}$ for all $A \in \mathcal{A}$.
ii) $\omega(\mathbb{1}) = \|\omega\| = \sup\{\omega(A^*A) : \|A\| = 1\}$.
iii) $|\omega(A)|^2 \leq \omega(A^*A)\|\omega\|$ for all $A \in \mathcal{A}$.
iv) $|\omega(A^*BA)| \leq \omega(A^*A)\|B\|$ for all $A, B \in \mathcal{A}$.

Proof. The proof of i) follows from Lemma 3.19 i) by taking $B = \mathbb{1}$. To see that the first equality in ii) is true, observe that

$$0 \leq \omega(\mathbb{1}^*\mathbb{1}) = \omega(\mathbb{1}) = \frac{\omega(\mathbb{1})}{\|\mathbb{1}\|} \leq \|\omega\| \tag{3.29}$$

where we have used uniqueness of the identity, i.e. that $\mathbb{1}^* = \mathbb{1}$, and non-triviality of $\mathcal{A}$, i.e. that $\|\mathbb{1}\| = 1$. It is also clear that, for any $A \in \mathcal{A}$

$$|\omega(A)|^2 = |\omega(\mathbb{1}^* A)|^2 \leq \omega(\mathbb{1})\omega(A^*A) \tag{3.30}$$

where we have applied Lemma 3.19 ii). If we further assume that $A \in \mathcal{A}$ satisfies $\|A\| = 1$, then (3.30) implies

$$\|\omega\|^2 \leq \omega(\mathbb{1})\|\omega\| \tag{3.31}$$

where we have used that $\|A^*A\| = \|A\|^2 = 1$. If $\|\omega\| = 0$, then (3.29) shows that $\omega(\mathbb{1}) = 0$ as well. Otherwise, $\omega(\mathbb{1}) = \|\omega\|$ now follows by combining the inequalities proven in (3.29) and (3.31). The claim in iii) now follows from (3.30). In fact, the second equality in ii) also follows from (3.30). Finally, iv) follows from the application of ii) to the positive functional $B \mapsto \omega(A^*BA)$. □

Note that iv) implies that, for any $A \in \mathcal{A}$ with $\omega(A^*A) \neq 0$,

$$\omega_A(B) := \frac{\omega(A^*BA)}{\omega(A^*A)} \quad \text{for all } B \in \mathcal{A} \tag{3.32}$$

defines a state ω_A on $\mathcal{A}$. This is the quantum analogue of starting with a measure, e.g. dx on $[0, 1]$, considering a non-negative function μ with $\int_0^1 \mu(x)dx < \infty$, and defining a new, normalized measure via

$$\frac{\mu(x)}{\int_0^1 \mu(x)dx} dx \tag{3.33}$$

References

1. S. K. Berberian, *Tensor products of Hilbert spaces*, `https://www.ma.utexas.edu/mp_arc/c/14/14-2.pdf`, 2014.
2. O. Bratteli and D. W. Robinson, *Operator algebras and quantum statistical mechanics*, 2 ed., vol. 1, Springer Verlag, 1987.
3. G. Chiribella, G.M. D'Ariano, and P. Perinotti, *Informational derivation of quantum theory*, Phys. Rev. A **84** (2011), 012311.
4. W. Heisenberg, *Zur Theorie des Ferromagnetismus*, Z. Phys. **49** (1928), 619.
5. V.R. Kadison and J.R. Ringrose, *Fundamentals of the theory of operator algebras: Elementary theory*, vol. 1, American Mathematical Society, 1997.
6. M.A. Nielsen and I.L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.
7. M. Ohya and D. Petz, *Quantum entropy and its use*, Springer, 1993.
8. D. Ruelle, *Statistical mechanics: Rigorous results*, Benjamin, New York, 1969.
9. J. Weidmann, *Linear operators in hilbert spaces*, Graduate Texts in Mathematics, vol. 68, Springer, 1980.
10. R. F. Werner, *Remarks on a quantum state extension problem*, Lett. Math. Phys. **19** (1990), 319–326.
11. K. Zhu, *An introduction to operator algebras*, Studies in Advanced Mathematics, CRC Press, 1993.

Exercises

Some of the exercises below simply ask you to provide a proof for properties mentioned in the introductory sections. Other exercises provide properties that will be useful in the following lectures.

Exercise 1.
a) Let M_n denote the algebra of observables of a quantum system with an n-dimensional Hilbert space. Show that for every state $\omega : M_n \to \mathbb{C}$, i.e., any normalized positive linear functional on the observable algebra, there exists a unique $n \times n$ density matrix ρ (i.e., a non-negative definite matrix of unit trace), such that

$$\omega(A) = \mathrm{Tr}\rho A, \text{ for all } A \in M_n.$$

b) Show that the state ω on M_n is pure iff the corresponding density matrix is a rank-one projection, i.e., there is a unit vector $\psi \in \mathbb{C}^n$, such that $\rho = |\psi\rangle\langle\psi|$.

Exercise 2.
a) Show that the density matrix ρ corresponding to a state ω on M_2 is given by

$$\rho = \frac{1}{2}\left(\mathbb{1} + \mathbf{x}\cdot\sigma\right), \text{ with } \mathbf{x}\in\mathbb{R}^3, x_i = \omega(\sigma^i). \tag{3.34}$$

b) Find necessary and sufficient conditions on the parameter $\mathbf{x}\in\mathbb{R}^3$, so that $\rho = (\mathbb{1} + \mathbf{x}\cdot\sigma)/2$ is a density matrix.
c) For which $\mathbf{x}$ is the corresponding state ω pure?

Exercise 3. Let α be an $*$-automorphism on the a C^*-algebra $\mathcal{A}$ (i.e., a norm-closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$, for some Hilbert space H).
a) Consider α as a linear transformation on the Banach space $\mathcal{A}$ and show that $\|\alpha\| = 1$.
b) Show that, in fact, $\|\alpha(A)\| = \|A\|$, for all $A\in\mathcal{A}$.

Exercise 4. Let α be a linear map $M_n \to M_n$. Show that α is a $*$-automorphisms of M_n if and only if there exists a unitary $U\in M_n$, such that $\alpha(A) = U^*AU$, for all $A\in M_n$.

Exercise 5. Consider a quantum system consisting of two components, one with an observable algebra M_n, and another with observable algebra M_m, for some positive integers n and m. Let ω be a state on $M_n\otimes M_m$, the observable algebra of the combined system.
a) Show that the restrictions ω_1 and ω_2 of ω to the subalgebras $M_n\otimes\mathbb{1}$ and $\mathbb{1}\otimes M_m$ of $M_n\otimes M_m$, are states of M_n and M_m, respectively.
b) Let ρ denote the density matrix of ω, Consider an orthonormal basis of tensor products $e_i\otimes f_k, 1\leq i\leq n, 1\leq k\leq m$, and let $\rho_{i,k;j,l}$ denote the matrix elements of ρ in this basis. Show that the matrix elements of ρ_1, the density matrix of ω_1, in the basis e_i, are given by

$$\rho_{i,j} = \sum_{k=1}^{m}\rho_{i,k;j,k}, \text{ for all } 1\leq i,j\leq n.$$

Exercise 6. For $d\geq 1$ let $\rho\in M_d$ be a density matrix. The *von Neumann entropy* of ρ is defined by the following expression:

$$S(\rho) = -\mathrm{Tr}\rho\log\rho.$$

The matrix $\rho\log\rho$ is defined by the standard function calculus applied to the continuous function $x\log x$ defined on $[0,1]$. Prove the following properties:
a) $0\leq S(\rho)\leq\log d$, for all $d\times d$ density matrices ρ.
b) If a density matrix ρ has vanishing entropy, i.e., $S(\rho) = 0$, then ρ corresponds to a pure state, i.e., $\rho = |\psi\rangle\langle\psi|\psi$, for a unit vector $\psi\in\mathbb{C}^d$.
c) $S(\rho) = \log d$ if and only if $\rho = d^{-1}\mathbb{1}$.

Exercise 7. Suppose $M_d = M_{d_1}\otimes M_{d_2}$, $d_1, d_2\geq 1$ (then, $d = d_1d_2$), and let ρ_1 and ρ_2 denote the results of taking partial trace of ρ over the second and first factor, respectively: $\rho_1 = \mathrm{Tr}_2\rho, \rho_2 = \mathrm{Tr}_1\rho$.
a) Prove the following inequality, which is called the *subadditivity* of the von Neumann entropy (Hint: use Klein's inequality):

$$S(\rho)\leq S(\rho_1) + S(\rho_2).$$

b) Show that $S(\rho) = S(\rho_1) + S(\rho_2)$ if and only of $\rho = \rho_1\otimes\rho_2$.

Exercise 8. Let $\psi\in\mathbb{C}^d = \mathbb{C}^{d_1}\otimes\mathbb{C}^{d_2}$ be a non-zero vector.
a) Prove that there exists n, $1\leq n\leq\min(d_1, d_2)$, and orthonormal vectors $\phi_1,\ldots,\phi_n\in\mathbb{C}^{d_1}$, and $\xi_1,\ldots,\xi_n\in\mathbb{C}^{d_2}$, and positive constants $c_1,\ldots,c_n$, such that

$$\psi = \sum_{i=1}^{n} c_i\phi_i\otimes\xi_i, \text{ and } \|\psi\|^2 = \sum_{i=1}^{n} c_i^2. \tag{3.35}$$

This is called the *Schmidt decomposition* of ψ.
b) For a unit vector ψ, derive expressions for the partial traces ρ_1 and ρ_2 of the density matrix $|\psi\rangle\langle\psi|\psi$, in terms of the data of the (3.35).
c) Using your answer for b), show that the von Neumann entropy for the partial traces is given by:

$$S(\rho_1) = S(\rho_2) = -2\sum_{i=1}^{n} c_i^2 \log c_i.$$

d) For a pure state corresponding to a unit vector $\psi \in \mathbb{C}^d = \mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$, the entanglement entropy $S_E(\psi)$ is defined by

$$S_E(\psi) = S(\mathrm{Tr}_2|\psi\rangle\langle\psi|\psi).$$

Show that $S_E(\psi) = 0$ if and only if ψ is a product vector.

Exercise 9. Let $H = H^* \in M_n$, and $\beta \geq 0$. Define $F_\beta(\rho)$ by

$$F_\beta(\rho) = \mathrm{Tr}\rho H \; - \beta^{-1} S(\rho). \tag{3.36}$$

Define a density matrix ρ_β as follows:

$$\rho_\beta = \frac{e^{-\beta H}}{Z_\beta}, \quad Z_\beta = \mathrm{Tr} e^{-\beta H}. \tag{3.37}$$

Prove that ρ_β is the unique density matrix satisfying

$$F_\beta(\rho_\beta) = \min\{F_\beta(\rho) \mid \rho \in M_n, \rho \geq 0, \mathrm{Tr}\rho = 1\}. \tag{3.38}$$

Hint: First prove then use the following inequality (due to Klein [8], and Ohya-Petz [7]): for any two non-negative definite matrices A and B, $0 \leq A, B \leq \mathbb{1}$ and such that $\ker B \subset \ker A$, we have

$$\mathrm{Tr} A(\log A - \log B) \geq \mathrm{Tr}(A - B) + \frac{1}{2}\mathrm{Tr}(A - B)^2. \tag{3.39}$$

For the next set of exercises, let $\mathcal{A}$ denote a unital C^*-algebra and $\mathcal{A}_0$ a dense subset of $\mathcal{A}$. By an automorphism of $\mathcal{A}$ we mean a bijective $*$-morphism $\mathcal{A} \to \mathcal{A}$. It follows that $\alpha(\mathbb{1}) = \mathbb{1}$ and $\ker\alpha = \{0\}$.

Exercise 10. Prove that the set of all automorphisms of $\mathcal{A}$ is a group under the composition of maps.

Exercise 11. Let α_n be an automorphism defined on $\mathcal{A}$ for all $n \geq 1$. (α_n) is said to converge strongly to a map $\alpha : \mathcal{A} \to \mathcal{A}$, if for all $A \in \mathcal{A}$,

$$\lim_{n\to\infty} \alpha_n(A) = \alpha(A).$$

a) Prove that if (α_n) converges strongly to α, α is an automorphism of $\mathcal{A}$.
b) Prove that if $\alpha_n(A) \to \alpha(A)$, for all $A \in \mathcal{A}_0$, then α_n converges strongly to α on $\mathcal{A}$.

Exercise 12. Let (α_n) be a sequence of automorphisms of $\mathcal{A}$. Prove that (α_n) converges strongly to α if and only if (α_n^{-1}) converges strongly to α^{-1}.

Exercise 13. A family $\{\alpha_t \mid t \in \mathbb{R}\}$ of automorphisms of $\mathcal{A}$ is called a one-parameter group of automorphisms on $\mathcal{A}$ if $t \mapsto \alpha_t$ is a representation of the additive group of real numbers into the automorphism of $\mathcal{A}$.
a) Prove that if for each $n \geq 1$, $\{\alpha_t^{(n)} \mid t \in \mathbb{R}\}$ is a one-parameter group of automorphisms on $\mathcal{A}$, such that for all $t \in [0, T]$, for some $T > 0$, $(\alpha_t^{(n)})$ converges strongly to an automorphism α_t on $\mathcal{A}$, then $(\alpha_t^{(n)})$ converges strongly to an automorphism α_t on $\mathcal{A}$ for all $t \in \mathbb{R}$, and
b) $\{\alpha_t \mid t \in \mathbb{R}\}$ is a one-parameter group of automorphisms of $\mathcal{A}$.

Exercise 14. Let $\{\alpha_t \mid t \in \mathbb{R}\}$ be a one-parameter group of automorphisms of $\mathcal{A}$. $\{\alpha_t \mid t \in \mathbb{R}\}$ is called strongly continuous if for all $A \in \mathcal{A}$, $t \mapsto \alpha_t(A)$ is continuous with respect to the norm topology on $\mathcal{A}$.
a) Prove that if for all $A \in \mathcal{A}_0$, $t \mapsto \alpha_t(A)$ is continuous, then $\{\alpha_t \mid t \in \mathbb{R}\}$ is strongly continuous.
b) Prove that if for all $A \in \mathcal{A}$, $t \mapsto \alpha_t(A)$ is continuous at $t = 0$, then $\{\alpha_t \mid t \in \mathbb{R}\}$ is strongly continuous.

Exercise 15. For each $n \geq 1$, let $\{\alpha_t^{(n)} \mid t \in \mathbb{R}\}$ be a strongly continuous one-parameter group of automorphisms on $\mathcal{A}$. Assume there exists $T > 0$ such that for all $t \in [0, T]$, $(\alpha_t^{(n)})$ converges strongly to an automorphism α_t on $\mathcal{A}$, uniformly for $t \in [0, T]$. This means that for all $A \in \mathcal{A}$, and $\epsilon > 0$ there exists N such that for all $n \geq N$ one has

$$\|\alpha^{(n)}(A) - \alpha_t(A)\| < \epsilon, \text{ for all } t \in [0, T].$$

Prove that the $\alpha_t^{(n)}$ converge strongly to a strongly continuous one-parameter group of automorphism of $\mathcal{A}$.

For the next two exercises, let G be a connected graph with finite vertex set V and edge set $E \subset V \times V$. For simplicity assume $(x, y) \in E$ implies $(y, x) \notin E$. Define the spin-1/2 Heisenberg ferromagnet on G with Hamiltonian H_G as follows:

$$H_G = \sum_{(x,y)\in E} (\mathbb{1} - 2t_{x,y}), \tag{3.40}$$

acting on the Hilbert space $\mathcal{H}_G = \bigotimes_{x\in V} \mathbb{C}^2$, and where $t_{x,y}$, for $x, y \in V, v \neq w$, denotes the operator on $\mathcal{H}_G$ defined by $t_{x,y} \bigotimes_{z\in V} u_z = \bigotimes_{z\in V} v_z$, where

$$v_z = \begin{cases} u_z & \text{if } z \notin \{x, y\} \\ u_x & \text{if } z = y \\ u_y & \text{if } z = x \end{cases} \tag{3.41}$$

Exercise 16. Find the eigenspace corresponding to the smallest eigenvalue of H_G. What is its dimension?

Exercise 17. Let $G = (V, E) = C_N$, the cycle of length N ($V = \{1, \ldots, N\}, E = \{(n, n+1) \mid n = 1, \ldots, N-1\} \cup \{(N, 1)\}$).
a) Find $\mathrm{spec}(H_{C_N})$.
b) For N even, show that the largest eigenvalue of H_{C_N} is simple.